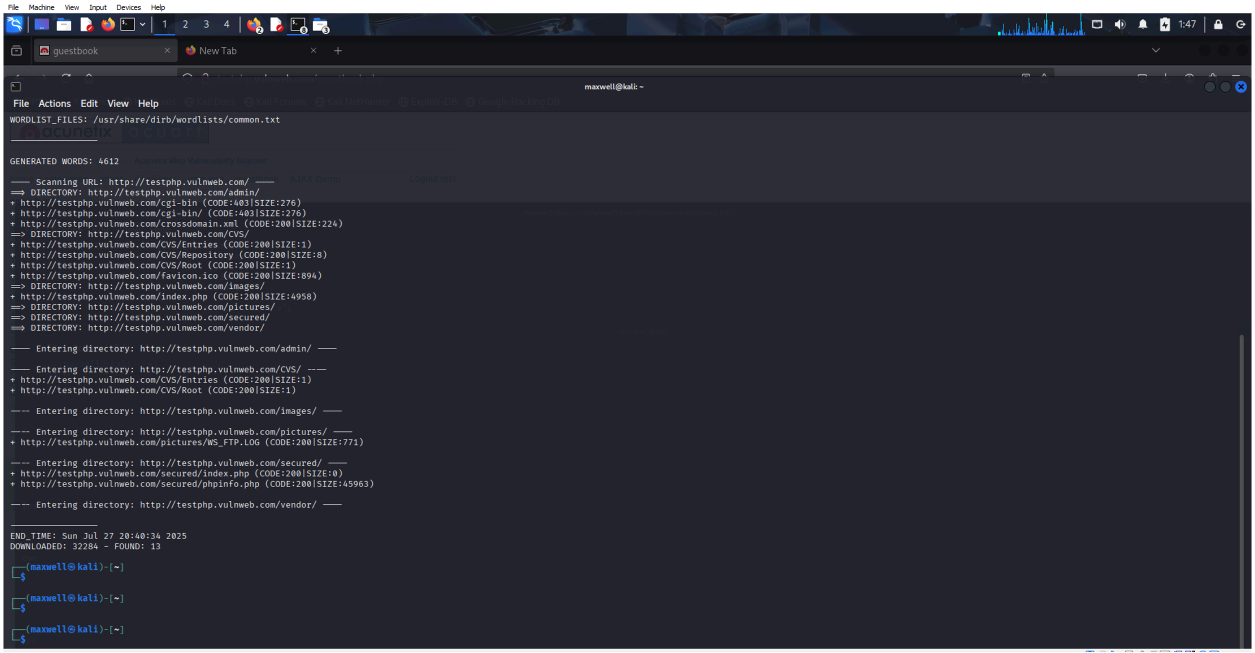
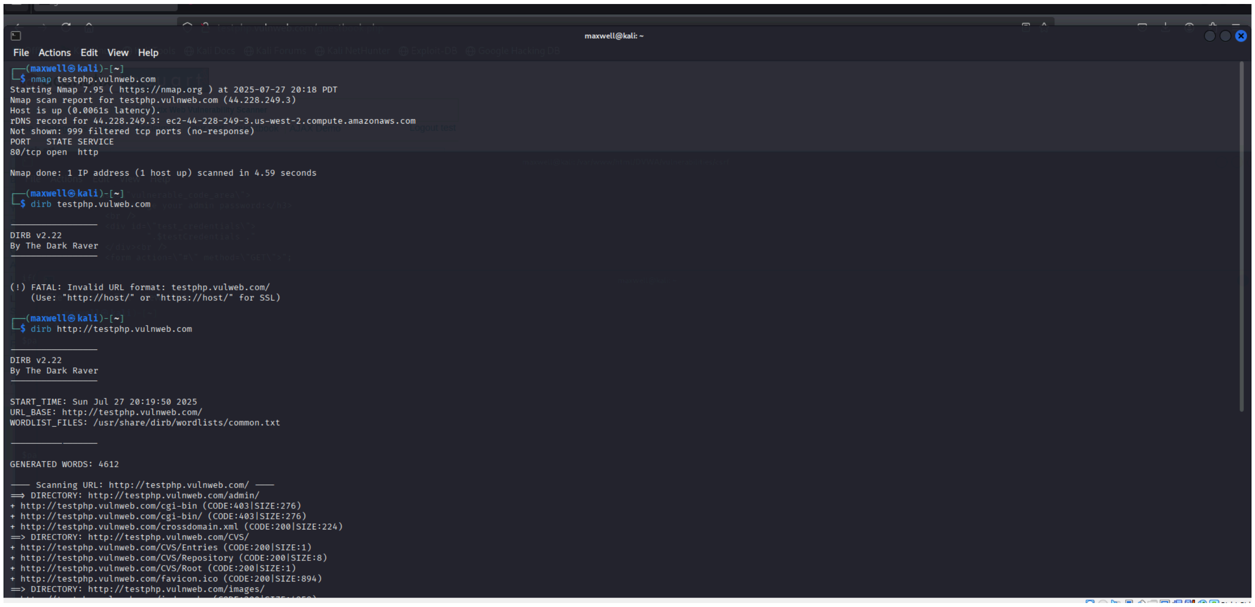
Task 4: Web Recon and Enumeration with Real Targets

Target selected: testphp.vulnweb.com,

Results of nmap and dirb scans:


File Machine View Input Devices Help
guestbook
New Tab
maxwell@kali: ~
File Actions Edit View Help

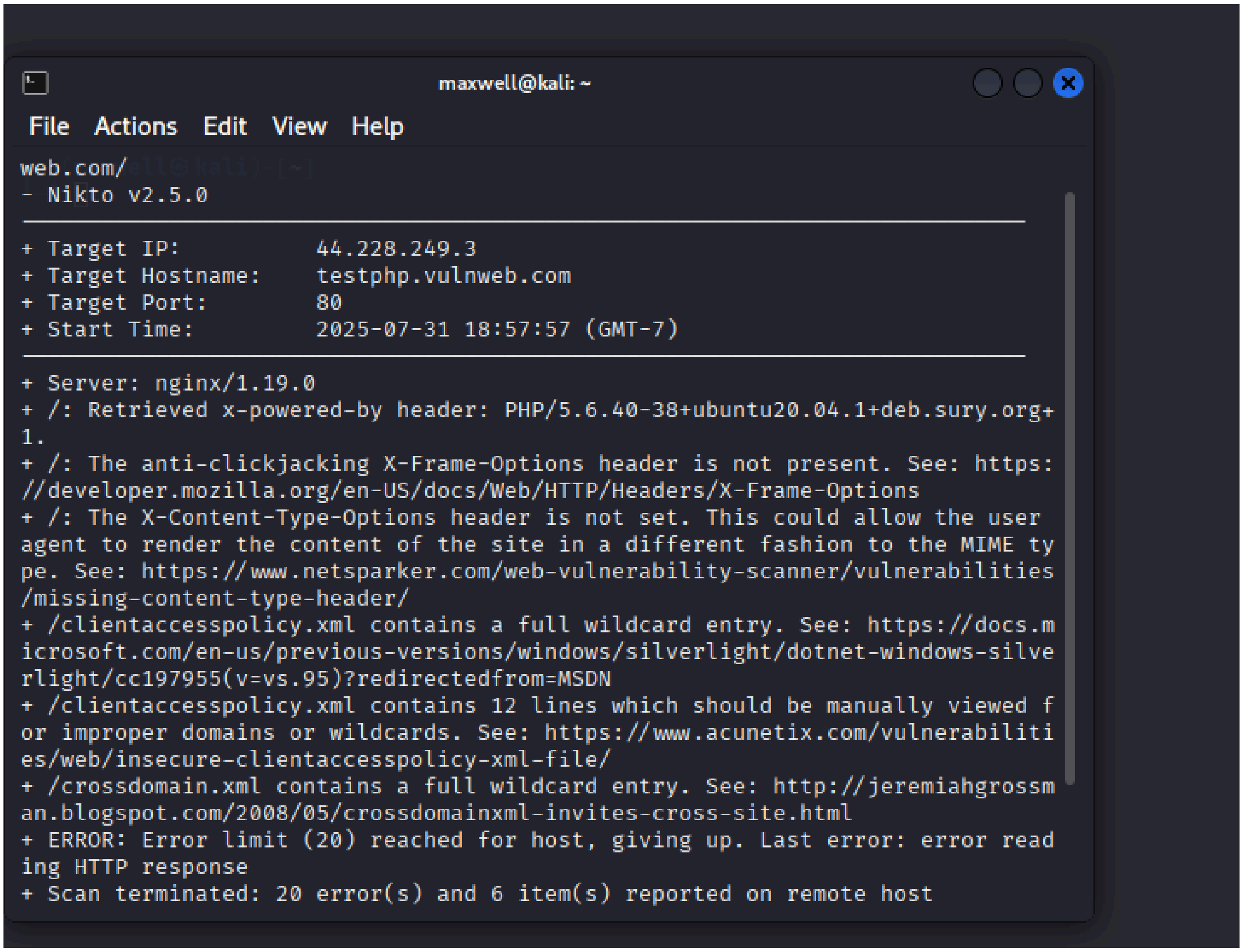
```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----

---- Entering directory: http://testphp.vulnweb.com/CVS/ ----
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)

---- Entering directory: http://testphp.vulnweb.com/images/ ----

---- Entering directory: http://testphp.vulnweb.com/pictures/ ----
+ http://testphp.vulnweb.com/pictures/WS_FTP.LOG (CODE:200|SIZE:771)

---- Entering directory: http://testphp.vulnweb.com/secured/ ----
+ http://testphp.vulnweb.com/secured/index.php (CODE:200|SIZE:0)
+ http://testphp.vulnweb.com/secured/phpinfo.php (CODE:200|SIZE:45963)

---- Entering directory: http://testphp.vulnweb.com/vendor/ ----

-----------------
END_TIME: Sun Jul 27 20:40:34 2025
DOWNLOADED: 32284 - FOUND: 13

┌──(maxwell㉿kali)-[~]
└─$

┌──(maxwell㉿kali)-[~]
└─$

┌──(maxwell㉿kali)-[~]
└─$
```



```
┌──(maxwell㉿kali)-[~]
└─$ nmap testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 20:18 PDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0061s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.59 seconds

┌──(maxwell㉿kali)-[~]
└─$ dirb testphp.vulweb.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------


(!) FATAL: Invalid URL format: testphp.vulweb.com/
    (Use: "http://host/" or "https://host/" for SSL)

┌──(maxwell㉿kali)-[~]
└─$ dirb http://testphp.vulnweb.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jul 27 20:19:50 2025
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
```

In summary, surfing to the most probable link testphp.vulnweb.com,/admin showed no admin panel results
Also the only port open is port 80 with the HTTPs service

When running nikto on the target it seems like XSS protections are not implemented.



```
web.com/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-07-31 18:57:57 (GMT-7)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+
1.
+ /: 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 ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.m
icrosoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silve
rlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed f
or improper domains or wildcards. See: https://www.acunetix.com/vulnerabiliti
es/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossm
an.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error read
ing HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
```