

*Made by Moez Javed*

# Comprehensive Assessment Script

— Manual (Kali, Ethical Use)



Moez Javed

# Comprehensive Assessment Script Manual (Kali, Ethical Use)

**Audience:** Students and interns learning how to run **authorized** reconnaissance and vulnerability assessments in a controlled lab or with written permission.

**Purpose:** Explain *why* combining tools matters, how to prepare a safe lab workflow, and how to run (and extend) a one-shot script that orchestrates Nmap → web checks (Nikto/Dirb/WPScan) → targeted Nmap vuln scripts → a preliminary Markdown report.

## ***Legal & Ethics***

- Run **only** on systems you own or have explicit written authorization to test.
- Use the script in a lab/VPN/segmented network.
- Disable any destructive checks; avoid denial-of-service.
- Treat outputs as sensitive and store them securely.

## ***1) Why combine tools?***

Security assessments are rarely a single tool job. A stitched workflow lets you: - Keep evidence together under a timestamped folder (reproducibility), - Reuse open-port lists to focus follow-up scans (efficiency), - Chain web-only actions **only** if web ports are present (signal over noise), - Produce a quick, human-readable report to brief your blue team.

## **2) Prerequisites (Kali/Linux)**

*Made by Moez Javed*

Install/update the tools we'll call from the script.

```
sudo apt update && sudo apt install -y \
```

```
nmap nikto dirb wpscan jq xsltproc
```

# optional helpers used later in the manual

```
(kali@kali)~$ sudo apt update && sudo apt install -y \
nmap nikto dirb wpscan jq xsltproc

[sudo] password for kali:
Hit:1 https://download.docker.com/linux/debian bookworm InRelease
Get:2 http://mirror.ourhost.az/kali kali-rolling InRelease [41.5 kB]
Get:3 http://mirror.ourhost.az/kali kali-rolling/main i386 Packages [20.7 MB]
Ign:4 https://apt.cutter.re/repo jammy InRelease
Ign:4 https://apt.cutter.re/repo jammy InRelease
Ign:4 https://apt.cutter.re/repo jammy InRelease
Get:5 http://mirror.ourhost.az/kali kali-rolling/main amd64 Packages [21.2 MB]
Err:4 https://apt.cutter.re/repo jammy InRelease
       Could not resolve 'apt.cutter.re'
Get:6 http://mirror.ourhost.az/kali kali-rolling/main i386 Contents (deb) [48.1 MB]
Get:7 http://mirror.ourhost.az/kali kali-rolling/main amd64 Contents (deb) [51.8 MB]
Get:8 http://mirror.ourhost.az/kali kali-rolling/contrib i386 Packages [98.5 kB]
Get:9 http://mirror.ourhost.az/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:10 http://mirror.ourhost.az/kali kali-rolling/contrib amd64 Contents (deb) [325 kB]
Get:11 http://mirror.ourhost.az/kali kali-rolling/contrib i386 Contents (deb) [182 kB]
Get:12 http://mirror.ourhost.az/kali kali-rolling/non-free amd64 Packages [200 kB]
Get:13 http://mirror.ourhost.az/kali kali-rolling/non-free i386 Packages [149 kB]
Get:14 http://mirror.ourhost.az/kali kali-rolling/non-free-firmware i386 Packages [10.8 kB]
Get:15 http://mirror.ourhost.az/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:16 http://mirror.ourhost.az/kali kali-rolling/non-free-firmware i386 Contents (deb) [27.2 kB]
Get:17 http://mirror.ourhost.az/kali kali-rolling/non-free-firmware amd64 Contents (deb) [27.2 kB]
Fetched 143 MB in 1min 23s (1.713 kB/s)
74 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch https://apt.cutter.re/repo/dists/jammy/InRelease Could not resolve 'apt.cutter.re'
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
nmap is already the newest version (7.95+dfsg-3kali1).
```

```
sudo apt install -y curl whatweb
```

**Tip:** Some scans (OS detection, SYN) work best with sudo/root. Run the script with sudo inside your lab.

```
(kali@kali)~$ sudo apt install -y curl whatweb
curl is already the newest version (8.15.0-1).
whatweb is already the newest version (0.6.1-1).
The following packages were automatically installed and are no longer required:
  docker-buildx-plugin  libgddata22  libriemann-client0  libvpx9  python3-packaging-whl  python3-wheel-whl
  docker-ce-rootless-extras  libgeos3.13.1  libsqlite3  linux-image-6.12.25-amd64  python3-pyinstaller-hooks-contrib  slirp4netns
  docker-cli  libhdf4-0-alt  libsigsegv2  pigz  python3-cachetools  python3-pyu2f
  docker-compose-plugin  libivykis0t64  libslirp0  python3-google-auth  python3-requests-oauthlib
  libdb11t64  libqt5ct-common1.8  libsoup-2.4-1  python3-kubernetes  python3-responses
  libgddata-common  librdkafka1  libsoup2.4-common  python3-rsa

Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 74
```

### 3) The orchestrator script (with safe defaults)

Create a working folder and script file:

```
mkdir -p ~/assessments && cd ~/assessments
```

```
nano assessment.sh
```

Paste the script below **exactly** (this version fixes line-break bugs and adds safety checks):

*Made by Moez Javed*

*Made by Moez Javed*

```
(kali@kali)-[~]  
$ mkdir -p ~/assessments && cd ~/assessments  
nano assessment.sh
```

```
#!/usr/bin/env bash
```

```
set -euo pipefail
```

```
(kali@kali)-[~]  
$ set -euo pipefail
```

```
#!/bin/bash
```

```
# =====
```

```
# Automated Security Assessment Script
```

```
# =====
```

```
# Check if target provided
```

```
if [ -z "$1" ]; then
```

```
    echo "Usage: $0 <TARGET-IP/HOSTNAME>"
```

```
    exit 1
```

```
fi
```

```
TARGET="$1"
```

```
OUTPUT_DIR="./assessment_$(date +%Y%m%d_%H%M%S)"
```

```
mkdir -p "$OUTPUT_DIR"
```

```
echo "[*] Starting comprehensive assessment of $TARGET"
```

*Made by Moez Javed*

*Made by Moez Javed*

```
echo "[*] Results will be stored in: $OUTPUT_DIR"
```

```
echo
```

```
# =====
```

```
# 1. Initial Nmap Scan
```

```
# =====
```

```
echo "[*] Running initial Nmap scan (top 1000 TCP ports)..."
```

```
nmap -sS -sV -sC -O -T3 -Pn -oA "$OUTPUT_DIR/nmap_scan" "$TARGET"
```

```
# Extract open ports
```

```
PORTS=$(grep -oP 'd+/open' "$OUTPUT_DIR/nmap_scan.gnmap" | cut -d/' -f1  
| tr '\n' ',' | sed 's/,,$//')
```

```
if [ -z "$PORTS" ]; then
```

```
    echo "[!] No open ports found in top 1000. Running full port scan..."
```

```
    nmap -p- -T4 -oA "$OUTPUT_DIR/nmap_full" "$TARGET"
```

```
    PORTS=$(grep -oP 'd+/open' "$OUTPUT_DIR/nmap_full.gnmap" | cut -d/' -  
f1 | tr '\n' ',' | sed 's/,,$//')
```

```
fi
```

```
if [ -z "$PORTS" ]; then
```

```
    echo "[!] No open ports detected on $TARGET. Exiting."
```

```
    exit 0
```

```
fi
```

```
echo "[*] Open ports detected: $PORTS"
```

*Made by Moez Javed*

*Made by Moez Javed*

*echo*

```
# =====
```

*# 2. Vulnerability Scan*

```
# =====
```

*echo "[\*] Running Nmap vulnerability scan on detected ports..."*

```
nmap --script vuln -p"$PORTS" "$TARGET" -oA  
"$OUTPUT_DIR/nmap_vuln_scan"
```

*echo*

```
# =====
```

*# 3. Web Application Scans*

```
# =====
```

*if echo "\$PORTS" | grep -q "80\|443\|8080\|8443"; then*

*echo "[\*] Web service detected. Running Nikto, Dirb, and WPScan..."*

```
nikto -h "http://$TARGET" -output "$OUTPUT_DIR/nikto_scan.txt"
```

```
dirb "http://$TARGET" -o "$OUTPUT_DIR/dirb_scan.txt"
```

```
wpscan --url "http://$TARGET" --enumerate ap,at,cb,dbe -o  
"$OUTPUT_DIR/wpscan.txt"
```

*echo "[\*] Web scans completed."*

*echo*

*else*

*echo "[\*] No common web ports found. Skipping web scans."*

*fi*

```
# =====
```

*# 4. Report Generation*

```
# =====
```

*Made by Moez Javed*

*Made by Moez Javed*

```
echo "[*] Generating preliminary report..."
cat > "$OUTPUT_DIR/preliminary_report.md" << EOF

# Security Assessment Report

**Target:** $TARGET

**Date:** $(date)

---

## Network Services

$(cat "$OUTPUT_DIR/nmap_scan.nmap" | grep -E "\d+/tcp|\d+/udp" || echo
"No services detected.")

---

## Potential Vulnerabilities

$(grep -h "VULNERABLE" "$OUTPUT_DIR"/*.txt 2>/dev/null || echo "No
automatic vulnerabilities detected.")

---

## Recommendations

- Review all identified services manually
- Investigate potential vulnerabilities in detail
- Perform authenticated testing where possible

EOF

echo "[*] Assessment complete!"

echo "[*] All results are saved in: $OUTPUT_DIR"
```

Save and close, then make it executable and run it:

*Made by Moez Javed*

*Made by Moez Javed*

```
chmod +x assessment.sh
```

```
sudo ./assessment.sh 10.0.2.15 # replace with your authorized lab target
```

**Output:** a timestamped folder assessment\_YYYYMMDD\_HHMMSS containing Nmap/Nikto/Dirb/WPScan outputs, a run.log, and a preliminary\_report.md.

```
(kali@kali)-[~/assessments]
$ sudo ./assessment.sh 10.0.2.15
[*] Starting comprehensive assessment of 10.0.2.15
[*] Running Nmap scan...
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 00:23 EDT
Nmap scan report for 10.0.2.15
Host is up (0.41s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: D-link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%), IBM i 7.4 (89%), ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital video projecto
r (89%), Sonus GSX9000 VoIP proxy (88%), Asus WL-500gP wireless broadband router (88%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 Enterprise Edition
SP2 (88%), Microsoft Windows Server 2003 SP2 (88%)
No exact OS matches for host (test conditions non-ideal).

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 0.63 ms 192.168.22.2
2 ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 267.46 seconds
```

#### *4) Step-by-step: what every command does*

##### *a) Nmap core scan*

```
sudo nmap -sS -sV -sC -O -A -T3 -Pn -oA ./nmap_scan 10.0.2.15
```

- -sS SYN scan (fast, less intrusive than full connect).
- -sV service/version detection.
- -sC default NSE scripts (safe).
- -O OS fingerprinting; -A adds aggressive detection (includes OS, traceroute, some scripts).
- -T3 balanced timing (safer in shared labs than -T4).
- -Pn skip host discovery (treat host as up).
- -oA write all formats (.nmap, .gnmap, .xml)

*Made by Moez Javed*



```
(kali@kali)~$ sudo nmap -sS -sV -sC -O -A -T3 -Pn -oA ./nmap_scan 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 00:33 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00021s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%), IBM 1 7.4 (89%), ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital video projecto
r (89%), Sonus GSX0000 VoIP proxy (88%), Asus WL-500gP wireless broadband router (88%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 SP2 (88%)
SP2 (88%), Microsoft Windows Server 2003 SP2 (88%)
No exact OS matches for host (test conditions non-ideal).

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 0.86 ms 192.168.22.2
2 ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 240.45 seconds
```

## ***b) Extract open ports from Nmap***

```
PORTS=$(grep -oP '\d+/\open/tcp' "$OUTPUT_DIR/nmap_scan.gnmap" | cut -d '/' -f1 | tr '\n' ',' | sed 's/,,$//')
```

```
(kali@kali)~$ PORTS=$(grep -oP '\d+/\open/tcp' "$OUTPUT_DIR/nmap_scan.gnmap" | cut -d '/' -f1 | tr '\n' ',' | sed 's/,,$//')
```

- Greps open TCP ports from the .gnmap file, plucks just the port numbers, converts newlines to commas for reuse, and trims the trailing comma.

## ***c) Conditional web checks***

- We only run Nikto/Dirb/WPScan if web-ish ports were found (80, 443, 8080, 8443).
- nikto runs once for HTTP and once for HTTPS; failures don't stop the script (|| true).
- dirb quickly enumerates common paths; for deeper tests, switch to a bigger wordlist.
- We try a **cheap** WP fingerprint (look for wp-content / wp-includes in HTML) before launching wpscan.

## ***d) Nmap vuln scripts***

```
nmap --script vuln -p"$PORTS" "$TARGET" -oA "$OUTPUT_DIR/nmap_vuln_scan"
```

- Runs NSE scripts tagged vuln **only on discovered ports**. Treat results as *findings to be verified*, not proof of exploitation.

#### *e) Preliminary report generation*

- Builds preliminary\_report.md with service lines, any “VULNERABLE” markers from tool outputs, and structured sections you can expand manually.

#### *5) How to read the results (triage guide)*

1. **Open ports & services:** Start with nmap\_scan.nmap and confirm the service banner makes sense for the host’s role.
2. **Vuln hints:** Review nmap\_vuln\_scan.nmap for CVE references **then verify manually**.
3. **Web checks:** Compare nikto\_\*.txt and dirb\_\*.txt; look for sensitive files, outdated server banners, default pages. If wpscan\_\*.txt exists, read the summary and plugin/theme enumeration results.
4. **Report:** Open preliminary\_report.md and add human analysis: false positives, compensating controls, and prioritized actions.

#### *6) Variations & safe extensions (optional)*

- **Safer timing:** If the target is fragile, drop to -T2 and remove -A (keep -sV -sC).
- **Scope files:** Replace single TARGET with a list and loop (while read h; do ... done < scope.txt).
- **Wordlists:** For dirb, specify another list: dirb http://\$TARGET /usr/share/wordlists/dirb/common.txt -o ....

- **WhatWeb:** Fast tech fingerprint: `whatweb -a 1 http://$TARGET | tee "$OUTPUT_DIR/whatweb.txt"`.
- **Nmap XML parsing:** Use `xsltproc` to render HTML from XML (`nmap -oX` then `xsltproc`).
- **Archive:** Zip everything: `tar -czf "$OUTPUT_DIR.tgz" -C "$OUTPUT_DIR" ..`

```
(kali@kali) [~/assessments]
$ sudo ./assessment.sh cinesagerecommender.vercel.app
[*] Starting comprehensive assessment of cinesagerecommender.vercel.app
[*] Results will be stored in: ./assessment_20250901_014816

[*] Running initial Nmap scan (top 1000 TCP ports)...
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 01:48 EDT
Nmap scan report for cinesagerecommender.vercel.app (64.29.17.67)
Host is up (0.027s latency).
Other addresses for cinesagerecommender.vercel.app (not scanned): 216.198.79.67
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Vercel
|_http-server-header: Vercel
|_http-title: Site doesn't have a title (text/plain).

fingerprint-strings:
  FourOhFourRequest:
    HTTP/1.0 308 Permanent Redirect
    Content-Type: text/plain
    Location: https://nice%20ports%2C/Tri%6Eity.txt%2ebak
    Refresh: 0;url=https://nice%20ports%2C/Tri%6Eity.txt%2ebak
    server: Vercel
    Redirecting ...
  GetRequest, HTTPOptions:
    HTTP/1.0 308 Permanent Redirect
    Content-Type: text/plain
    Location: https://
    Refresh: 0;url=https://
    server: Vercel
    Redirecting ...
```

*Made by Moez Javed*

```
Redirecting ...
443/tcp open  ssl/http Golang net/http server
ssl-cert: Subject: commonName=*.vercel.app
Subject Alternative Name: DNS:*.vercel.app, DNS:vercel.app
Not valid before: 2025-08-24T16:25:33
Not valid after: 2025-11-22T16:25:32
_http-title: Cinesage
fingerprint-strings:
FourOhFourRequest:
HTTP/1.0 404 Not Found
Cache-Control: public, max-age=0, must-revalidate
Content-Length: 107
Content-Type: text/plain; charset=utf-8
Date: Mon, 01 Sep 2025 05:51:24 GMT
Server: Vercel
Strict-Transport-Security: max-age=63072000
X-Vercel-Error: DEPLOYMENT_NOT_FOUND
X-Vercel-Id: dxb1::9g79q-1756705884355-02227021af91
deployment could not be found on Vercel.
DEPLOYMENT_NOT_FOUND
dxb1::9g79q-1756705884355-02227021af91
GenericLines, Help, RTSPRequest:
HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close
Request
GetRequest:
HTTP/1.0 404 Not Found
Cache-Control: public, max-age=0, must-revalidate
Content-Length: 107
Content-Type: text/plain; charset=utf-8
```

```
HTTPOptions:
HTTP/1.0 404 Not Found
Cache-Control: public, max-age=0, must-revalidate
Content-Length: 107
Content-Type: text/plain; charset=utf-8
Date: Mon, 01 Sep 2025 05:51:24 GMT
Server: Vercel
Strict-Transport-Security: max-age=63072000
X-Vercel-Error: DEPLOYMENT_NOT_FOUND
X-Vercel-Id: dxb1::fpt42-1756705884069-8f70e15c54db
deployment could not be found on Vercel.
DEPLOYMENT_NOT_FOUND
dxb1::fpt42-1756705884069-8f70e15c54db
_http-server-header: Vercel
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF:Port80-TCP:V=7.95XI=7XD=9/1XTime=68853453XP=x86_64-pc-linux-gnu%(GetRe
SF:quest,8A,"HTTP/1.0\\x20308\\x20Permanent\\x20Redirect\\r\\nContent-Type:\\x2
SF:0text/plain\\r\\nLocation:\\x20https://\\r\\nRefresh:\\x200;url=https://\\r\\
SF:nserver:\\x20Vercel\\r\\n\\r\\nRedirecting\\.\\.\\.")%(HTTPOptions,8A,"HTTP/1
SF:.0\\x20308\\x20Permanent\\x20Redirect\\r\\nContent-Type:\\x20text/plain\\r\\nLo
SF:cation:\\x20https://\\r\\nRefresh:\\x200;url=https://\\r\\nserver:\\x20Verce
SF:l\\r\\n\\r\\nRedirecting\\.\\.\\.")%(FourOhFourRequest,D0,"HTTP/1.0\\x20308\\x
SF:20Permanent\\x20Redirect\\r\\nContent-Type:\\x20text/plain\\r\\nLocation:\\x20
SF:https://\\nice%20ports%2C/Tri%6Eity\\.txt%2ebak\\r\\nRefresh:\\x200;url=http
SF:s://\\nice%20ports%2C/Tri%6Eity\\.txt%2ebak\\r\\nserver:\\x20Vercel\\r\\n\\r\\nR
SF:edirecting\\.\\.\\.");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF:Port443-TCP:V=7.95XI=7XD=9/1XTime=68853459XP=x86_64-pc-linux-gnu%
SF:r(GetRequest,1B3,"HTTP/1.0\\x20404\\x20Not\\x20Found\\r\\nCache-Control:\\x2
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 289.18 seconds

[\*] Open ports detected: 80,443

*Made by Moez Javed*

```
[*] Running Nmap vulnerability scan on detected ports ...
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 01:53 EDT
Nmap scan report for cinesagerecommender.vercel.app (64.29.17.131)
Host is up (0.013s latency).
Other addresses for cinesagerecommender.vercel.app (not scanned): 216.198.79.131

PORT      STATE SERVICE
80/tcp    open  http
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp   open  https
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|_ /webtrends/: Potentially interesting folder
|_ /web_usage/: Potentially interesting folder
|_ /win2k/: Potentially interesting folder
|_ /window/: Potentially interesting folder
|_ /windows/: Potentially interesting folder
|_ /win/: Potentially interesting folder
|_ /winnt/: Potentially interesting folder
|_ /word/: Potentially interesting folder
|_ /work/: Potentially interesting folder
|_ /world/: Potentially interesting folder
|_ /wsdocs/: Potentially interesting folder
|_ /WS_FTP/: Potentially interesting folder
|_ /wstats/: Potentially interesting folder
|_ /wusage/: Potentially interesting folder
|_ /www0/: Potentially interesting folder
```

```
|_ /sitecore%20modules/staging/service/api.asmx: Sitecore.NET (CMS)
|_ /sitecore%20modules/staging/workdir: Sitecore.NET (CMS)
|_ /sitecore/system/Settings/Security/Profiles: Sitecore.NET (CMS)
|_ http-dombased-xss: Couldn't find any DOM based XSS
http-slowloris-check:
  VULNERABLE:
    Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs: CVE:CVE-2007-6750
    Slowloris tries to keep many connections to the target web server open and hold
    them open as long as possible. It accomplishes this by opening connections to
    the target web server and sending a partial request. By doing so, it starves
    the http server's resources causing Denial Of Service.

    Disclosure date: 2009-09-17
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
      http://hackers.org/slowloris/
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 636.82 seconds
```

```
[*] Web service detected. Running Nikto, Dirb, and WPScan ...
- Nikto v2.5.0

+ Multiple IPs found: 64.29.17.195, 216.198.79.195
+ Target IP: 64.29.17.195
+ Target Hostname: cinesagerecommender.vercel.app
+ Target Port: 80
+ Start Time: 2025-09-01 02:03:43 (GMT-4)

+ Server: Vercel
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'refresh' found, with contents: 0:url=https://cinesagerecommender.vercel.app/.
+ /: 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://cinesagerecommender.vercel.app/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /database.js: IP address found in the 'x-vercel-id' header. The IP is 'b1::8'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /database.js: Uncommon header 'x-vercel-id' found, with contents: dxb1::8m2x9-1756706854187-b1851b206e40.
+ /file/../../../../../../../../etc/: Uncommon header 'x-vercel-error' found, with contents: BAD_REQUEST.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 5 error(s) and 6 item(s) reported on remote host
+ End Time: 2025-09-01 02:39:49 (GMT-4) (2166 seconds)

+ 1 host(s) tested
```



*Made by Moez Javed*

```
DIRB v2.22
By The Dark Raver

OUTPUT_FILE: ./assessment_20250901_014816/dirb_scan.txt
START_TIME: Mon Sep  1 02:39:49 2025
URL_BASE: http://cinesagerecommender.vercel.app/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

Scanning URL: http://cinesagerecommender.vercel.app/
```

*TARGET=cinesagerecommender.vercel.app*

*OUTPUT\_DIR=~/.assessments/results\_\$(date +%Y%m%d\_%H%M%S)*

*mkdir -p "\$OUTPUT\_DIR"*

```
(kali㉿kali)-[~/assessments]
$ TARGET=cinesagerecommender.vercel.app
OUTPUT_DIR=~/.assessments/results_$(date +%Y%m%d_%H%M%S)
mkdir -p "$OUTPUT_DIR"
```

*echo "Running Nikto..."*

*nikto -h "http://\$TARGET" -o "\$OUTPUT\_DIR/nikto\_scan.txt" || true*

*nikto -h "https://\$TARGET" -ssl -o "\$OUTPUT\_DIR/nikto\_ssl\_scan.txt" || true*

*echo "Running Dirb..."*

*dirb "http://\$TARGET" -o "\$OUTPUT\_DIR/dirb\_scan.txt" || true*

*dirb "https://\$TARGET" -o "\$OUTPUT\_DIR/dirb\_ssl\_scan.txt" || true*

*Made by Moez Javed*

```
(kali@kali) [~/assessments]
$ echo "Running Nikto..."
nikto -h "http://$TARGET" -o "$OUTPUT_DIR/nikto_scan.txt" || true
nikto -h "https://$TARGET" -ssl -o "$OUTPUT_DIR/nikto_ssl_scan.txt" || true

echo "Running Dirb..."
dirb "http://$TARGET" -o "$OUTPUT_DIR/dirb_scan.txt" || true
dirb "https://$TARGET" -o "$OUTPUT_DIR/dirb_ssl_scan.txt" || true

Running Nikto ...
- Nikto v2.5.0

+ Multiple IPs found: 216.198.79.3, 64.29.17.3
+ Target IP: 216.198.79.3
+ Target Hostname: cinesagerecommender.vercel.app
+ Target Port: 80
+ Start Time: 2025-09-01 03:06:28 (GMT-4)

+ Server: Vercel
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'refresh' found, with contents: 0;url=https://cinesagerecommender.vercel.app/
+ /: 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://cinesagerecommender.vercel.app/
```

```
+ /: 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://cinesagerecommender.vercel.app/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 2 error(s) and 3 item(s) reported on remote host
+ End Time: 2025-09-01 03:38:56 (GMT-4) (1948 seconds)

+ 1 host(s) tested
- Nikto v2.5.0

+ Multiple IPs found: 216.198.79.3, 64.29.17.3
+ Target IP: 216.198.79.3
+ Target Hostname: cinesagerecommender.vercel.app
+ Target Port: 443

+ SSL Info: Subject: /CN=*.vercel.app
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=Let's Encrypt/CN=R13
+ Start Time: 2025-09-01 03:39:02 (GMT-4)

+ Server: Vercel
+ /: Retrieved access-control-allow-origin header: *.
+ /: IP address found in the 'x-vercel-id' header. The IP is 'b1::4f'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-vercel-cache' found, with contents: HIT.
+ /: Uncommon header 'content-disposition' found, with contents: inline.
+ /: Uncommon header 'x-vercel-id' found, with contents: dxb1:14fnd-1756712369293-b2bd2296f108.
+ /: 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/
```

## 7) Troubleshooting

- **No ports found:** Host firewalled; try -Pn, slower timing, or confirm target/route.
- **Nikto/Dirb time out:** Service may be HTTPS-only or behind WAF; try https:// explicitly.
- **WPScan missing:** Install/update: `sudo apt install wpscan` or `gem install wpscan`.
- **Permission errors:** Re-run with `sudo` (some scans require elevated privileges).

- **Report empty:** Check run.log for errors and confirm files exist in the output dir.

### ***9) Safety checklist (print & tape near your monitor)***

- ☐ Do I have written authorization (or is this a designated lab box)?
- ☐ Are my scan timings conservative for this environment?
- ☐ Am I capturing outputs with timestamps and not overwriting previous runs?
- ☐ Did I store results in an approved, access-controlled folder?
- ☐ Did I verify any “vulnerable” findings manually before reporting?

### **Appendix — One-liners you can reuse**

*# Quick open-port list from Nmap XML using awk*

```
awk -F "" '/portid=/ && /state state="open"/ {print $4}' nmap_scan.xml | paste -sd, -
```

*# Safer baseline Nmap*

```
nmap -sS -sV -sC -T3 -oA baseline <target>
```

*# Render Nmap XML to HTML (requires xsltproc)*

```
xsltproc /usr/share/nmap/nmap.xsl nmap_scan.xml > nmap_scan.html
```

*# Quick WordPress check (cheap)*

```
curl -ksS http://<target> | grep -qi 'wp-content|wp-includes' && echo "WordPress likely"
```

*End of manual.*