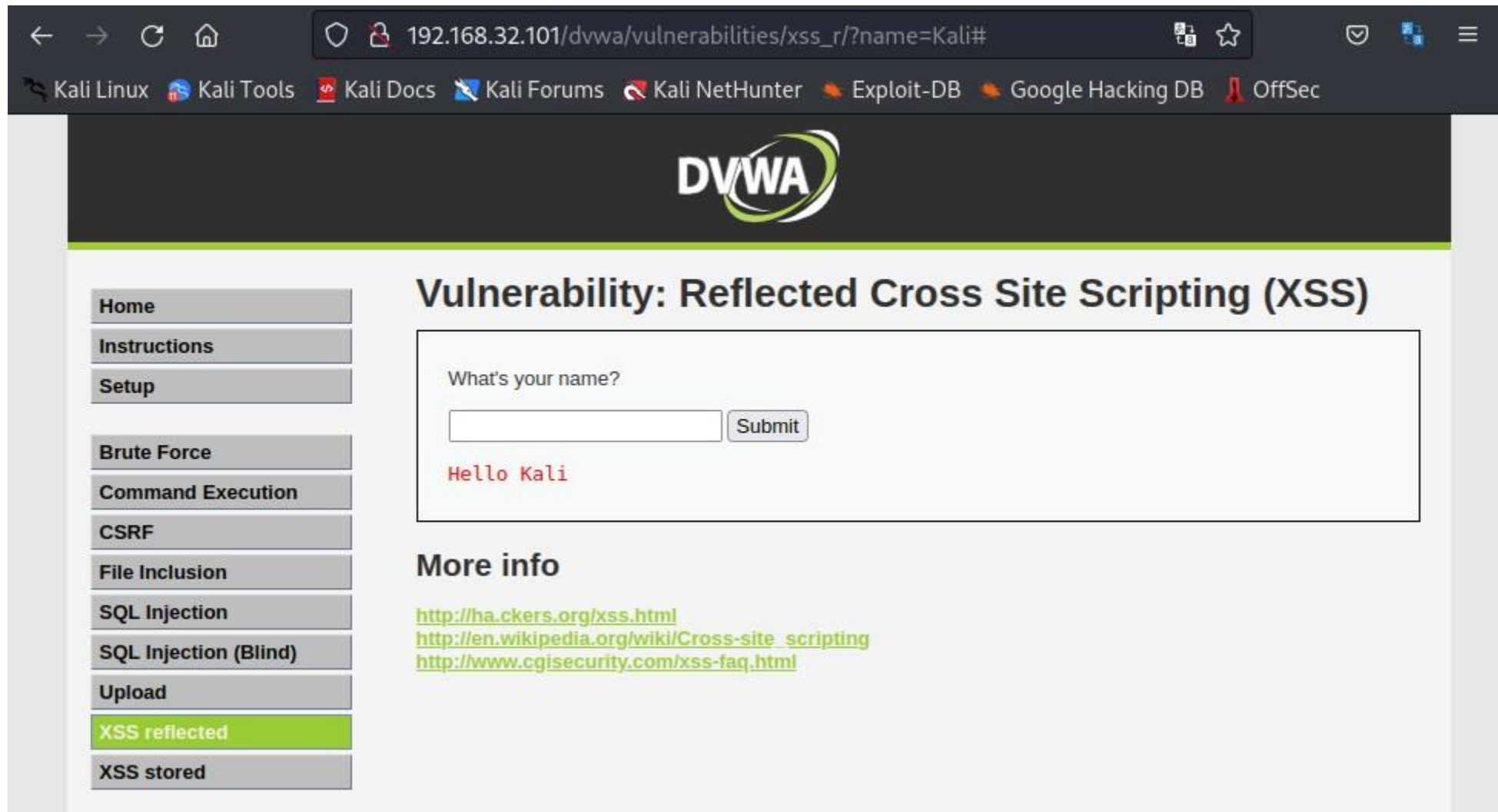


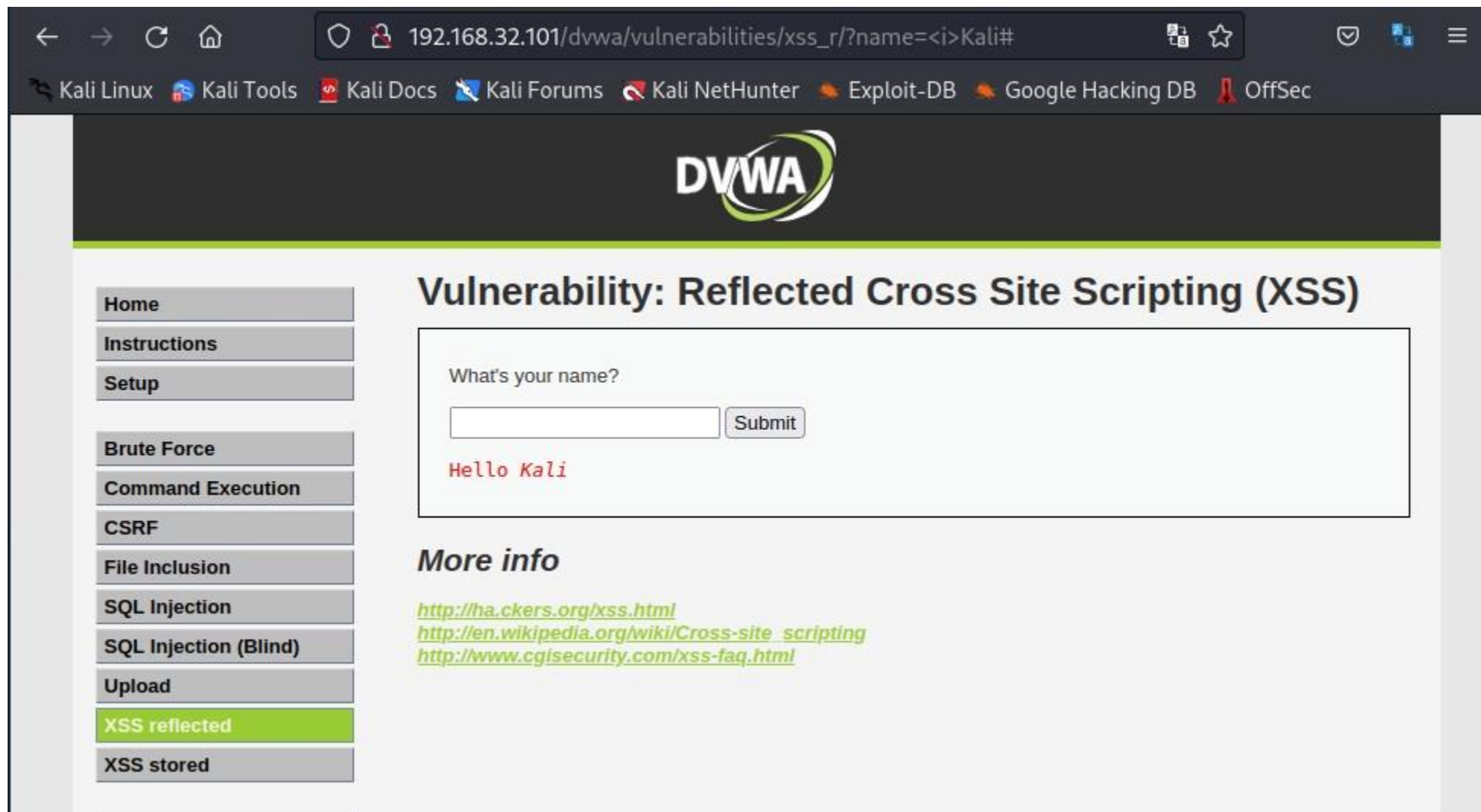
Exploit VM Metasploitable da VM Kali

XSS reflected e SQL Injection



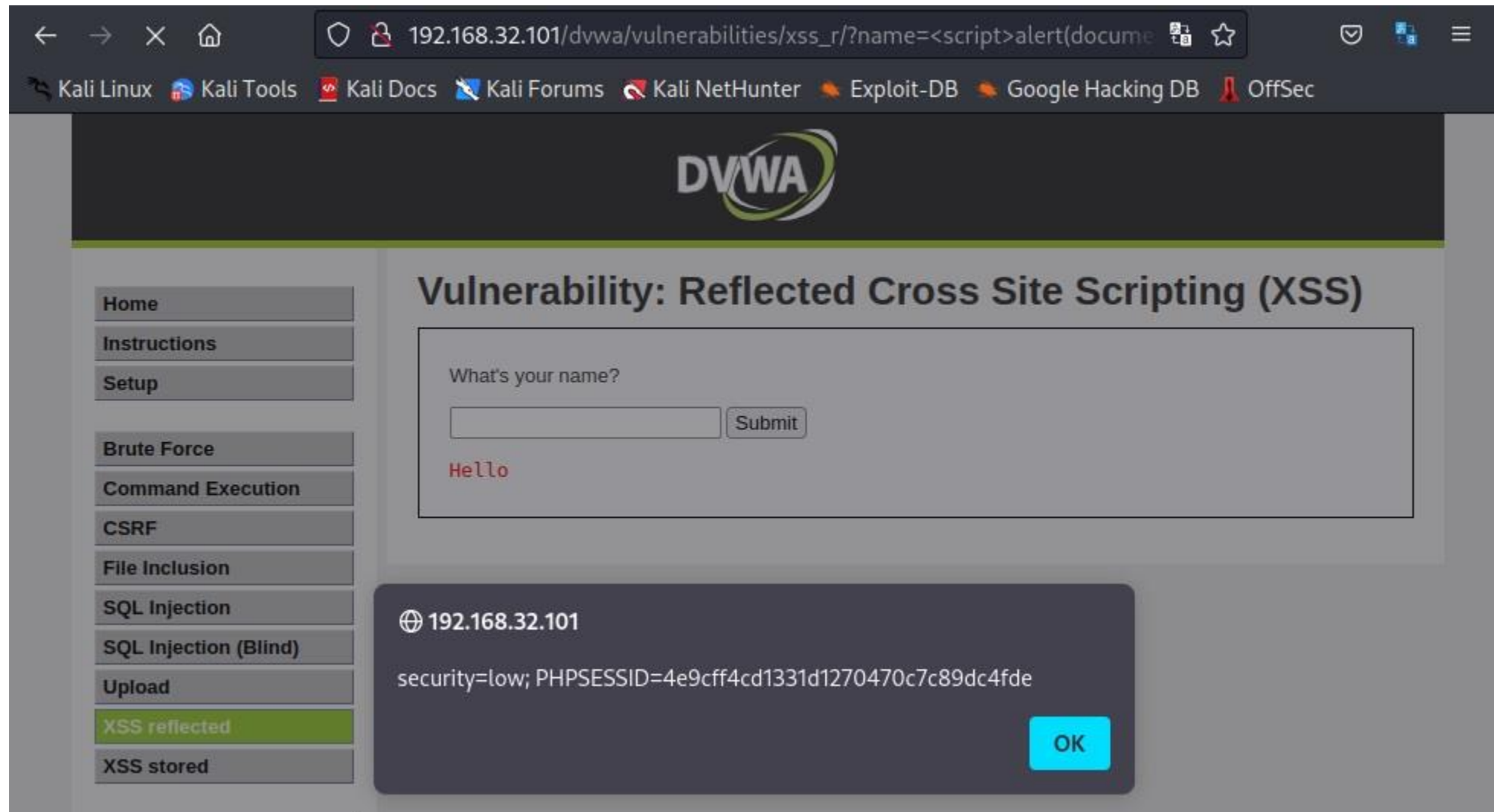
XSS reflected (part. 1)

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione XSS reflected, premendo qualsiasi carattere, in questo caso digitando: *Kali*, nel campo What's your name?, e cliccando il pulsante Submit, o premendo Invio, nell'URL della Web App, si nota l'aggiunta della stringa: *?name=Kali#*, per mezzo di una richiesta GET.



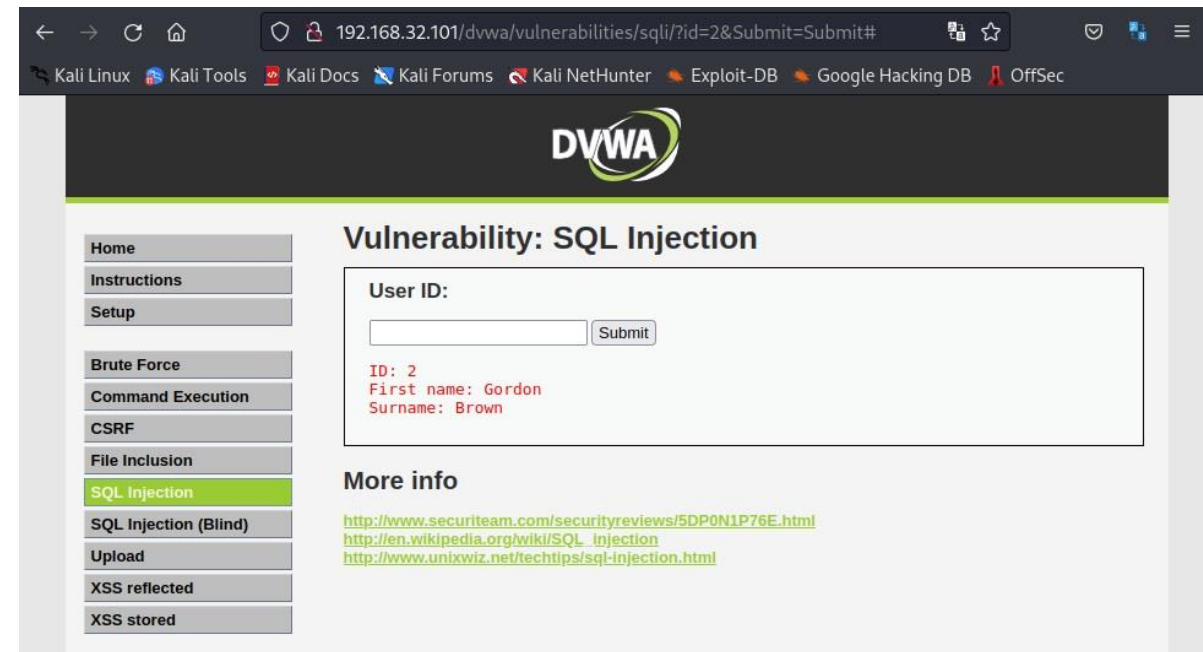
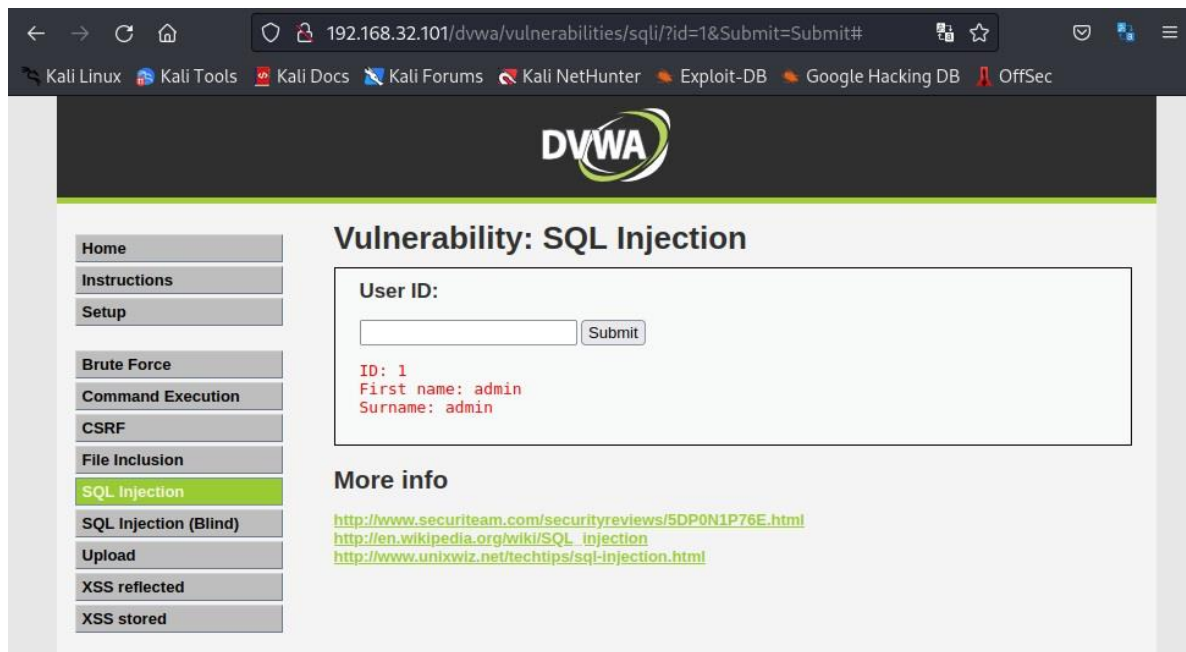
XSS reflected (part. 2)

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione XSS refected, nel campo What's your name?, si può inserire del codice HTML e sfruttare le vulnerabilità XSS per attaccare gli utenti di un sito. In questo caso, digitando: `<i>Kali`, e cliccando il pulsante Submit, viene restituito come output una stringa in corsivo e, nell'URL della Web App, si nota l'aggiunta della stringa: `?name=<i>Kali#`, dove il tag `<i>` consente di scrivere un testo in corsivo.



XSS reflected (part. 3)

Dalla VM Kali si accede alla DVWA della VM Metasploitable per inserire lo script: `<script>alert(document.cookie)</script>` e, dopo l'invio, la Web App, risponde con un cookie di allerta.




SQL Injection (part. 1)

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione SQL Injection, digitando: 1, nel campo User ID, e cliccando il pulsante Submit, o premendo Invio, la Web App, restituisce il Nome ed il Cognome dell'ID 1, mentre digitando: 2, restituisce il Nome ed il Cognome dell'ID 2.

← → ↻ 🏠 192.168.32.101/dvwa/vulnerabilities/sqli/?id=1'OR'1'%3D'1&Submit=Sub 📄 ☆ 📁 🛡️ 🌐 ☰

Kali Linux 🌐 Kali Tools 📄 Kali Docs 🌐 Kali Forums 🛡️ Kali NetHunter 🔥 Exploit-DB 🔥 Google Hacking DB 🛡️ OffSec



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

Vulnerability: SQL Injection

User ID:

Submit

ID: 1'OR'1'='1
First name: admin
Surname: admin

ID: 1'OR'1'='1
First name: Gordon
Surname: Brown

ID: 1'OR'1'='1
First name: Hack
Surname: Me

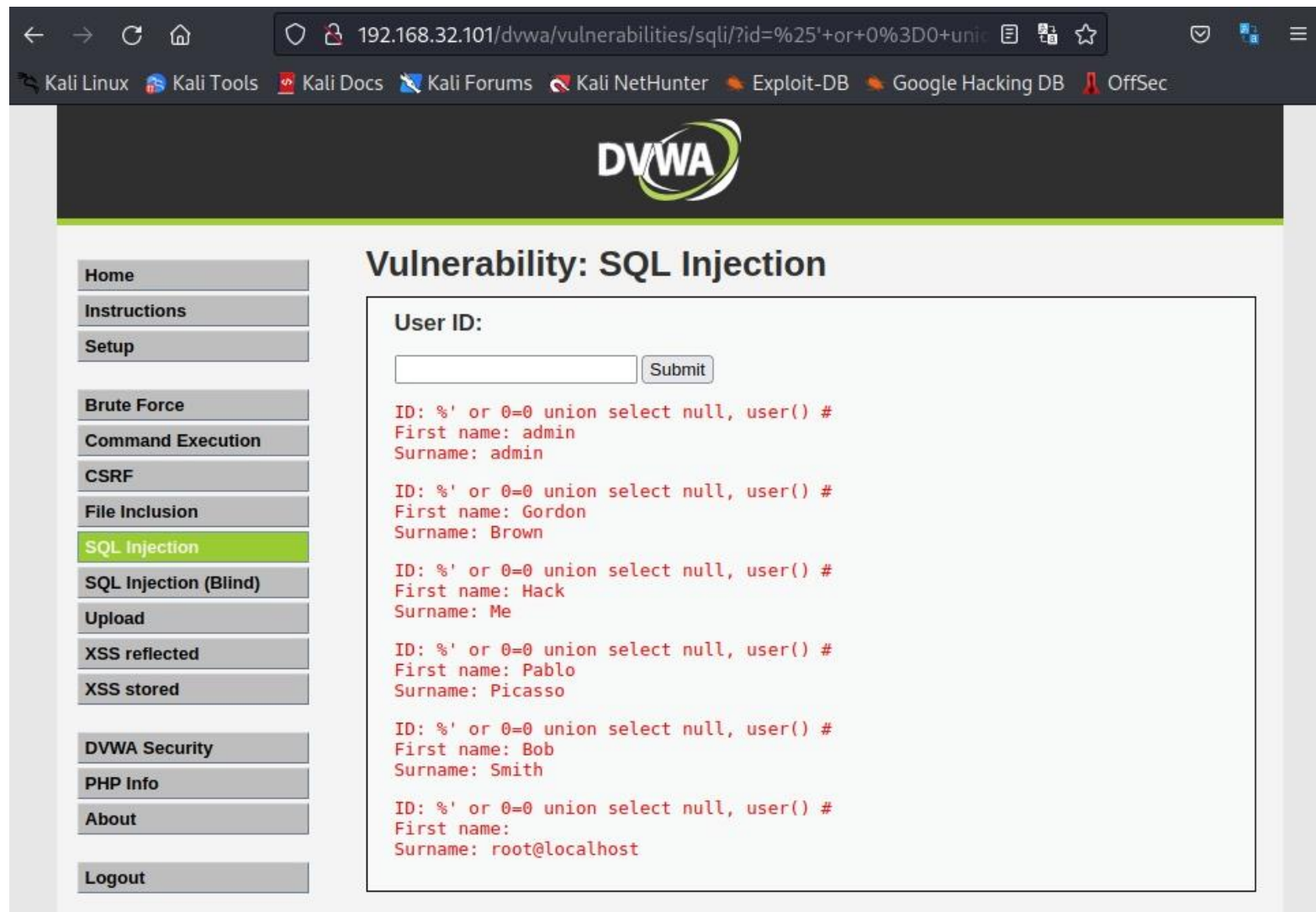
ID: 1'OR'1'='1
First name: Pablo
Surname: Picasso

ID: 1'OR'1'='1
First name: Bob
Surname: Smith

More info

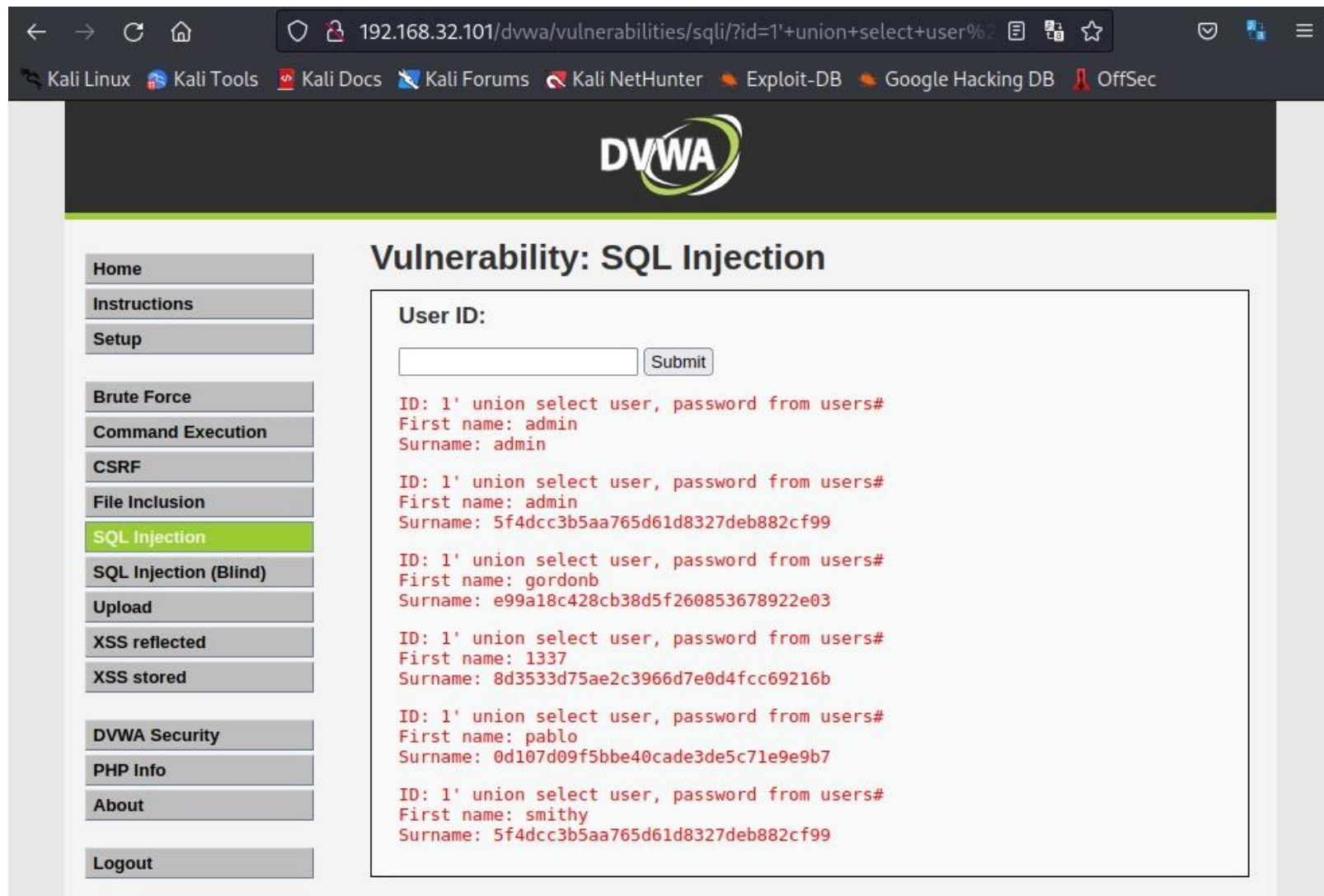
SQL Injection (part. 2)

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione SQL Injection, digitando: `1'OR'1'='1`, nel campo User ID, e cliccando il pulsante Submit, o premendo Invio, la Web App, restituisce il Nome ed il Cognome di tutti gli ID, perché, la query, restituisce tutte le entry della tabella.



SQL Injection (part. 3)

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione SQL Injection, digitando: `%' or 0=0 union select null, user() #`, nel campo User ID, e cliccando il pulsante Submit, o premendo Invio, la Web App, sfruttando le vulnerabilità di SQL, restituisce ulteriori informazioni degli utenti.



SQL Injection (part. 4)

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione SQL Injection, digitando: *1' union select user, password from users#*, nel campo User ID, e cliccando il pulsante Submit, o premendo Invio, la Web App, sfruttando le vulnerabilità di SQL, restituisce le credenziali di tutti gli utenti.