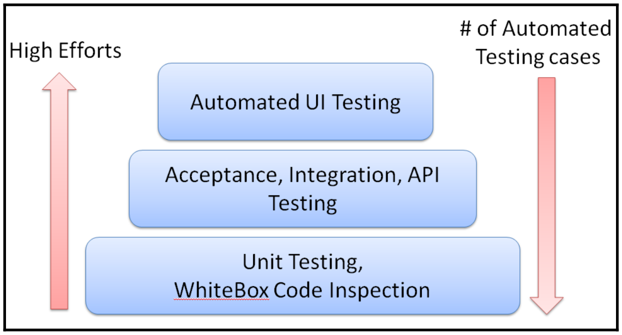
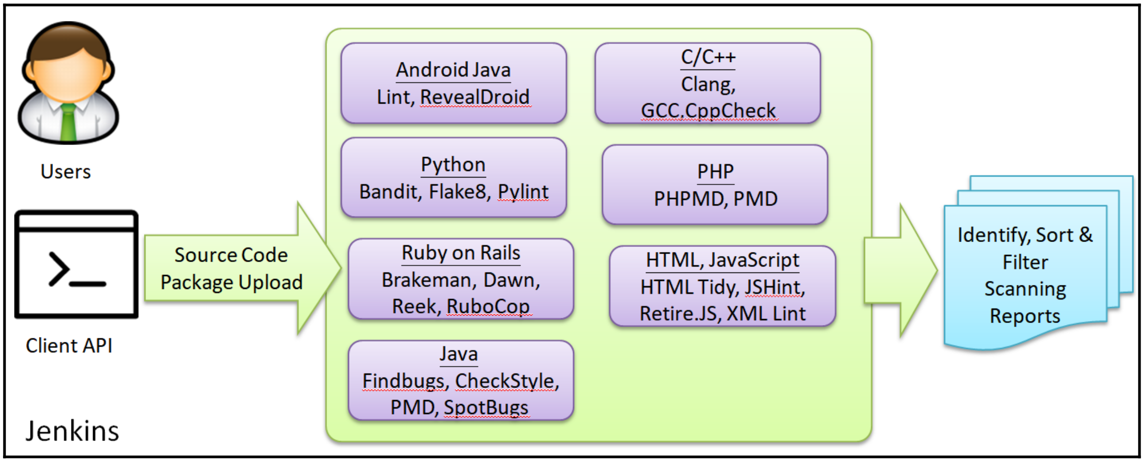
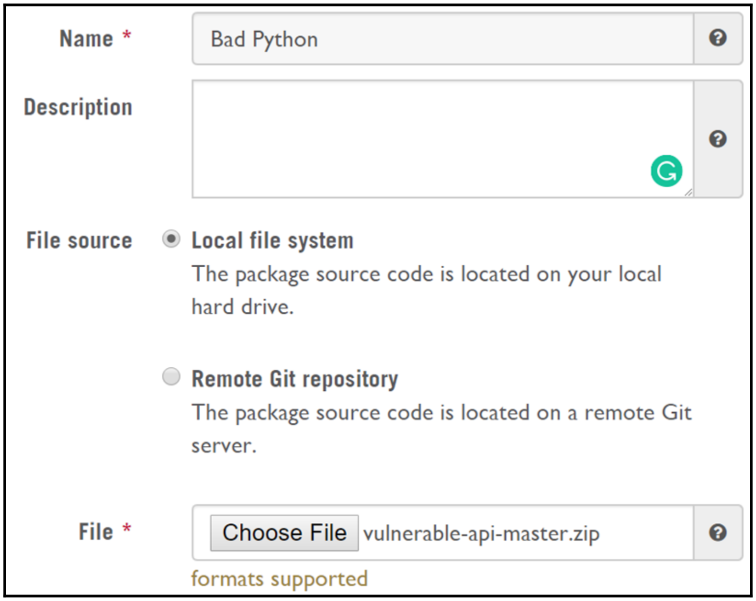
Chapter 2:
Integrating Security and Automation


High Efforts
# of Automated Testing cases
Automated UI Testing
Acceptance, Integration, API Testing
Unit Testing, WhiteBox Code Inspection

Chapter 3: Secure Code Inspection


Users
Client API
Jenkins
Source Code Package Upload
Android Java Lint, RevealDroid
C/C++ Clang, GCC,CppCheck
Python Bandit, Flake8, Pylint
PHP PHPMD, PMD
Ruby on Rails Brakeman, Dawn, Reek, RuboCop
HTML, JavaScript HTML Tidy, JSHint, Retire.JS, XML Lint
Java Findbugs, CheckStyle, PMD, SpotBugs
Identify, Sort & Filter Scanning Reports



Name * Bad Python

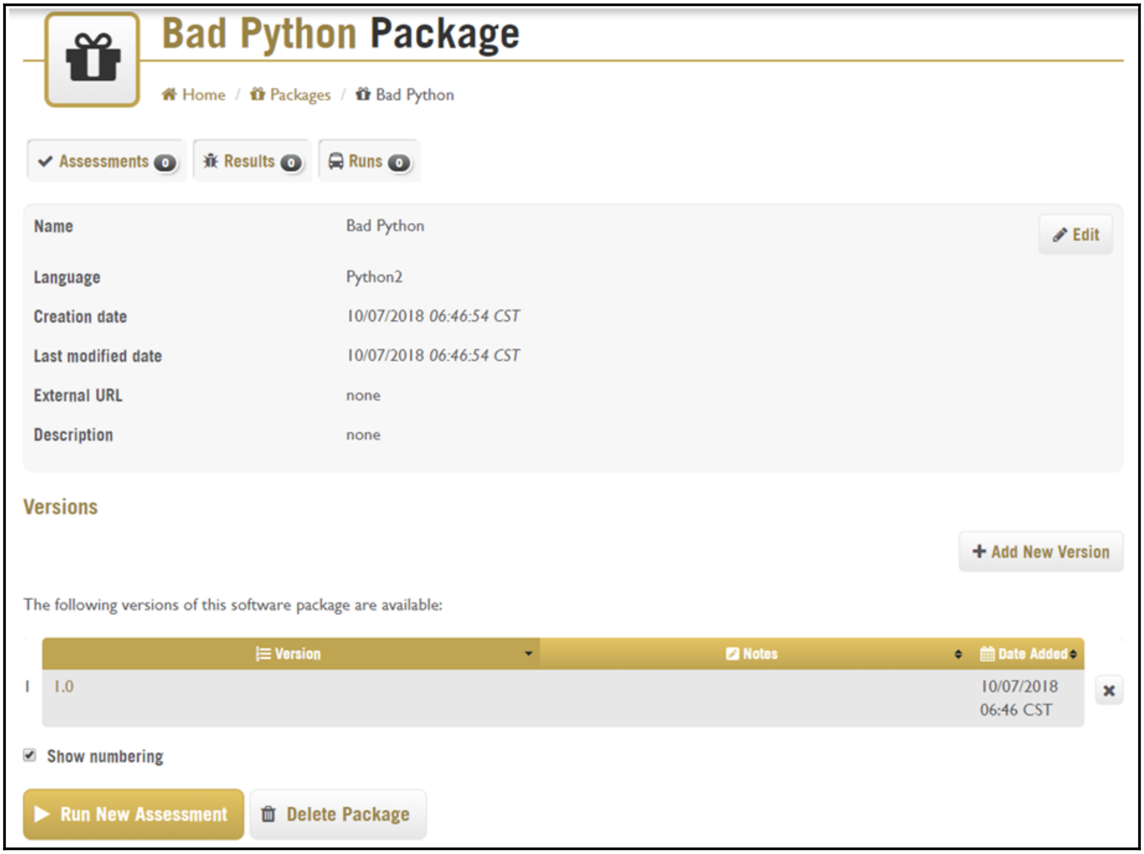
Description

File source

● Local file system
The package source code is located on your local hard drive.

○ Remote Git repository
The package source code is located on a remote Git server.

File * Choose File vulnerable-api-master.zip
formats supported



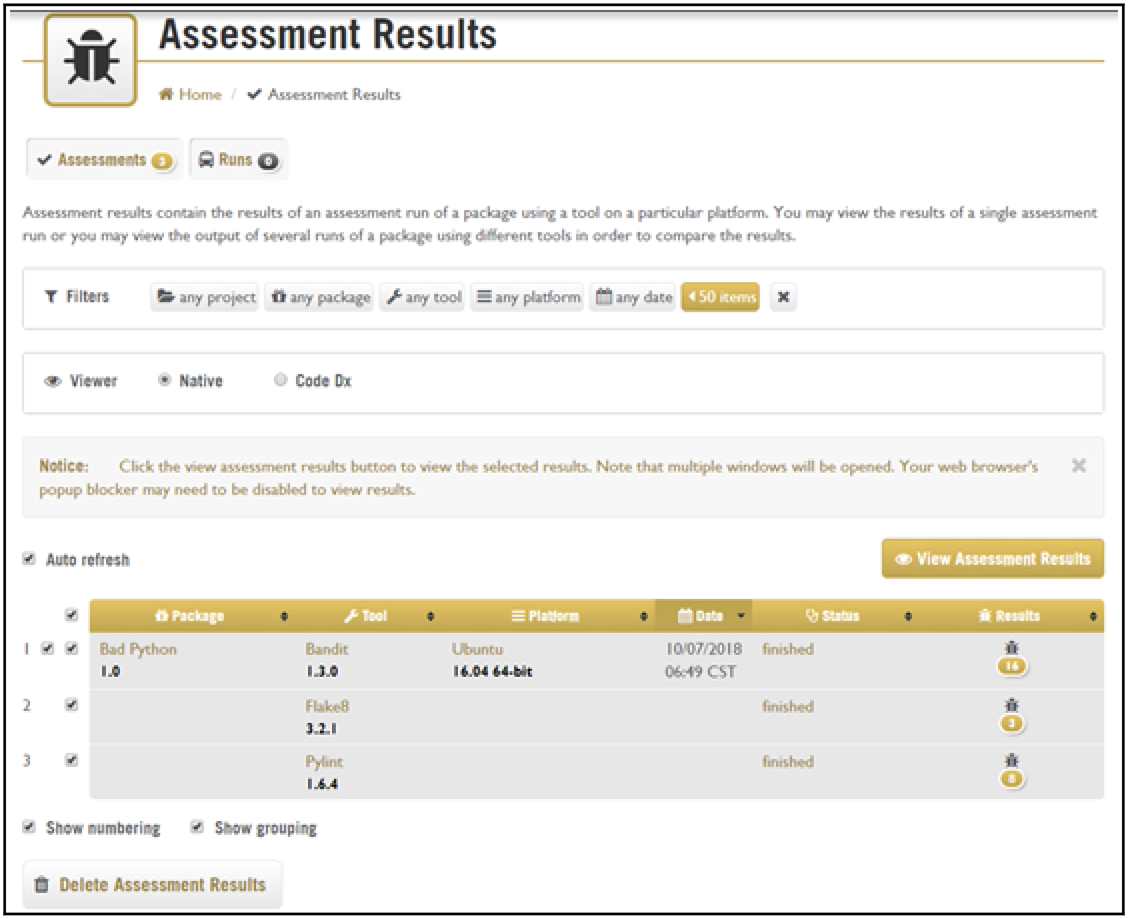
Name	Bad Python
Language	Python2
Creation date	10/07/2018 *06:46:54 CST*
Last modified date	10/07/2018 *06:46:54 CST*
External URL	none
Description	none

Versions

The following versions of this software package are available:

	Version	Notes	Date Added	
1	1.0		10/07/2018 06:46 CST	✖

☑ Show numbering



Assessment Results

Home / ✓ Assessment Results

Assessment results contain the results of an assessment run of a package using a tool on a particular platform. You may view the results of a single assessment run or you may view the output of several runs of a package using different tools in order to compare the results.

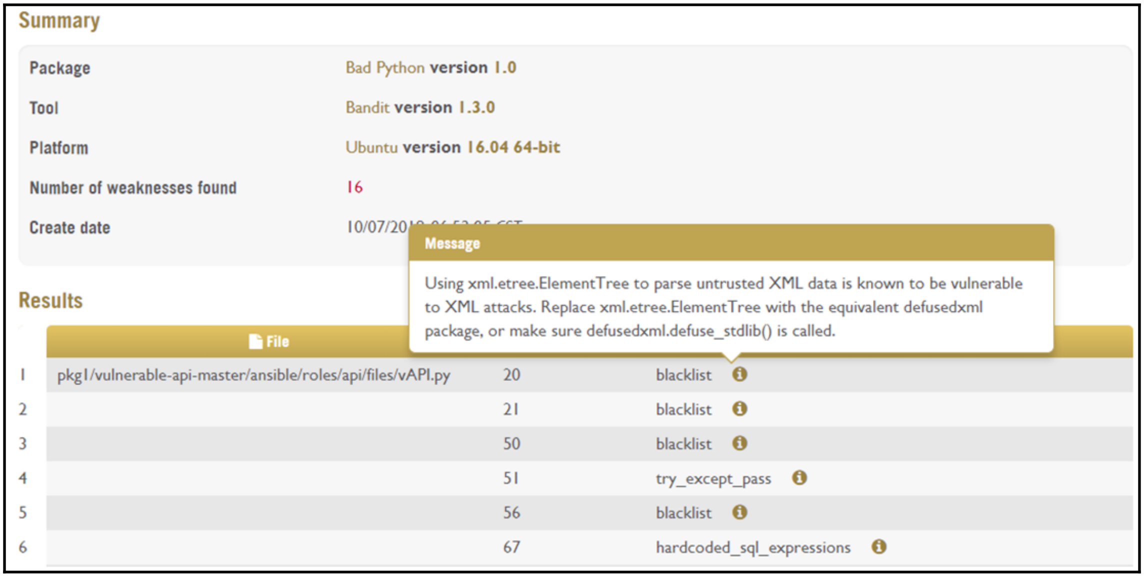
Viewer ● Native ○ Code Dx

Notice: Click the view assessment results button to view the selected results. Note that multiple windows will be opened. Your web browser's popup blocker may need to be disabled to view results.

☑ Auto refresh

		☑	Package	Tool	Platform	Date	Status	Results
1	☑	☑	Bad Python 1.0	Bandit 1.3.0	Ubuntu 16.04 64-bit	10/07/2018 06:49 CST	finished	16
2		☑		Flake8 3.2.1			finished	3
3		☑		Pylint 1.6.4			finished	8

☑ Show numbering ☑ Show grouping



Summary

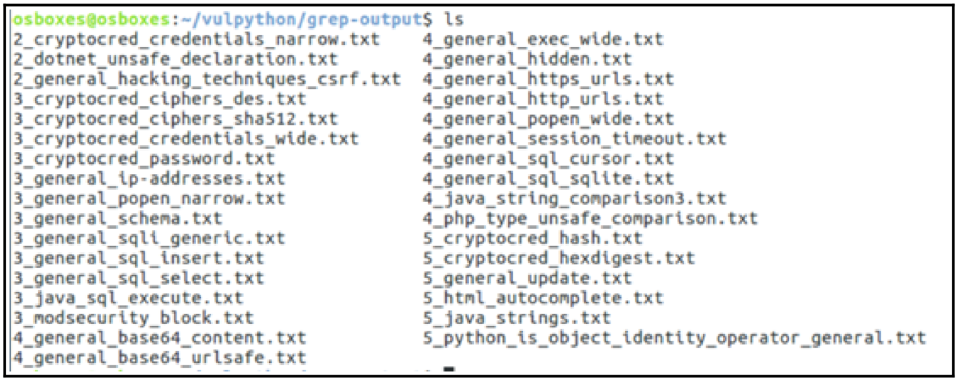
Package	Bad Python **version 1.0**
Tool	Bandit **version 1.3.0**
Platform	Ubuntu **version 16.04 64-bit**
Number of weaknesses found	16
Create date	10/07/20

Message

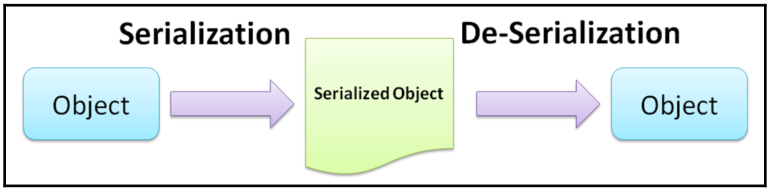
Using xml.etree.ElementTree to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree with the equivalent defusedxml package, or make sure defusedxml.defuse_stdlib() is called.

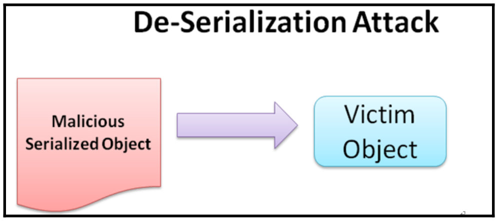
Results

	File			
1	pkg1/vulnerable-api-master/ansible/roles/api/files/vAPI.py	20	blacklist	ℹ
2		21	blacklist	ℹ
3		50	blacklist	ℹ
4		51	try_except_pass	ℹ
5		56	blacklist	ℹ
6		67	hardcoded_sql_expressions	ℹ

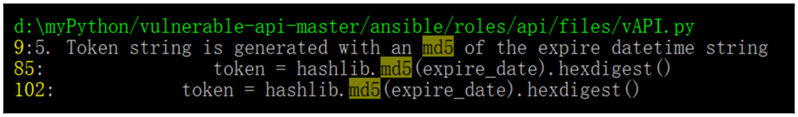


```
osboxes@osboxes:~/vulpython/grep-output$ ls
2_cryptocred_credentials_narrow.txt     4_general_exec_wide.txt
2_dotnet_unsafe_declaration.txt         4_general_hidden.txt
2_general_hacking_techniques_csrf.txt   4_general_https_urls.txt
3_cryptocred_ciphers_des.txt            4_general_http_urls.txt
3_cryptocred_ciphers_sha512.txt         4_general_popen_wide.txt
3_cryptocred_credentials_wide.txt       4_general_session_timeout.txt
3_cryptocred_password.txt               4_general_sql_cursor.txt
3_general_ip-addresses.txt              4_general_sql_sqlite.txt
3_general_popen_narrow.txt              4_java_string_comparison3.txt
3_general_schema.txt                    4_php_type_unsafe_comparison.txt
3_general_sqli_generic.txt              5_cryptocred_hash.txt
3_general_sql_insert.txt                5_cryptocred_hexdigest.txt
3_general_sql_select.txt                5_general_update.txt
3_java_sql_execute.txt                  5_html_autocomplete.txt
3_modsecurity_block.txt                 5_java_strings.txt
4_general_base64_content.txt            5_python_is_object_identity_operator_general.txt
4_general_base64_urlsafe.txt
```

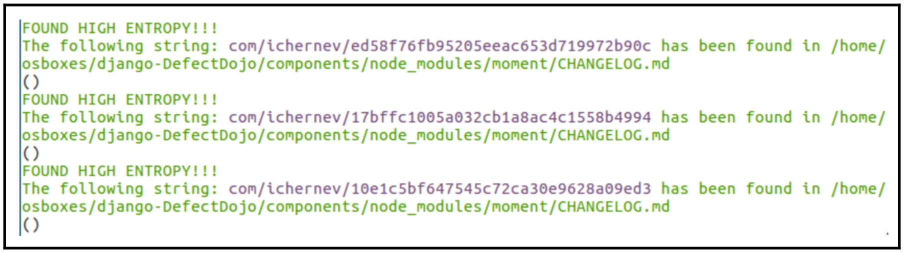



De-Serialization Attack
Malicious Serialized Object
Victim Object

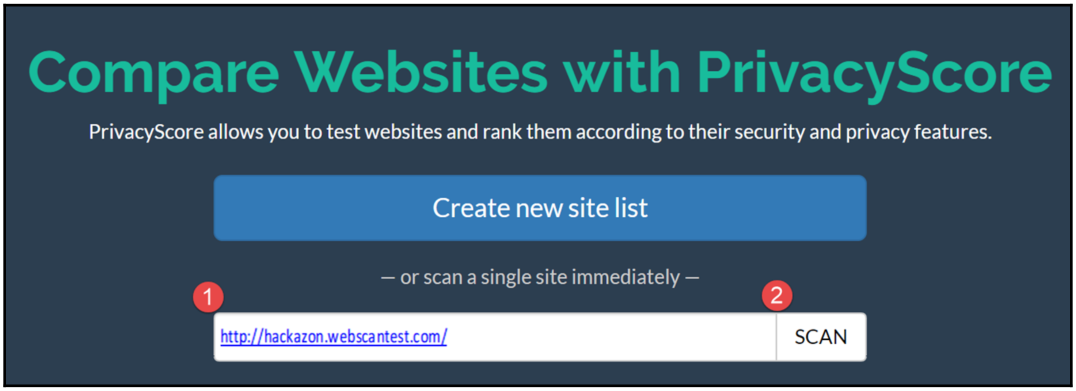
Chapter 4:
Sensitive Information and Privacy Testing



```
d:\myPython/vulnerable-api-master/ansible/roles/api/files/vAPI.py
9:5. Token string is generated with an md5 of the expire datetime string
85:                 token = hashlib.md5(expire_date).hexdigest()
102:            token = hashlib.md5(expire_date).hexdigest()
```



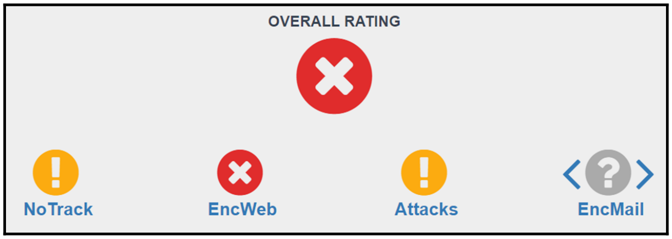
```
FOUND HIGH ENTROPY!!!
The following string: com/ichernev/ed58f76fb95205eeac653d719972b90c has been found in /home/
osboxes/django-DefectDojo/components/node_modules/moment/CHANGELOG.md
()
FOUND HIGH ENTROPY!!!
The following string: com/ichernev/17bffc1005a032cb1a8ac4c1558b4994 has been found in /home/
osboxes/django-DefectDojo/components/node_modules/moment/CHANGELOG.md
()
FOUND HIGH ENTROPY!!!
The following string: com/ichernev/10e1c5bf647545c72ca30e9628a09ed3 has been found in /home/
osboxes/django-DefectDojo/components/node_modules/moment/CHANGELOG.md
()
```



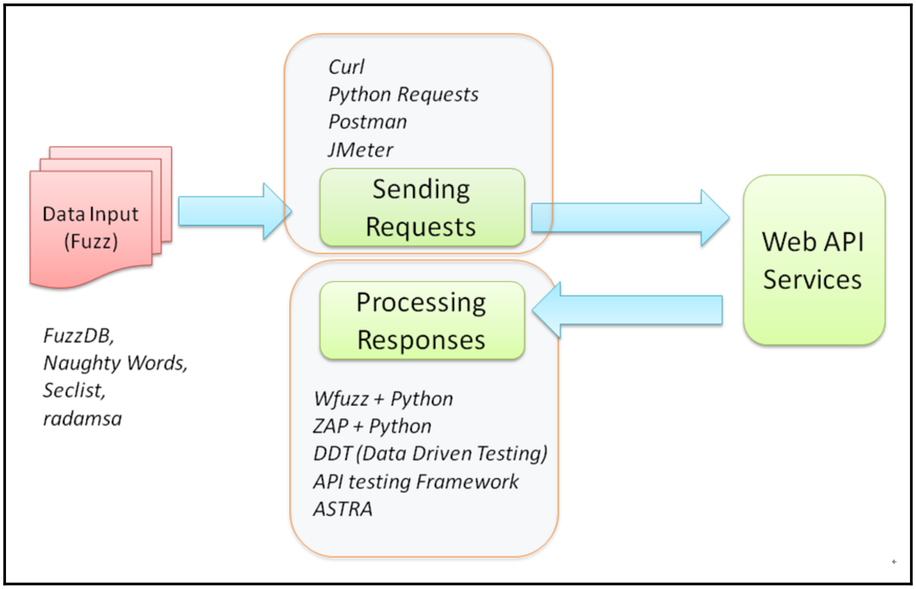
Compare Websites with PrivacyScore

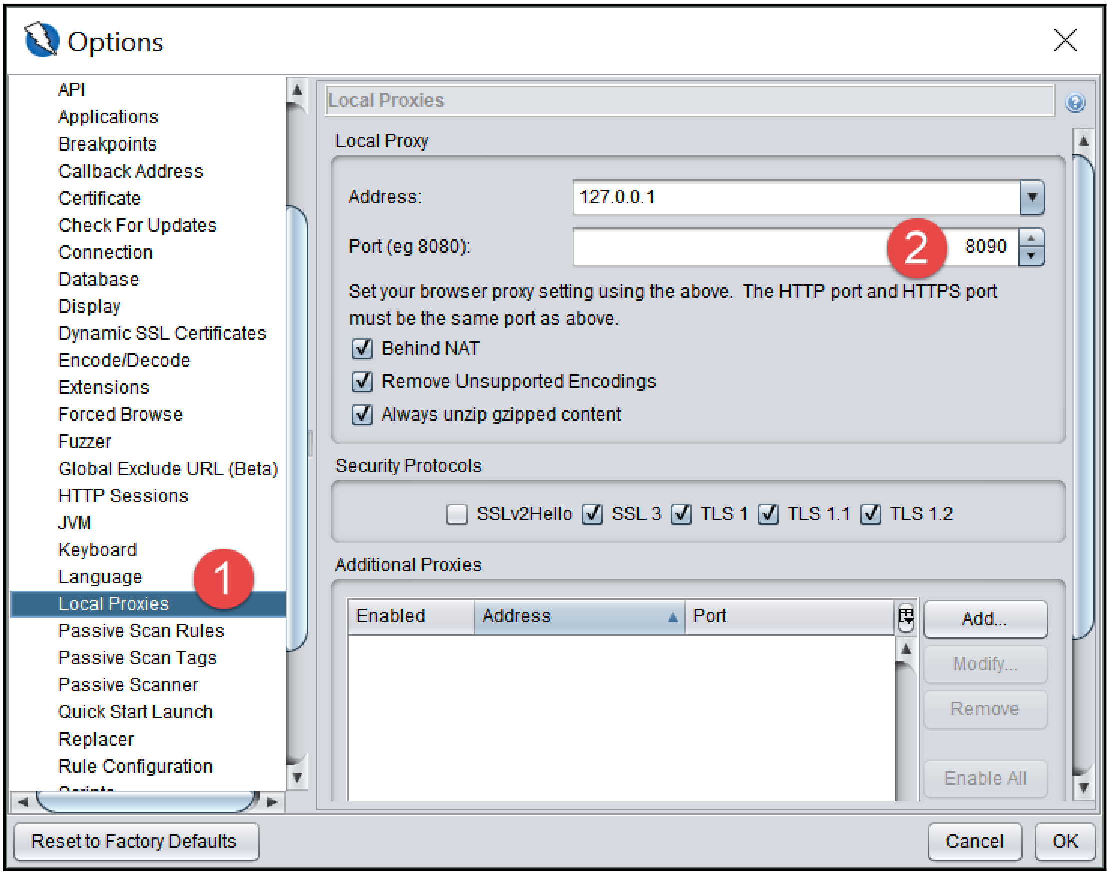
PrivacyScore allows you to test websites and rank them according to their security and privacy features.

Create new site list
— or scan a single site immediately —
1
2
http://hackazon.webscantest.com/
SCAN



Chapter 5: Security API and Fuzz Testing





Local Proxies

Local Proxy

Address: 127.0.0.1

Port (eg 8080): 8090

Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.

☑ Behind NAT

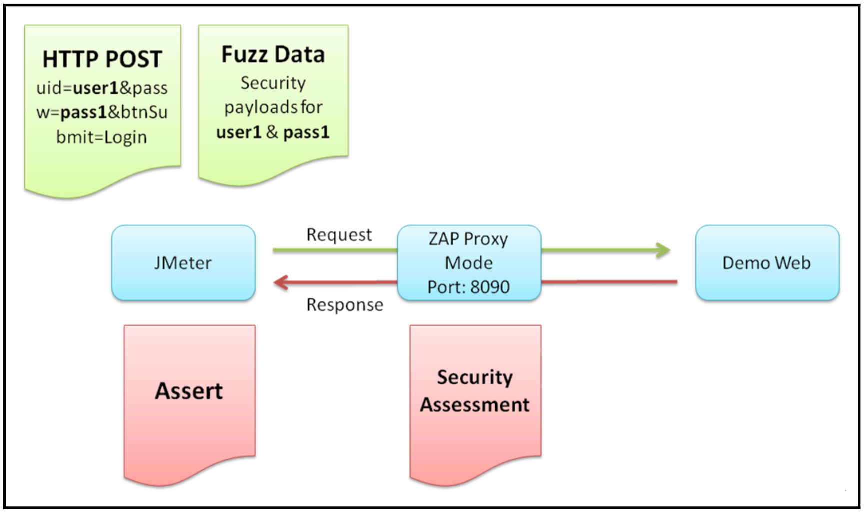
☑ Remove Unsupported Encodings

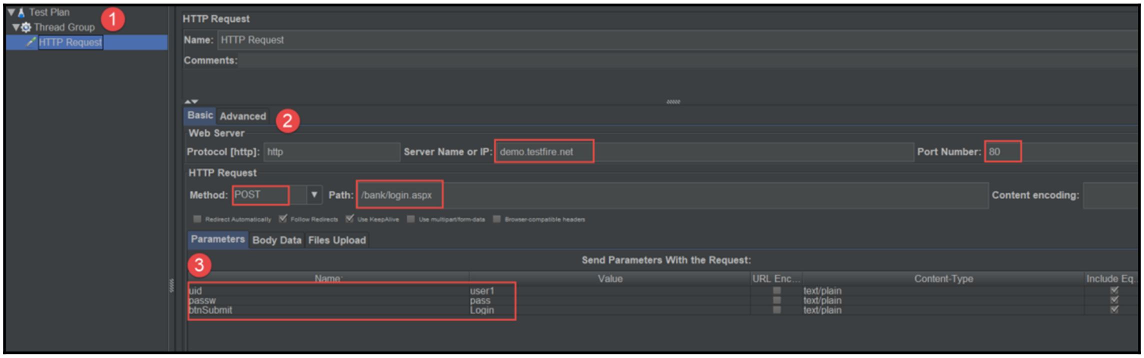
☑ Always unzip gzipped content

Security Protocols

□ SSLv2Hello ☑ SSL 3 ☑ TLS 1 ☑ TLS 1.1 ☑ TLS 1.2

Additional Proxies


HTTP POST
uid=**user1**&passw=**pass1**&btnSubmit=Login
Fuzz Data
Security payloads for **user1** & **pass1**
JMeter
Request
Response
ZAP Proxy Mode Port: 8090
Demo Web
Assert
Security Assessment



HTTP Request

Name: HTTP Request

Comments:

Basic | Advanced

Web Server

Protocol [http]: http   Server Name or IP: demo.testfire.net   Port Number: 80

HTTP Request

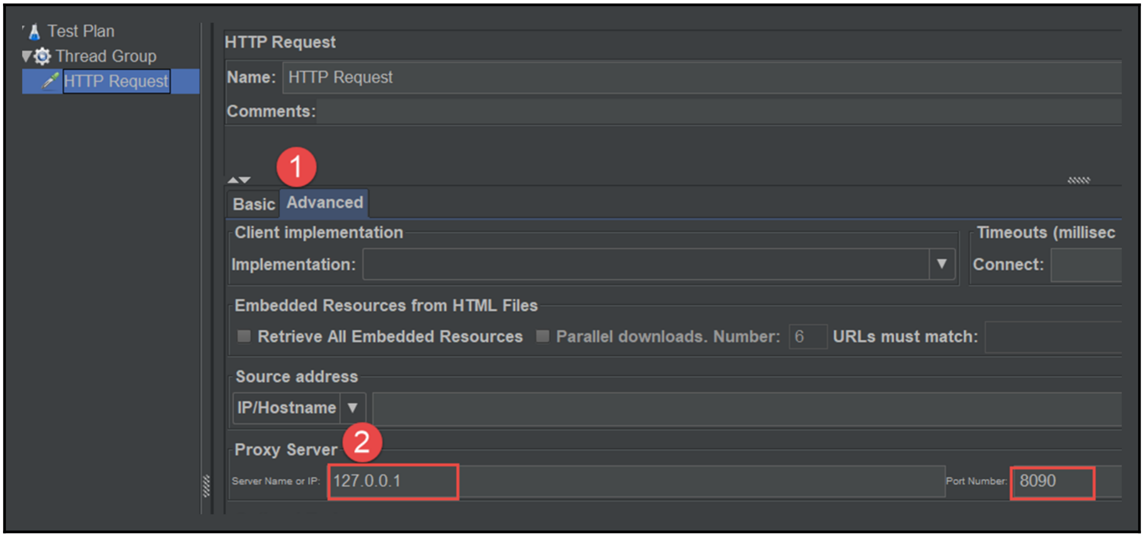
Method: POST   Path: /bank/login.aspx   Content encoding:

☐ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive ☐ Use multipart/form-data ☐ Browser-compatible headers

Parameters | Body Data | Files Upload

Send Parameters With the Request:

Name:	Value	URL Enc...	Content-Type	Include Eq...
uid	user1	☐	text/plain	☑
passw	pass	☐	text/plain	☑
btnSubmit	Login	☐	text/plain	☑



HTTP Request

Name: HTTP Request

Comments:

Client implementation

Implementation:

Timeouts (millisec

Connect:

Embedded Resources from HTML Files

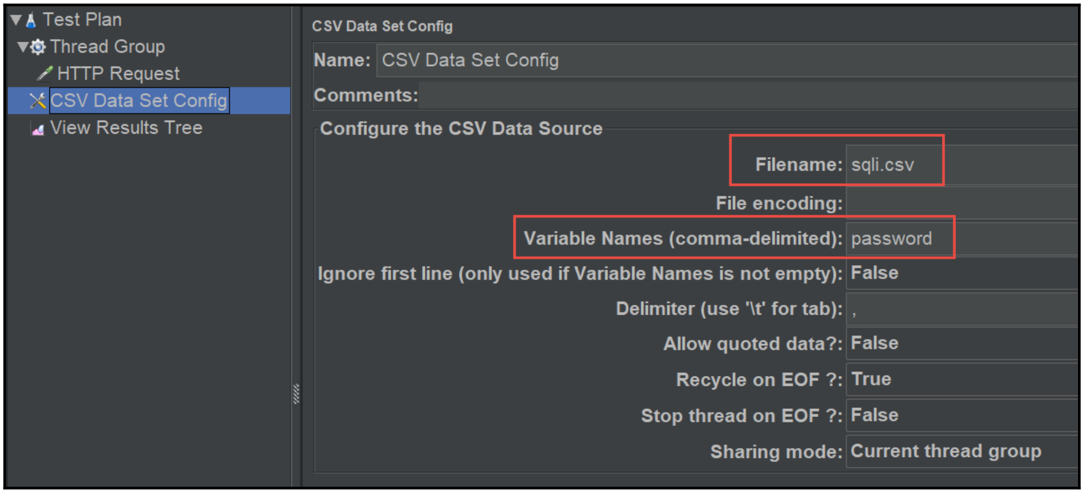
□ Retrieve All Embedded Resources □ Parallel downloads. Number: 6 URLs must match:

Source address

IP/Hostname ▼

Proxy Server

Server Name or IP: 127.0.0.1 Port Number: 8090



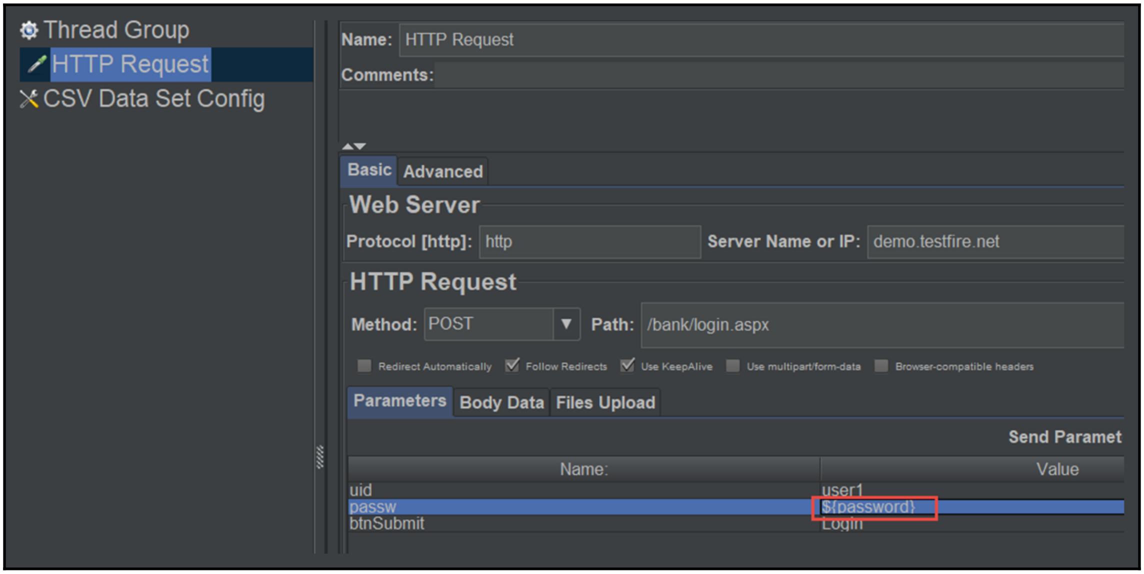
CSV Data Set Config

Name: CSV Data Set Config

Comments:

Configure the CSV Data Source

Filename:	sqli.csv
File encoding:	
Variable Names (comma-delimited):	password
Ignore first line (only used if Variable Names is not empty):	False
Delimiter (use '\t' for tab):	,
Allow quoted data?:	False
Recycle on EOF ?:	True
Stop thread on EOF ?:	False
Sharing mode:	Current thread group



Name: HTTP Request

Comments:

Web Server

Protocol [http]: http

Server Name or IP: demo.testfire.net

HTTP Request

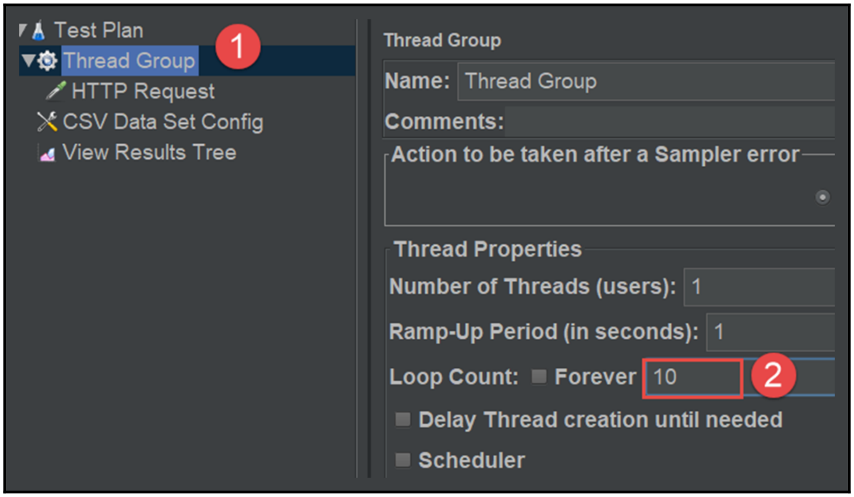
Method: POST ▼

Path: /bank/login.aspx

□ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive □ Use multipart/form-data □ Browser-compatible headers

Send Paramet

Name:	Value
uid	user1
passw	${password}
btnSubmit	Login



Thread Group

Name: Thread Group

Comments:

Action to be taken after a Sampler error

Thread Properties

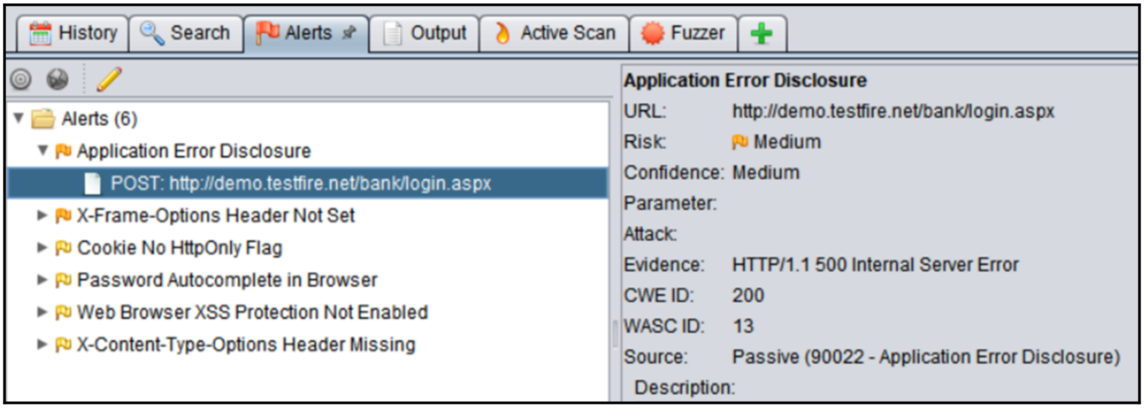
Number of Threads (users): 1

Ramp-Up Period (in seconds): 1

Loop Count: □ Forever 10

□ Delay Thread creation until needed

□ Scheduler

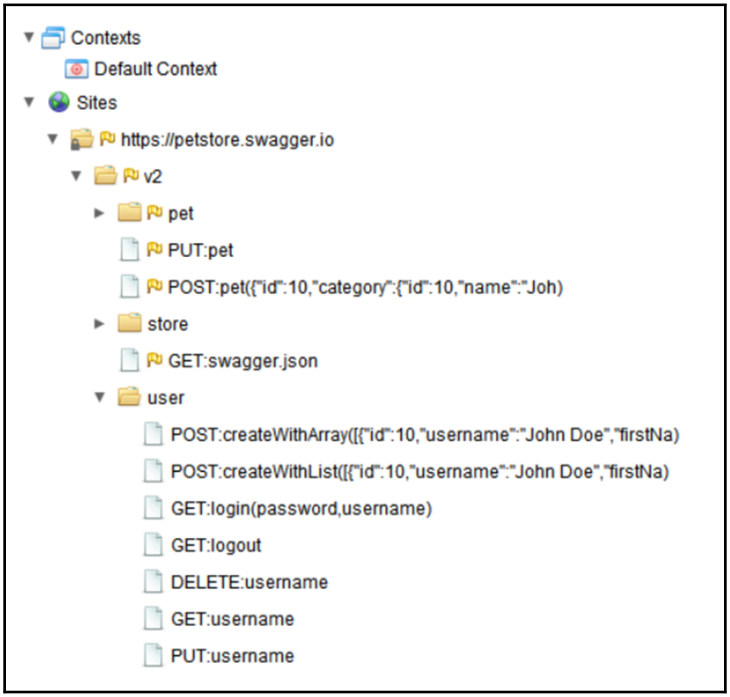


- Alerts (6)
  - Application Error Disclosure
    - POST: http://demo.testfire.net/bank/login.aspx
  - X-Frame-Options Header Not Set
  - Cookie No HttpOnly Flag
  - Password Autocomplete in Browser
  - Web Browser XSS Protection Not Enabled
  - X-Content-Type-Options Header Missing

Application Error Disclosure

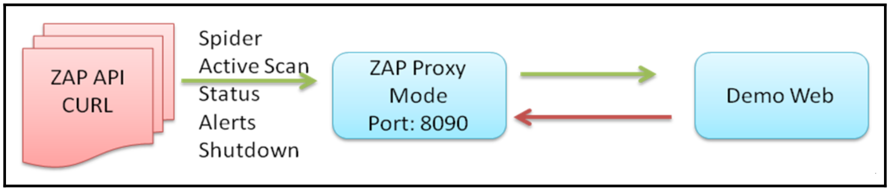
URL:	http://demo.testfire.net/bank/login.aspx
Risk:	Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	HTTP/1.1 500 Internal Server Error
CWE ID:	200
WASC ID:	13
Source:	Passive (90022 - Application Error Disclosure)

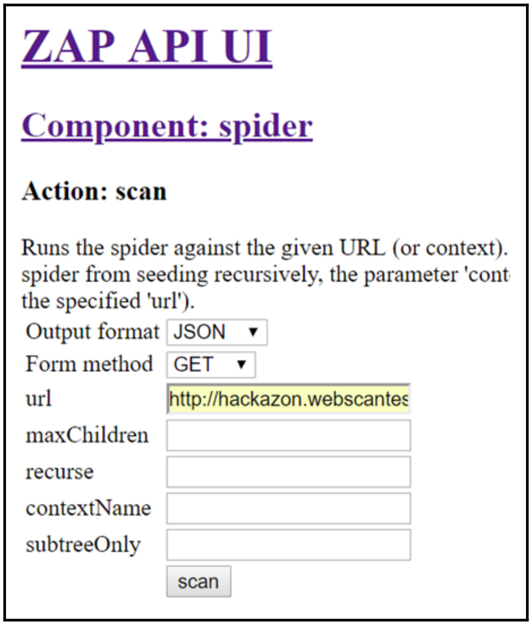
Description:



- Contexts
  - Default Context
- Sites
  - https://petstore.swagger.io
    - v2
      - pet
      - PUT:pet
      - POST:pet({"id":10,"category":{"id":10,"name":"Joh)
      - store
      - GET:swagger.json
      - user
        - POST:createWithArray([{"id":10,"username":"John Doe","firstNa)
        - POST:createWithList([{"id":10,"username":"John Doe","firstNa)
        - GET:login(password,username)
        - GET:logout
        - DELETE:username
        - GET:username
        - PUT:username

Chapter 6: Web Application Security Testing





ZAP API UI

Component: spider

Action: scan

Runs the spider against the given URL (or context). spider from seeding recursively, the parameter 'cont the specified 'url').

Output format JSON ▾

Form method GET ▾

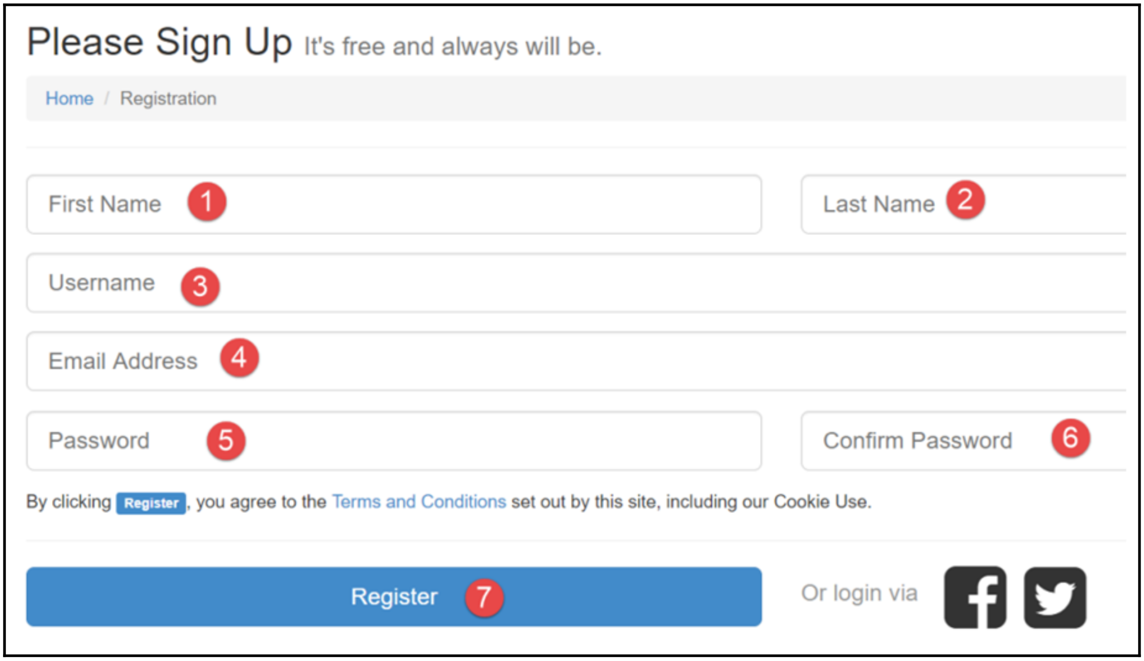
url http://hackazon.webscantes

maxChildren

recurse

contextName

subtreeOnly



Please Sign Up It's free and always will be.

Home / Registration

First Name 1

Last Name 2

Username 3

Email Address 4

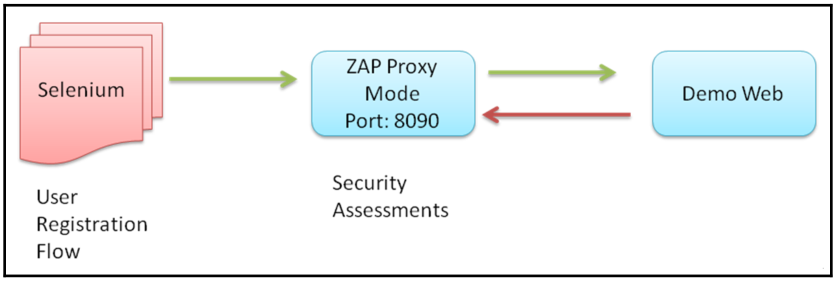
Password 5

Confirm Password 6

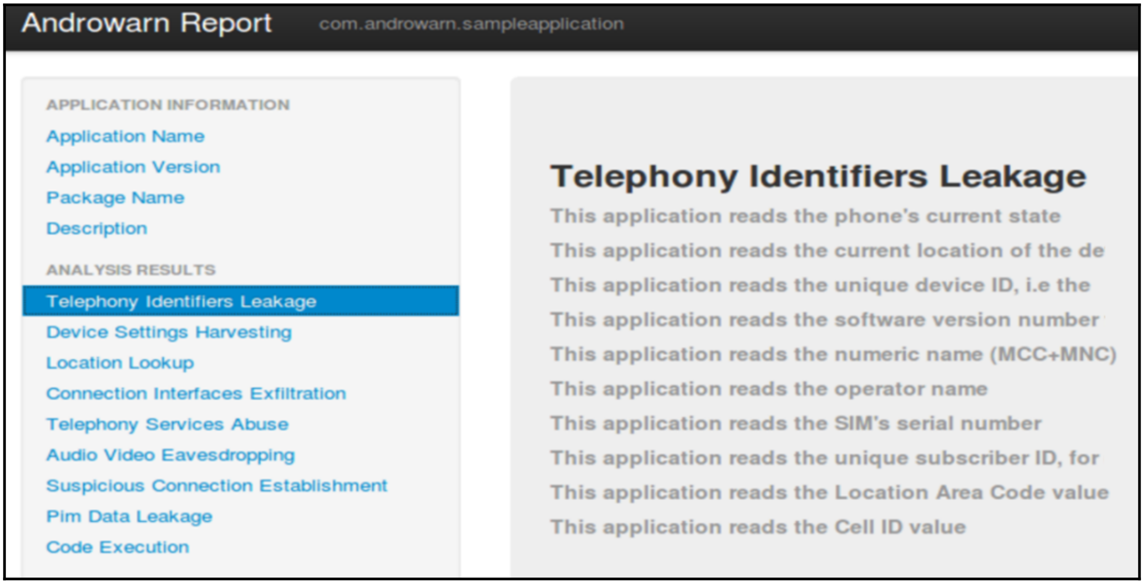
By clicking Register, you agree to the Terms and Conditions set out by this site, including our Cookie Use.

Register 7

Or login via



Chapter 7: Android Security Testing



Androwarn Report com.androwarn.sampleapplication

APPLICATION INFORMATION

- Application Name
- Application Version
- Package Name
- Description

ANALYSIS RESULTS

- Telephony Identifiers Leakage
- Device Settings Harvesting
- Location Lookup
- Connection Interfaces Exfiltration
- Telephony Services Abuse
- Audio Video Eavesdropping
- Suspicious Connection Establishment
- Pim Data Leakage
- Code Execution

Telephony Identifiers Leakage

This application reads the phone's current state

This application reads the current location of the de

This application reads the unique device ID, i.e the

This application reads the software version number

This application reads the numeric name (MCC+MNC)

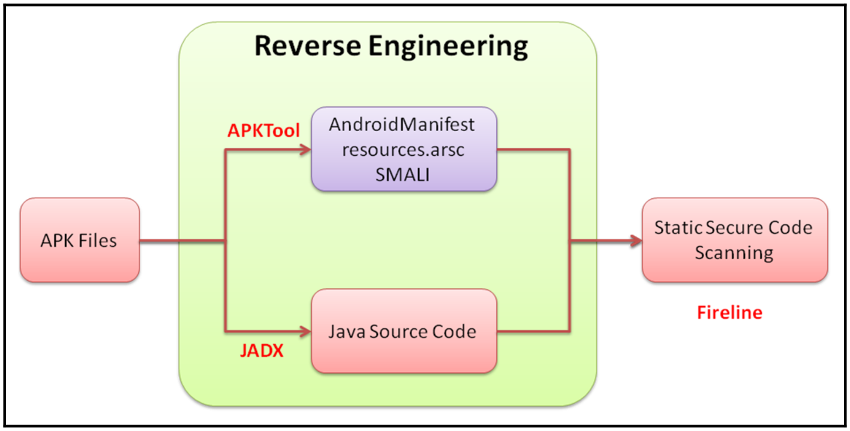
This application reads the operator name

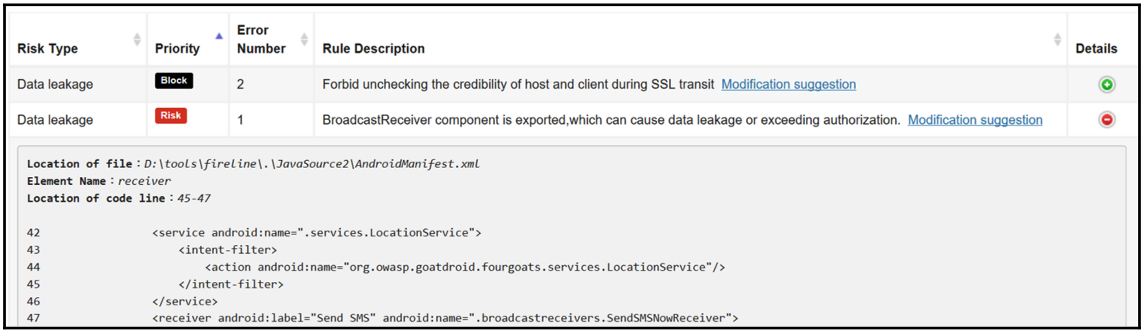
This application reads the SIM's serial number

This application reads the unique subscriber ID, for

This application reads the Location Area Code value

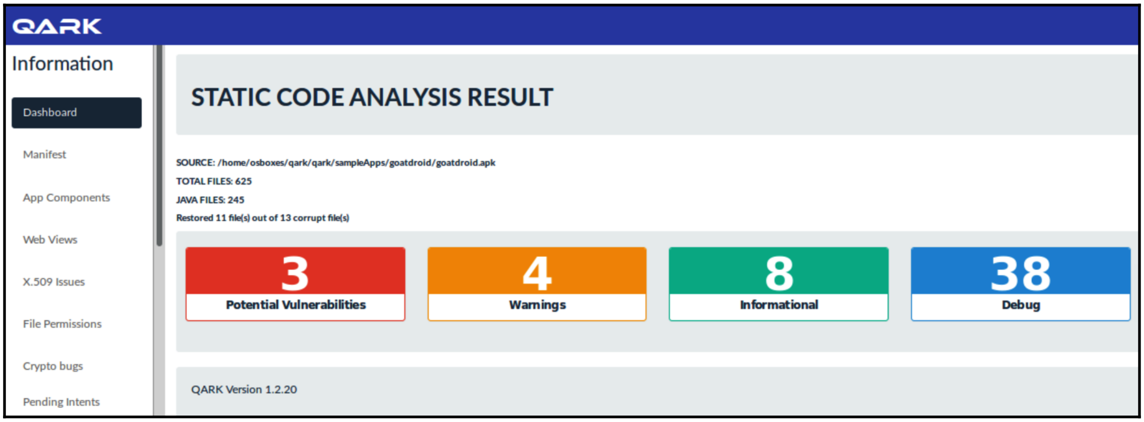
This application reads the Cell ID value





Risk Type	Priority	Error Number	Rule Description	Details
Data leakage	Block	2	Forbid unchecking the credibility of host and client during SSL transit Modification suggestion	⊕
Data leakage	Risk	1	BroadcastReceiver component is exported,which can cause data leakage or exceeding authorization. Modification suggestion	⊖

```
Location of file：D:\tools\fireline\.\JavaSource2\AndroidManifest.xml
Element Name：receiver
Location of code line：45-47

42            <service android:name=".services.LocationService">
43                <intent-filter>
44                    <action android:name="org.owasp.goatdroid.fourgoats.services.LocationService"/>
45                </intent-filter>
46            </service>
47            <receiver android:label="Send SMS" android:name=".broadcastreceivers.SendSMSNowReceiver">
```

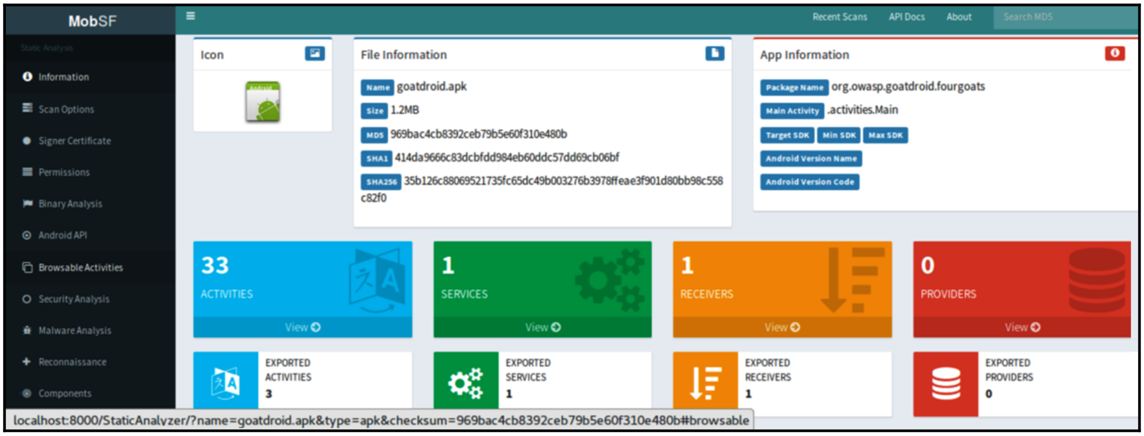


STATIC CODE ANALYSIS RESULT

SOURCE: /home/osboxes/qark/qark/sampleApps/goatdroid/goatdroid.apk
TOTAL FILES: 625
JAVA FILES: 245
Restored 11 file(s) out of 13 corrupt file(s)

3	4	8	38
Potential Vulnerabilities	Warnings	Informational	Debug

QARK Version 1.2.20



File Information

Name goatdroid.apk
Size 1.2MB
MD5 969bac4cb8392ceb79b5e60f310e480b
SHA1 414da9666c83dcbfdd984eb60ddc57dd69cb06bf
SHA256 35b126c88069521735fc65dc49b003276b3978ffeae3f901d80bb98c558c82f0

App Information

Package Name org.owasp.goatdroid.fourgoats
Main Activity .activities.Main
Target SDK Min SDK Max SDK
Android Version Name
Android Version Code

33 ACTIVITIES

1 SERVICES

1 RECEIVERS

0 PROVIDERS

EXPORTED ACTIVITIES 3

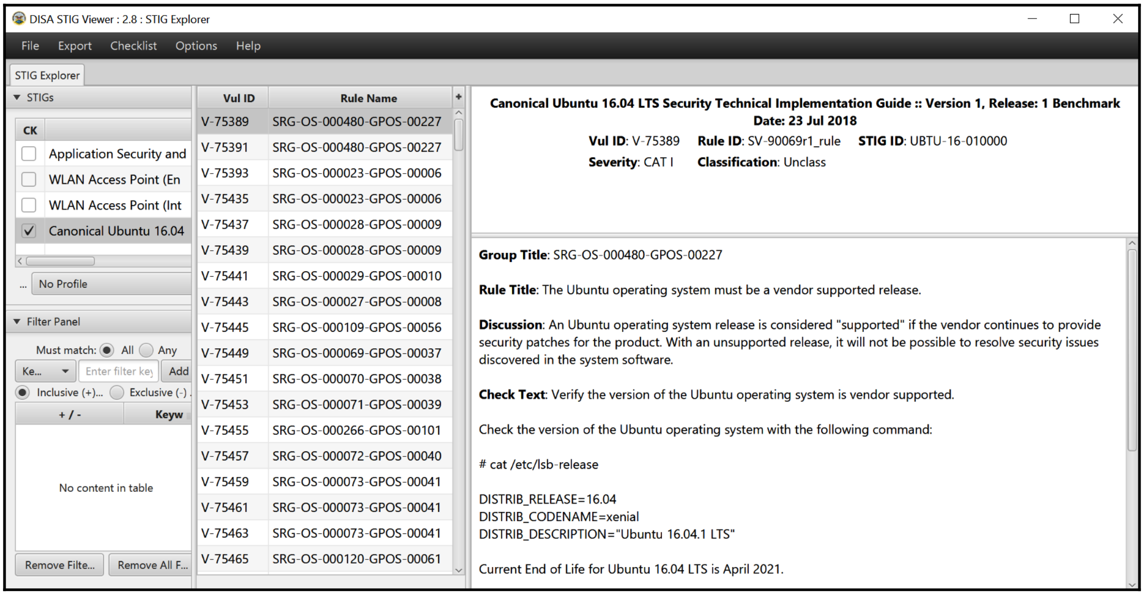
EXPORTED SERVICES 1

EXPORTED RECEIVERS 1

EXPORTED PROVIDERS 0

localhost:8000/StaticAnalyzer/?name=goatdroid.apk&type=apk&checksum=969bac4cb8392ceb79b5e60f310e480b#browsable

Chapter 8: Infrastructure Security



Vul ID	Rule Name
V-75389	SRG-OS-000480-GPOS-00227
V-75391	SRG-OS-000480-GPOS-00227
V-75393	SRG-OS-000023-GPOS-00006
V-75435	SRG-OS-000023-GPOS-00006
V-75437	SRG-OS-000028-GPOS-00009
V-75439	SRG-OS-000028-GPOS-00009
V-75441	SRG-OS-000029-GPOS-00010
V-75443	SRG-OS-000027-GPOS-00008
V-75445	SRG-OS-000109-GPOS-00056
V-75449	SRG-OS-000069-GPOS-00037
V-75451	SRG-OS-000070-GPOS-00038
V-75453	SRG-OS-000071-GPOS-00039
V-75455	SRG-OS-000266-GPOS-00101
V-75457	SRG-OS-000072-GPOS-00040
V-75459	SRG-OS-000073-GPOS-00041
V-75461	SRG-OS-000073-GPOS-00041
V-75463	SRG-OS-000073-GPOS-00041
V-75465	SRG-OS-000120-GPOS-00061

Canonical Ubuntu 16.04 LTS Security Technical Implementation Guide :: Version 1, Release: 1 Benchmark Date: 23 Jul 2018

Vul ID: V-75389 **Rule ID**: SV-90069r1_rule **STIG ID**: UBTU-16-010000
Severity: CAT I **Classification**: Unclass

Group Title: SRG-OS-000480-GPOS-00227

Rule Title: The Ubuntu operating system must be a vendor supported release.

Discussion: An Ubuntu operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Check Text: Verify the version of the Ubuntu operating system is vendor supported.

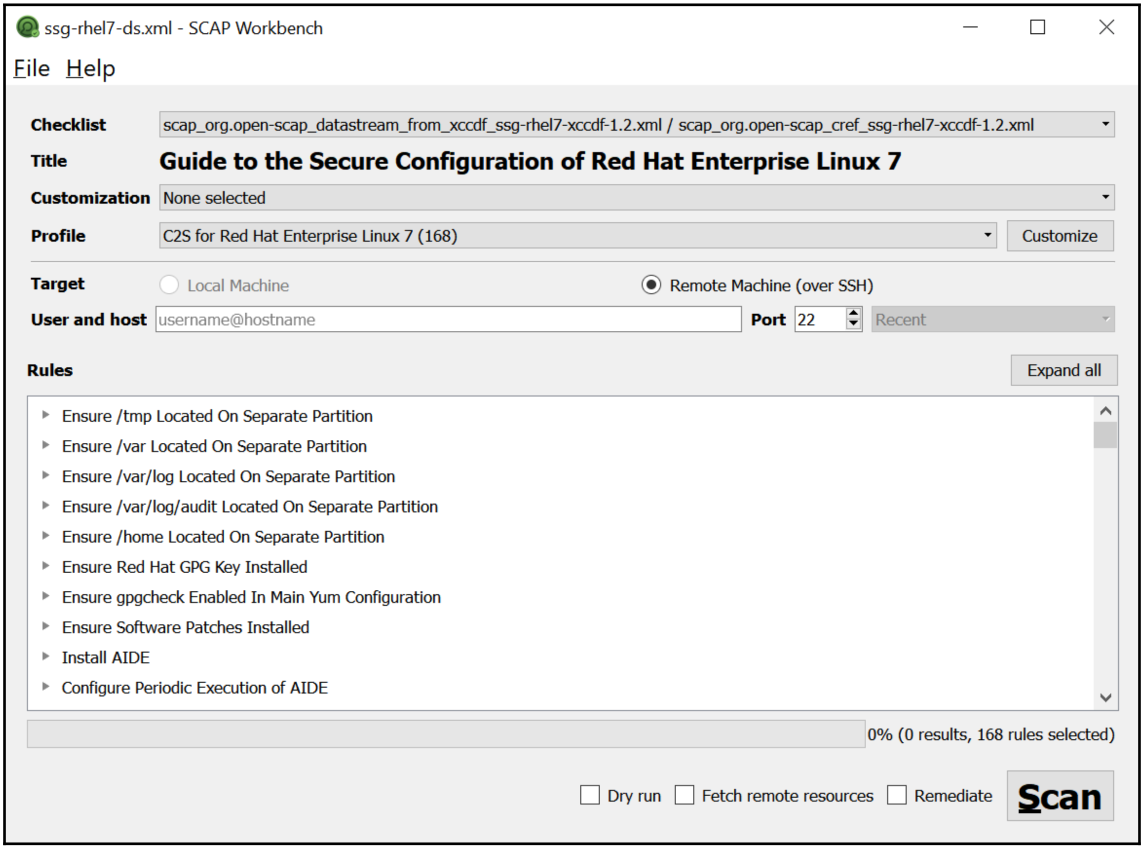
Check the version of the Ubuntu operating system with the following command:

```
# cat /etc/lsb-release

DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.1 LTS"
```

Current End of Life for Ubuntu 16.04 LTS is April 2021.

SCAP Security Guides

- for Fedora Linux
- for Red Hat Enterprise Linux 7
- for Red Hat Enterprise Linux 6
- for Red Hat Enterprise OpenStack Platform 7
- for CentOS 7
- for CentOS 6
- for Scientific Linux 7
- for Scientific Linux 6
- for Debian 8
- for Ubuntu 14.04
- for Ubuntu 16.04
- for Wind River Linux
- for Chromium
- for Firefox
- for Java Runtime Environment
- for Webmin



Checklist scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml / scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml

Title Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Customization None selected

Profile C2S for Red Hat Enterprise Linux 7 (168)

Target ○ Local Machine ● Remote Machine (over SSH)

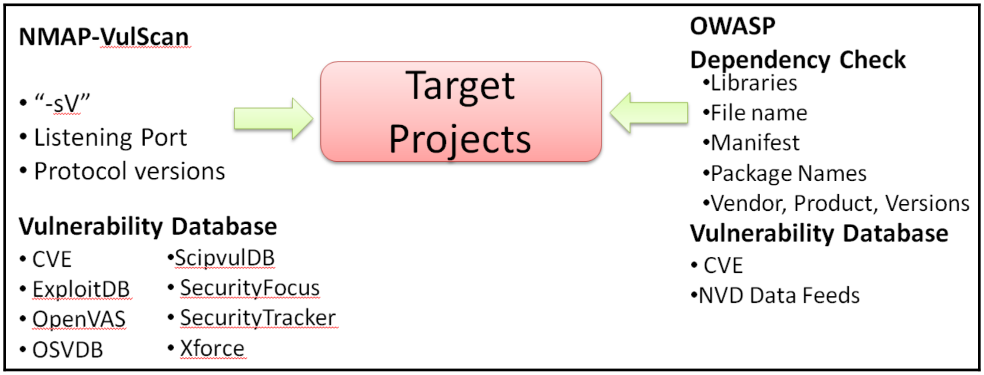
User and host username@hostname **Port** 22 Recent

Rules

- Ensure /tmp Located On Separate Partition
- Ensure /var Located On Separate Partition
- Ensure /var/log Located On Separate Partition
- Ensure /var/log/audit Located On Separate Partition
- Ensure /home Located On Separate Partition
- Ensure Red Hat GPG Key Installed
- Ensure gpgcheck Enabled In Main Yum Configuration
- Ensure Software Patches Installed
- Install AIDE
- Configure Periodic Execution of AIDE

0% (0 results, 168 rules selected)

☐ Dry run ☐ Fetch remote resources ☐ Remediate



NMAP-VulScan

- "-sV"
- Listening Port
- Protocol versions

Target Projects

OWASP Dependency Check

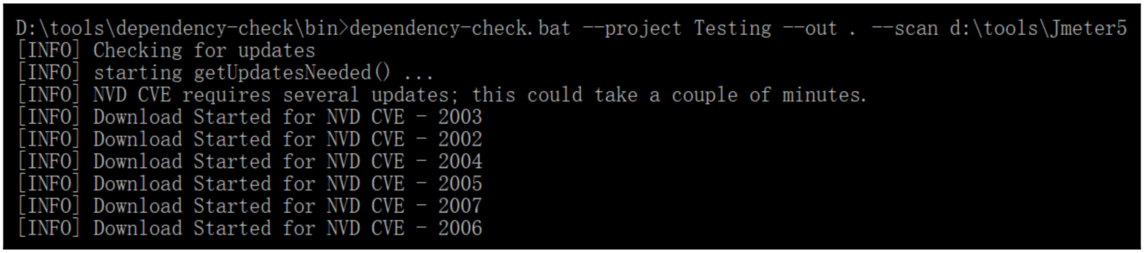
- Libraries
- File name
- Manifest
- Package Names
- Vendor, Product, Versions

Vulnerability Database

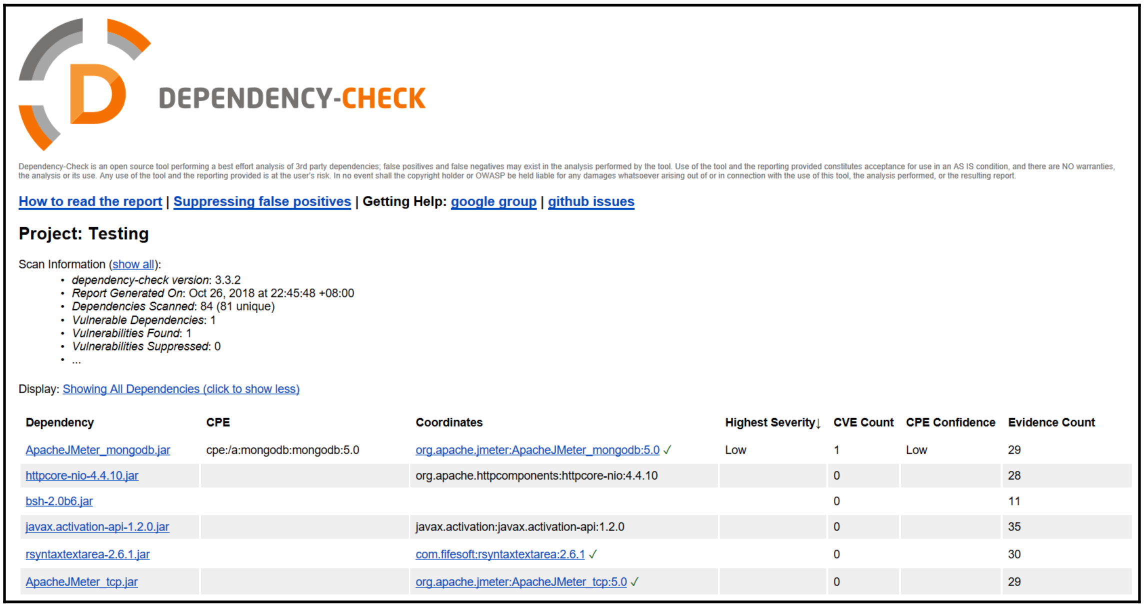
- CVE
- ExploitDB
- OpenVAS
- OSVDB
- ScipvulDB
- SecurityFocus
- SecurityTracker
- Xforce

Vulnerability Database

- CVE
- NVD Data Feeds



```
D:\tools\dependency-check\bin>dependency-check.bat --project Testing --out . --scan d:\tools\Jmeter5
[INFO] Checking for updates
[INFO] starting getUpdatesNeeded() ...
[INFO] NVD CVE requires several updates; this could take a couple of minutes.
[INFO] Download Started for NVD CVE - 2003
[INFO] Download Started for NVD CVE - 2002
[INFO] Download Started for NVD CVE - 2004
[INFO] Download Started for NVD CVE - 2005
[INFO] Download Started for NVD CVE - 2007
[INFO] Download Started for NVD CVE - 2006
```



DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

How to read the report | Suppressing false positives | Getting Help: google group | github issues

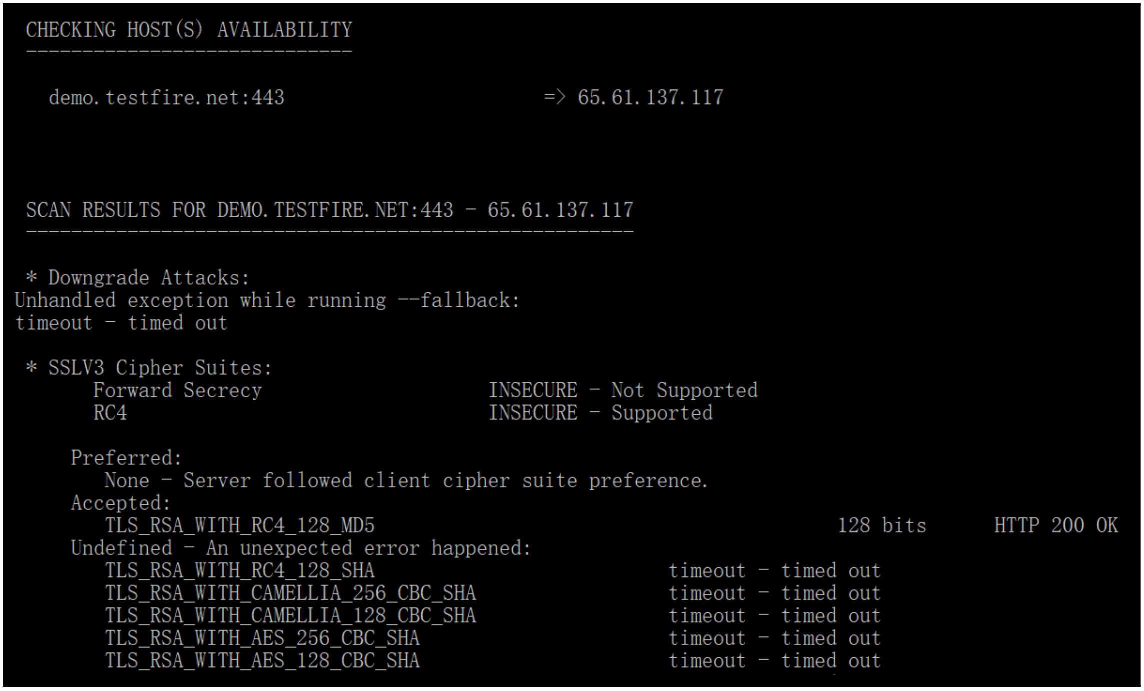
Project: Testing

Scan Information (show all):

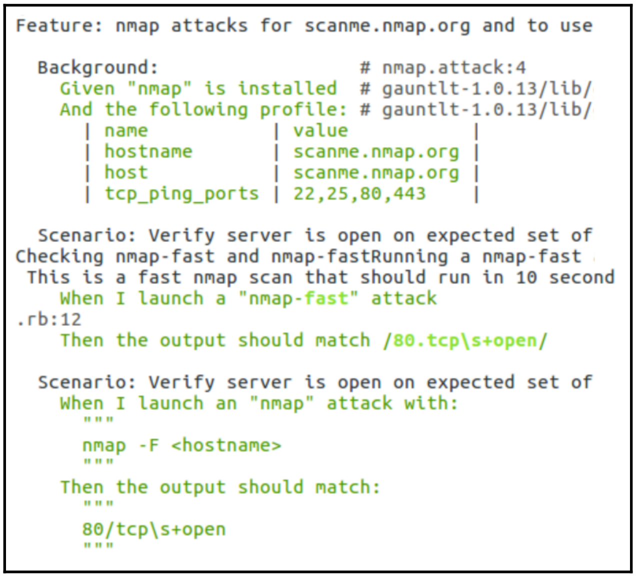
- *dependency-check version*: 3.3.2
- *Report Generated On*: Oct 26, 2018 at 22:45:48 +08:00
- *Dependencies Scanned*: 84 (81 unique)
- *Vulnerable Dependencies*: 1
- *Vulnerabilities Found*: 1
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing All Dependencies (click to show less)

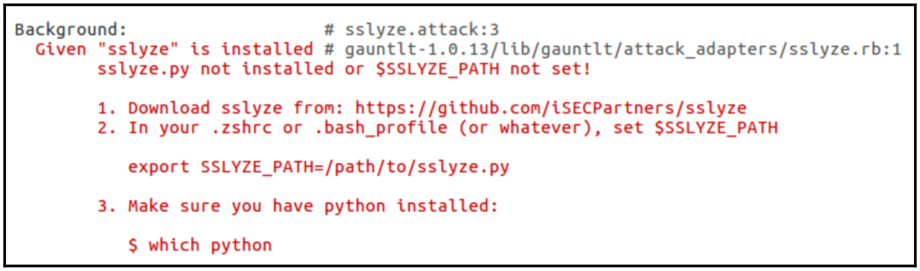
Dependency	CPE	Coordinates	Highest Severity↓	CVE Count	CPE Confidence	Evidence Count
ApacheJMeter_mongodb.jar	cpe:/a:mongodb:mongodb:5.0	org.apache.jmeter:ApacheJMeter_mongodb:5.0 ✓	Low	1	Low	29
httpcore-nio-4.4.10.jar		org.apache.httpcomponents:httpcore-nio:4.4.10		0		28
bsh-2.0b6.jar				0		11
javax.activation-api-1.2.0.jar		javax.activation:javax.activation-api:1.2.0		0		35
rsyntaxtextarea-2.6.1.jar		com.fifesoft:rsyntaxtextarea:2.6.1 ✓		0		30
ApacheJMeter_tcp.jar		org.apache.jmeter:ApacheJMeter_tcp:5.0 ✓		0		29



```
 CHECKING HOST(S) AVAILABILITY
 -----------------------------

   demo.testfire.net:443                       => 65.61.137.117




 SCAN RESULTS FOR DEMO.TESTFIRE.NET:443 - 65.61.137.117
 ------------------------------------------------------

 * Downgrade Attacks:
Unhandled exception while running --fallback:
timeout - timed out

 * SSLV3 Cipher Suites:
       Forward Secrecy                    INSECURE - Not Supported
       RC4                                INSECURE - Supported

     Preferred:
        None - Server followed client cipher suite preference.
     Accepted:
        TLS_RSA_WITH_RC4_128_MD5                                         128 bits      HTTP 200 OK
     Undefined - An unexpected error happened:
        TLS_RSA_WITH_RC4_128_SHA                          timeout - timed out
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 timeout - timed out
        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 timeout - timed out
        TLS_RSA_WITH_AES_256_CBC_SHA                      timeout - timed out
        TLS_RSA_WITH_AES_128_CBC_SHA                      timeout - timed out
```

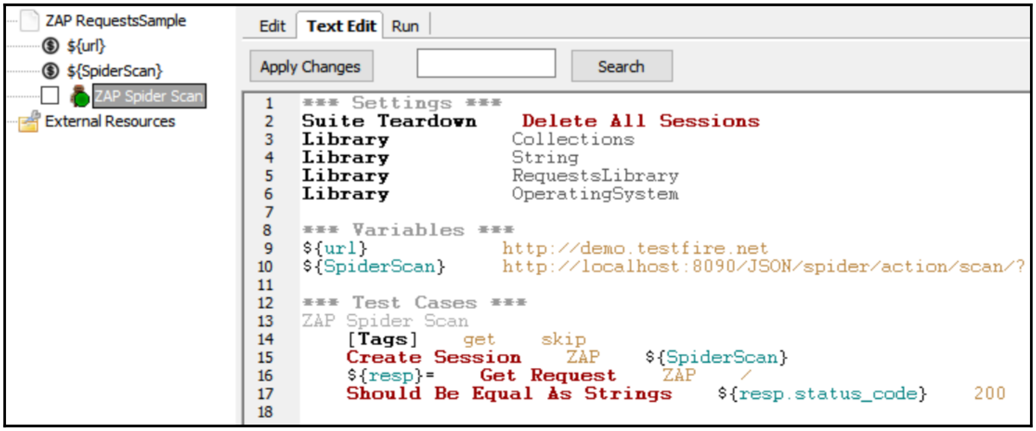


```
Feature: nmap attacks for scanme.nmap.org and to use

  Background:                        # nmap.attack:4
    Given "nmap" is installed        # gauntlt-1.0.13/lib/
    And the following profile:       # gauntlt-1.0.13/lib/
      | name           | value           |
      | hostname       | scanme.nmap.org |
      | host           | scanme.nmap.org |
      | tcp_ping_ports | 22,25,80,443    |

  Scenario: Verify server is open on expected set of
Checking nmap-fast and nmap-fastRunning a nmap-fast
 This is a fast nmap scan that should run in 10 second
    When I launch a "nmap-fast" attack
.rb:12
    Then the output should match /80.tcp\s+open/

  Scenario: Verify server is open on expected set of
    When I launch an "nmap" attack with:
      """
      nmap -F <hostname>
      """
    Then the output should match:
      """
      80/tcp\s+open
      """
```

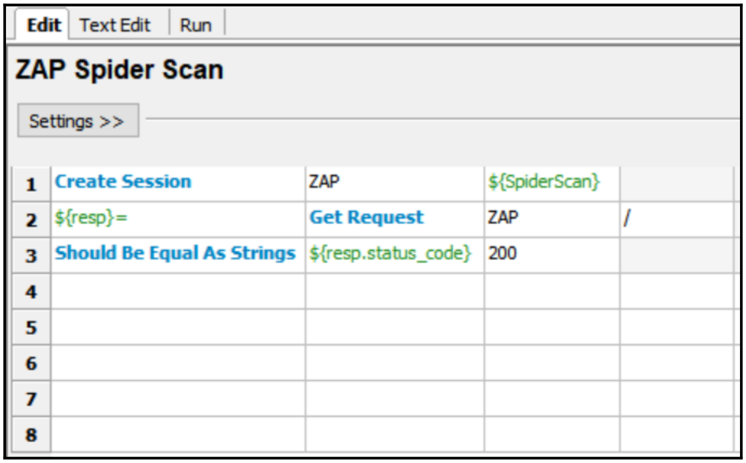


```
Background:                   # sslyze.attack:3
  Given "sslyze" is installed # gauntlt-1.0.13/lib/gauntlt/attack_adapters/sslyze.rb:1
        sslyze.py not installed or $SSLYZE_PATH not set!

        1. Download sslyze from: https://github.com/iSECPartners/sslyze
        2. In your .zshrc or .bash_profile (or whatever), set $SSLYZE_PATH

           export SSLYZE_PATH=/path/to/sslyze.py

        3. Make sure you have python installed:

           $ which python
```

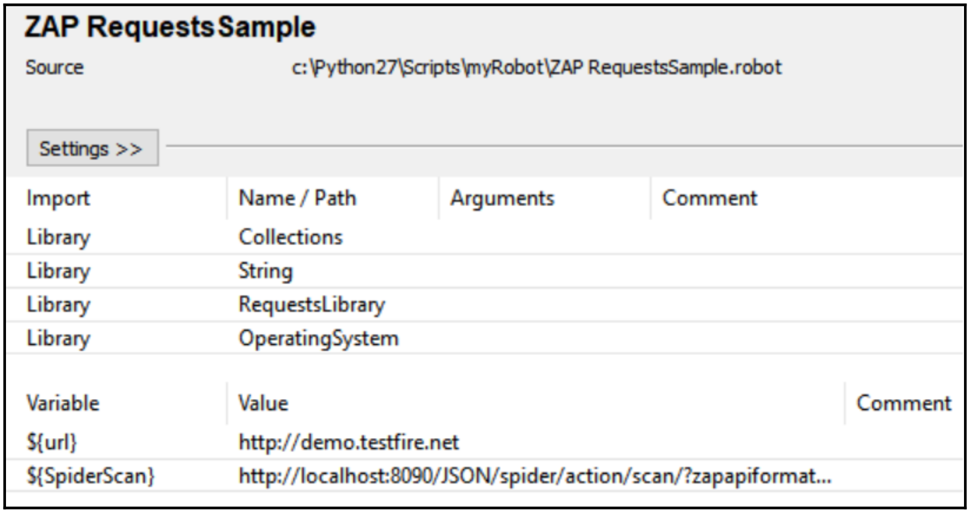
Chapter 9:
BDD Acceptance Security Testing



```
*** Settings ***
Suite Teardown    Delete All Sessions
Library           Collections
Library           String
Library           RequestsLibrary
Library           OperatingSystem

*** Variables ***
${url}            http://demo.testfire.net
${SpiderScan}     http://localhost:8090/JSON/spider/action/scan/?

*** Test Cases ***
ZAP Spider Scan
    [Tags]    get    skip
    Create Session    ZAP    ${SpiderScan}
    ${resp}=    Get Request    ZAP    /
    Should Be Equal As Strings    ${resp.status_code}    200

```



1	Create Session	ZAP	${SpiderScan}	
2	${resp}=	Get Request	ZAP	/
3	Should Be Equal As Strings	${resp.status_code}	200	
4				
5				
6				
7				
8				



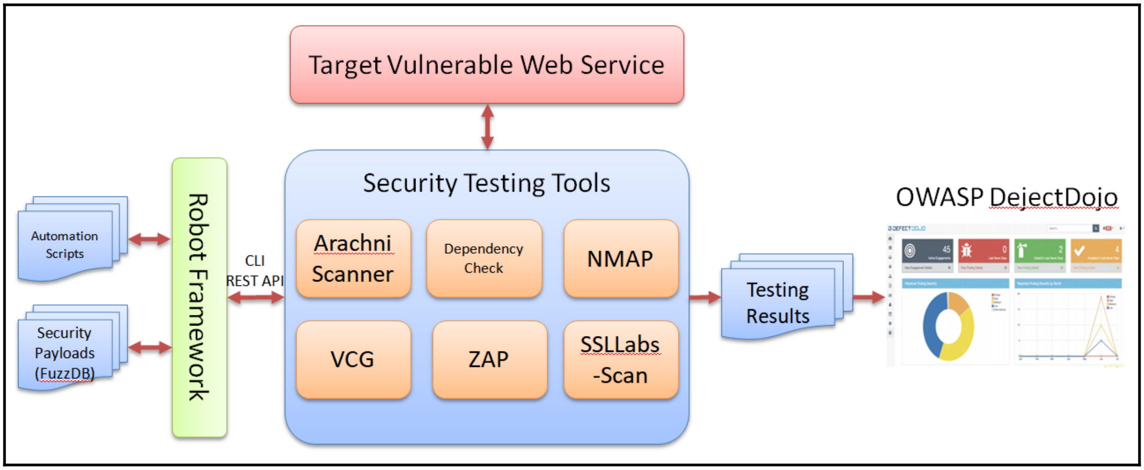
ZAP RequestsSample

Source c:\Python27\Scripts\myRobot\ZAP RequestsSample.robot

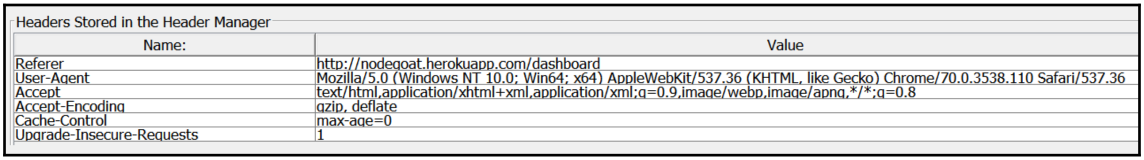
Import	Name / Path	Arguments	Comment
Library	Collections		
Library	String		
Library	RequestsLibrary		
Library	OperatingSystem		

Variable	Value	Comment
${url}	http://demo.testfire.net	
${SpiderScan}	http://localhost:8090/JSON/spider/action/scan/?zapapiformat...	

Chapter 10:
Project Background and Automation Approach

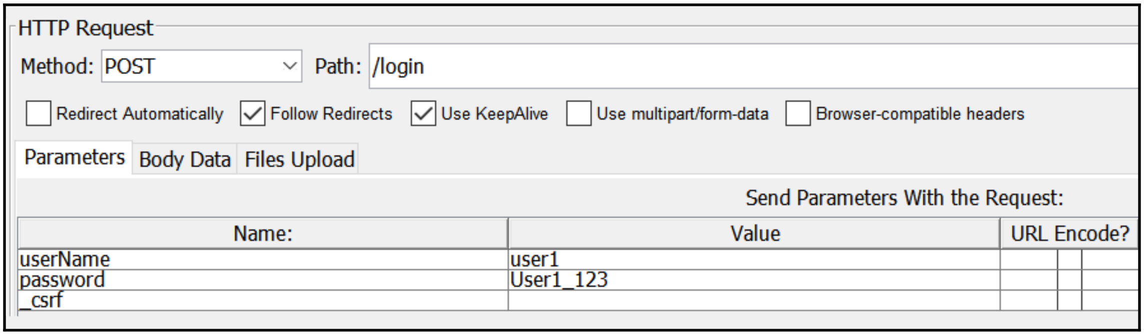


Chapter 11:
Automated Testing for Web Applications



Headers Stored in the Header Manager

Name:	Value
Referer	http://nodegoat.herokuapp.com/dashboard
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding	gzip, deflate
Cache-Control	max-age=0
Upgrade-Insecure-Requests	1



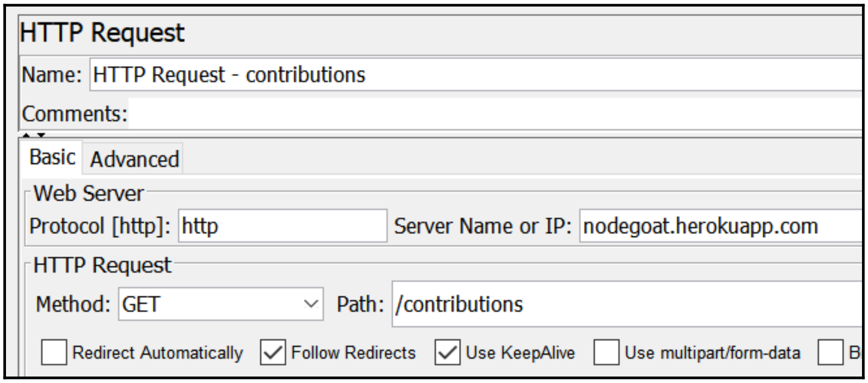
HTTP Request

Method: POST Path: /login

☐ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive ☐ Use multipart/form-data ☐ Browser-compatible headers

Send Parameters With the Request:

Name:	Value	URL Encode?
userName	user1	
password	User1_123	
_csrf		



HTTP Request

Name: HTTP Request - contributions

Comments:

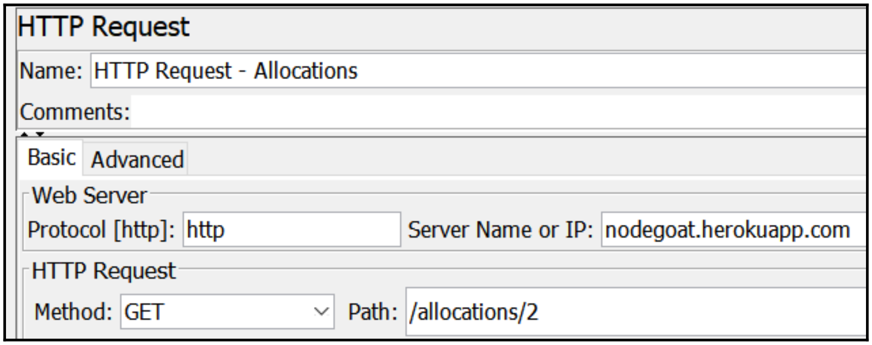
Web Server

Protocol [http]: http Server Name or IP: nodegoat.herokuapp.com

HTTP Request

Method: GET Path: /contributions

☐ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive ☐ Use multipart/form-data ☐ B



HTTP Request

Name: HTTP Request - Allocations

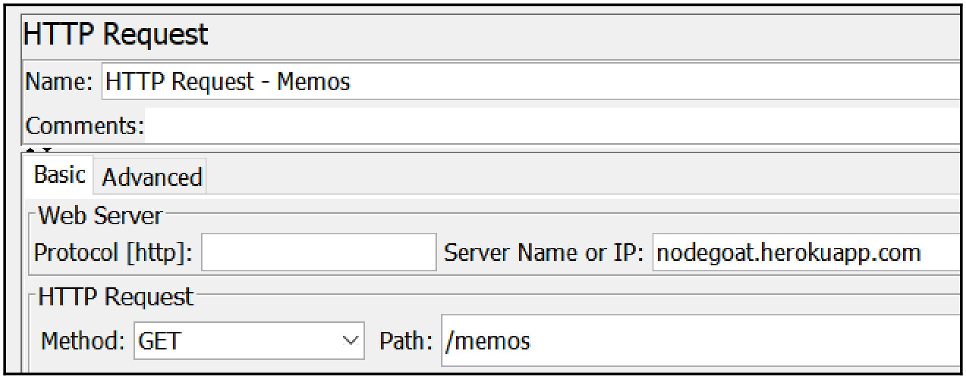
Comments:

Web Server

Protocol [http]: http Server Name or IP: nodegoat.herokuapp.com

HTTP Request

Method: GET Path: /allocations/2



HTTP Request

Name: HTTP Request - Memos

Comments:

Web Server

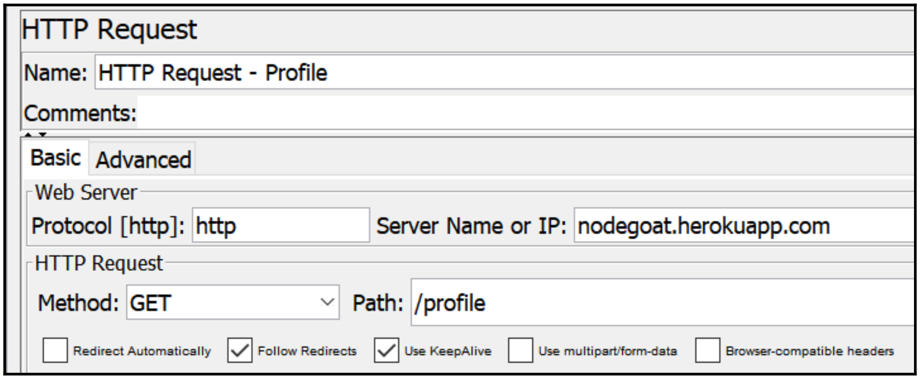
Protocol [http]:

Server Name or IP: nodegoat.herokuapp.com

HTTP Request

Method: GET

Path: /memos



HTTP Request

Name: HTTP Request - Profile

Comments:

Web Server

Protocol [http]: http

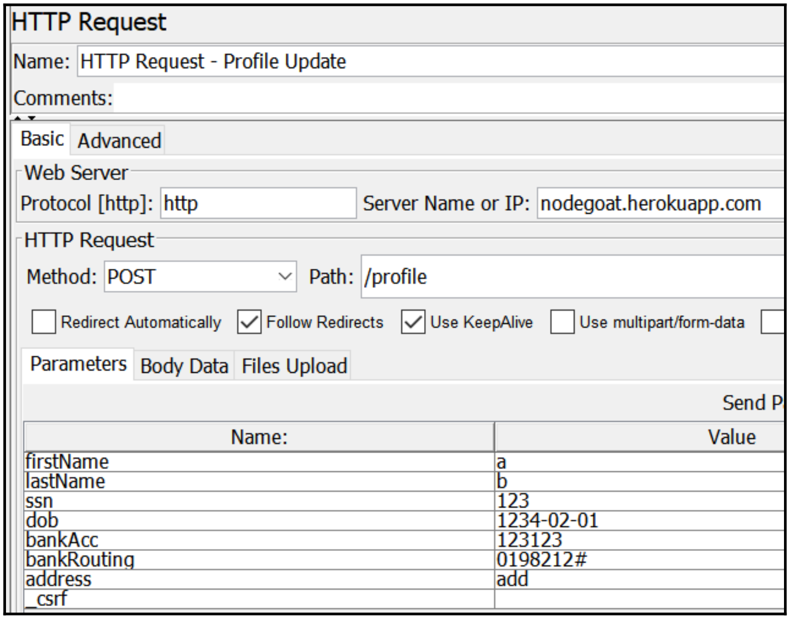
Server Name or IP: nodegoat.herokuapp.com

HTTP Request

Method: GET

Path: /profile

☐ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive ☐ Use multipart/form-data ☐ Browser-compatible headers



HTTP Request

Name: HTTP Request - Profile Update

Comments:

Web Server

Protocol [http]: http

Server Name or IP: nodegoat.herokuapp.com

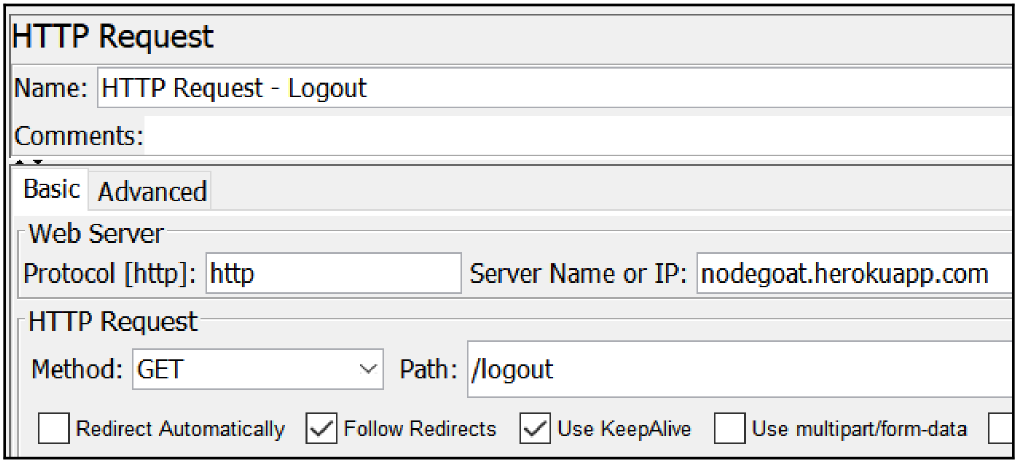
HTTP Request

Method: POST

Path: /profile

□ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive □ Use multipart/form-data □

Name:	Value
firstName	a
lastName	b
ssn	123
dob	1234-02-01
bankAcc	123123
bankRouting	0198212#
address	add
_csrf	



HTTP Request

Name: HTTP Request - Logout

Comments:

Web Server

Protocol [http]: http

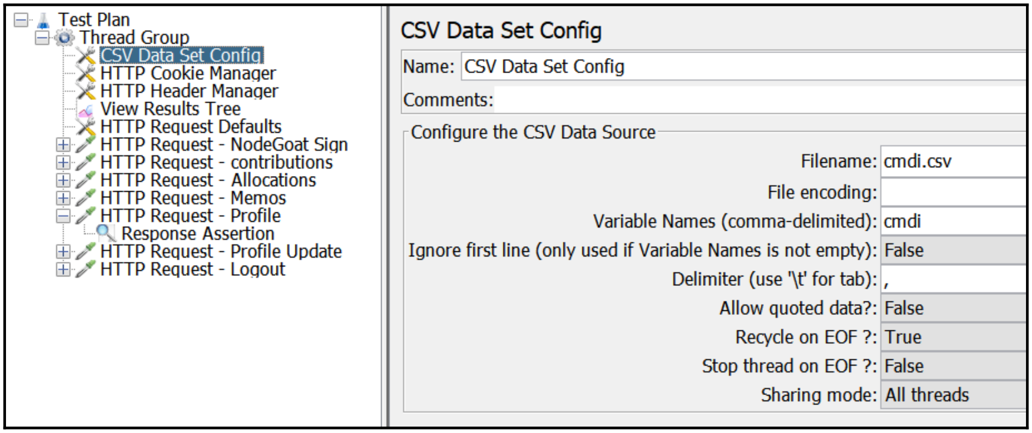
Server Name or IP: nodegoat.herokuapp.com

HTTP Request

Method: GET

Path: /logout

□ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive □ Use multipart/form-data □



- Test Plan
  - Thread Group
    - CSV Data Set Config
    - HTTP Cookie Manager
    - HTTP Header Manager
    - View Results Tree
    - HTTP Request Defaults
    - HTTP Request - NodeGoat Sign
    - HTTP Request - contributions
    - HTTP Request - Allocations
    - HTTP Request - Memos
    - HTTP Request - Profile
      - Response Assertion
    - HTTP Request - Profile Update
    - HTTP Request - Logout

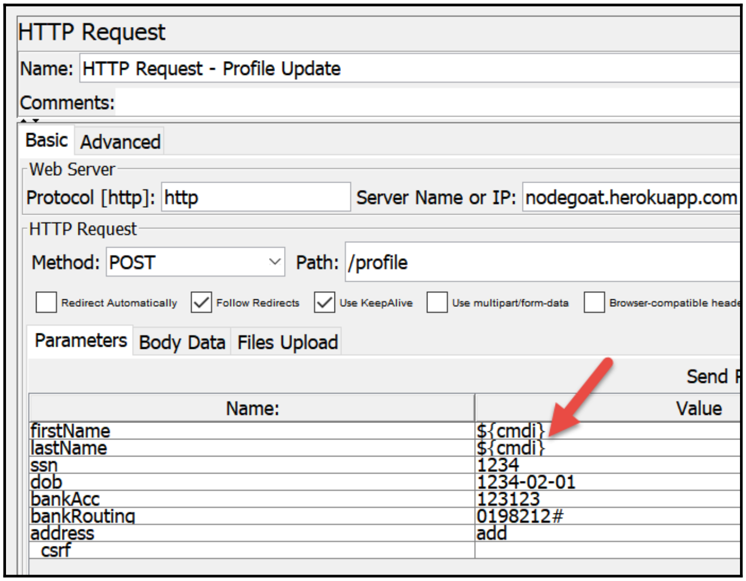
CSV Data Set Config

Name: CSV Data Set Config

Comments:

Configure the CSV Data Source

Filename:	cmdi.csv
File encoding:	
Variable Names (comma-delimited):	cmdi
Ignore first line (only used if Variable Names is not empty):	False
Delimiter (use '\t' for tab):	,
Allow quoted data?:	False
Recycle on EOF ?:	True
Stop thread on EOF ?:	False
Sharing mode:	All threads



HTTP Request

Name: HTTP Request - Profile Update

Comments:

Web Server

Protocol [http]: http Server Name or IP: nodegoat.herokuapp.com

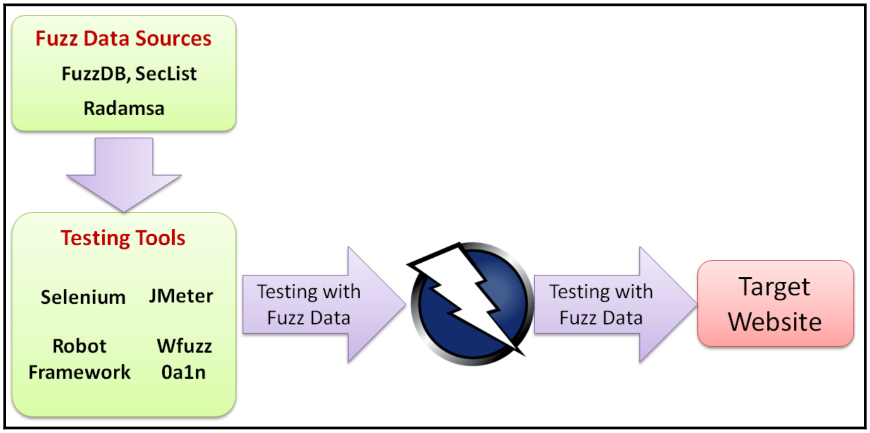
HTTP Request

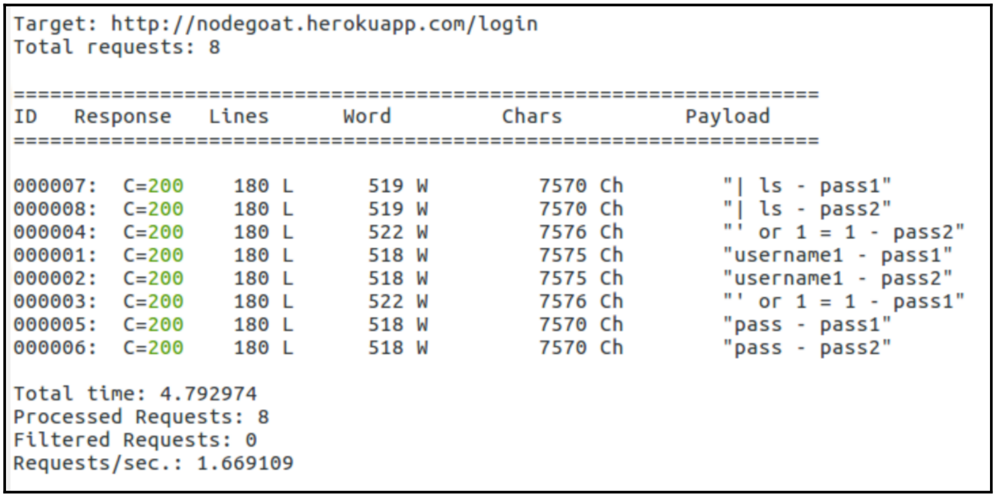
Method: POST Path: /profile

□ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive □ Use multipart/form-data □ Browser-compatible heade

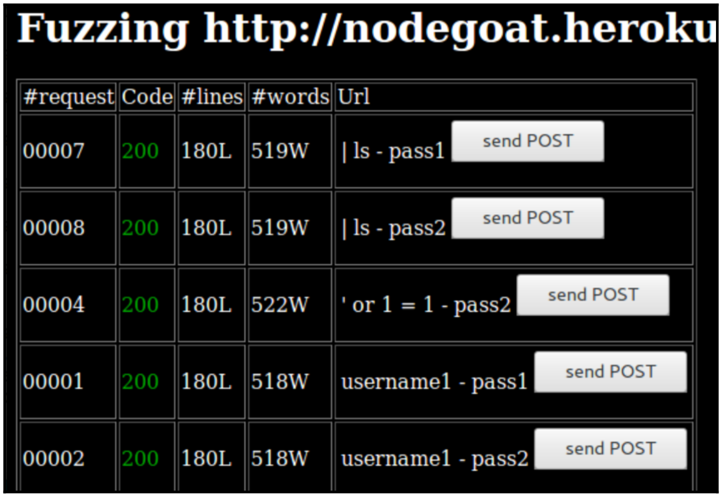
Name:	Value
firstName	${cmdi}
lastName	${cmdi}
ssn	1234
dob	1234-02-01
bankAcc	123123
bankRouting	0198212#
address	add
csrf	

Chapter 12:
Automated Fuzz API Security Testing



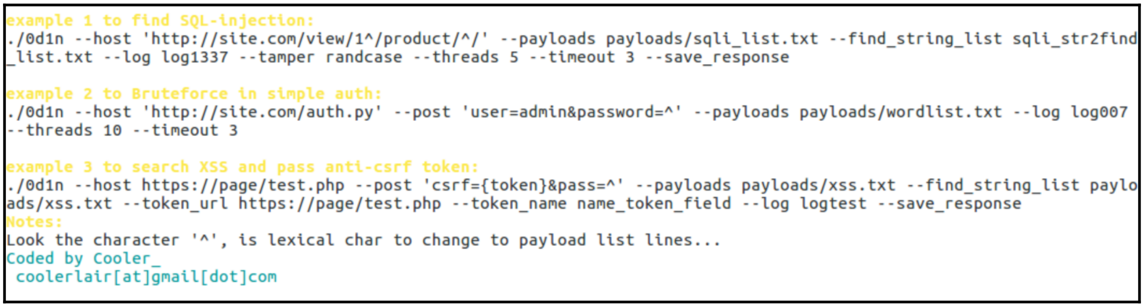


```
Target: http://nodegoat.herokuapp.com/login
Total requests: 8

==================================================================
ID    Response   Lines      Word         Chars          Payload
==================================================================

000007:   C=200     180 L      519 W        7570 Ch        "| ls - pass1"
000008:   C=200     180 L      519 W        7570 Ch        "| ls - pass2"
000004:   C=200     180 L      522 W        7576 Ch        "' or 1 = 1 - pass2"
000001:   C=200     180 L      518 W        7575 Ch        "username1 - pass1"
000002:   C=200     180 L      518 W        7575 Ch        "username1 - pass2"
000003:   C=200     180 L      522 W        7576 Ch        "' or 1 = 1 - pass1"
000005:   C=200     180 L      518 W        7570 Ch        "pass - pass1"
000006:   C=200     180 L      518 W        7570 Ch        "pass - pass2"

Total time: 4.792974
Processed Requests: 8
Filtered Requests: 0
Requests/sec.: 1.669109
```

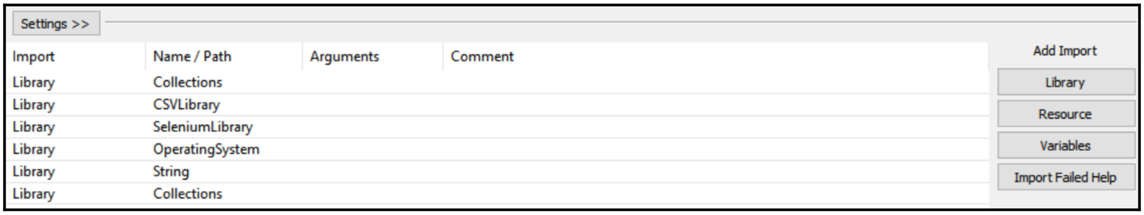


Fuzzing http://nodegoat.heroku

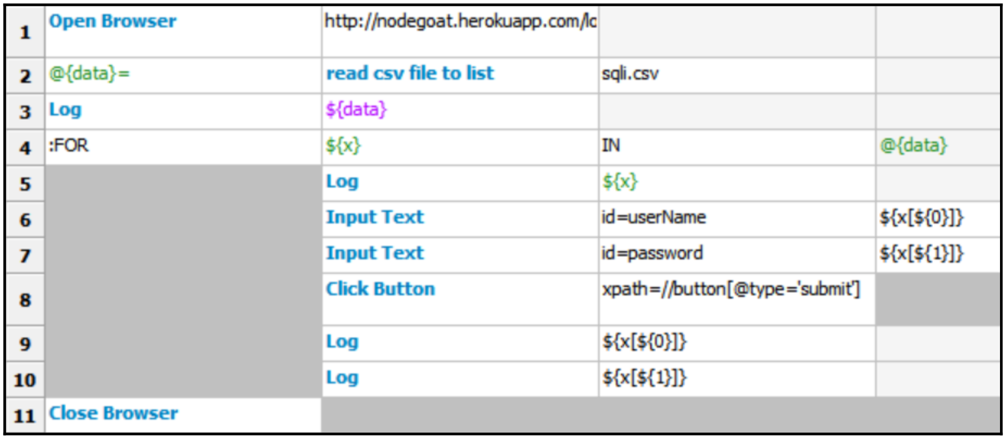
#request	Code	#lines	#words	Url
00007	200	180L	519W	| ls - pass1 send POST
00008	200	180L	519W	| ls - pass2 send POST
00004	200	180L	522W	' or 1 = 1 - pass2 send POST
00001	200	180L	518W	username1 - pass1 send POST
00002	200	180L	518W	username1 - pass2 send POST



```
example 1 to find SQL-injection:
./0d1n --host 'http://site.com/view/1^/product/^/' --payloads payloads/sqli_list.txt --find_string_list sqli_str2find
_list.txt --log log1337 --tamper randcase --threads 5 --timeout 3 --save_response

example 2 to Bruteforce in simple auth:
./0d1n --host 'http://site.com/auth.py' --post 'user=admin&password=^' --payloads payloads/wordlist.txt --log log007
--threads 10 --timeout 3

example 3 to search XSS and pass anti-csrf token:
./0d1n --host https://page/test.php --post 'csrf={token}&pass=^' --payloads payloads/xss.txt --find_string_list paylo
ads/xss.txt --token_url https://page/test.php --token_name name_token_field --log logtest --save_response
Notes:
Look the character '^', is lexical char to change to payload list lines...
Coded by Cooler_
 coolerlair[at]gmail[dot]com
```

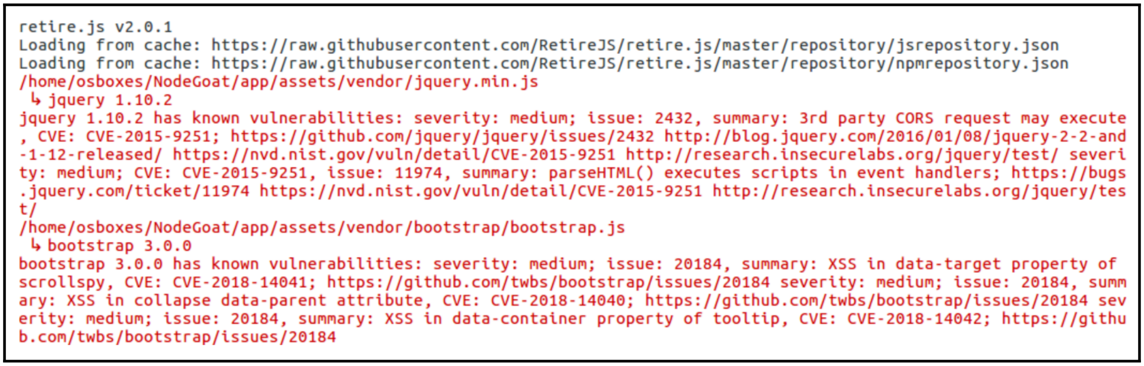


Import	Name / Path	Arguments	Comment
Library	Collections		
Library	CSVLibrary		
Library	SeleniumLibrary		
Library	OperatingSystem		
Library	String		
Library	Collections		

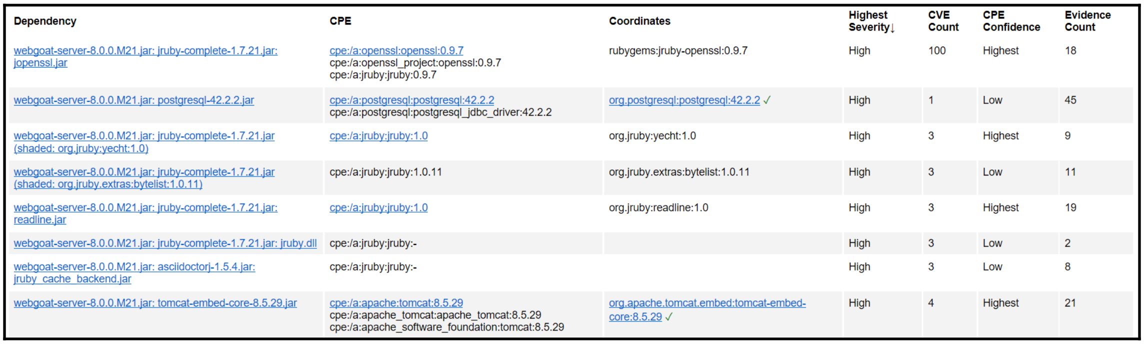


1	Open Browser	http://nodegoat.herokuapp.com/lo		
2	@{data}=	read csv file to list	sqli.csv	
3	Log	${data}		
4	:FOR	${x}	IN	@{data}
5		Log	${x}	
6		Input Text	id=userName	${x[${0}]}
7		Input Text	id=password	${x[${1}]}
8		Click Button	xpath=//button[@type='submit']	
9		Log	${x[${0}]}	
10		Log	${x[${1}]}	
11	Close Browser			

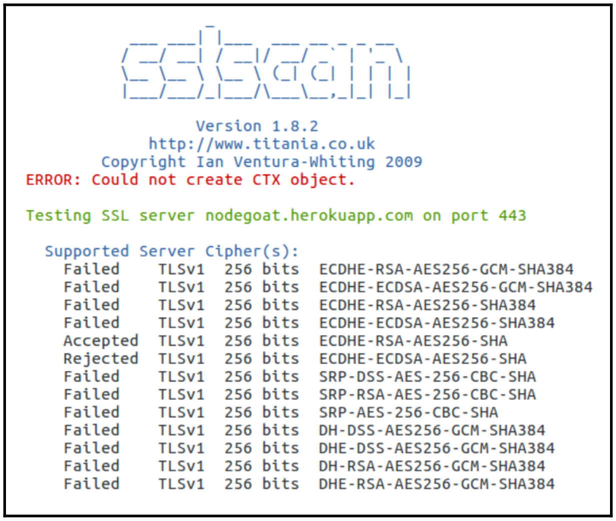
Chapter 13:
Automated Infrastructure Security



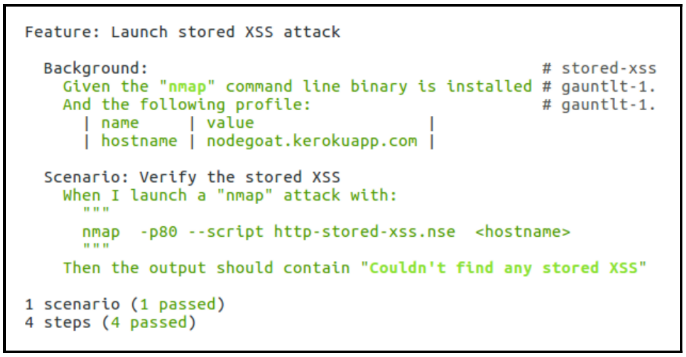
```
retire.js v2.0.1
Loading from cache: https://raw.githubusercontent.com/RetireJS/retire.js/master/repository/jsrepository.json
Loading from cache: https://raw.githubusercontent.com/RetireJS/retire.js/master/repository/npmrepository.json
/home/osboxes/NodeGoat/app/assets/vendor/jquery.min.js
 ↳ jquery 1.10.2
jquery 1.10.2 has known vulnerabilities: severity: medium; issue: 2432, summary: 3rd party CORS request may execute
, CVE: CVE-2015-9251; https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and
-1-12-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 http://research.insecurelabs.org/jquery/test/ severi
ty: medium; CVE: CVE-2015-9251, issue: 11974, summary: parseHTML() executes scripts in event handlers; https://bugs
.jquery.com/ticket/11974 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 http://research.insecurelabs.org/jquery/tes
t/
/home/osboxes/NodeGoat/app/assets/vendor/bootstrap/bootstrap.js
 ↳ bootstrap 3.0.0
bootstrap 3.0.0 has known vulnerabilities: severity: medium; issue: 20184, summary: XSS in data-target property of
scrollspy, CVE: CVE-2018-14041; https://github.com/twbs/bootstrap/issues/20184 severity: medium; issue: 20184, summ
ary: XSS in collapse data-parent attribute, CVE: CVE-2018-14040; https://github.com/twbs/bootstrap/issues/20184 sev
erity: medium; issue: 20184, summary: XSS in data-container property of tooltip, CVE: CVE-2018-14042; https://githu
b.com/twbs/bootstrap/issues/20184
```



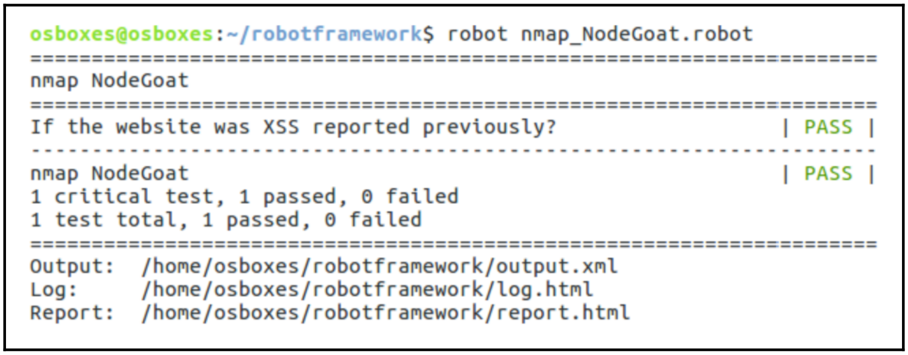
Dependency	CPE	Coordinates	Highest Severity↓	CVE Count	CPE Confidence	Evidence Count
webgoat-server-8.0.0.M21.jar: jruby-complete-1.7.21.jar: jopenssl.jar	cpe:/a:openssl:openssl:0.9.7 cpe:/a:openssl_project:openssl:0.9.7 cpe:/a:jruby:jruby:0.9.7	rubygems:jruby-openssl:0.9.7	High	100	Highest	18
webgoat-server-8.0.0.M21.jar: postgresql-42.2.2.jar	cpe:/a:postgresql:postgresql:42.2.2 cpe:/a:postgresql:postgresql_jdbc_driver:42.2.2	org.postgresql:postgresql:42.2.2 ✓	High	1	Low	45
webgoat-server-8.0.0.M21.jar: jruby-complete-1.7.21.jar (shaded: org.jruby:yecht:1.0)	cpe:/a:jruby:jruby:1.0	org.jruby:yecht:1.0	High	3	Highest	9
webgoat-server-8.0.0.M21.jar: jruby-complete-1.7.21.jar (shaded: org.jruby.extras:bytelist:1.0.11)	cpe:/a:jruby:jruby:1.0.11	org.jruby.extras:bytelist:1.0.11	High	3	Low	11
webgoat-server-8.0.0.M21.jar: jruby-complete-1.7.21.jar: readline.jar	cpe:/a:jruby:jruby:1.0	org.jruby:readline:1.0	High	3	Highest	19
webgoat-server-8.0.0.M21.jar: jruby-complete-1.7.21.jar: jruby.dll	cpe:/a:jruby:jruby:-		High	3	Low	2
webgoat-server-8.0.0.M21.jar: asciidoctorj-1.5.4.jar: jruby_cache_backend.jar	cpe:/a:jruby:jruby:-		High	3	Low	8
webgoat-server-8.0.0.M21.jar: tomcat-embed-core-8.5.29.jar	cpe:/a:apache:tomcat:8.5.29 cpe:/a:apache_tomcat:apache_tomcat:8.5.29 cpe:/a:apache_software_foundation:tomcat:8.5.29	org.apache.tomcat.embed:tomcat-embed-core:8.5.29 ✓	High	4	Highest	21



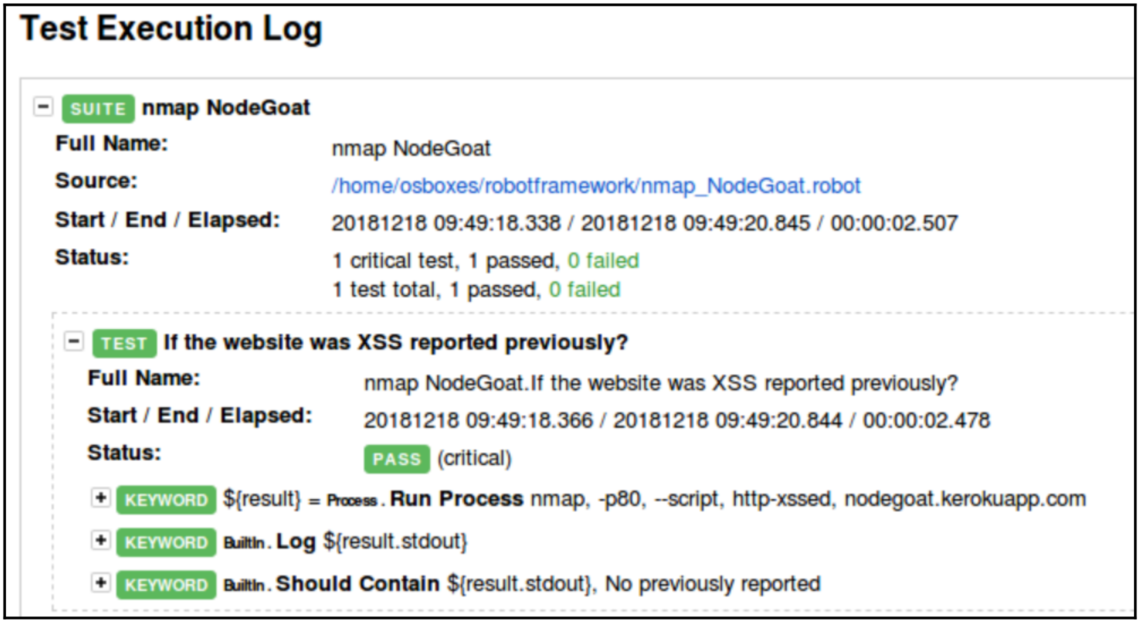
```
                   _
           ___ ___| |___  ___ __ _ _ __
          / __/ __| / __|/ __/ _` | '_ \
          \__ \__ \ \__ \ (_| (_| | | | |
          |___/___/_|___/\___\__,_|_| |_|

                  Version 1.8.2
             http://www.titania.co.uk
        Copyright Ian Ventura-Whiting 2009
ERROR: Could not create CTX object.

Testing SSL server nodegoat.herokuapp.com on port 443

  Supported Server Cipher(s):
    Failed    TLSv1  256 bits  ECDHE-RSA-AES256-GCM-SHA384
    Failed    TLSv1  256 bits  ECDHE-ECDSA-AES256-GCM-SHA384
    Failed    TLSv1  256 bits  ECDHE-RSA-AES256-SHA384
    Failed    TLSv1  256 bits  ECDHE-ECDSA-AES256-SHA384
    Accepted  TLSv1  256 bits  ECDHE-RSA-AES256-SHA
    Rejected  TLSv1  256 bits  ECDHE-ECDSA-AES256-SHA
    Failed    TLSv1  256 bits  SRP-DSS-AES-256-CBC-SHA
    Failed    TLSv1  256 bits  SRP-RSA-AES-256-CBC-SHA
    Failed    TLSv1  256 bits  SRP-AES-256-CBC-SHA
    Failed    TLSv1  256 bits  DH-DSS-AES256-GCM-SHA384
    Failed    TLSv1  256 bits  DHE-DSS-AES256-GCM-SHA384
    Failed    TLSv1  256 bits  DH-RSA-AES256-GCM-SHA384
    Failed    TLSv1  256 bits  DHE-RSA-AES256-GCM-SHA384
```



```
Feature: Launch stored XSS attack

  Background:                                          # stored-xss
    Given the "nmap" command line binary is installed # gauntlt-1.
    And the following profile:                         # gauntlt-1.
      | name     | value                  |
      | hostname | nodegoat.kerokuapp.com |

  Scenario: Verify the stored XSS
    When I launch a "nmap" attack with:
      """
      nmap  -p80 --script http-stored-xss.nse  <hostname>
      """
    Then the output should contain "Couldn't find any stored XSS"

1 scenario (1 passed)
4 steps (4 passed)
```



```
osboxes@osboxes:~/robotframework$ robot nmap_NodeGoat.robot
==============================================================================
nmap NodeGoat
==============================================================================
If the website was XSS reported previously?                           | PASS |
------------------------------------------------------------------------------
nmap NodeGoat                                                         | PASS |
1 critical test, 1 passed, 0 failed
1 test total, 1 passed, 0 failed
==============================================================================
Output:  /home/osboxes/robotframework/output.xml
Log:     /home/osboxes/robotframework/log.html
Report:  /home/osboxes/robotframework/report.html
```



Test Execution Log

− SUITE **nmap NodeGoat**

Full Name: nmap NodeGoat

Source: /home/osboxes/robotframework/nmap_NodeGoat.robot

Start / End / Elapsed: 20181218 09:49:18.338 / 20181218 09:49:20.845 / 00:00:02.507

Status: 1 critical test, 1 passed, 0 failed
1 test total, 1 passed, 0 failed

− TEST **If the website was XSS reported previously?**

Full Name: nmap NodeGoat.If the website was XSS reported previously?

Start / End / Elapsed: 20181218 09:49:18.366 / 20181218 09:49:20.844 / 00:00:02.478

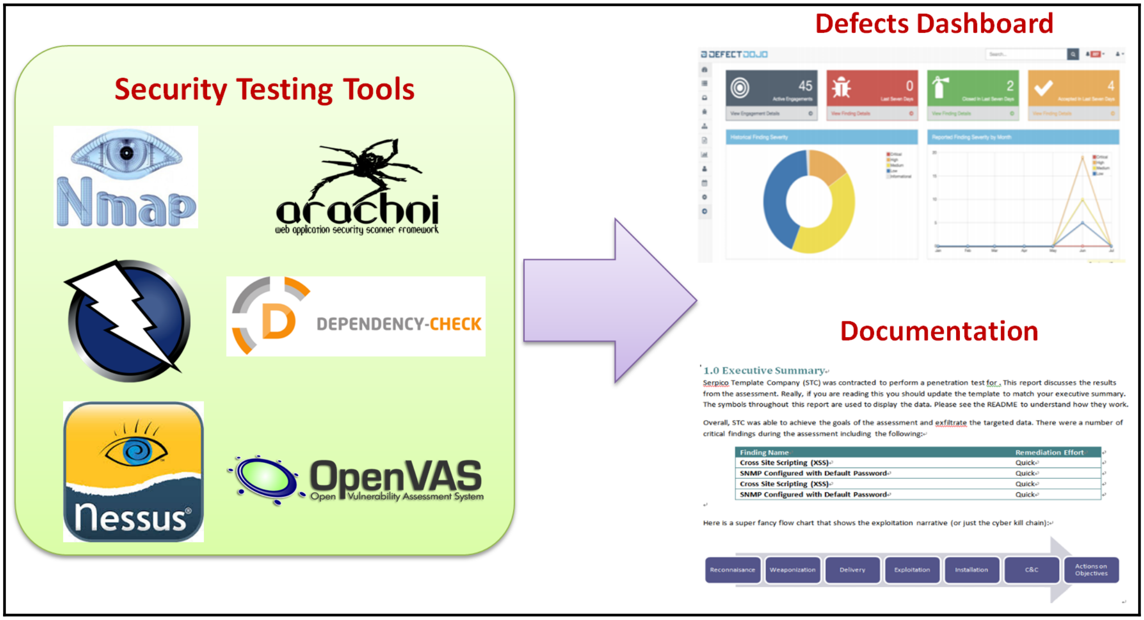
Status: PASS (critical)

+ KEYWORD ${result} = Process . **Run Process** nmap, -p80, --script, http-xssed, nodegoat.kerokuapp.com

+ KEYWORD BuiltIn . **Log** ${result.stdout}

+ KEYWORD BuiltIn . **Should Contain** ${result.stdout}, No previously reported

Chapter 14:
Managing and Presenting Test Results



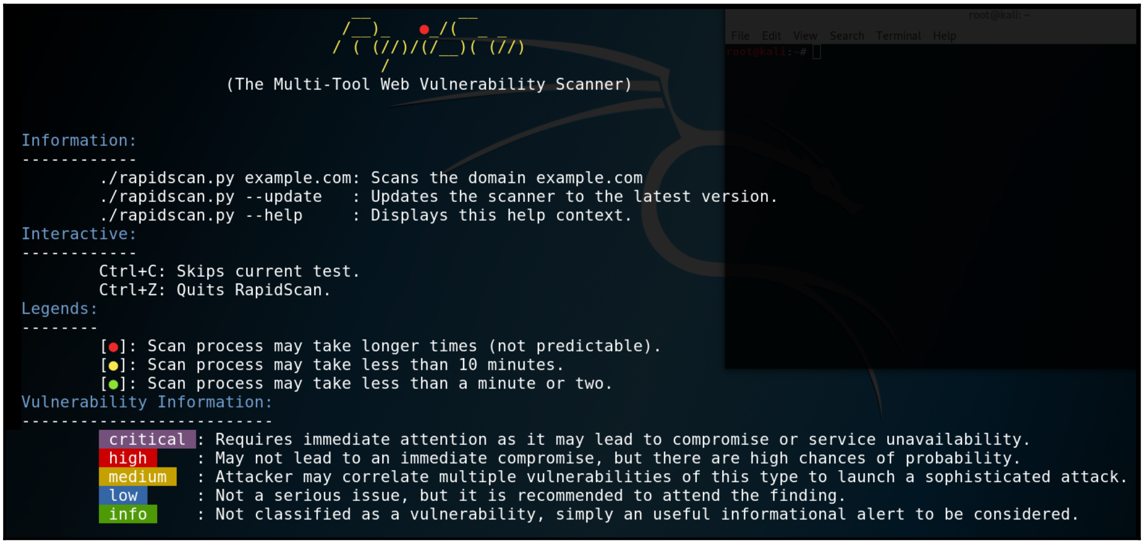
1.0 Executive Summary

Serpico Template Company (STC) was contracted to perform a penetration test for . This report discusses the results from the assessment. Really, if you are reading this you should update the template to match your executive summary. The symbols throughout this report are used to display the data. Please see the README to understand how they work.

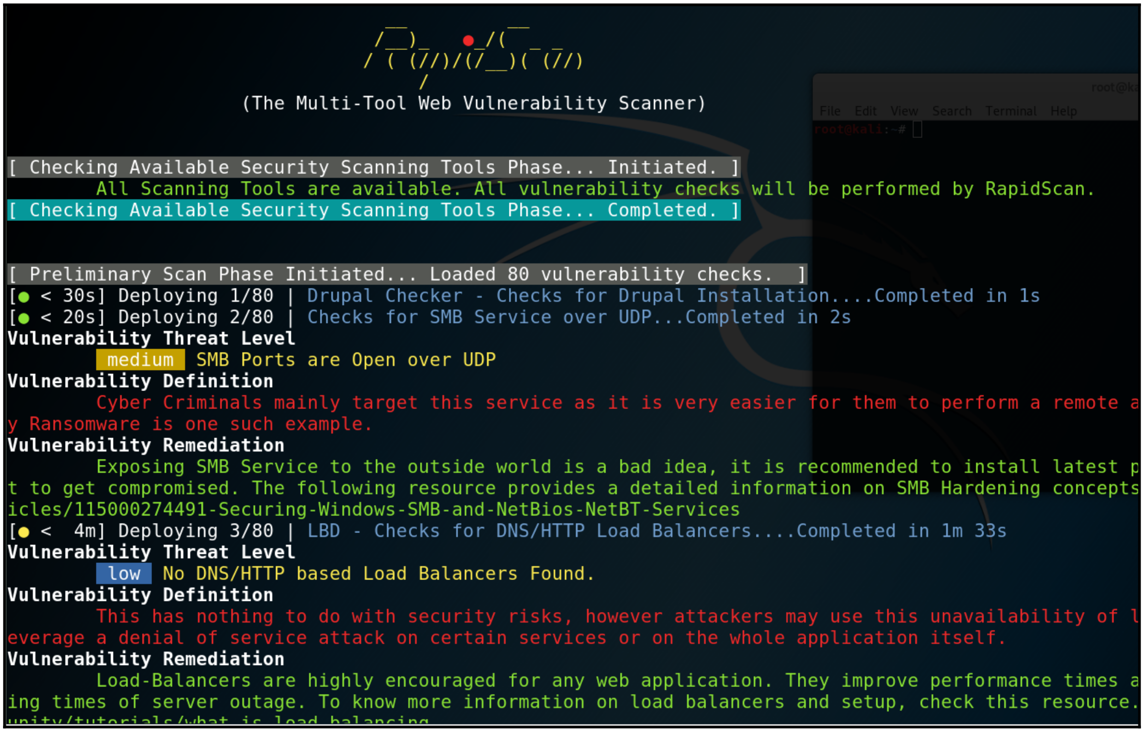
Overall, STC was able to achieve the goals of the assessment and exfiltrate the targeted data. There were a number of critical findings during the assessment including the following:

Finding Name	Remediation Effort
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick

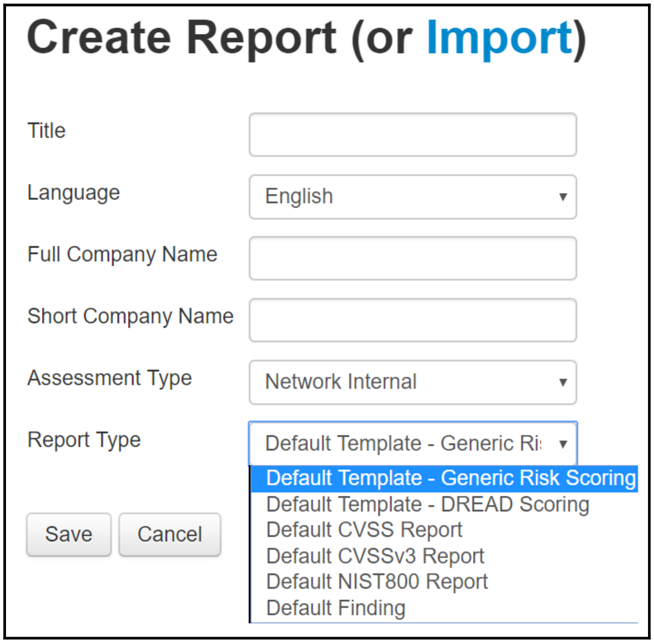
Here is a super fancy flow chart that shows the exploitation narrative (or just the cyber kill chain):



```
                         __          __
                        /__)_   ●_/(  _ _
                       / ( (//)/(/__)( (//)
                            /
            (The Multi-Tool Web Vulnerability Scanner)


Information:
------------
        ./rapidscan.py example.com: Scans the domain example.com
        ./rapidscan.py --update   : Updates the scanner to the latest version.
        ./rapidscan.py --help     : Displays this help context.
Interactive:
------------
        Ctrl+C: Skips current test.
        Ctrl+Z: Quits RapidScan.
Legends:
--------
        [●]: Scan process may take longer times (not predictable).
        [●]: Scan process may take less than 10 minutes.
        [●]: Scan process may take less than a minute or two.
Vulnerability Information:
--------------------------
        critical : Requires immediate attention as it may lead to compromise or service unavailability.
        high     : May not lead to an immediate compromise, but there are high chances of probability.
        medium   : Attacker may correlate multiple vulnerabilities of this type to launch a sophisticated attack.
        low      : Not a serious issue, but it is recommended to attend the finding.
        info     : Not classified as a vulnerability, simply an useful informational alert to be considered.
```

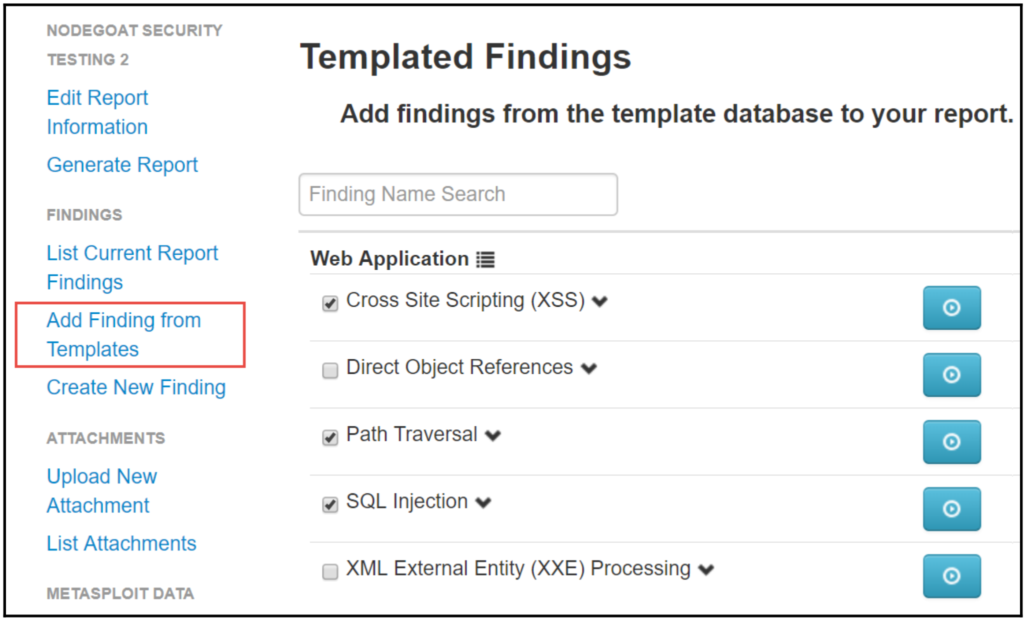


```
                        __         __
                       /__)_   ● _/(  _ _
                      / ( (//)/(/__)( (//)
                           /
                  (The Multi-Tool Web Vulnerability Scanner)


[ Checking Available Security Scanning Tools Phase... Initiated. ]
        All Scanning Tools are available. All vulnerability checks will be performed by RapidScan.
[ Checking Available Security Scanning Tools Phase... Completed. ]


[ Preliminary Scan Phase Initiated... Loaded 80 vulnerability checks.  ]
[● < 30s] Deploying 1/80 | Drupal Checker - Checks for Drupal Installation....Completed in 1s
[● < 20s] Deploying 2/80 | Checks for SMB Service over UDP...Completed in 2s
Vulnerability Threat Level
        medium  SMB Ports are Open over UDP
Vulnerability Definition
        Cyber Criminals mainly target this service as it is very easier for them to perform a remote a
y Ransomware is one such example.
Vulnerability Remediation
        Exposing SMB Service to the outside world is a bad idea, it is recommended to install latest p
t to get compromised. The following resource provides a detailed information on SMB Hardening concepts
icles/115000274491-Securing-Windows-SMB-and-NetBios-NetBT-Services
[● <  4m] Deploying 3/80 | LBD - Checks for DNS/HTTP Load Balancers....Completed in 1m 33s
Vulnerability Threat Level
        low  No DNS/HTTP based Load Balancers Found.
Vulnerability Definition
        This has nothing to do with security risks, however attackers may use this unavailability of l
everage a denial of service attack on certain services or on the whole application itself.
Vulnerability Remediation
        Load-Balancers are highly encouraged for any web application. They improve performance times a
ing times of server outage. To know more information on load balancers and setup, check this resource.
unity/tutorials/what-is-load-balancing
```



Create Report (or Import)

Title	
Language	English ▾
Full Company Name	
Short Company Name	
Assessment Type	Network Internal ▾
Report Type	Default Template - Generic Ri ▾



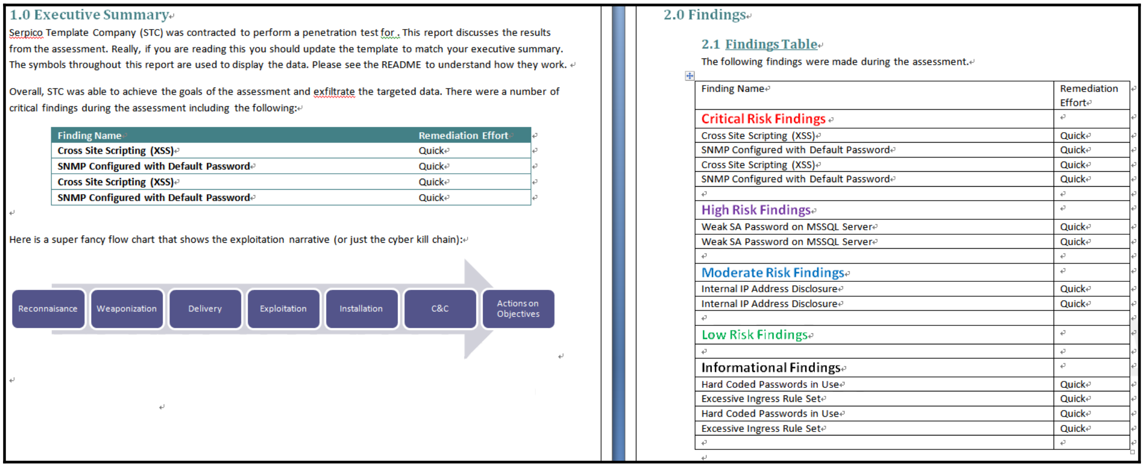
Templated Findings

Add findings from the template database to your report.

Finding Name Search

Web Application

- ☑ Cross Site Scripting (XSS)
- □ Direct Object References
- ☑ Path Traversal
- ☑ SQL Injection
- □ XML External Entity (XXE) Processing



1.0 Executive Summary

Serpico Template Company (STC) was contracted to perform a penetration test for . This report discusses the results from the assessment. Really, if you are reading this you should update the template to match your executive summary. The symbols throughout this report are used to display the data. Please see the README to understand how they work.

Overall, STC was able to achieve the goals of the assessment and exfiltrate the targeted data. There were a number of critical findings during the assessment including the following:

Finding Name	Remediation Effort
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick

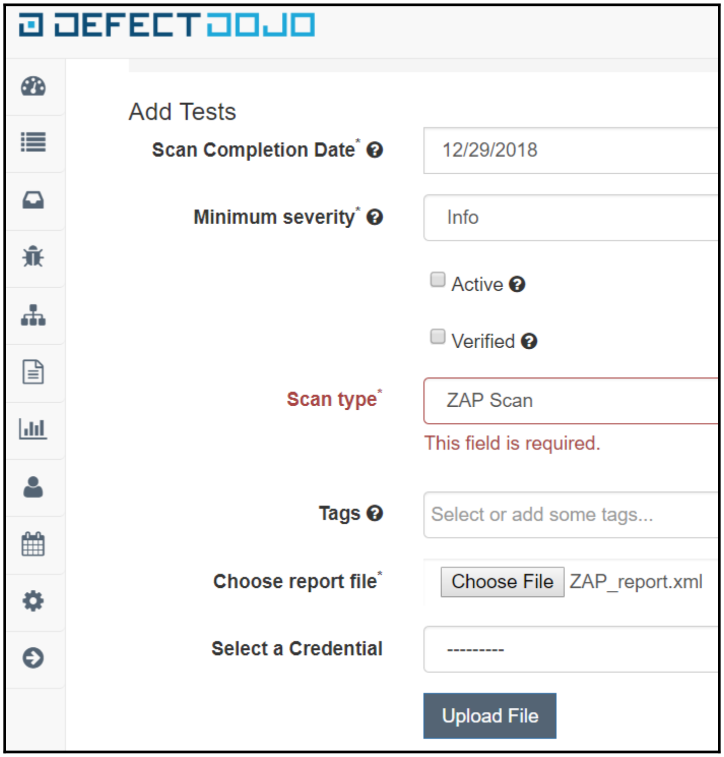
Here is a super fancy flow chart that shows the exploitation narrative (or just the cyber kill chain):

2.0 Findings

2.1 Findings Table

The following findings were made during the assessment.

Finding Name	Remediation Effort
Critical Risk Findings	
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick
High Risk Findings	
Weak SA Password on MSSQL Server	Quick
Weak SA Password on MSSQL Server	Quick
Moderate Risk Findings	
Internal IP Address Disclosure	Quick
Internal IP Address Disclosure	Quick
Low Risk Findings	
Informational Findings	
Hard Coded Passwords in Use	Quick
Excessive Ingress Rule Set	Quick
Hard Coded Passwords in Use	Quick
Excessive Ingress Rule Set	Quick



Add Tests

Scan Completion Date* : 12/29/2018

Minimum severity* : Info

☐ Active

☐ Verified

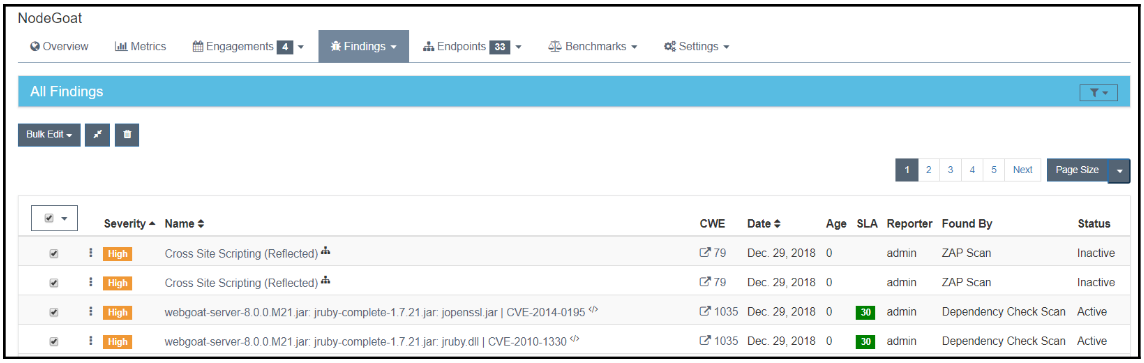
Scan type* : ZAP Scan

This field is required.

Tags : Select or add some tags...

Choose report file* : Choose File ZAP_report.xml

Select a Credential : ---------

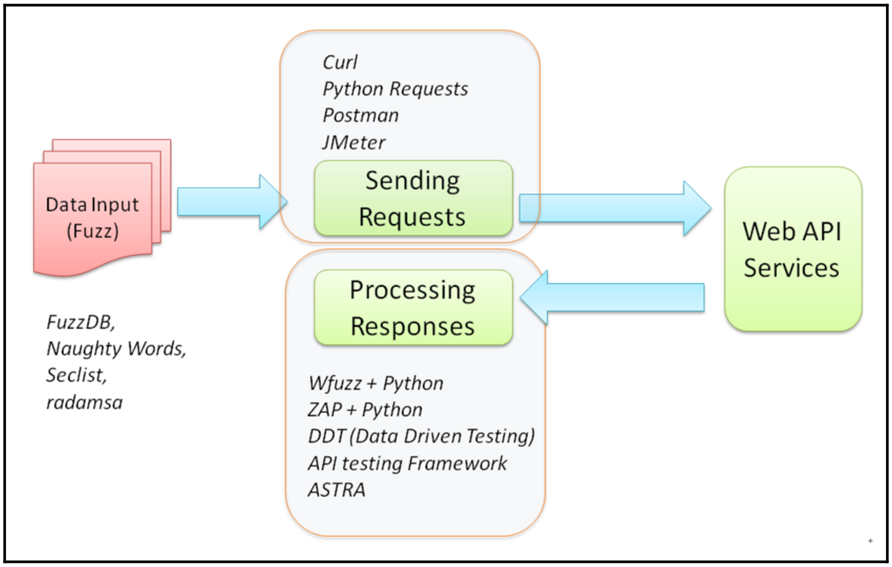


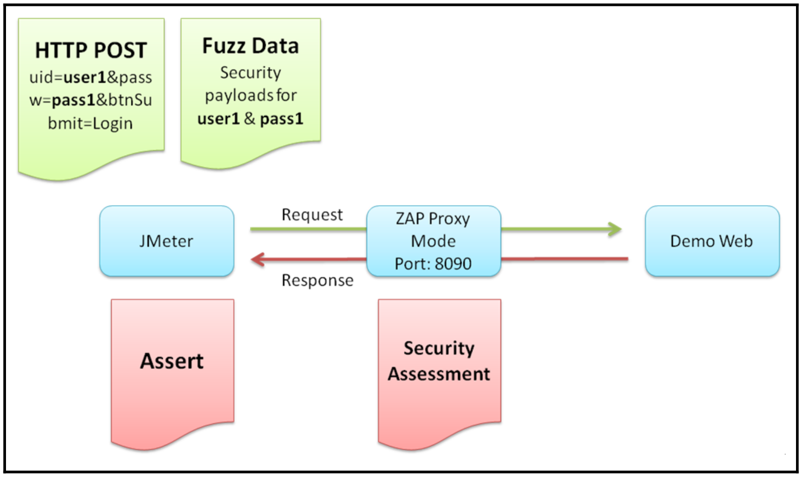
NodeGoat

All Findings

☑		Severity	Name	CWE	Date	Age	SLA	Reporter	Found By	Status
☑	⋮	High	Cross Site Scripting (Reflected)	79	Dec. 29, 2018	0		admin	ZAP Scan	Inactive
☑	⋮	High	Cross Site Scripting (Reflected)	79	Dec. 29, 2018	0		admin	ZAP Scan	Inactive
☑	⋮	High	webgoat-server-8.0.0.M21.jar: jruby-complete-1.7.21.jar: jopenssl.jar | CVE-2014-0195	1035	Dec. 29, 2018	0	30	admin	Dependency Check Scan	Active
☑	⋮	High	webgoat-server-8.0.0.M21.jar: jruby-complete-1.7.21.jar: jruby.dll | CVE-2010-1330	1035	Dec. 29, 2018	0	30	admin	Dependency Check Scan	Active

Chapter 15:
Summary of Automation Security Testing Ti ps




HTTP POST
uid=user1&passw=pass1&btnSubmit=Login
Fuzz Data
Security payloads for user1 & pass1
JMeter
Request
Response
ZAP Proxy Mode Port: 8090
Demo Web
Assert
Security Assessment