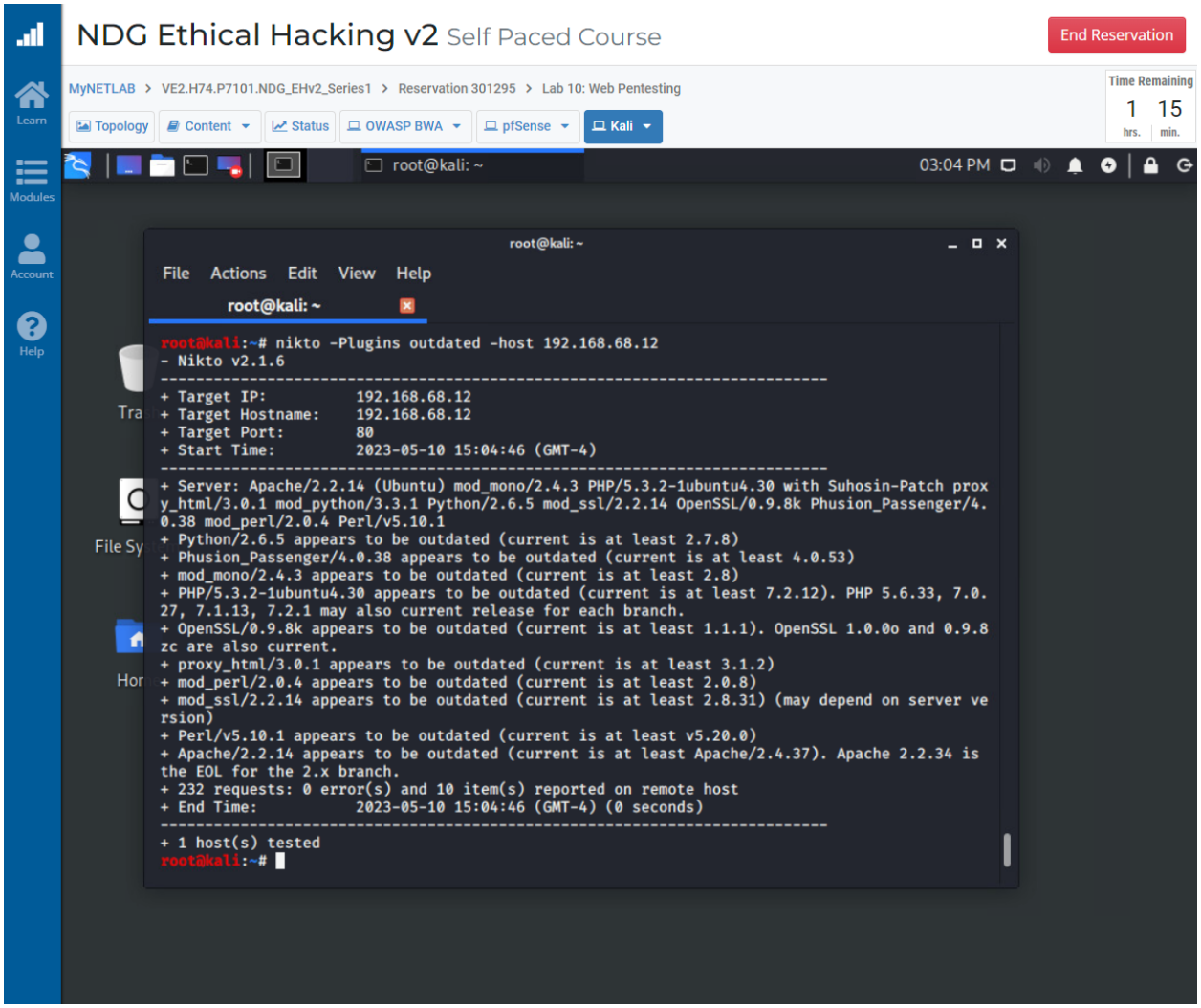
Jason Palmeri
CS53C
Lab 10
Timothy Ryan

Web Pentesting

```
root@kali:~# nikto -host 192.168.68.12
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.68.12
+ Target Hostname:    192.168.68.12
+ Target Port:        80
+ Start Time:         2023-05-10 15:03:35 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch prox
y_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.
0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Server may leak inodes via ETags, header found with file /, inode: 286483, size: 28067, mti
me: Thu Jul 30 22:55:52 2015
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to prote
ct against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
 content of the site in a different fashion to the MIME type
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2
```

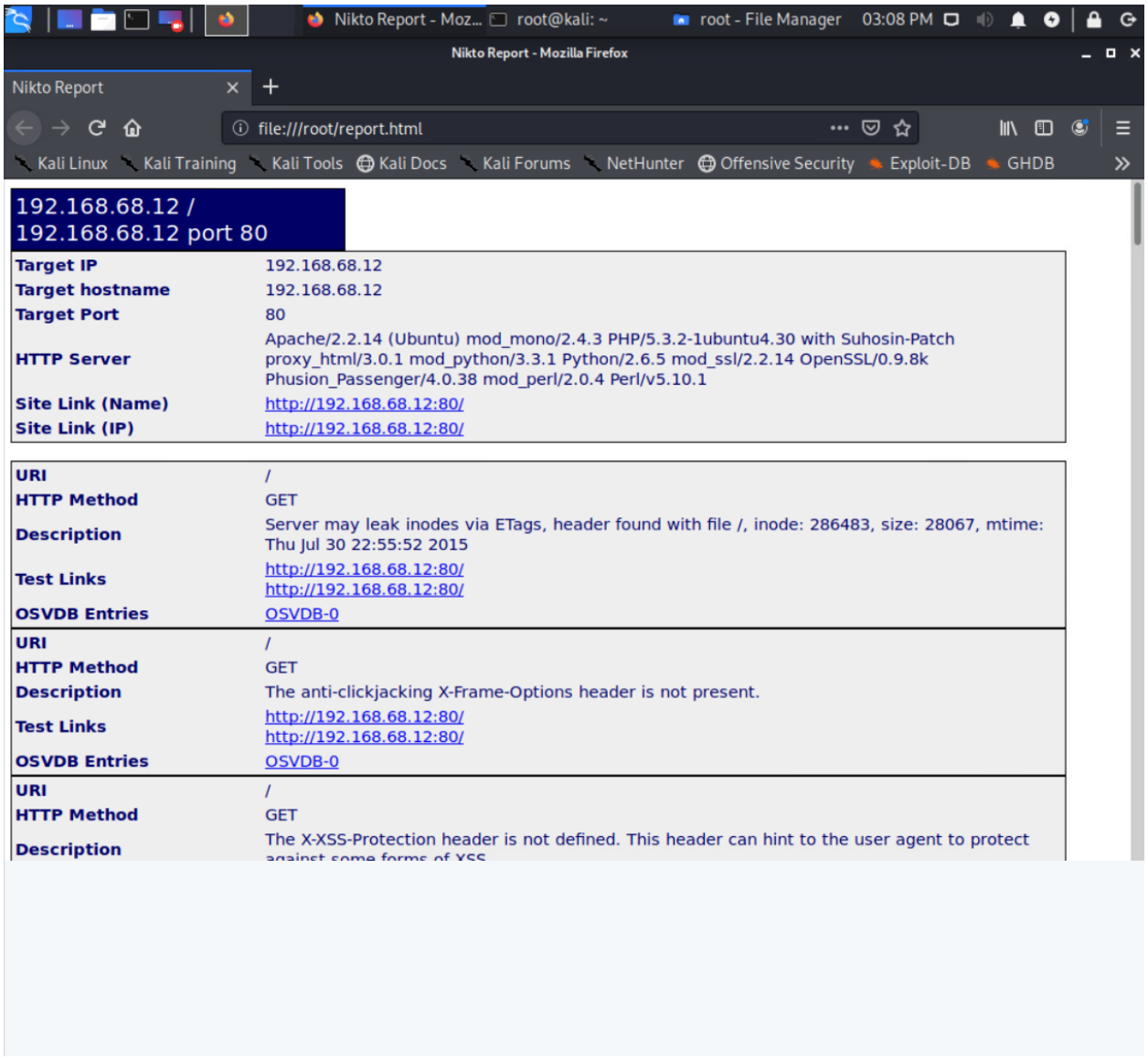
```
Plugin: clientaccesspolicy
 clientaccesspolicy.xml - Checks whether a client access file exists, and if it contains a wi
ldcard entry.
 Written by Sullo, Dirk, Copyright (C) 2012 Chris Sullo and Dr. Wetter IT-Consulting

Plugin: content_search
 Content Search - Search resultant content for interesting strings
 Written by Sullo, Copyright (C) 2010 Chris Sullo

Plugin: cookies
 HTTP Cookie Internal IP - Looks for internal IP addresses in cookies returned from an HTTP r
equest.
 Written by Sullo, Copyright (C) 2010 Chris Sullo

Defined plugin macros:
 @@DEFAULT = "@@ALL;-@@EXTRAS;tests(report:500)"
  (expanded) = "report_nbe;fileops;robots;strutshock;dishwasher;ms10_070;msgs;paths;dir_trave
rsal;report_text;report_csv;put_del_test;clientaccesspolicy;sitefiles;report_html;headers;ssl
;domino;parked;favicon;outdated;report_json;drupal;negotiate;auth;cookies;httpoptions;apacheu
sers;multiple_index;cgi;docker_registry;origin_reflection;report_sqlg;shellshock;apache_expec
t_xss;content_search;report_xml;tests(report:500)"
 @@EXTRAS = "dictionary;siebel;embedded"
 @@ALL = "origin_reflection;robots;negotiate;dir_traversal;auth;multiple_index;siebel;report_
text;put_del_test;dishwasher;report_nbe;httpoptions;report_csv;paths;domino;report_sqlg;shell
shock;report_html;fileops;favicon;docker_registry;ssl;report_json;msgs;apacheusers;sitefiles;
ms10_070;tests;dictionary;outdated;strutshock;headers;apache_expect_xss;embedded;drupal;repor
t_xml;parked;cgi;clientaccesspolicy;content_search;cookies"
 @@NONE = ""
root@kali:~#
```

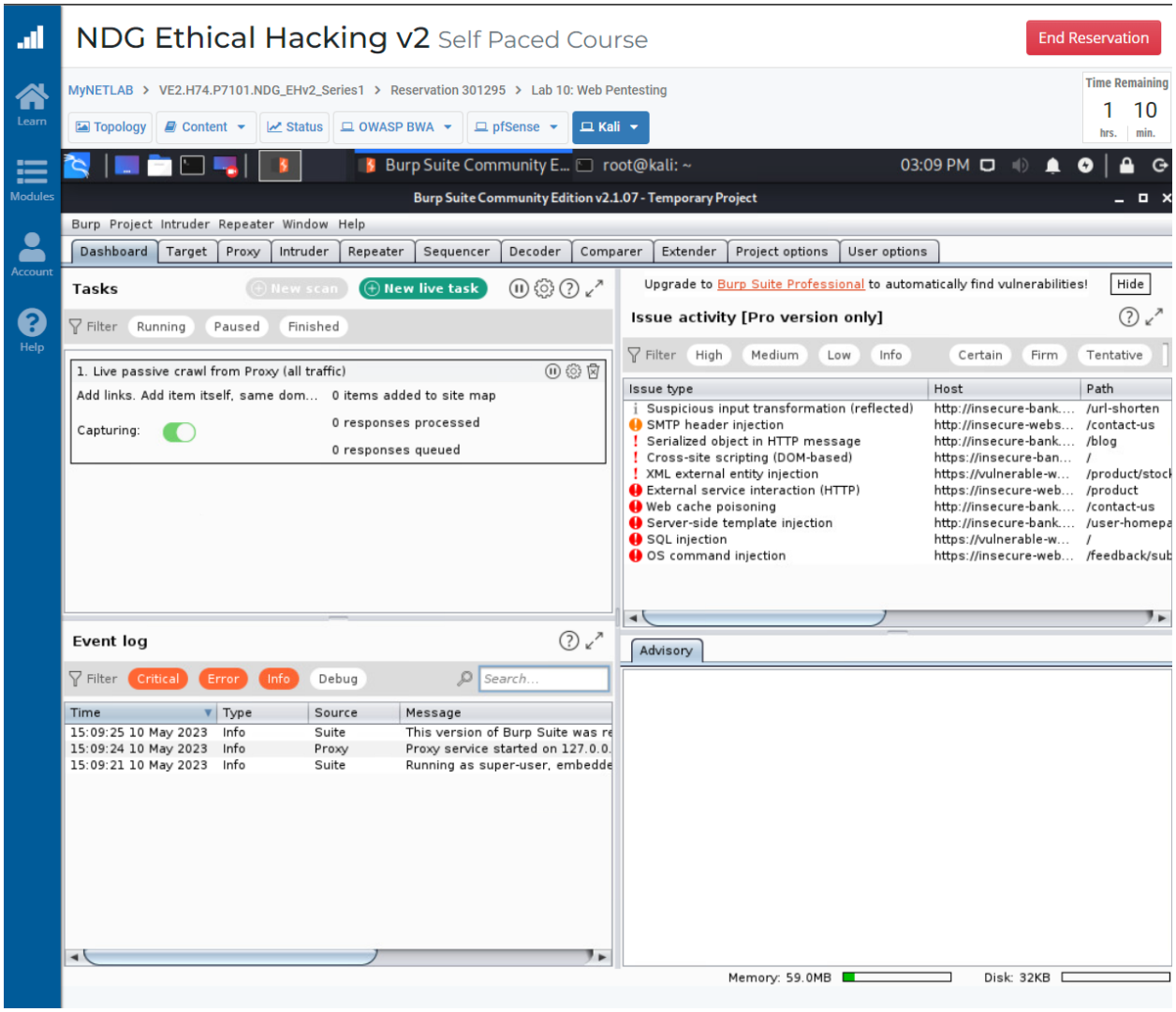


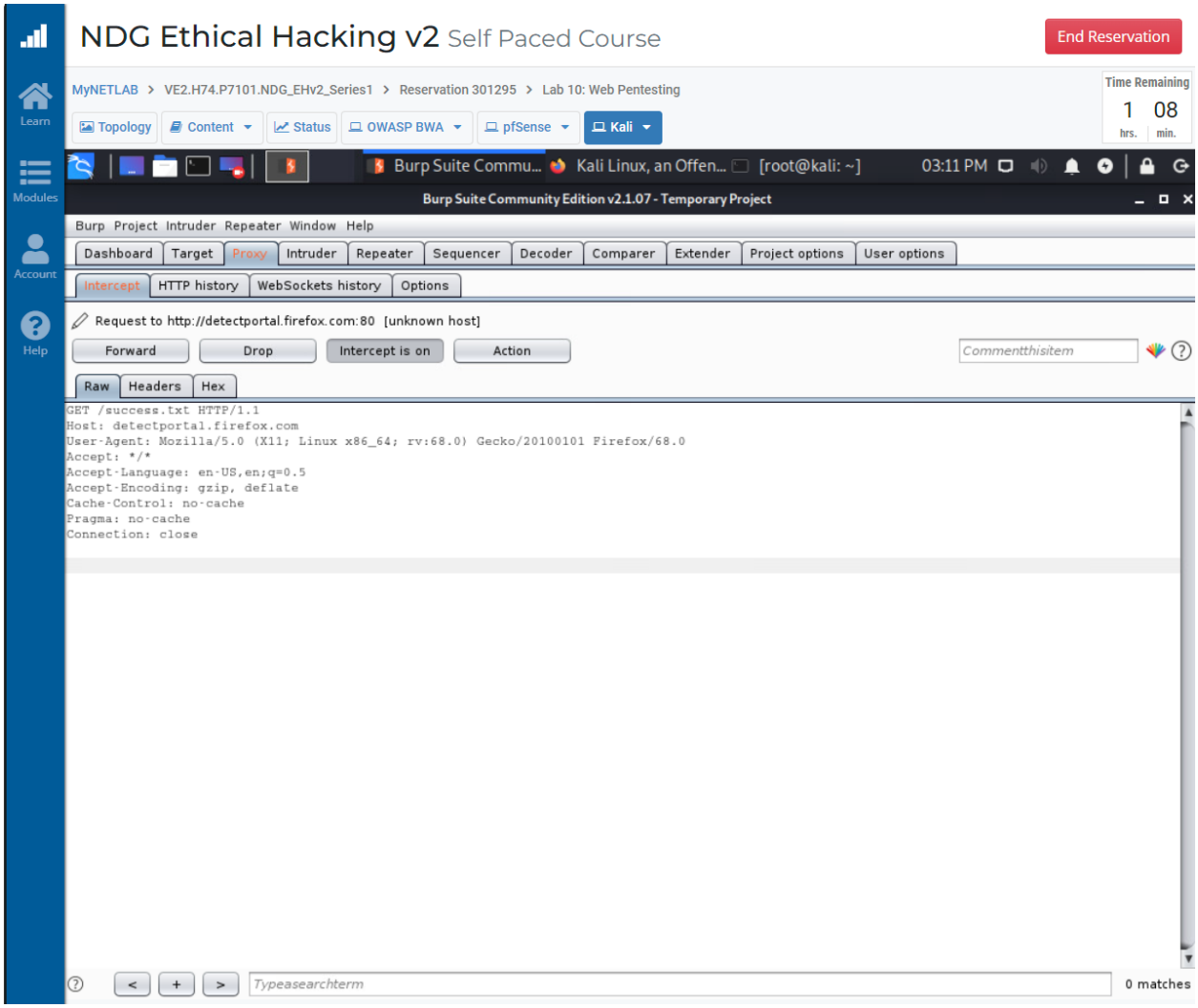

```
+ 1 host(s) tested
root@kali:~# nikto -Plugins -httpoptions -host 192.168.68.12
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.68.12
+ Target Hostname:    192.168.68.12
+ Target Port:        80
+ Start Time:         2023-05-10 15:05:09 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ 232 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2023-05-10 15:05:10 (GMT-4) (1 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

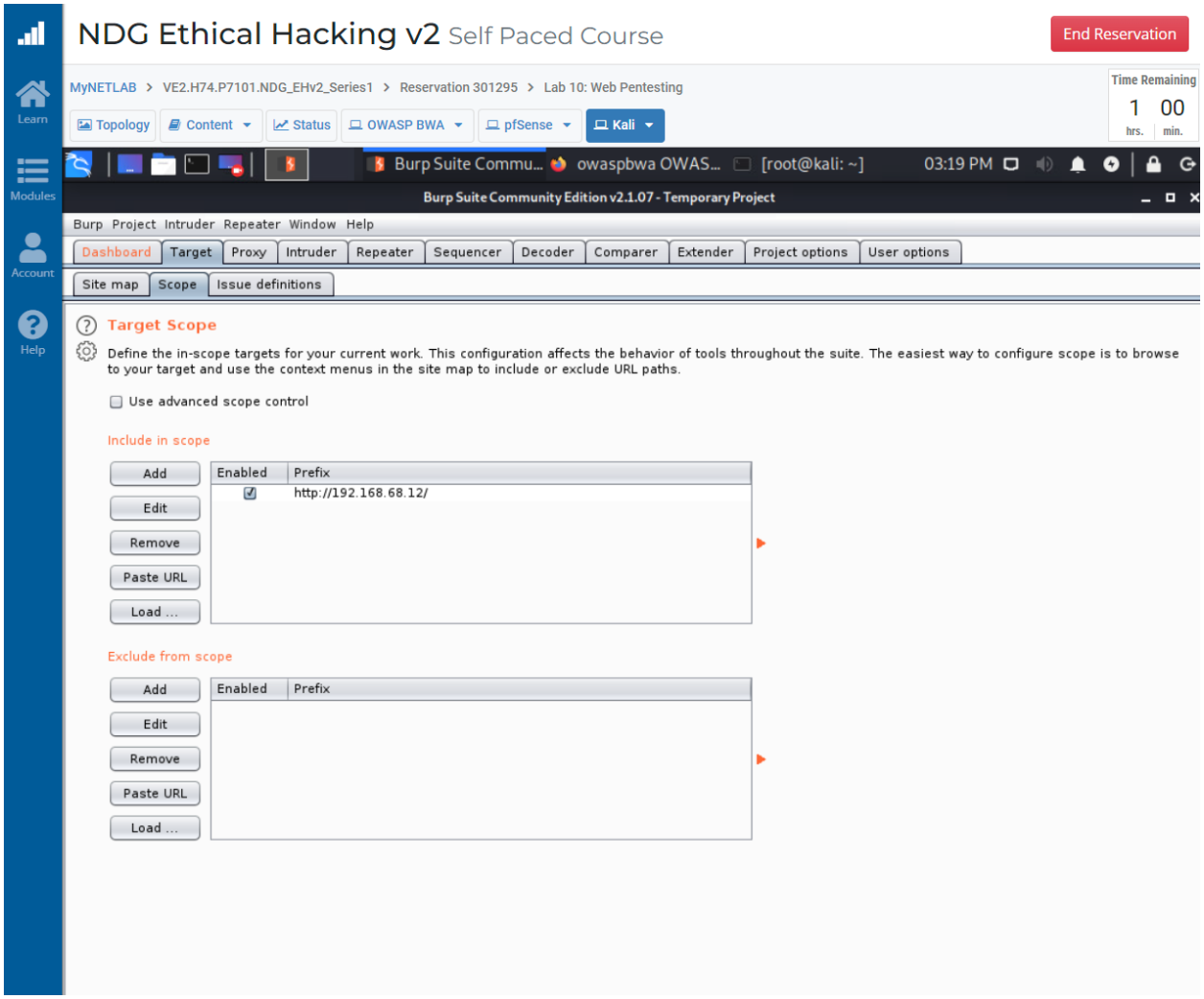
```
root@kali:~# nikto -Plugins msgs -host 192.168.68.12
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.68.12
+ Target Hostname:    192.168.68.12
+ Target Port:        80
+ Start Time:         2023-05-10 15:05:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch prox
y_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.
0.38 mod_perl/2.0.4 Perl/v5.10.1
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ss
l 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ 232 requests: 0 error(s) and 1 item(s) reported on remote host
+ End Time:           2023-05-10 15:05:29 (GMT-4) (0 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

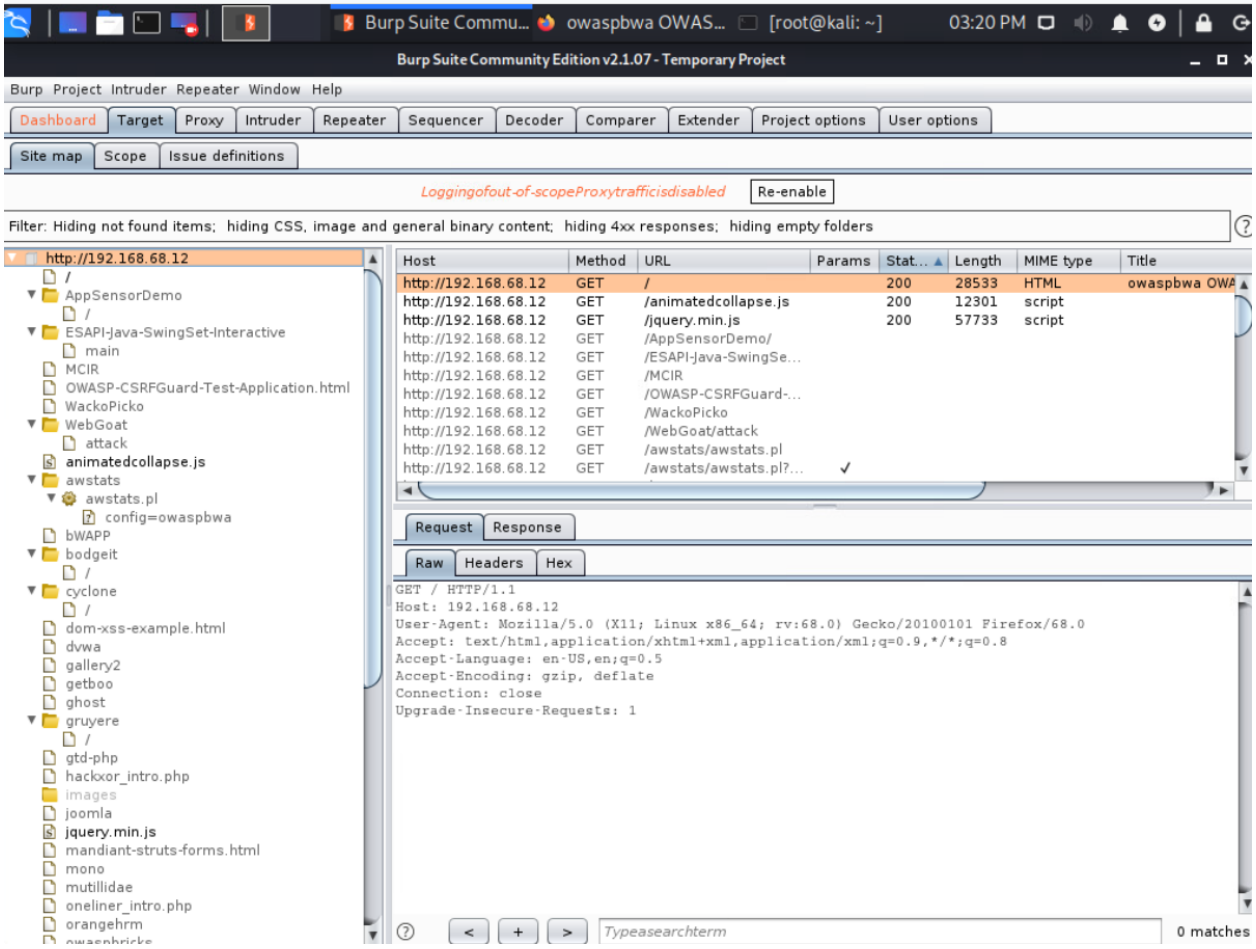
```
root@kali:~# nikto -Plugins tests -host 192.168.68.12
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.68.12
+ Target Hostname:    192.168.68.12
+ Target Port:        80
+ Start Time:         2023-05-10 15:06:02 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch prox
y_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.
0.38 mod_perl/2.0.4 Perl/v5.10.1
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected o
r limited to authorized hosts.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protec
ted or limited to authorized hosts.
+ 24629 requests: 1 error(s) and 8 item(s) reported on remote host
+ End Time:           2023-05-10 15:06:55 (GMT-4) (53 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

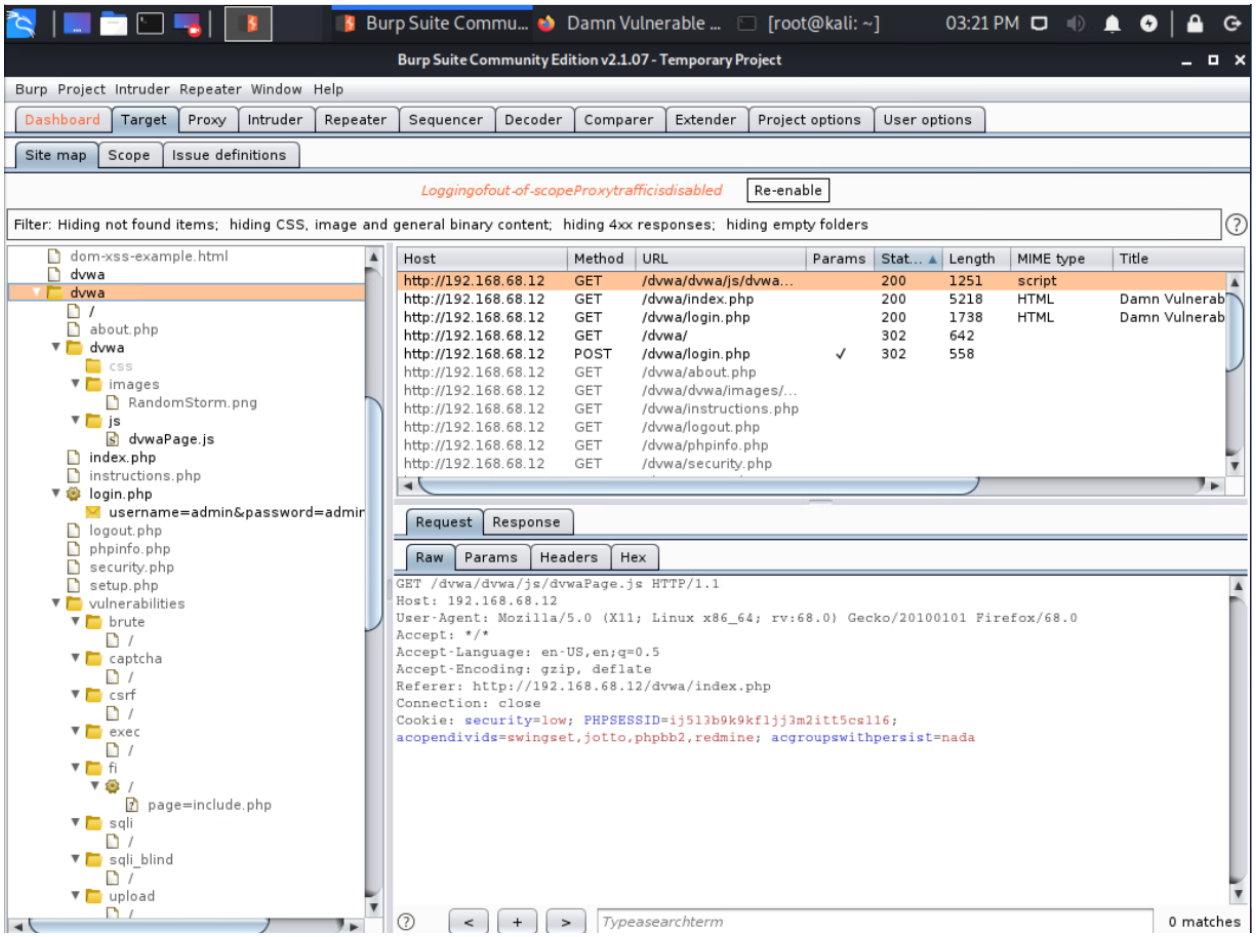

Nikto Report - Moz...
root@kali: ~
root - File Manager
03:08 PM
Nikto Report - Mozilla Firefox
Nikto Report
file:///root/report.html
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
192.168.68.12 /
192.168.68.12 port 80
Target IP 192.168.68.12
Target hostname 192.168.68.12
Target Port 80
HTTP Server Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Site Link (Name) http://192.168.68.12:80/
Site Link (IP) http://192.168.68.12:80/
URI /
HTTP Method GET
Description Server may leak inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: Thu Jul 30 22:55:52 2015
Test Links http://192.168.68.12:80/ http://192.168.68.12:80/
OSVDB Entries OSVDB-0
URI /
HTTP Method GET
Description The anti-clickjacking X-Frame-Options header is not present.
Test Links http://192.168.68.12:80/ http://192.168.68.12:80/
OSVDB Entries OSVDB-0
URI /
HTTP Method GET
Description The X-XSS-Protection header is not defined. This header can hint to the user agent to protect

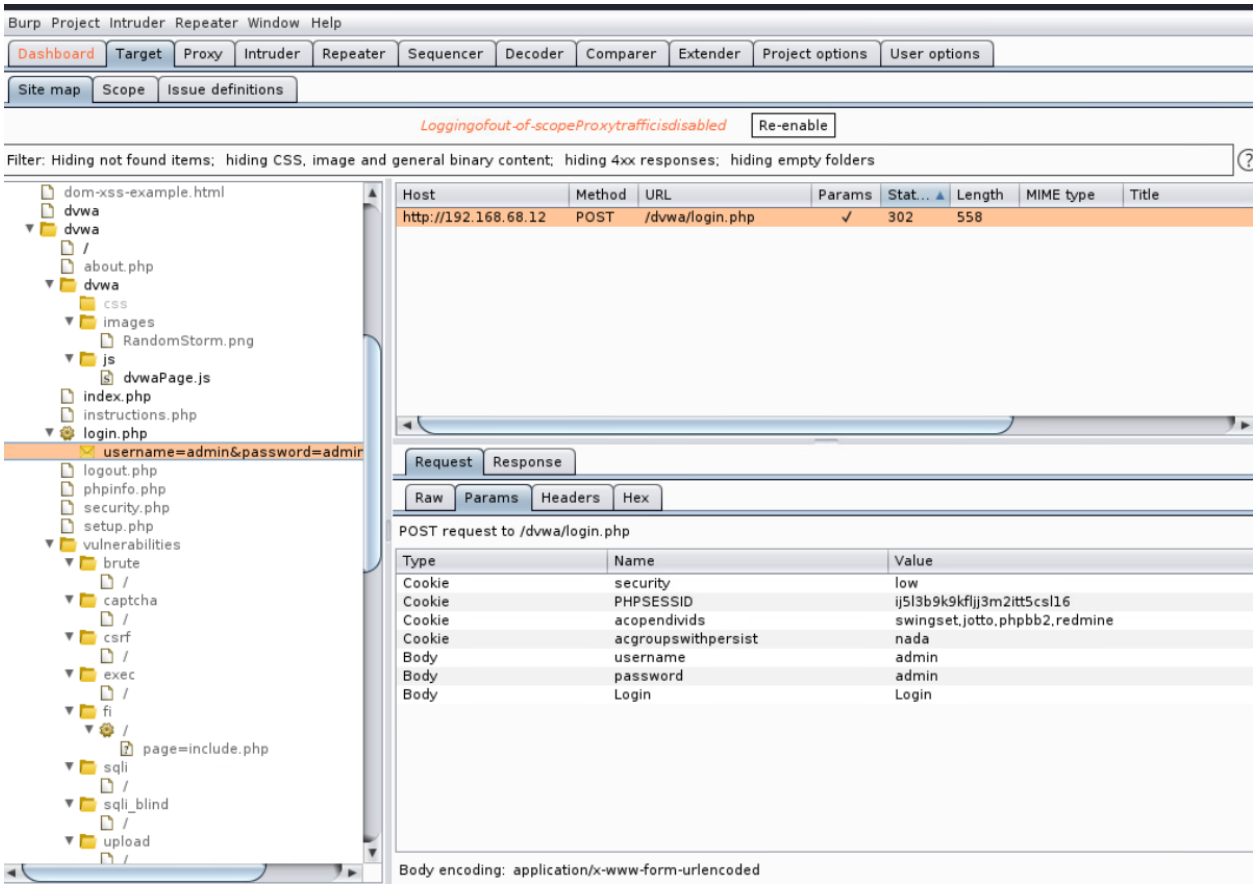

NDG Ethical Hacking v2 Self Paced Course
End Reservation
MyNETLAB > VE2.H74.P7101.NDG_EHv2_Series1 > Reservation 301295 > Lab 10: Web Pentesting
Time Remaining
1 hrs. 10 min.
Topology
Content
Status
OWASP BWA
pfSense
Kali
Learn
Modules
Account
Help
Burp Suite Community E...
root@kali: ~
03:09 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Tasks
New scan
New live task
Filter
Running
Paused
Finished
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same dom...
0 items added to site map
Capturing:
0 responses processed
0 responses queued
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Hide
Issue activity [Pro version only]
Filter
High
Medium
Low
Info
Certain
Firm
Tentative
Issue type
Host
Path
Suspicious input transformation (reflected)
http://insecure-bank...
/url-shorten
SMTP header injection
http://insecure-webs...
/contact-us
Serialized object in HTTP message
http://insecure-bank...
/blog
Cross-site scripting (DOM-based)
https://insecure-ban...
/
XML external entity injection
https://vulnerable-w...
/product/stock
External service interaction (HTTP)
https://insecure-web...
/product
Web cache poisoning
http://insecure-bank...
/contact-us
Server-side template injection
http://insecure-bank...
/user-homepa
SQL injection
https://vulnerable-w...
/
OS command injection
https://insecure-web...
/feedback/sub
Event log
Filter
Critical
Error
Info
Debug
Search...
Time
Type
Source
Message
15:09:25 10 May 2023
Info
Suite
This version of Burp Suite was re
15:09:24 10 May 2023
Info
Proxy
Proxy service started on 127.0.0.
15:09:21 10 May 2023
Info
Suite
Running as super-user, embedde
Advisory
Memory: 59.0MB
Disk: 32KB

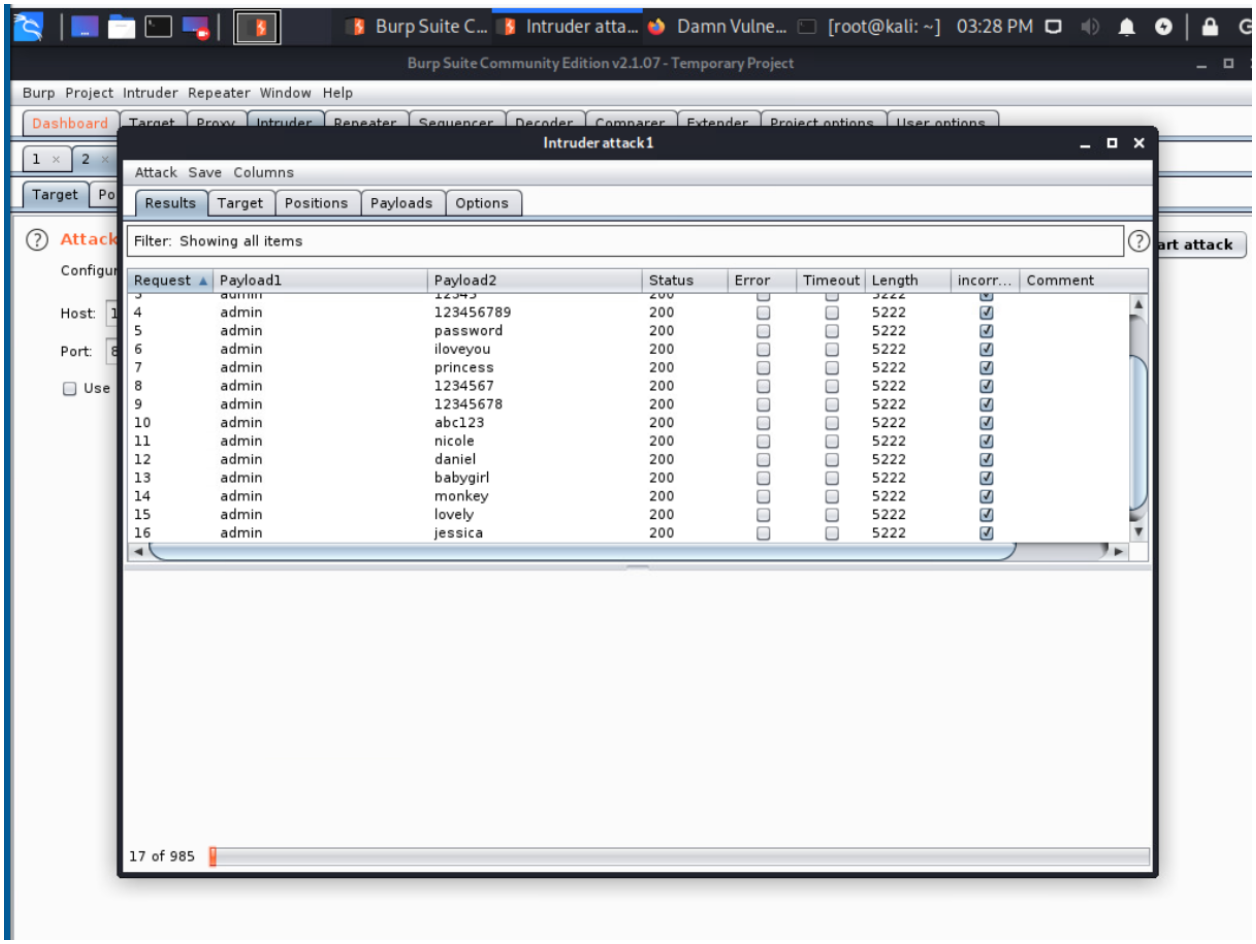

NDG Ethical Hacking v2 Self Paced Course
End Reservation
MyNETLAB > VE2.H74.P7101.NDG_EHv2_Series1 > Reservation 301295 > Lab 10: Web Pentesting
Time Remaining
1 hrs. 08 min.
Topology
Content
Status
OWASP BWA
pfSense
Kali
Learn
Modules
Account
Help
Burp Suite Commu...
Kali Linux, an Offen...
[root@kali: ~]
03:11 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://detectportal.firefox.com:80 [unknown host]
Forward
Drop
Intercept is on
Action
Commentthisitem
Raw Headers Hex
GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Typeasearchterm
0 matches


NDG Ethical Hacking v2 Self Paced Course
End Reservation
MyNETLAB > VE2.H74.P7101.NDG_EHv2_Series1 > Reservation 301295 > Lab 10: Web Pentesting
Time Remaining
1 00
hrs. min.
Topology
Content
Status
OWASP BWA
pfSense
Kali
Learn
Modules
Account
Help
Burp Suite Commu...
owaspbwa OWAS...
[root@kali: ~]
03:19 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Site map
Scope
Issue definitions
Target Scope
Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.
Use advanced scope control
Include in scope
Add
Edit
Remove
Paste URL
Load ...
Enabled
Prefix
http://192.168.68.12/
Exclude from scope
Add
Edit
Remove
Paste URL
Load ...
Enabled
Prefix


Burp Suite Commu...
owaspbwa OWAS...
[root@kali: ~]
03:20 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Site map Scope Issue definitions
Loggingofout-of-scopeProxytrafficisdisabled
Re-enable
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://192.168.68.12
/
AppSensorDemo
/
ESAPI-Java-SwingSet-Interactive
main
MCIR
OWASP-CSRFGuard-Test-Application.html
WackoPicko
WebGoat
attack
animatedcollapse.js
awstats
awstats.pl
config=owaspbwa
bWAPP
bodgeit
/
cyclone
/
dom-xss-example.html
dvwa
gallery2
getboo
ghost
gruyere
/
gtd-php
hackxor_intro.php
images
joomla
jquery.min.js
mandiant-struts-forms.html
mono
mutillidae
oneliner_intro.php
orangehrm
Host Method URL Params Stat... Length MIME type Title
http://192.168.68.12 GET / 200 28533 HTML owaspbwa OWA
http://192.168.68.12 GET /animatedcollapse.js 200 12301 script
http://192.168.68.12 GET /jquery.min.js 200 57733 script
http://192.168.68.12 GET /AppSensorDemo/
http://192.168.68.12 GET /ESAPI-Java-SwingSe...
http://192.168.68.12 GET /MCIR
http://192.168.68.12 GET /OWASP-CSRFGuard-...
http://192.168.68.12 GET /WackoPicko
http://192.168.68.12 GET /WebGoat/attack
http://192.168.68.12 GET /awstats/awstats.pl
http://192.168.68.12 GET /awstats/awstats.pl?... ✓
Request Response
Raw Headers Hex
GET / HTTP/1.1
Host: 192.168.68.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Typeasearchterm
0 matches


Burp Suite Commu...
Damn Vulnerable ...
[root@kali: ~]
03:21 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Site map Scope Issue definitions
Loggingofout-of-scopeProxytrafficisdisabled
Re-enable
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
dom-xss-example.html
dvwa
dvwa
/
about.php
dvwa
css
images
RandomStorm.png
js
dvwaPage.js
index.php
instructions.php
login.php
username=admin&password=admin
logout.php
phpinfo.php
security.php
setup.php
vulnerabilities
brute
captcha
csrf
exec
fi
page=include.php
sqli
sqli_blind
upload
Host Method URL Params Stat... Length MIME type Title
http://192.168.68.12 GET /dvwa/dvwa/js/dvwa... 200 1251 script
http://192.168.68.12 GET /dvwa/index.php 200 5218 HTML Damn Vulnerab
http://192.168.68.12 GET /dvwa/login.php 200 1738 HTML Damn Vulnerab
http://192.168.68.12 GET /dvwa/ 302 642
http://192.168.68.12 POST /dvwa/login.php ✓ 302 558
http://192.168.68.12 GET /dvwa/about.php
http://192.168.68.12 GET /dvwa/dvwa/images/...
http://192.168.68.12 GET /dvwa/instructions.php
http://192.168.68.12 GET /dvwa/logout.php
http://192.168.68.12 GET /dvwa/phpinfo.php
http://192.168.68.12 GET /dvwa/security.php
Request Response
Raw Params Headers Hex
GET /dvwa/dvwa/js/dvwaPage.js HTTP/1.1
Host: 192.168.68.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.68.12/dvwa/index.php
Connection: close
Cookie: security=low; PHPSESSID=ij513b9k9kf1jj3m2itt5csl16;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
< + >
Typeasearchterm
0 matches


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Site map Scope Issue definitions
Loggingofout-of-scopeProxytrafficisdisabled
Re-enable
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
dom-xss-example.html
dvwa
dvwa
/
about.php
dvwa
css
images
RandomStorm.png
js
dvwaPage.js
index.php
instructions.php
login.php
username=admin&password=admin
logout.php
phpinfo.php
security.php
setup.php
vulnerabilities
brute
/
captcha
/
csrf
/
exec
/
fi
/
page=include.php
sqli
/
sqli_blind
/
upload
/
Host Method URL Params Stat... Length MIME type Title
http://192.168.68.12 POST /dvwa/login.php ✓ 302 558
Request Response
Raw Params Headers Hex
POST request to /dvwa/login.php
Type Name Value
Cookie security low
Cookie PHPSESSID ij5l3b9k9kfljj3m2itt5csl16
Cookie acopendivids swingset,jotto,phpbb2,redmine
Cookie acgroupswithpersist nada
Body username admin
Body password admin
Body Login Login
Body encoding: application/x-www-form-urlencoded


Burp Suite C...
Intruder atta...
Damn Vulne...
[root@kali: ~]
03:28 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intruder attack 1
Attack Save Columns
Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload1
Payload2
Status
Error
Timeout
Length
incorr...
Comment
4 admin 123456789 200 5222
5 admin password 200 5222
6 admin iloveyou 200 5222
7 admin princess 200 5222
8 admin 1234567 200 5222
9 admin 12345678 200 5222
10 admin abc123 200 5222
11 admin nicole 200 5222
12 admin daniel 200 5222
13 admin babygirl 200 5222
14 admin monkey 200 5222
15 admin lovely 200 5222
16 admin jessica 200 5222
17 of 985