Web Application Scanning Automated Vulnerability Discovery

TARGET: https://shophumm.com/

Scope: self-hosted bug bounty program

(Security | humm group)

Submitted By; Prashant Senger

To:- Skill Horizon

Assignment no.:-5

1. Recon And Discovery

--> Nmap: To see wheter the target is up or not

Command: nmap -sn <target>

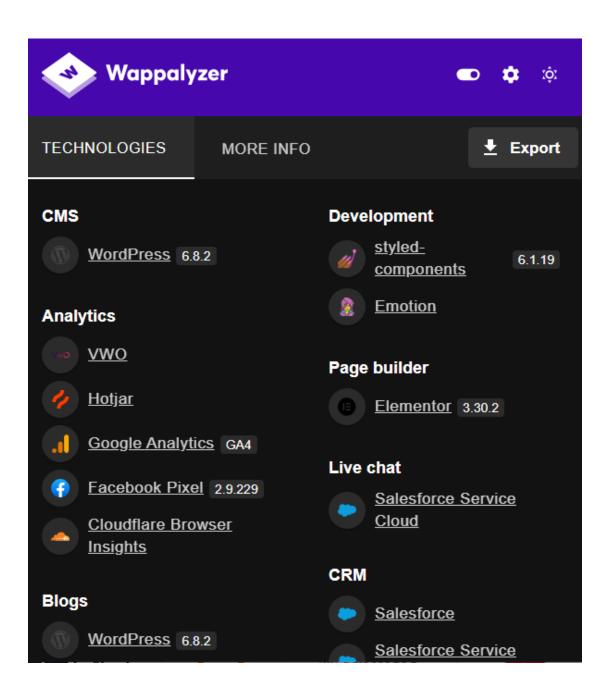
```
$ ping shophumm.com
PING shophumm.com (108.156.39.77) 56(84) bytes of data.
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=1 ttl=242 time=246 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=2 ttl=242 time=244 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=3 ttl=242 time=245 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=3 ttl=242 time=245 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=4 ttl=242 time=245 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=5 ttl=242 time=244 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=5 ttl=242 time=244 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=4 ttl=242 time=245 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=5 ttl=242 time=245 ms
64 bytes from server-108-156-39-77.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=5 ttl=242 time=244 ms
64 bytes from server-108-156-39-75.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=5 ttl=242 time=244 ms
64 bytes from server-108-156-39-75.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=5 ttl=242 time=244 ms
64 bytes from server-108-156-39-55.lhr50.r.cloudfront.net (108.156.39.77): icmp_seq=5 ttl=242 time=244 ms
64 bytes from server-108-156-39-55.lhr50.r.cloudfront.net (108.156.39.69)
64 bytes from server-108-156-39-55.lhr50.r.cloudfront.net (108.156.39.53: server-108-156-39-53.lhr50.r.cloudfront.net (108.156.39.53: server-108-156-39-53.lhr
```

To find Open port on target and runningh services and version & to perfrom half tcp scan

Command: nmap -sS -sC -sV <Target.com>

Port: 80,443 is open and 53

2. To identify Web Technology of target use whatweb wapplayzer extension



--> Target seems to be running on wordpress cms

```
(sengar© kali)-[~/intern]
$ curl -1 https://www.shophumm.com/
HTTP/2 200
date: Mon, 15 Sep 2025 10:02:20 GMT
content-type: text/html; charset=UTF-8
server: cloudflare
cf-ray: 97f-719b2ae7ld9c0-DEL
cf-cache-status: HIT
age: 696
cache-control: public, max-age=3600
expires: Mon, 15 Sep 2025 11:02:20 GMT
last-modified: Mon, 15 Sep 2025 11:02:20 GMT
last-modified: Mon, 15 Sep 2025 99:41:51 GMT
link: <a href="https://www.shophumm.com/wp-json/y; rel="https://api.w.org/", <a href="https://www.shophumm.com/wp-json/y; rel="https://api.w.org/", <a href="https://www.shophumm.com/wp-json/wp/v2/pages/2">https://www.shophumm.com/wp-json/wp/v2/pages/2</a>; rel="alternate"; title="J
SON"; type="application/json", <a href="https://www.shophum.com/wp-json/wp/v2/pages/2">https://www.shophum.com/wp-json/wp/v2/pages/2</a>; rel="alternate"; title="J
SON"; type="application/json", <a href="
```

Also, The target is protected by waf i.e Cloudflare probably block ouir scanning requests..

3. -->DIRECTORY DISCOVERY

Feroxbuster

```
—(sengar®kali)-[~/intern]
-$ feroxbuster -u https://www.shophumm.com -w /usr/share/seclists/Discovery/Web-Content/CMS/wordpress.fuzz.txt -C 301,404,302,403 -t 60
             Target Url
                                                                                     https://www.shophumm.com
          Target Url
Threads
Wordlist
Status Code Filters
Timeout (secs)
User-Agent
Config File
Extract Links
HTTP methods
Recursion Depth
New Version Available
                                                                                     /usr/share/seclists/Discovery/Web-Content/CMS/wordpress.fuzz.txt
[301, 404, 302, 403]
                                                                                   /
feroxbuster/2.11.0
/etc/feroxbuster/ferox-config.toml
true
[GET]
                                                                                   https://github.com/epi052/feroxbuster/releases/latest
₩ Press [ENTER] to use the Scan Management Menu™
                                                                                                                1c https://www.shophumm.com/wp-admin/admin-ajax.php
199c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
0c https://www.shophumm.com/
                                                      GET
GET
GET
                                                                                                           Oc https://www.shophumm.com/wp-admin/css/color-picker.min.css
Oc https://www.shophumm.com/wp-admin/css/color-picker.min.css
Oc https://www.shophumm.com/wp-admin/css/customize-controls-rtl.css
Oc https://www.shophumm.com/wp-admin/css/customize-controls.min.css
Oc https://www.shophumm.com/wp-admin/css/farbtastic.css
Oc https://www.shophumm.com/wp-admin/css/farbtastic-rtl.css
Oc https://www.shophumm.com/wp-admin/css/farbtastic-rtl.css
Oc https://www.shophumm.com/wp-admin/css/color-picker-rtl.css
Oc https://www.shophumm.com/wp-admin/css/media-rtl.min.css
Oc https://www.shophumm.com/wp-admin/css/media-rtl.min.css
Oc https://www.shophumm.com/wp-admin/css/media-rtl.min.css
Oc https://www.shophumm.com/wp-admin/css/wp-admin-rtl.css
Oc https://www.shophumm.com/wp-admin/css/wp-admin-rtl.min.css
Oc https://www.shophumm.com/wp-admin/css/wp-admin-rtl.min.css
Oc https://www.shophumm.com/wp-admin/js/accordion.min.js
2933c https://www.shophumm.com/wp-admin/js/accordion.js
                      GET
GET
GET
                      GET
GET
GET
                      GET
GET
GET
GET
GET
                       GET
GET
```

Got Some wp Directories wP-admin/js files,css

--> Automated Scanner

Nikto to scan web based vulnrebility

--> Nikto -h < target.com>

```
-(sengar⊕kali)-[~/intern]
 —$ nikto −h shophumm.com
- Nikto v2.5.0
+ Multiple IPs found: 108.156.39.77, 108.156.39.113, 108.156.39.69, 108.156.39.53
 Target IP:
                      108.156.39.77
+ Target Hostname:
                      shophumm.com
+ Target Port:
+ Start Time:
                      2025-09-15 15:33:22 (GMT5.5)
+ Server: CloudFront
+ /: Retrieved via header: 1.1 f73d71dfa047571774d2c0460e5108ec.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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 t
he MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://shophumm.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Findings:- Nothing to be interesting

--> Nuceli is template based automated scanner that scan the website usinmg ymal based templates

Nuceli –u < target.com> -t /templates/location



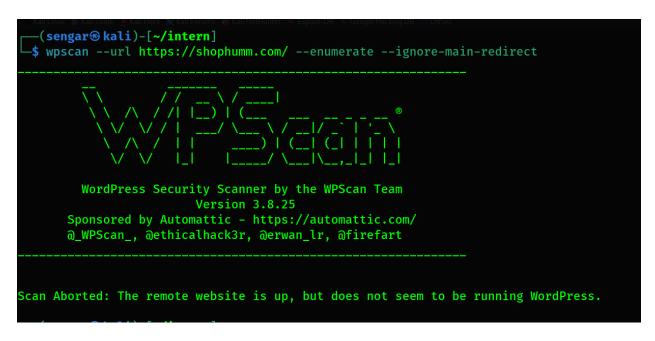
-->Found rsa git keys that are public keys(azure)

WPSCAN

--> USING WP-SCAN to identify potential WordPress vulnerabilities

Wpscan –u <target.com> --enumerate –ap – vp –wp-content-dir

--> for plugins, themes and directory listing



--> Not Useful not able to determine wheter the Sitey on wordpress or not.