

# Web Application Scanning Automated Vulnerability Discovery

TARGET: <https://shophummm.com/>

*Scope: self-hosted bug bounty program*

([Security](#) | [hummm 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>`**

```
(sengar@kali)~[~/intern]
$ 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=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
^C
--- shophumm.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4016ms
rtt min/avg/max/mdev = 244.349/244.882/245.788/0.504 ms

(sengar@kali)~[~/intern]
$ nmap -sn shophumm.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-15 15:26 IST
Nmap scan report for shophumm.com (108.156.39.53)
Host is up (0.25s latency).
Other addresses for shophumm.com (not scanned): 108.156.39.113 108.156.39.77 108.156.39.69
rDNS record for 108.156.39.53: server-108-156-39-53.lhr50.r.cloudfront.net
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

(sengar@kali)~[~/intern]
```

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


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

```
(sengar@kali)~/intern
$ sudo nmap -sC -sV -sS -A shophumm.com
[sudo] password for sengar:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-15 15:28 IST
Nmap scan report for shophumm.com (108.156.39.53)
Host is up (0.092s latency).
Other addresses for shophumm.com (not scanned): 108.156.39.113 108.156.39.77 108.156.39.69
rDNS record for 108.156.39.53: server-108-156-39-53.lhr50.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10
80/tcp    open  http         Amazon CloudFront httpd
|_ http-server-header: CloudFront
443/tcp   open  ssl/http     Amazon CloudFront httpd
|_ http-server-header: CloudFront
|_ ssl-cert: Subject: commonName=shophumm.com
| Subject Alternative Name: DNS:shophumm.com
| Not valid before: 2025-05-02T00:00:00
|_ Not valid after: 2026-05-31T23:59:59
|_ http-title: ERROR: The request could not be satisfied
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 25 hops
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7
```

**Port: 80,443 is open and 53**


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

```
(sengar@kali)~/intern
$ whatweb https://www.shophumm.com/
https://www.shophumm.com/ [200 OK] Cookies[__cf_bm], Country[UNITED STATES][US], Email[AU@3x.svg,CA@3x.svg,IE@3x.svg], Frame, HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[104.18.21.234], JQuery[2.5.19,3.7.1], MetaGenerator[Elementor 3.30.2; features: additional_custom_breakpoints; settings: css_print_method-external, google_font-disabled, font_display-auto,WordPress 6.8.2], Open-Graph-Protocol[website], PoweredBy[-link], Script[application/ld+json,speculationrules,text/html,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Home | humm group], UncommonHeaders[cf-ray,cf-cache-status,link,cf-apo-via,cf-edge-cache,x-content-type-options,alt-svc], WordPress[6.8.2], X-Frame-Options[sameorigin]
```


 **Wappalyzer**

TECHNOLOGIES


MORE INFO


 **Export**


**CMS**


 [WordPress](#) 6.8.2


**Analytics**

 [VWO](#)


 [Hotjar](#)

 [Google Analytics](#) GA4


 [Facebook Pixel](#) 2.9.229


 [Cloudflare Browser Insights](#)

**Blogs**


 [WordPress](#) 6.8.2

**Development**


 [styled-components](#) 6.1.19

 [Emotion](#)


**Page builder**


 [Elementor](#) 3.30.2

**Live chat**

 [Salesforce Service Cloud](#)

**CRM**

 [Salesforce](#)

 [Salesforce Service](#)

--> *Target seems to be running on wordpress cms*

```
(sengar@kali) ~/intern
$ curl -I 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: 97f749b2ae71d9c0-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 09:41:51 GMT
link: <https://www.shophumm.com/wp-json/>; rel="https://api.w.org/", <https://www.shophumm.com/wp-json/wp/v2/pages/2>; rel="alternate"; title="J
SON"; type="application/json", <https://www.shophumm.com/>; rel=shortlink
strict-transport-security: max-age=31536000; includeSubDomains; preload
vary: Accept-Encoding
cf-apo-via: tcache
cf-edge-cache: cache,platform=wordpress
x-content-type-options: nosniff
x-frame-options: sameorigin
set-cookie: __cf_bm=ImBk6.vRDFHhMBm46AP4Ge8Z62jZTZBjx38btppEDHc-1757930540-1.0.1.1-y3xOX8jMBPUqw.0uPPnzSetPZ5hn.8ARS85gjldiFVfcHtGa1ZEVYKkwcU5ii
I6tsVdc2RFtRLmf7m53Umlts4ILkZXbSqeUw4pIdIKWAPY; path=/; expires=Mon, 15-Sep-25 10:32:20 GMT; domain=.shophumm.com; HttpOnly; Secure; SameSite=No
ne
alt-svc: h3=":443"; ma=86400
```

***Also, The target is protected by waf i.e  
Cloudflare probably block our 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

FERROXBUSTER
by Ben "epi" Risher ver: 2.11.0

Target Url      https://www.shophumm.com
Threads         60
Wordlist         /usr/share/seclists/Discovery/Web-Content/CMS/wordpress.fuzz.txt
Status Code Filters [301, 404, 302, 403]
Timeout (secs)   7
User-Agent       feroxbuster/2.11.0
Config File      /etc/feroxbuster/ferox-config.toml
Extract Links    true
HTTP methods     [GET]
Recursion Depth  4
New Version Available https://github.com/epi052/feroxbuster/releases/latest

⚙️ Press [ENTER] to use the Scan Management Menu™

400 GET 1l 1w 1c https://www.shophumm.com/wp-admin/admin-ajax.php
403 GET 7l 20w 199c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 0l 0w 0c https://www.shophumm.com/
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/color-picker.min.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/dashboard.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/customize-controls-rtl.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/customize-controls.min.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/farbtastic.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/dashboard-rtl.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/farbtastic-rtl.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/color-picker-rtl.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/media-rtl.min.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/media.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/wp-admin-rtl.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/wp-admin-rtl.min.css
200 GET 0l 0w 0c https://www.shophumm.com/wp-admin/css/widgets-rtl.css
200 GET 2l 9w 758c https://www.shophumm.com/wp-admin/js/accordion.min.js
200 GET 87l 354w 2933c https://www.shophumm.com/wp-admin/js/accordion.js
```

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

*--> Automated Scanner*

# ***Nikto to scan web based vulnerability***

***--> 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: 80
+ 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 the 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 using yml based templates

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

```
(sengar@kali)~(~/intern)
$ nuceli -u https://shophumm.com
# Home
projectdiscovery.io

WARN Found 156 templates loaded with deprecated protocol syntax, update before v3 for continued support.
WARN Found 1 templates with syntax error (use -validate flag for further examination)
WARN Found 1 templates with runtime error (use -validate flag for further examination)
INFO Current nuclei version: v3.4.10 (latest)
INFO Current nuclei-templates version: v10.2.0 (latest)
INFO New templates added in latest release: 114
INFO Templates loaded for current scan: 8511
INFO Executing 8155 signed templates from projectdiscovery/nuceli-templates
WARN Loading 156 unsigned templates for scan. Use with caution.
INFO Targets loaded for current scan: 1
INFO Templates clustered: 1960 (Reduced 1848 Requests)
INFO Using Interactsh Server: cast-pro
INFO azure-domain-tenant [http] [info] https://login.microsoftonline.com:443/shophumm.com/v2.0/.well-known/openid-configuration [{"f36345b5-4c52-46d7-a323-aae46bd9d7d1"}]
external-service-interaction [http] [info] https://shophumm.com
missing-srl [http] [info] https://www.shophumm.com/ [{"https://www.shophumm.com/wp-includes/js/wp-util.min.js?ver=6.8.2", "https://www.shophumm.com/app/plugins/wp-search-with-algolia/js/algoliasearch/dist/algoliasearch-lite.umd.js?ver=2.1
0.1", "https://www.shophumm.com/app/plugins/elementor/assets/lib/swiper/v8/swiper.min.js?ver=8.4.5", "https://www.shophumm.com/wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997ee", "https://www.shophumm.com/app/plugins/dynamicconditions
Public/js/dynamic-conditions-public.js?ver=1.7.5", "https://www.shophumm.com/app/plugins/search-filter-pro/public/assets/js/search-filter-build.min.js?ver=2.5.19", "https://www.shophumm.com/app/plugins/ele-custom-skin/assets/js/ecs.js?ver=
1.1.9", "https://www.shophumm.com/app/plugins/essential-addons-for-elementor-lite/assets/front-end/js/view/general.min.js?ver=6.2.4", "https://www.shophumm.com/wp-includes/js/underscore.min.js?ver=1.13.7", "https://www.shophumm.com/app/plugi
ns/neve-pro-addon/includes/modules/footer/footer.js?build/front-end.js?ver=3.1.1", "https://www.shophumm.com/app/plugins/elementor-pro/assets/js/webpack-pro.runtime.min.js?ver=3.30.0", "https://www.shophumm.com/wp-includes/js/di
st/hooks.min.js?ver=463a3d49d11f1f8ba0", "https://www.shophumm.com/app/plugins/elementor-pro/assets/js/frontend.min.js?ver=3.30.0", "https://www.shophumm.com/app/themes/neve-flexi/js/custom.js?ver=1.1", "https://www.shophumm.com/wp-include
s/js/jquery/jquery.min.js?ver=3.7.1", "https://www.shophumm.com/app/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.30.2", "https://www.shophumm.com/app/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.30.2", "https://
www.shophumm.com/app/plugins/wp-search-with-algolia/js/autocomplete.js/dist/autocomplete.min.js?ver=2.10.1", "https://www.shophumm.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1", "https://www.shophumm.com/app/plugins/search-filt
er-elementor/assets/v2/js/search-filter-elementor.js?ver=1.4.1", "https://www.shophumm.com/app/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min.js?ver=3.30.2", "https://www.shophumm.com/app/themes/neve/assets/js/build/modern/fronte
r.js?ver=4.1.2", "https://www.shophumm.com/app/plugins/elementor/assets/js/frontend.min.js?ver=3.30.2", "https://www.shophumm.com/app/plugins/elementor-pro/assets/js/elements-handlers.min.js?ver=3.30.0", "https://www.shophumm.com/app/plugin
s/search-filter-pro/public/assets/js/choose.jquery.min.js?ver=2.5.19", "https://www.shophumm.com/app/plugins/ele-custom-skin/assets/js/ecs.js?ver=1.1.9", "https://www.shophumm.com/app/uploads/essential-addons-elementor/ea-el-
2.js?ver=1749742185", "https://www.shophumm.com/app/plugins/elementor/assets/js/ecspro.js?ver=3.2.5", "https://www.shophumm.com/app/plugins/neve-pro-addon/includes/modules/elementor-booster/assets/js/track.js?ver=3.1.1", "https://w
w.shophumm.com/app/plugins/wp-search-with-algolia/js/autocomplete-noconflict.js?ver=2.10.1", "https://www.shophumm.com/wp-includes/js/jquery/ui/core.min.js?ver=1.13.3", "https://www.shophumm.com/app/plugins/essential-addons-for-elementor-l
ite/assets/front-end/js/view/general.min.css?ver=6.2.0", "https://cdn.shophumm.com/hum/uploads/elementor/css/post-113.css?ver=1754545086", "https://www.shophumm.com/app/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css?ver=3.
30.2", "https://www.shophumm.com/app/plugins/elementor/assets/css/widget-image.min.css?ver=3.30.2", "https://www.shophumm.com/app/plugins/elementor/assets/css/widget-heading.min.css?ver=3.30.2", "https://cdn.shophumm.com/hum/uploads/element
or/css/post-1157.css?ver=1597143569", "https://use.typekit.net/orb7xwv.css", "https://www.shophumm.com/app/plugins/search-filter-pro/public/assets/css/search-filter.min.css?ver=2.5.19", "https://www.shophumm.com/app/plugins/elementor/assets/
lib/elementor-icons.min.css?ver=5.43.0", "https://www.shophumm.com/wp-includes/css/dashicons.min.css?ver=6.8.2", "https://www.shophumm.com/app/plugins/neve-pro-addon/includes/modules/elementor-booster/assets/css/style.min.css?ver=
3.1.1", "https://www.shophumm.com/app/plugins/ele-custom-skin/assets/css/ecs-style.css?ver=3.1.9", "https://cdn.shophumm.com/hum/uploads/elementor/css/post-634.css?ver=1754545086", "https://www.shophumm.com/app/plugins/elementor/assets/lib
font-awesome/css/font-awesome.min.css?ver=5.15.3", "https://www.shophumm.com/app/plugins/elementor/assets/lib/font-awesome/css/brands.min.css?ver=5.15.3", "https://www.shophumm.com/app/plugins/neve-pro-addon/includes/modules/blog_pro/assets
style.min.css?ver=3.1.1", "https://cdn.shophumm.com/hum/uploads/elementor/css/custom-front-end.min.css?ver=1754545084", "https://www.shophumm.com/app/plugins/wp-search-with-algolia/css/algolia-autocomplete.css?ver=2.10.1", "https://www.sho
pumm.com/app/plugins/elementor/assets/css/widget-social-icons.min.css?ver=3.30.2", "https://www.shophumm.com/app/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css?ver=8.4.5", "https://www.shophumm.com/app/uploads/essential-addons-el
ementor/ea-el-2.css?ver=1749742185", "https://www.shophumm.com/app/plugins/elementor/assets/lib/font-awesome/css/all.min.css?ver=3.1.1", "https://cdn.shophumm.com/hum/uploads/elementor/css/post-2.css?ver=1754545268", "https://www.shophumm.co
/app/plugins/dynamic-content-for-elementor/assets/css/style.min.css?ver=3.3.10", "https://www.shophumm.com/app/plugins/dynamic-content-for-elementor/assets/css/dynamic-visibility.min.css?ver=3.3.10", "https://cdn.shophumm.com/hum/uploads/
elementor/css/custom-apple-webkit.min.css?ver=1754545084", "https://www.shophumm.com/app/plugins/elementor/assets/css/conditionals/e-swiper.min.css?ver=3.30.2", "https://www.shophumm.com/app/themes/neve/style-main-new.min.css?ver=4.1.2"]
[shophumm.com]
}
```

--> 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**

[illegible]

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