Internship Studio

Ethical Hacking Internship

Name - Aryan Sharma

Task - 2

Create a Presentation using Powerpoints or Google Slides, The slide should contain a screenshot of Netsparker found vulnerabilities, screenshot should contain the report which Netsparker generated so that we can check the difference between the actual and your submitted report.

Alert - Since i am using MacBook Pro, i was not able to install Netsparker because it was not available on the internet for free, so i used online vulnerability tester Nikto.

Procedure -

1) Visit the site which has to be penetration test like in my case it was http://zero.webappsecurity.com/
2) Enter the domain in niko which has to been scanned for vulnerabilities.
3) Define customisations as per your need.
4) Nikto will start scanning automatically.
5) Critical Vulnerability found - **Out of date version (Tomcat).**

Screenshot - Screenshots of all the vulnerabilities found.

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          (proxied)
+ Target Hostname:    zero.webappsecurity.com
+ Target Port:        80
+ Proxy:              localhost:8118
+ Start Time:         2022-03-21 17:18:01 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ 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
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH (May be proxy's
methods, not server's)
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files
on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on
the web server.
+ HTTP method: 'PATCH' may allow client to issue patch commands to server. See RFC-5789.
+ Server banner has changed from 'Apache-Coyote/1.1' to 'Apache/2.2.6 (Win32) mod_ssl/2.2.6
OpenSSL/0.9.8e mod_jk/1.2.40' which may suggest a WAF, load balancer or proxy is in place
+ Server leaks inodes via ETags, header found with file /cgi-bin/post-query, fields: 0xW/46
0x1368929102000
+ /cgi-bin/post-query: Echoes back result of your POST
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line
in the Apache conf file or restrict access to allowed sources.
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'content-disposition' found, with contents: attachment;
filename="readme.txt"
+ OSVDB-3092: /readme.txt: This might be interesting...
+ /admin/index.html: Admin login page/section found.
+ /login.html: Admin login page/section found.
+ /manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/status: Default Tomcat Server Status interface found
+ /server-status: Apache server-status interface found (pass protected)
+ 10066 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2022-03-21 17:57:05 (GMT3) (2344 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Download in PDF

Result - All the vulnerabilities were scanned with the help of niko, netsparker.