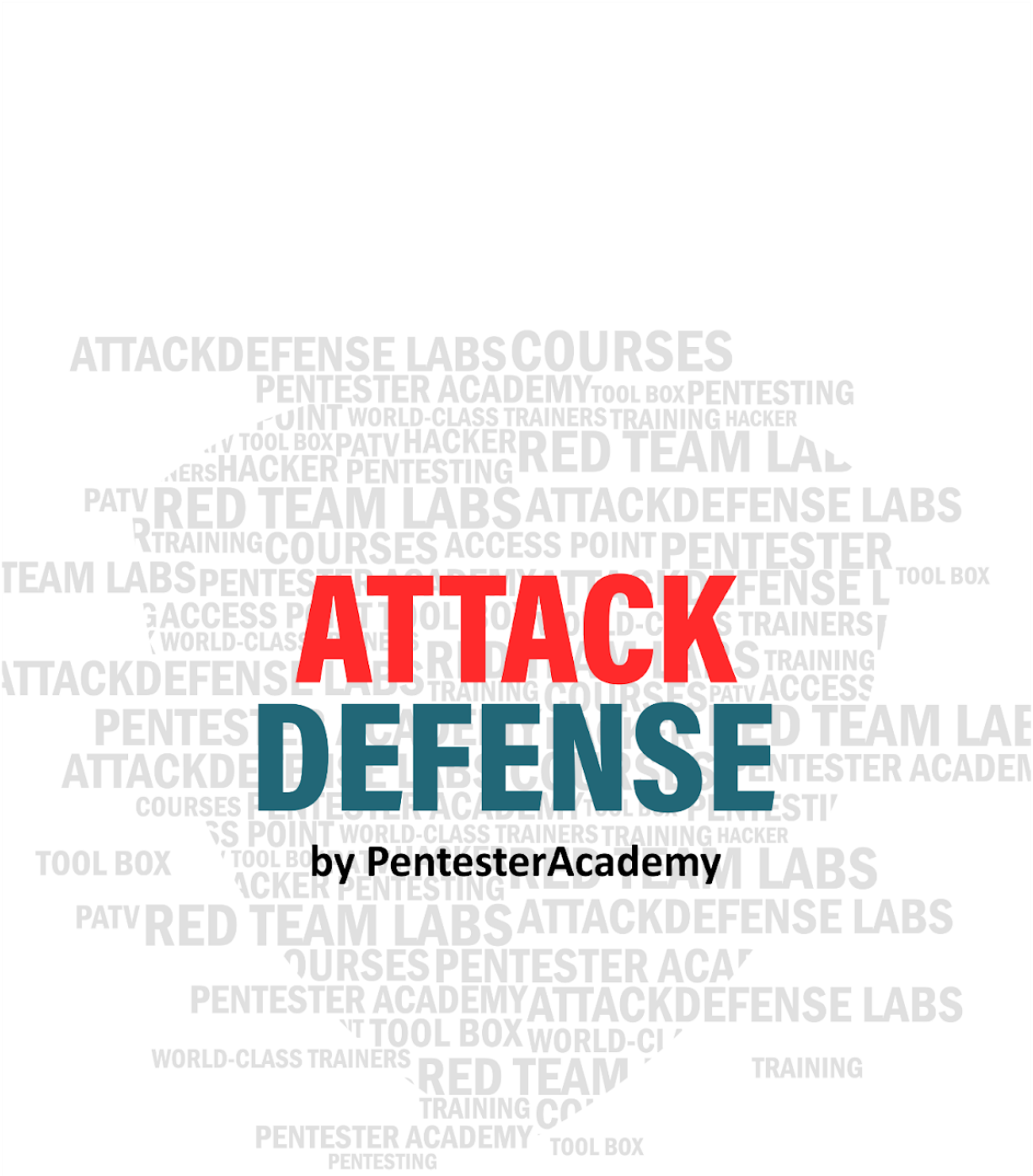

ATTACK
DEFENSE
by PentesterAcademy

Name	Nikto: Automatic WebApp Scanning
URL	https://www.attackdefense.com/challengedetails?cid=2057
Type	DevSecOps Basics: Dynamic Code Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Challenge Description

Nikto is an open-source web scanner that performs automated tests on the web applications.

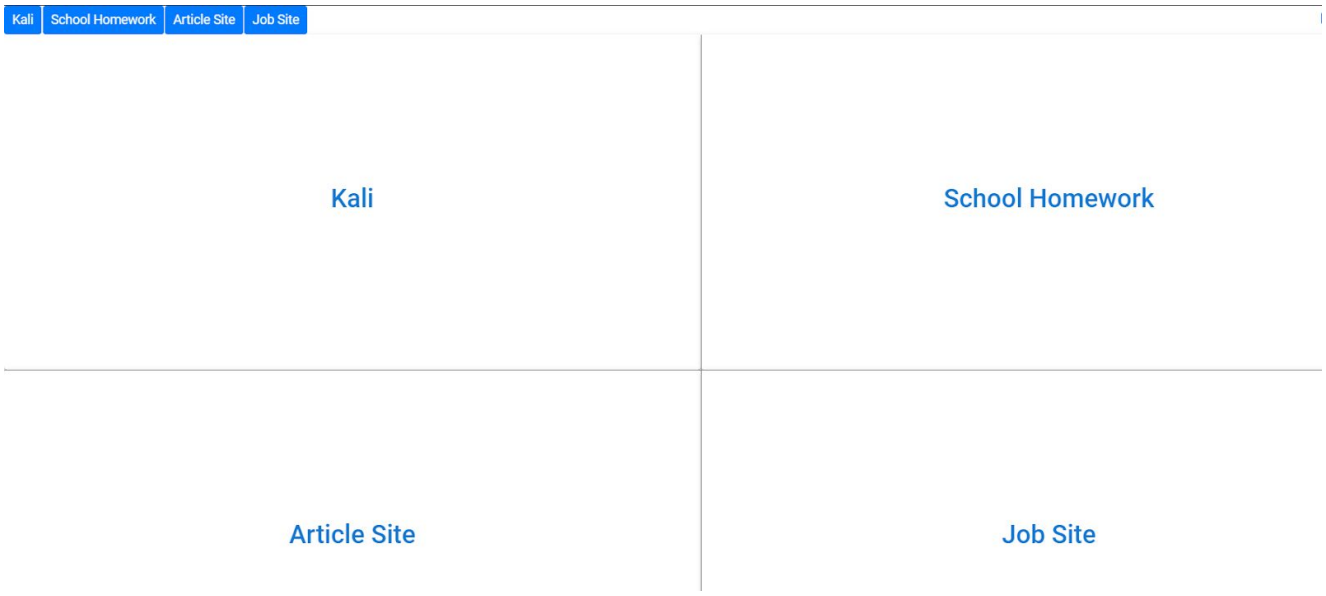
A Kali GUI machine (kali-gui) is provided to the user with Nikto installed on it.Three examples of vulnerable web portals are also provided. The details of these portals:

Web Portal	Web Portal URL
School Homework Web Portal	school-homework
Article Web Portal	article-site
Job Advertisement Web Portal	job-site

Objective: Identify the vulnerabilities in web applications using Nikto!

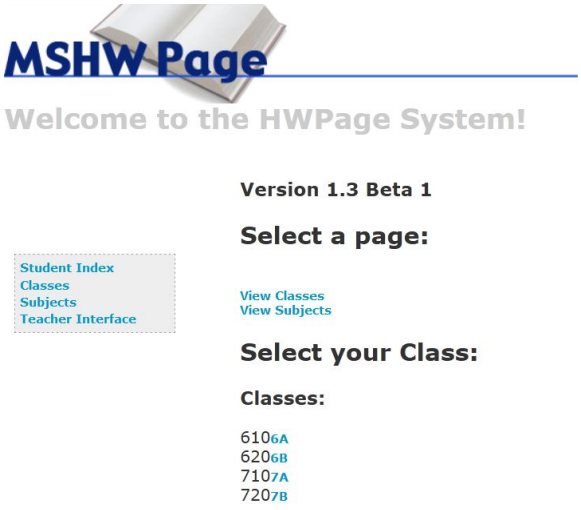
Lab Setup

On starting the lab, the following interface will be accessible to the user.

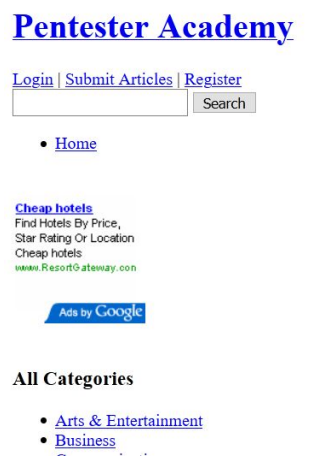


On choosing (clicking the text in the center) top left panel, The **Kali GUI** will open in a new tab

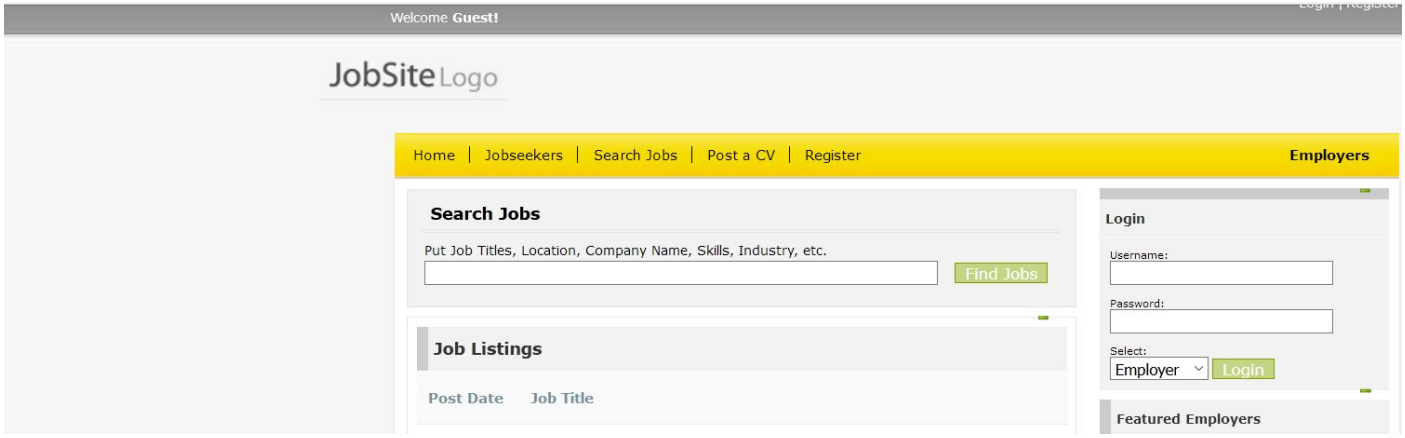
Similarly on selecting the top right panel, a web UI of **School Homework UI** will open in a new tab.



On selecting the bottom left panel, a web UI of **Article Site UI** will open in a new tab.



And on selecting the bottom right panel, a web UI of **Job Site UI** will open in a new tab.



Solution

Step 1: Check the available options of the nikto tool.

Command: nikto --help

```
root@kali-gui:~# nikto --help
Unknown option: help

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
```

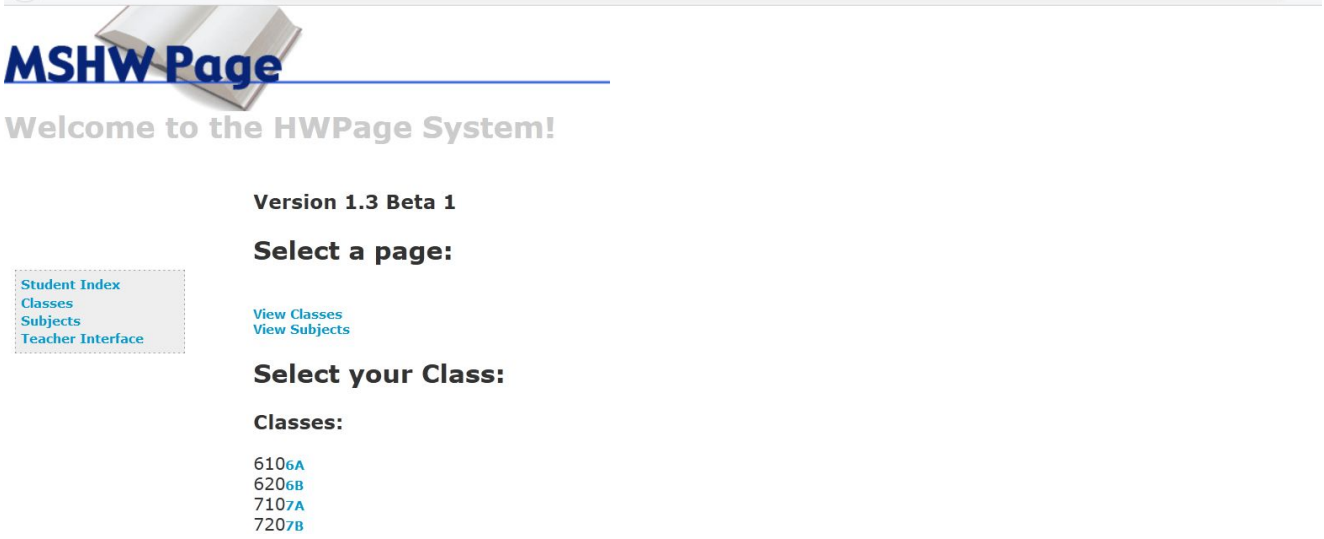
```
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
```

```
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

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

root@kali-gui:~#
```

We will take one example at a time and run the tool on that.

Example 1: Homework Site

Step 1: Open the web application from the interface



Step 2: Run the nikto scan on homework-site and find possible vulnerabilities in the target.

Command: nikto -h http://school-homework

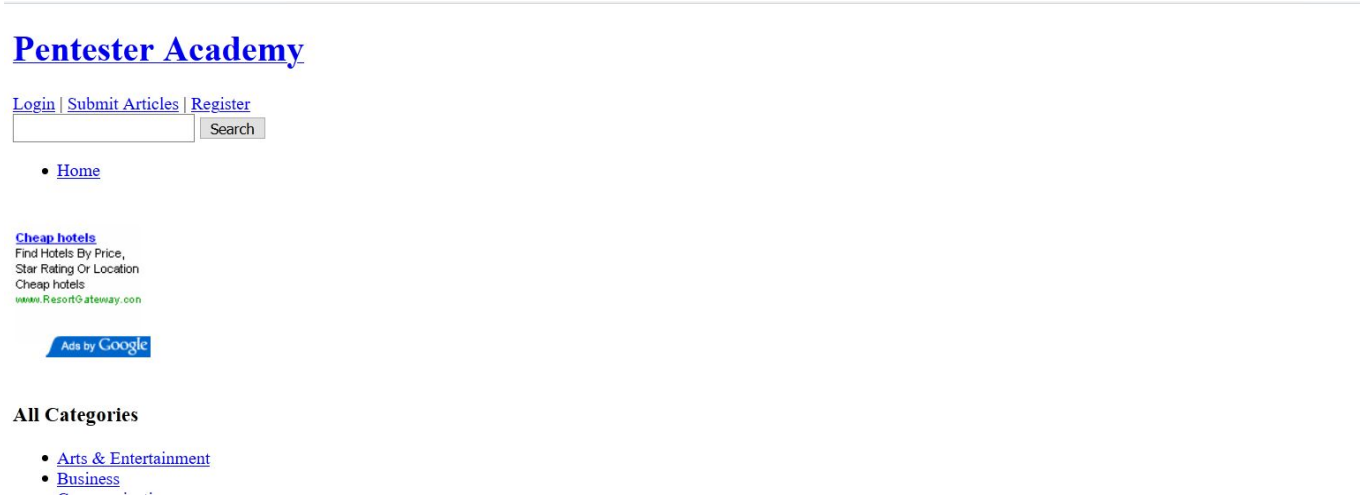
```
root@kali-gui:~# nikto -h http://school-homework
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.170.67.4
+ Target Hostname:    school-homework
+ Target Port:        80
+ Start Time:         2020-09-20 13:34:43 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26
+ 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 protect 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
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names
. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: in
dex.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via
 certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
 certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
 certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
 certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /down/: This might be interesting...
+ OSVDB-3092: /html/: This might be interesting...
+ OSVDB-3092: /info/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 1640424, size: 5108, mtime:
 Tue Aug 28 16:18:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8491 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2020-09-20 13:34:54 (GMT5.5) (11 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali-gui:~#
```

Issues Detected

- Outdated Apache Version
- Missing headers
- Sensitive Information via HTTP Requests

Example 2: Article Site

Step 1: Open the web application from the interface



Step 2: Run the nikto scan on article-site and find possible vulnerabilities in the target.

Command: nikto -h http://article-site

```
root@kali-gui:~# nikto -h http://article-site
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.170.67.5
+ Target Hostname:    article-site
+ Target Port:        80
+ Start Time:         2020-09-20 13:39:18 (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.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect 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
+ Cookie PHPSESSID created without the httponly flag
+ 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.
+ /phpinfo.php: Output from the phpinfo() function was found.
```

```
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin ac
counts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to v
erify.
+ OSVDB-3092: /install/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a
 lot of system information.
```

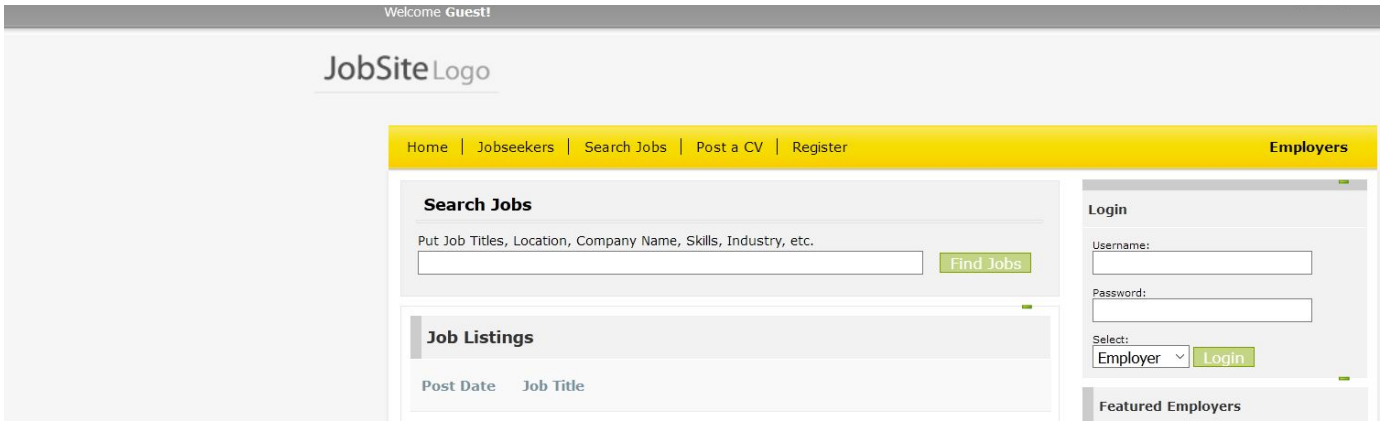
```
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /htaccess.txt: Default Joomla! htaccess.txt file found. This should be removed or renamed.
+ /admin/login.php: Admin login page/section found.
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /.git/config: Git config file found. Infos about repo details may be present.
+ 8491 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time:           2020-09-20 13:40:04 (GMT5.5) (46 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali-gui:~#
```

Issues Detected

- Cross-Site Scripting
- Sensitive Files found (phpinfo)
- Installation directory found

Example 3: Job Site

Step 1: Open the web application from the interface



Step 2: Run the nikto scan on job-site and find possible vulnerabilities in the target.

Command: nikto -h http://job-site

```
root@kali-gui:~# nikto -h http://job-site
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.170.67.6
+ Target Hostname:    job-site
+ Target Port:        80
+ Start Time:         2020-09-20 13:43:44 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26
+ 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 protect 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
+ Cookie PHPSESSID created without the httponly flag
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names
. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: in
dex.php
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the
 2.x branch.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
 certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
 certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /html/: This might be interesting...
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /job/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /register/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 1640424, size: 5108, mtime:
 Tue Aug 28 16:18:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 8491 requests: 0 error(s) and 23 item(s) reported on remote host
+ End Time:           2020-09-20 13:43:54 (GMT5.5) (10 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali-gui:~#
```

Issues Detected

- PHPSESSID created without the httponly flag
- Apache version outdated

Learnings

Perform Dynamic Code Analysis using Nikto tool.