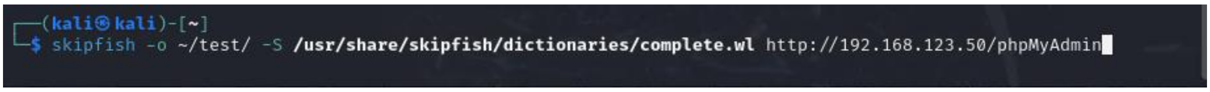
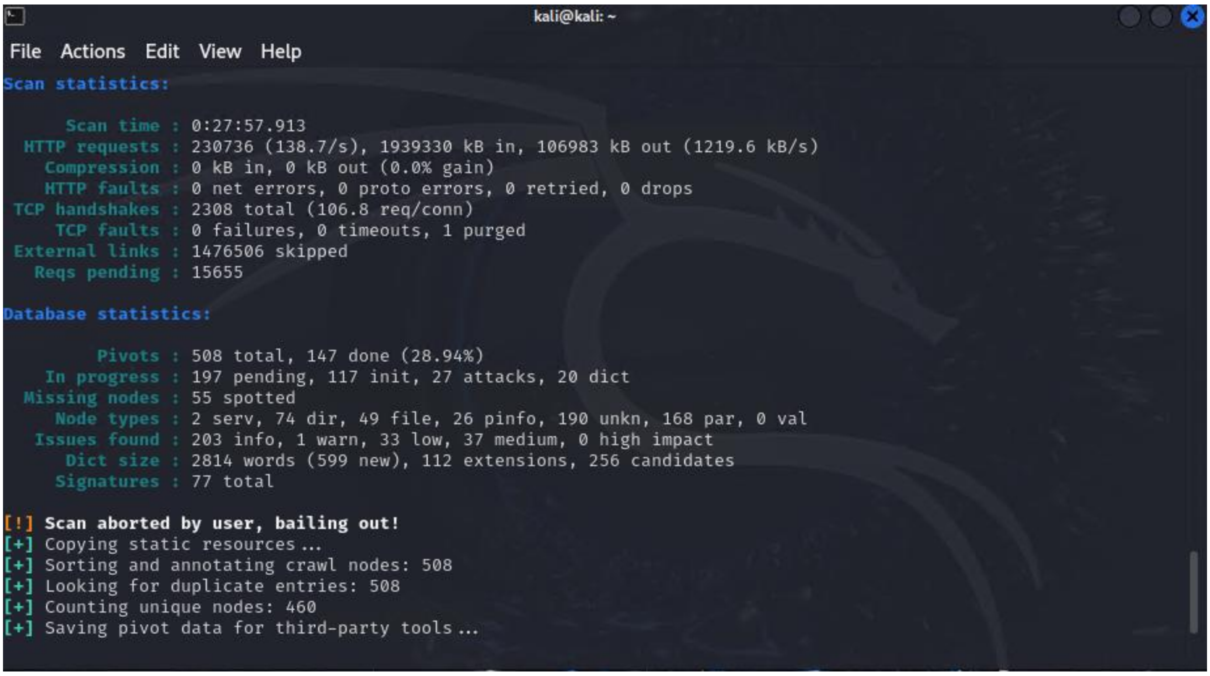
Lab 1



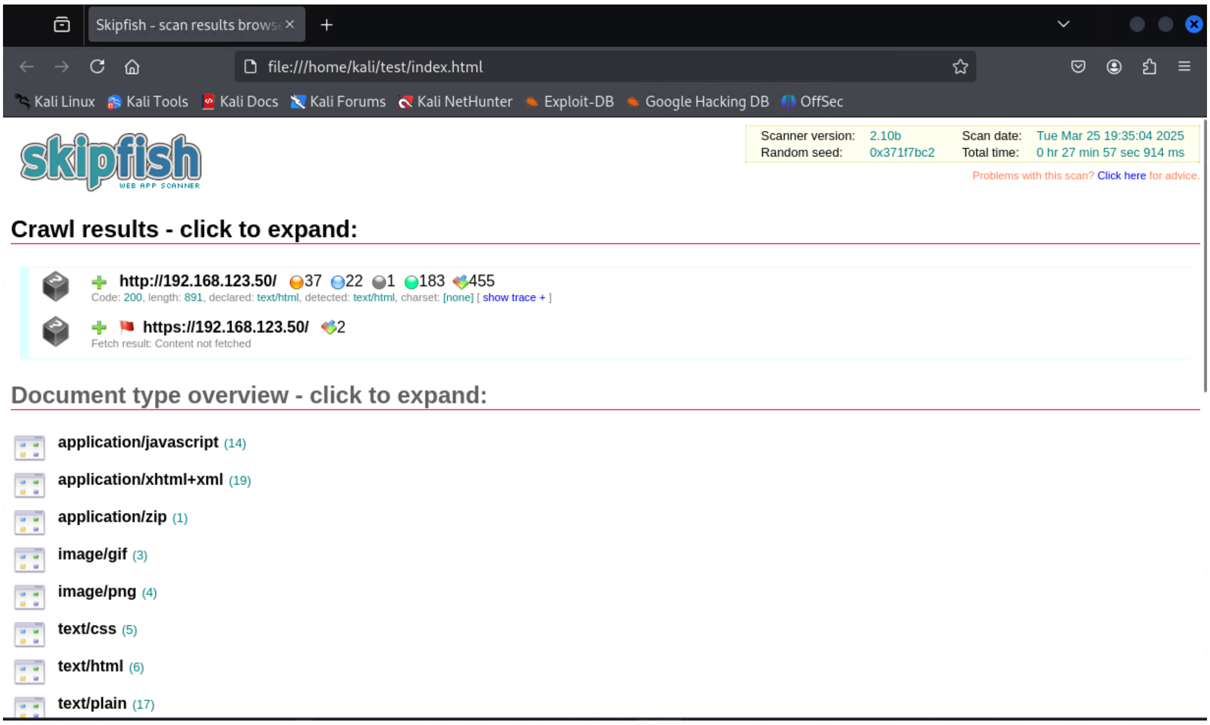
```
┌──(kali㉿kali)-[~]
└─$ skipfish -o ~/test/ -S /usr/share/skipfish/dictionaries/complete.wl http://192.168.123.50/phpMyAdmin
```

Ran skip fish towards jcu eh lab



```
Scan statistics:

      Scan time : 0:27:57.913
  HTTP requests : 230736 (138.7/s), 1939330 kB in, 106983 kB out (1219.6 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 2308 total (106.8 req/conn)
     TCP faults : 0 failures, 0 timeouts, 1 purged
 External links : 1476506 skipped
   Reqs pending : 15655

Database statistics:

         Pivots : 508 total, 147 done (28.94%)
    In progress : 197 pending, 117 init, 27 attacks, 20 dict
  Missing nodes : 55 spotted
     Node types : 2 serv, 74 dir, 49 file, 26 pinfo, 190 unkn, 168 par, 0 val
   Issues found : 203 info, 1 warn, 33 low, 37 medium, 0 high impact
      Dict size : 2814 words (599 new), 112 extensions, 256 candidates
     Signatures : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 508
[+] Looking for duplicate entries: 508
[+] Counting unique nodes: 460
[+] Saving pivot data for third-party tools...
```

Took longer than estimated time, I exited manually



Scanner version: 2.10b Scan date: Tue Mar 25 19:35:04 2025
Random seed: 0x371f7bc2 Total time: 0 hr 27 min 57 sec 914 ms

Problems with this scan? Click here for advice.

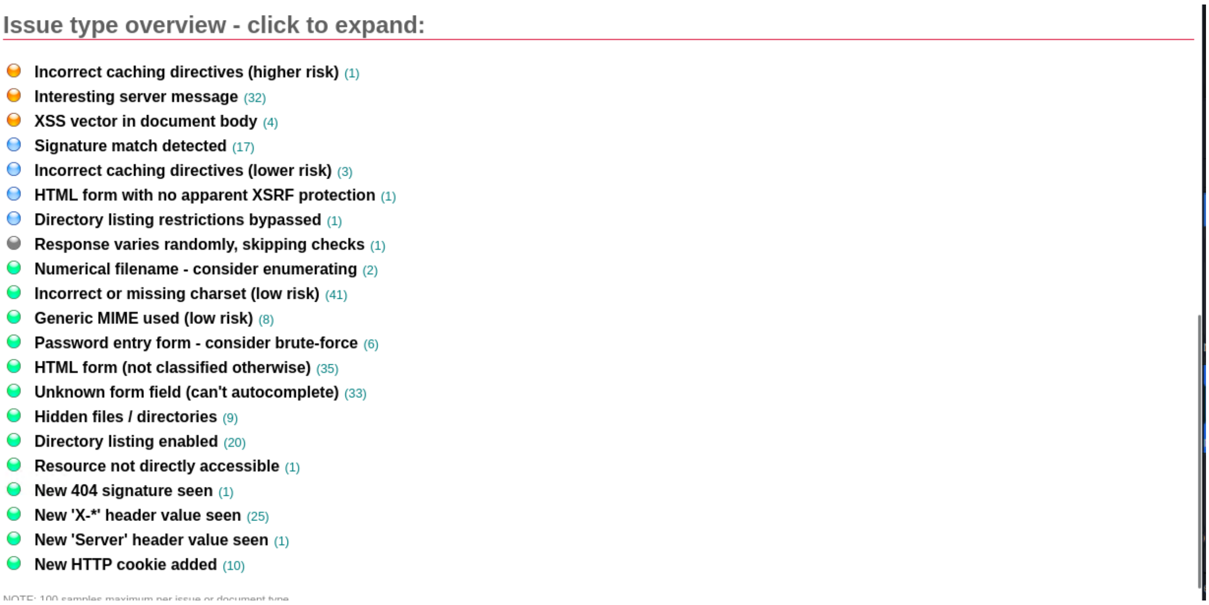
Crawl results - click to expand:

http://192.168.123.50/ 37 22 1 183 455
Code: 200, length: 891, declared: text/html, detected: text/html, charset: [none] [show trace +]

https://192.168.123.50/ 2
Fetch result: Content not fetched

Document type overview - click to expand:

application/javascript (14)
application/xhtml+xml (19)
application/zip (1)
image/gif (3)
image/png (4)
text/css (5)
text/html (6)
text/plain (17)



Issue type overview - click to expand:

- 🟠 **Incorrect caching directives (higher risk)** (1)
- 🟠 **Interesting server message** (32)
- 🟠 **XSS vector in document body** (4)
- 🔵 **Signature match detected** (17)
- 🔵 **Incorrect caching directives (lower risk)** (3)
- 🔵 **HTML form with no apparent XSRF protection** (1)
- 🔵 **Directory listing restrictions bypassed** (1)
- ⚫ **Response varies randomly, skipping checks** (1)
- 🟢 **Numerical filename - consider enumerating** (2)
- 🟢 **Incorrect or missing charset (low risk)** (41)
- 🟢 **Generic MIME used (low risk)** (8)
- 🟢 **Password entry form - consider brute-force** (6)
- 🟢 **HTML form (not classified otherwise)** (35)
- 🟢 **Unknown form field (can't autocomplete)** (33)
- 🟢 **Hidden files / directories** (9)
- 🟢 **Directory listing enabled** (20)
- 🟢 **Resource not directly accessible** (1)
- 🟢 **New 404 signature seen** (1)
- 🟢 **New 'X-*' header value seen** (25)
- 🟢 **New 'Server' header value seen** (1)
- 🟢 **New HTTP cookie added** (10)

NOTE: 100 samples maximum per issue or document type.

These screenshots are result of scan

Findings are

Incorrect caching directives: Can lead to sensitive data being stored in cache

XSS vector in document body: May indicate possible Cross-Site Scripting vulnerabilities

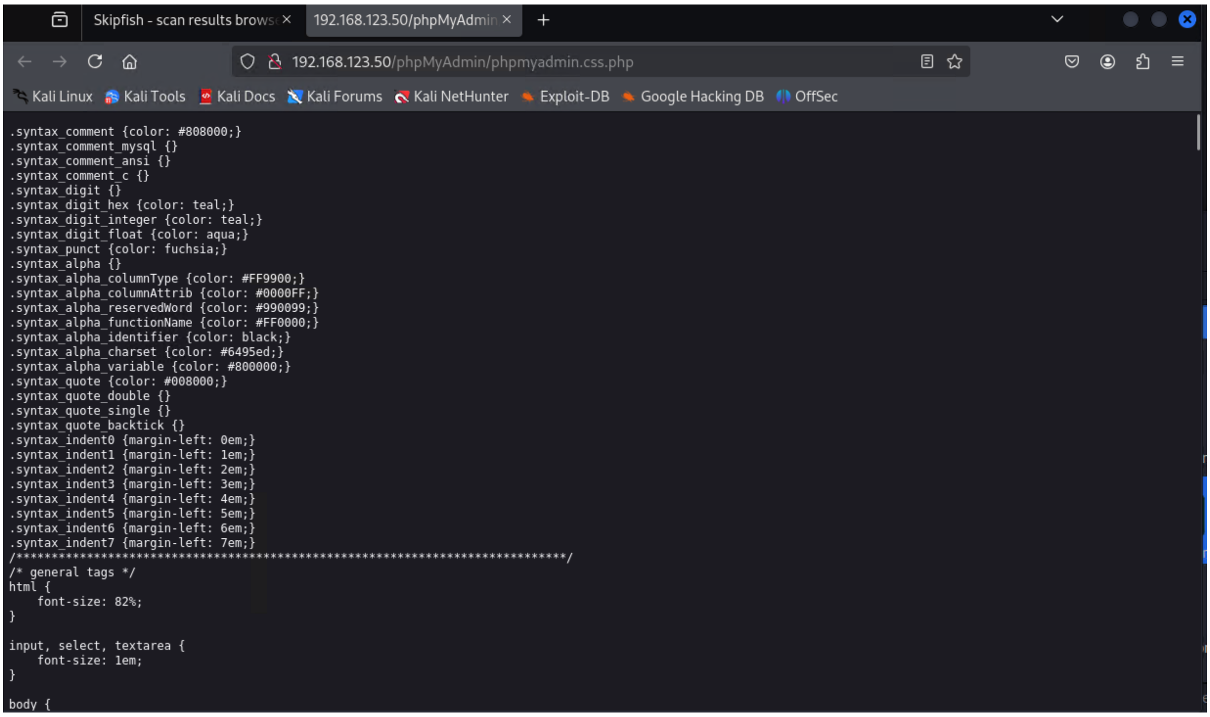
Interesting server messages: May leak information about server config or behaviour

Directory listing enabled: Exposes internal file structure, which attackers can use to gather more intel

Hidden files/directories: These could be forgotten or sensitive files unintentionally exposed

Password entry forms: May be brute-forceable or improperly secured

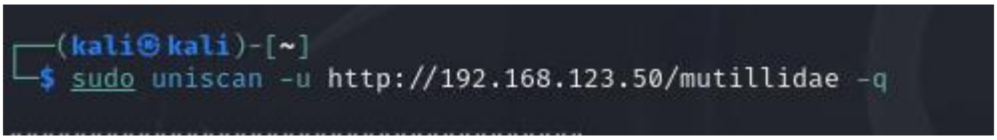
No XSRF protection in an HTML form: Puts the server at risk of Cross-Site Request Forgery


Skipfish - scan results brows
192.168.123.50/phpMyAdmin
192.168.123.50/phpMyAdmin/phpmyadmin.css.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
.syntax_comment {color: #808000;}
.syntax_comment_mysql {}
.syntax_comment_ansi {}
.syntax_comment_c {}
.syntax_digit {}
.syntax_digit_hex {color: teal;}
.syntax_digit_integer {color: teal;}
.syntax_digit_float {color: aqua;}
.syntax_punct {color: fuchsia;}
.syntax_alpha {}
.syntax_alpha_columnType {color: #FF9900;}
.syntax_alpha_columnAttrib {color: #0000FF;}
.syntax_alpha_reservedWord {color: #990099;}
.syntax_alpha_functionName {color: #FF0000;}
.syntax_alpha_identifier {color: black;}
.syntax_alpha_charset {color: #6495ed;}
.syntax_alpha_variable {color: #800000;}
.syntax_quote {color: #008000;}
.syntax_quote_double {}
.syntax_quote_single {}
.syntax_quote_backtick {}
.syntax_indent0 {margin-left: 0em;}
.syntax_indent1 {margin-left: 1em;}
.syntax_indent2 {margin-left: 2em;}
.syntax_indent3 {margin-left: 3em;}
.syntax_indent4 {margin-left: 4em;}
.syntax_indent5 {margin-left: 5em;}
.syntax_indent6 {margin-left: 6em;}
.syntax_indent7 {margin-left: 7em;}
/******************************************************************************/
/* general tags */
html {
    font-size: 82%;
}

input, select, textarea {
    font-size: 1em;
}

body {
```

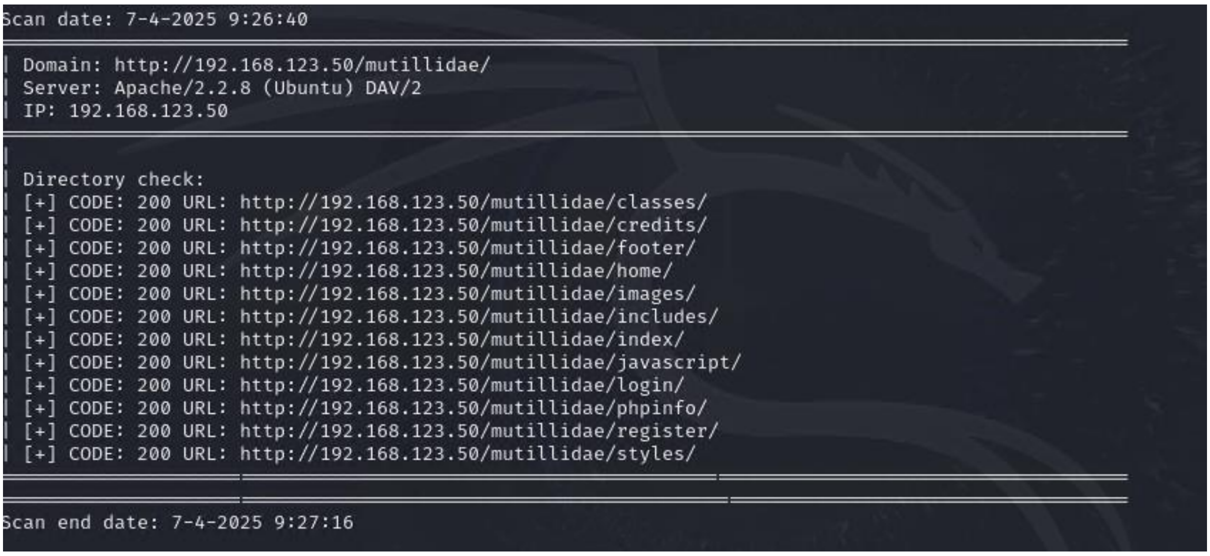
In the content of incorrect caching directive, the css format is visible showing incorrect caching

Lab 2



```
┌──(kali㉿kali)-[~]
└─$ sudo uniscan -u http://192.168.123.50/mutillidae -q
```

Ran uniscan -q on eh lab



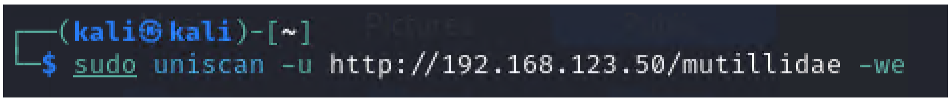
```
Scan date: 7-4-2025 9:26:40
═══════════════════════════════════════════════════════════════════════════
| Domain: http://192.168.123.50/mutillidae/
| Server: Apache/2.2.8 (Ubuntu) DAV/2
| IP: 192.168.123.50
═══════════════════════════════════════════════════════════════════════════
|
| Directory check:
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/classes/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/credits/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/footer/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/home/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/images/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/includes/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/index/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/javascript/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/login/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/phpinfo/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/register/
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/styles/
═══════════════════════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════════════════════
Scan end date: 7-4-2025 9:27:16
```

Uniscan found several open folders on the website, like /phpinfo/, /login/, and /register/.

These could be used to find more information or weaknesses during a security test

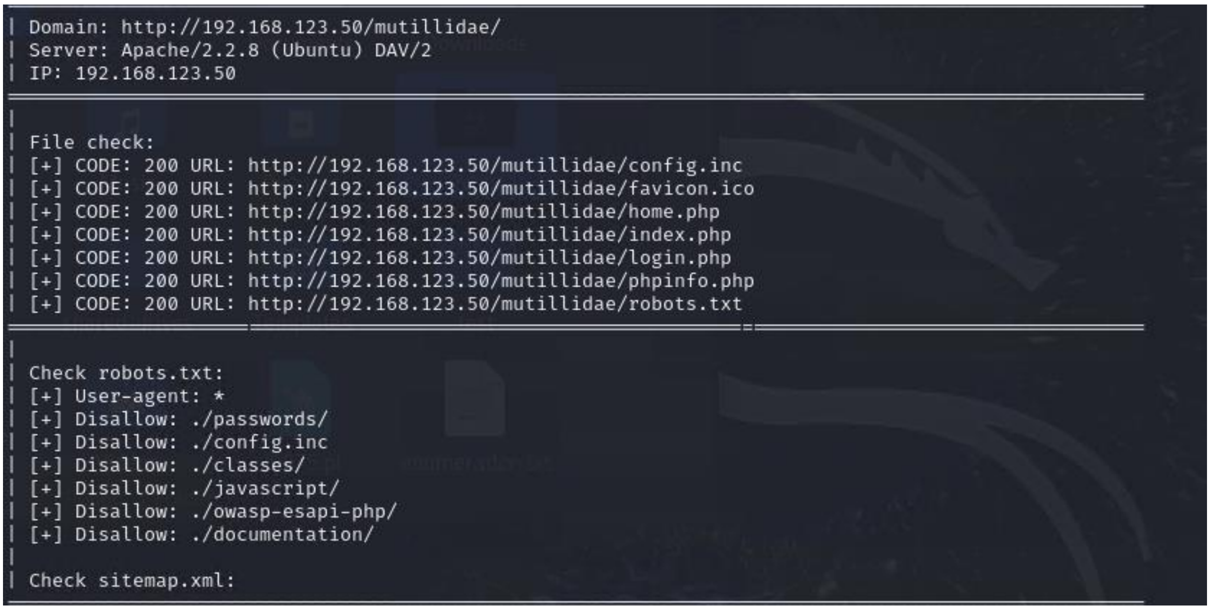
The /phpinfo/ page is especially risky because it can show details about the server

This kind of scan helps spot areas that might need better protection



```
┌──(kali㉿kali)-[~]
└─$ sudo uniscan -u http://192.168.123.50/mutillidae -we
```

Ran -we scan



```
| Domain: http://192.168.123.50/mutillidae/
| Server: Apache/2.2.8 (Ubuntu) DAV/2
| IP: 192.168.123.50
================================================================
|
| File check:
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/config.inc
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/favicon.ico
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/home.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/index.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/login.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/phpinfo.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/robots.txt
================================================================
|
| Check robots.txt:
| [+] User-agent: *
| [+] Disallow: ./passwords/
| [+] Disallow: ./config.inc
| [+] Disallow: ./classes/
| [+] Disallow: ./javascript/
| [+] Disallow: ./owasp-esapi-php/
| [+] Disallow: ./documentation/
|
| Check sitemap.xml:
================================================================
```

The -we scan found several important files like /config.inc, /login.php, and /phpinfo.php. It also found a robots.txt file which listed restricted paths like /passwords/ and /config.inc/. These hidden or sensitive directories might contain sensitive data or vulnerabilities and are good targets for further exploit