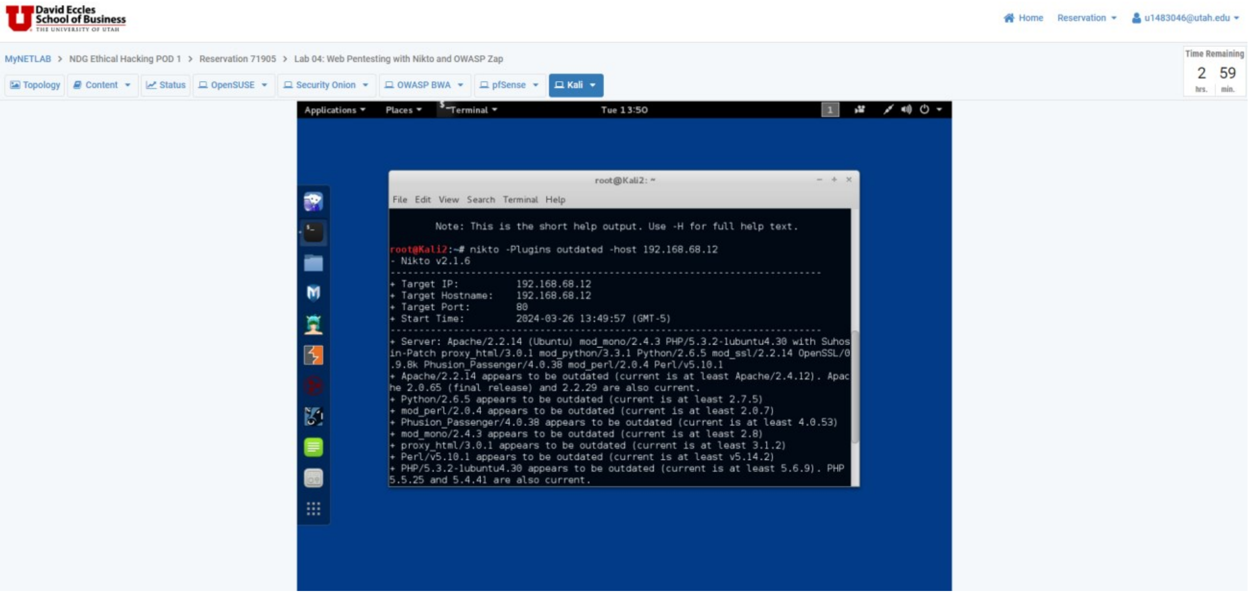
Vu Nguyen

UID: u1483046

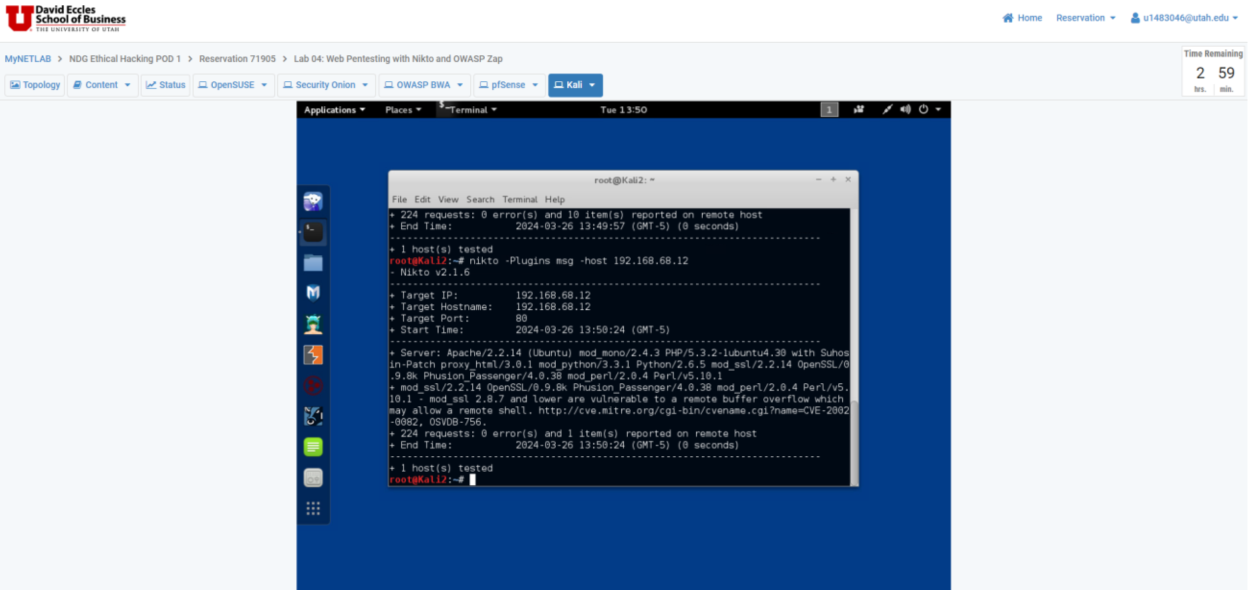
Assignment 16 - Web App Pen Testing (Lab and Quiz)

1. Section 1, Step 9


David Eccles School of Business
Home
Reservation
u1483046@utah.edu
MyNETLAB > NDG Ethical Hacking POD 1 > Reservation 71905 > Lab 04: Web Pentesting with Nikto and OWASP Zap
Time Remaining 2 hrs. 59 min.
Topology
Content
Status
OpenSUSE
Security Onion
OWASP BWA
pfSense
Kali
Applications
Places
Terminal
Tue 13:50
root@Kali2: ~
File Edit View Search Terminal Help

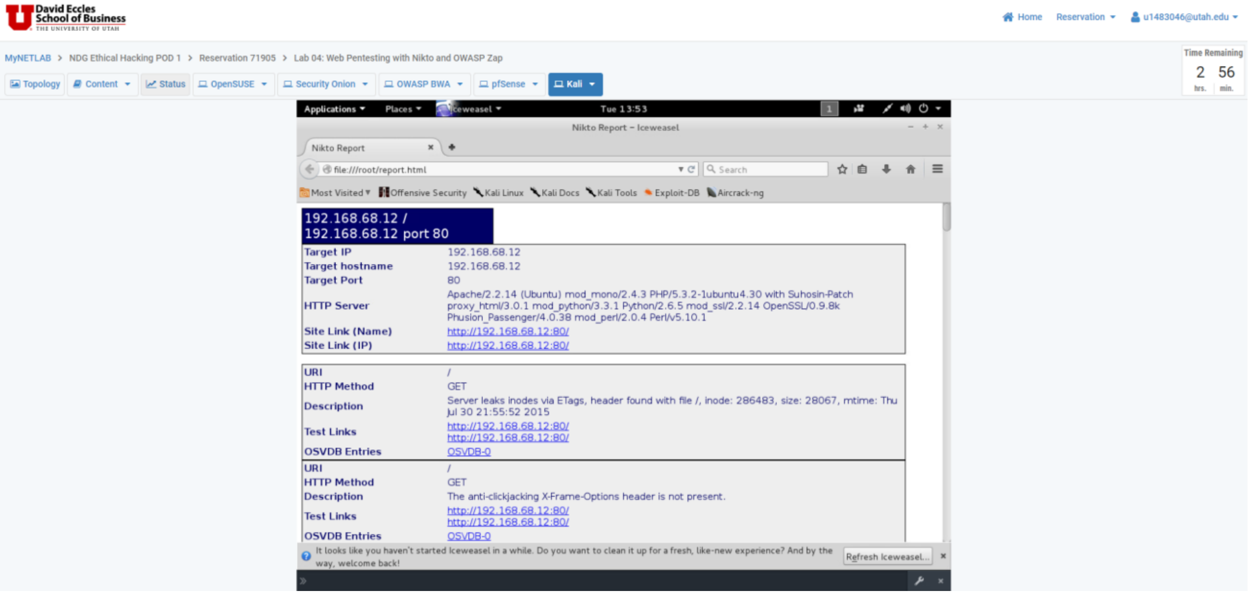
```
        Note: This is the short help output. Use -H for full help text.

root@Kali2:~# nikto -Plugins outdated -host 192.168.68.12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:         2024-03-26 13:49:57 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhos
in-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
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.12). Apac
he 2.0.65 (final release) and 2.2.29 are also current.
+ Python/2.6.5 appears to be outdated (current is at least 2.7.5)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.7)
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 5.6.9). PHP
5.5.25 and 5.4.41 are also current.
```

2. Section 1, Step 11


David Eccles School of Business
Home
Reservation
u1483046@utah.edu
MyNETLAB > NDG Ethical Hacking POD 1 > Reservation 71905 > Lab 04: Web Pentesting with Nikto and OWASP Zap
Time Remaining 2 hrs. 59 min.
Topology
Content
Status
OpenSUSE
Security Onion
OWASP BWA
pfSense
Kali
Applications
Places
Terminal
Tue 13:50
root@Kali2: ~
File Edit View Search Terminal Help

```
+ 224 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2024-03-26 13:49:57 (GMT-5) (0 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@Kali2:~# nikto -Plugins msg -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:         2024-03-26 13:50:24 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhos
in-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
+ 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 2.8.7 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.
+ 224 requests: 0 error(s) and 1 item(s) reported on remote host
+ End Time:           2024-03-26 13:50:24 (GMT-5) (0 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@Kali2:~#
```

3. Section 1, Step 16



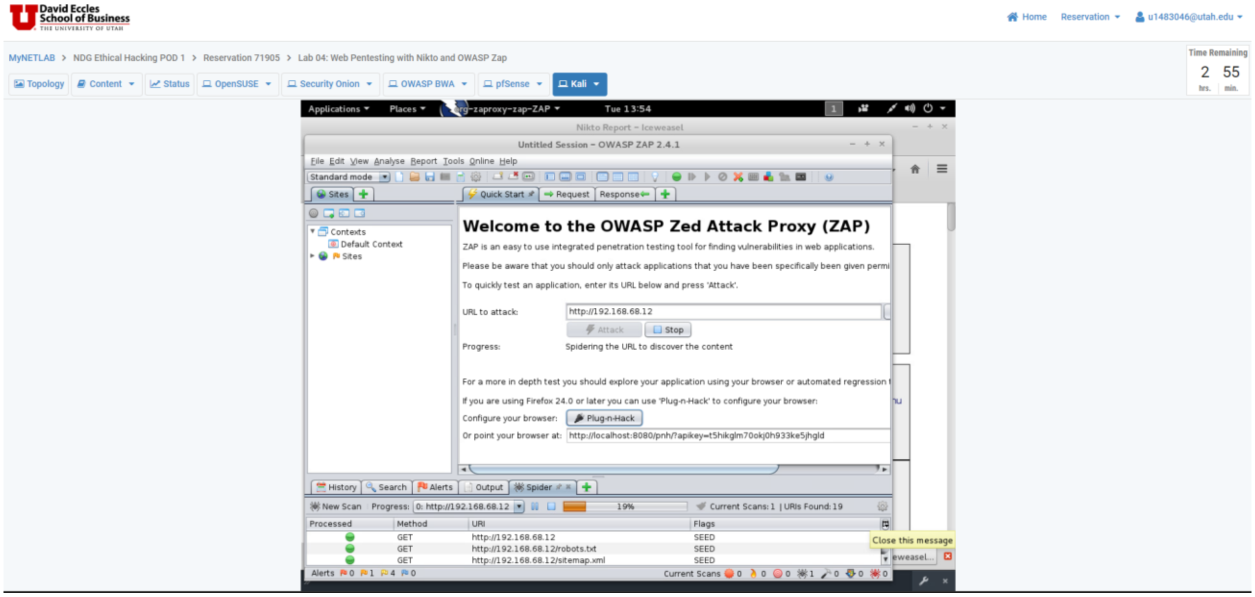
192.168.68.12 /
192.168.68.12 port 80

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 leaks inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: Thu Jul 30 21:55:52 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

It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

4. Section 2, Step 3



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permi

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://192.168.68.12

Progress: Spidering the URL to discover the content

For a more in depth test you should explore your application using your browser or automated regression t

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser:

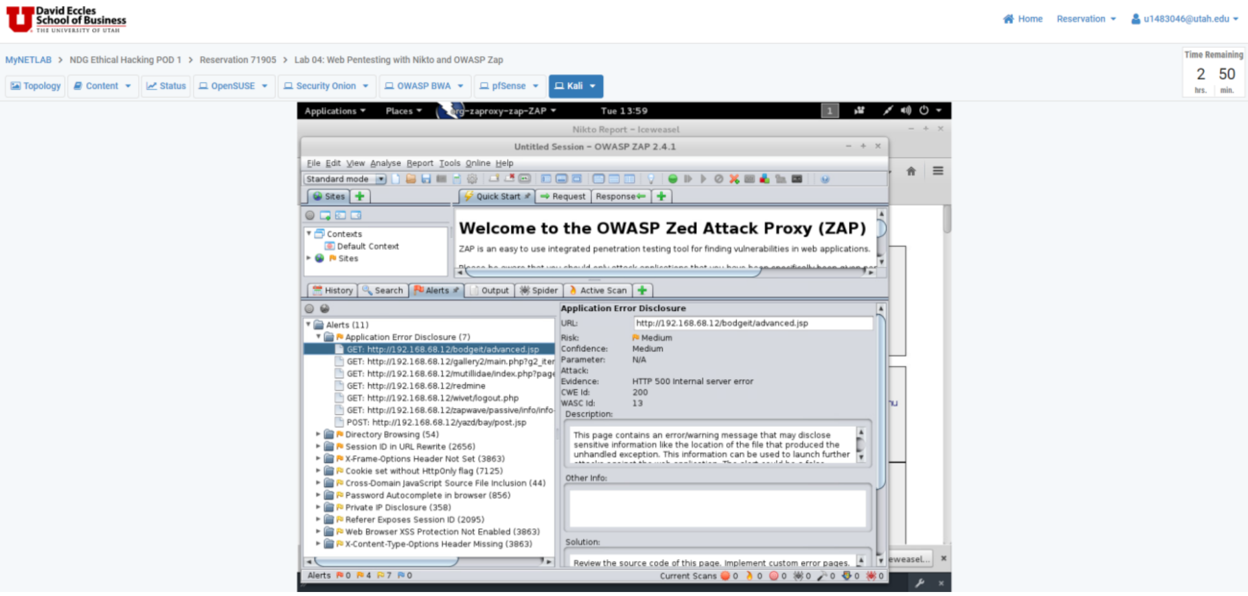
Or point your browser at: http://localhost:8080/pnh/?apikey=t5hikglm70okj0h933ke5jhgld

Progress: 0: http://192.168.68.12 19% Current Scans: 1 | URIs Found: 19

Processed	Method	URI	Flags
●	GET	http://192.168.68.12	SEED
●	GET	http://192.168.68.12/robots.txt	SEED
●	GET	http://192.168.68.12/sitemap.xml	SEED

Alerts 0 1 4 0 Current Scans 0 0 0 1 0 0 0

5. Section 2, Step 5



Contexts
Default Context
Sites

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

```
Alerts (11)
  Application Error Disclosure (7)
    GET: http://192.168.68.12/bodgeit/advanced.jsp
    GET: http://192.168.68.12/gallery2/main.php?g2_iter
    GET: http://192.168.68.12/mutillidae/index.php?page
    GET: http://192.168.68.12/redmine
    GET: http://192.168.68.12/wivet/logout.php
    GET: http://192.168.68.12/zapwave/passive/info/info-
    POST: http://192.168.68.12/yazd/bay/post.jsp
  Directory Browsing (54)
  Session ID in URL Rewrite (2656)
  X-Frame-Options Header Not Set (3863)
  Cookie set without HttpOnly flag (7125)
  Cross-Domain JavaScript Source File Inclusion (44)
  Password Autocomplete in browser (856)
  Private IP Disclosure (358)
  Referer Exposes Session ID (2095)
  Web Browser XSS Protection Not Enabled (3863)
  X-Content-Type-Options Header Missing (3863)
```

Application Error Disclosure

URL: http://192.168.68.12/bodgeit/advanced.jsp
Risk: Medium
Confidence: Medium
Parameter: N/A
Attack:
Evidence: HTTP 500 Internal server error
CWE Id: 200
WASC Id: 13

Description:

This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further

Other Info:

Solution:

Review the source code of this page. Implement custom error pages.

Alerts 0 4 7 0   Current Scans 0 0 0 0 0 0 0