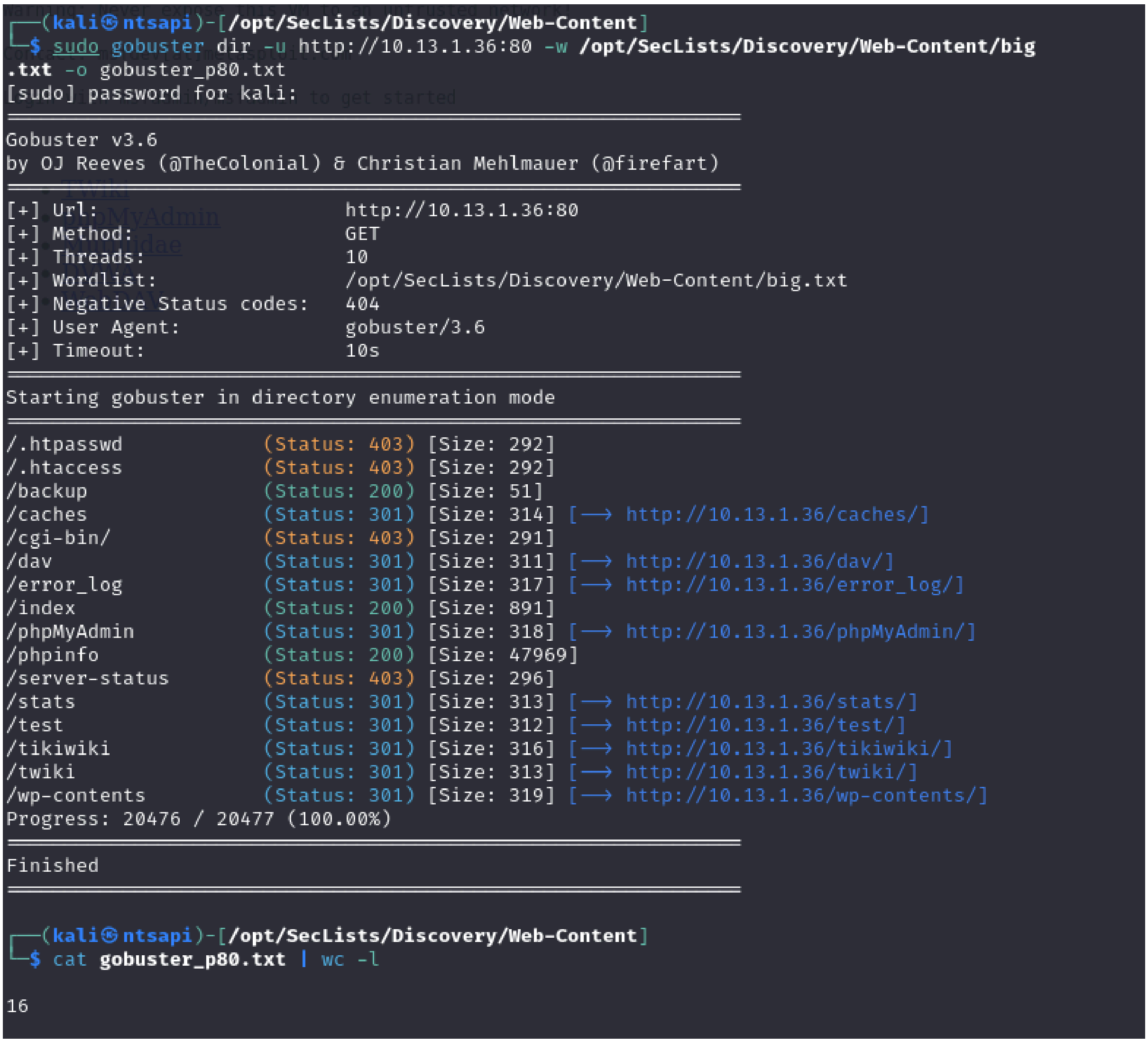
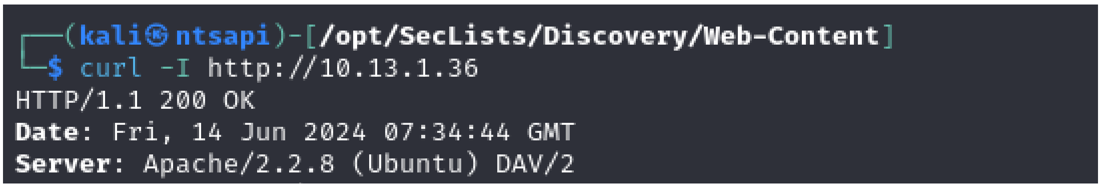
HTTP Enumerator:

1. How many files could you find on port 80?
   Your response: 16



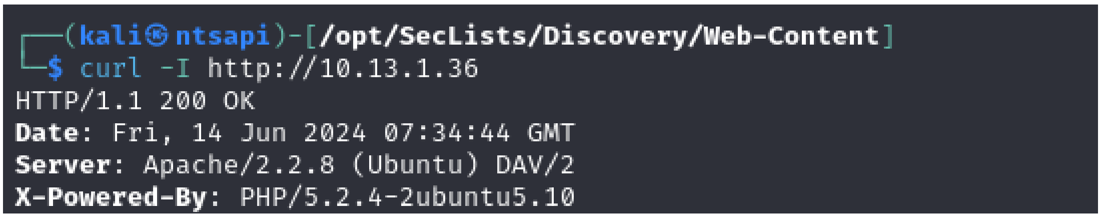
```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ sudo gobuster dir -u http://10.13.1.36:80 -w /opt/SecLists/Discovery/Web-Content/big
.txt -o gobuster_p80.txt
[sudo] password for kali:
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.13.1.36:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /opt/SecLists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 292]
/backup               (Status: 200) [Size: 51]
/caches               (Status: 301) [Size: 314] [--> http://10.13.1.36/caches/]
/cgi-bin/             (Status: 403) [Size: 291]
/dav                  (Status: 301) [Size: 311] [--> http://10.13.1.36/dav/]
/error_log            (Status: 301) [Size: 317] [--> http://10.13.1.36/error_log/]
/index                (Status: 200) [Size: 891]
/phpMyAdmin           (Status: 301) [Size: 318] [--> http://10.13.1.36/phpMyAdmin/]
/phpinfo              (Status: 200) [Size: 47969]
/server-status        (Status: 403) [Size: 296]
/stats                (Status: 301) [Size: 313] [--> http://10.13.1.36/stats/]
/test                 (Status: 301) [Size: 312] [--> http://10.13.1.36/test/]
/tikiwiki             (Status: 301) [Size: 316] [--> http://10.13.1.36/tikiwiki/]
/twiki                (Status: 301) [Size: 313] [--> http://10.13.1.36/twiki/]
/wp-contents          (Status: 301) [Size: 319] [--> http://10.13.1.36/wp-contents/]
Progress: 20476 / 20477 (100.00%)
===============================================================
Finished
===============================================================

┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ cat gobuster_p80.txt | wc -l

16
```

2. What is the version of apache?
   Your response



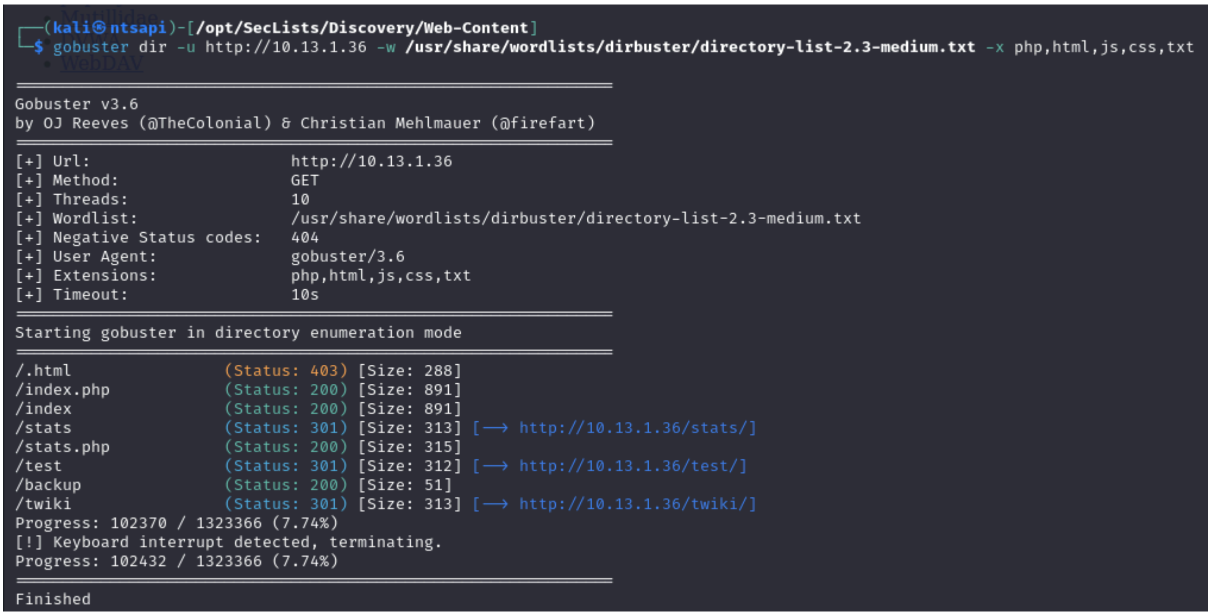
```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ curl -I http://10.13.1.36
HTTP/1.1 200 OK
Date: Fri, 14 Jun 2024 07:34:44 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

3. What is the version of php ?
   Your response



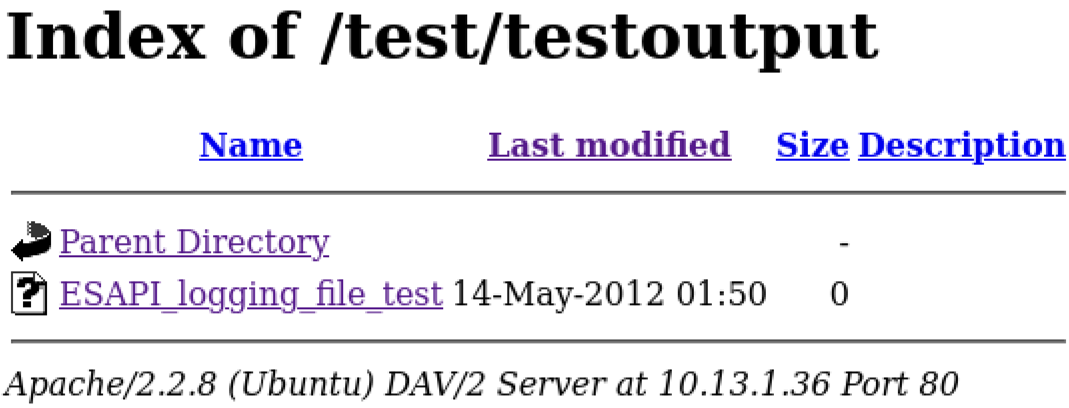
```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ curl -I http://10.13.1.36
HTTP/1.1 200 OK
Date: Fri, 14 Jun 2024 07:34:44 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

4. What server extension is installed?
   Your response: .php



```
┌──(kali㉿ntsapi)-[/opt/SecLists/Discovery/Web-Content]
└─$ gobuster dir -u http://10.13.1.36 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,js,css,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.13.1.36
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,js,css,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 288]
/index.php            (Status: 200) [Size: 891]
/index                (Status: 200) [Size: 891]
/stats                (Status: 301) [Size: 313] [--> http://10.13.1.36/stats/]
/stats.php            (Status: 200) [Size: 315]
/test                 (Status: 301) [Size: 312] [--> http://10.13.1.36/test/]
/backup               (Status: 200) [Size: 51]
/twiki                (Status: 301) [Size: 313] [--> http://10.13.1.36/twiki/]
Progress: 102370 / 1323366 (7.74%)
[!] Keyboard interrupt detected, terminating.
Progress: 102432 / 1323366 (7.74%)
===============================================================
Finished
```

5. What is the name of the file in testoutput?
   Your response

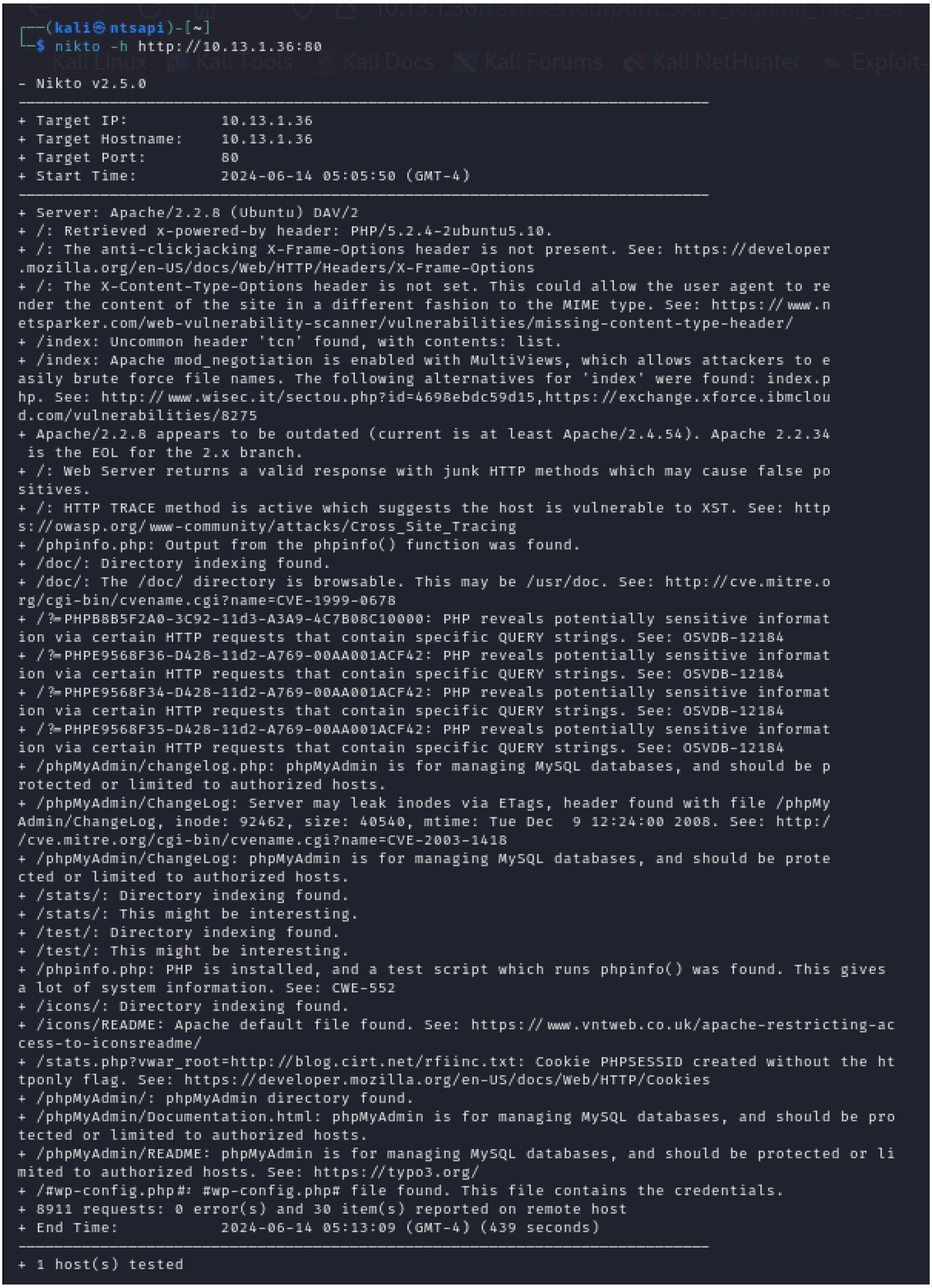


Index of /test/testoutput

Name	Last modified	Size	Description
Parent Directory		-	
ESAPI_logging_file_test	14-May-2012 01:50	0	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.13.1.36 Port 80

6. Do a scan with Nikto on port 80.
   Your response:

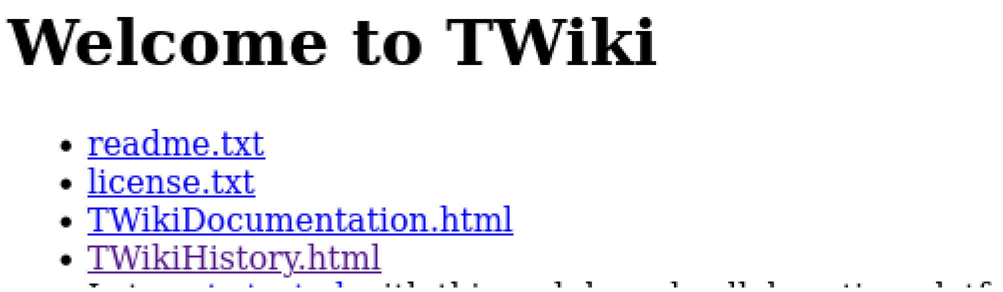


```
┌──(kali㉿ntsapi)-[~]
└─$ nikto -h http://10.13.1.36:80

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.13.1.36
+ Target Hostname:    10.13.1.36
+ Target Port:        80
+ Start Time:         2024-06-14 05:05:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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 re
nder the content of the site in a different fashion to the MIME type. See: https://www.n
etsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
asily brute force file names. The following alternatives for 'index' were found: index.p
hp. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmclou
d.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34
 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false po
sitives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: http
s://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.o
rg/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be p
rotected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMy
Admin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http:/
/cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be prote
cted or limited to authorized hosts.
+ /stats/: Directory indexing found.
+ /stats/: This might be interesting.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives
a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-ac
cess-to-iconsreadme/
+ /stats.php?vwar_root=http://blog.cirt.net/rfiinc.txt: Cookie PHPSESSID created without the ht
tponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be pro
tected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or li
mited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8911 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2024-06-14 05:13:09 (GMT-4) (439 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

An informative file in php seems to be available, what is its name?

+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552

7. What application has a name that starts with T and ends with Y?
Your response:**TwikiHistory**



Welcome to TWiki

- readme.txt
- license.txt
- TWikiDocumentation.html
- TWikiHistory.html

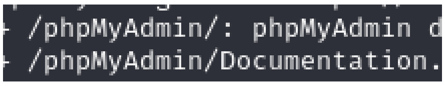
8. What curl command can you use to see the server version?
   Your response:

   curl -I http://10.13.1.36

9. What tool for enumerating files does it do recursively? (By default)
   Your response: ffuf

   ffuf -w /opt/SecLists/Discovery/Web-Content/big.txt -u http://10.13.1.36/FUZZ -recursion -recursion-depth 1

10. What other administration application is currently also on port 80?
    Your response:



```
| /phpMyAdmin/: phpMyAdmin d
| /phpMyAdmin/Documentation.
```