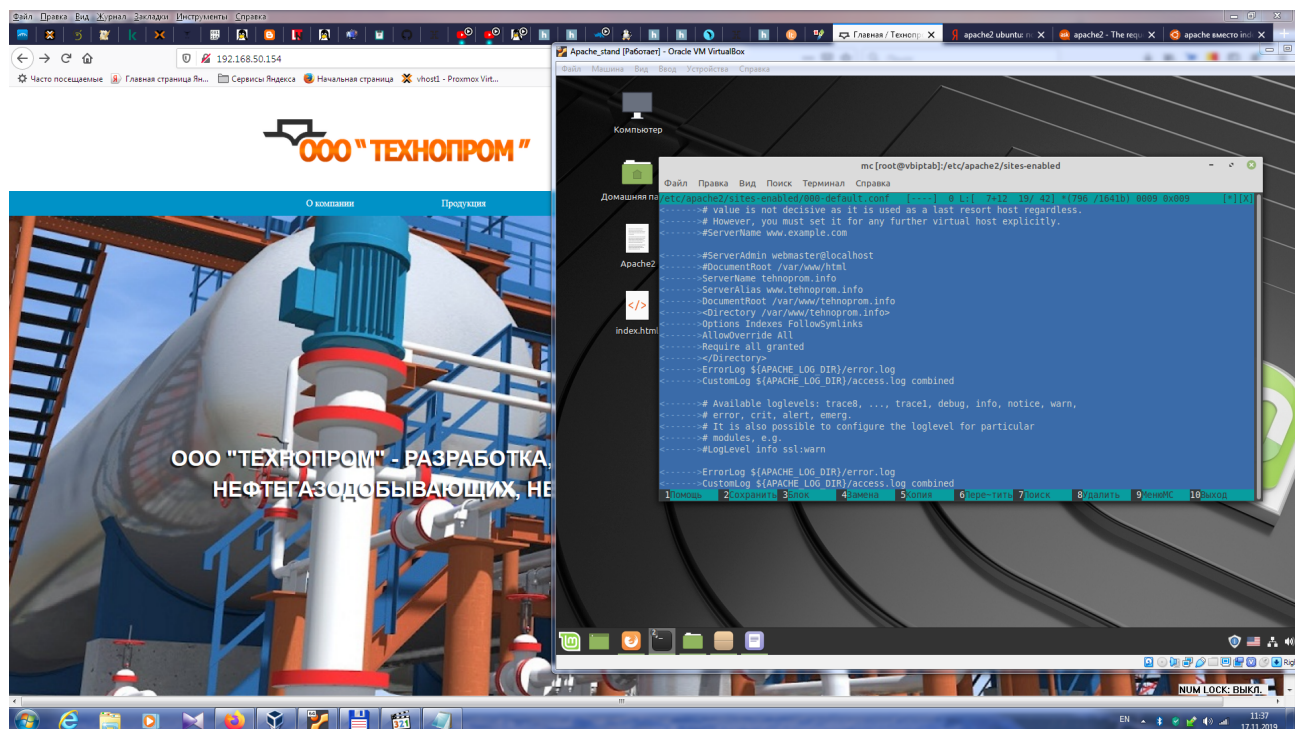
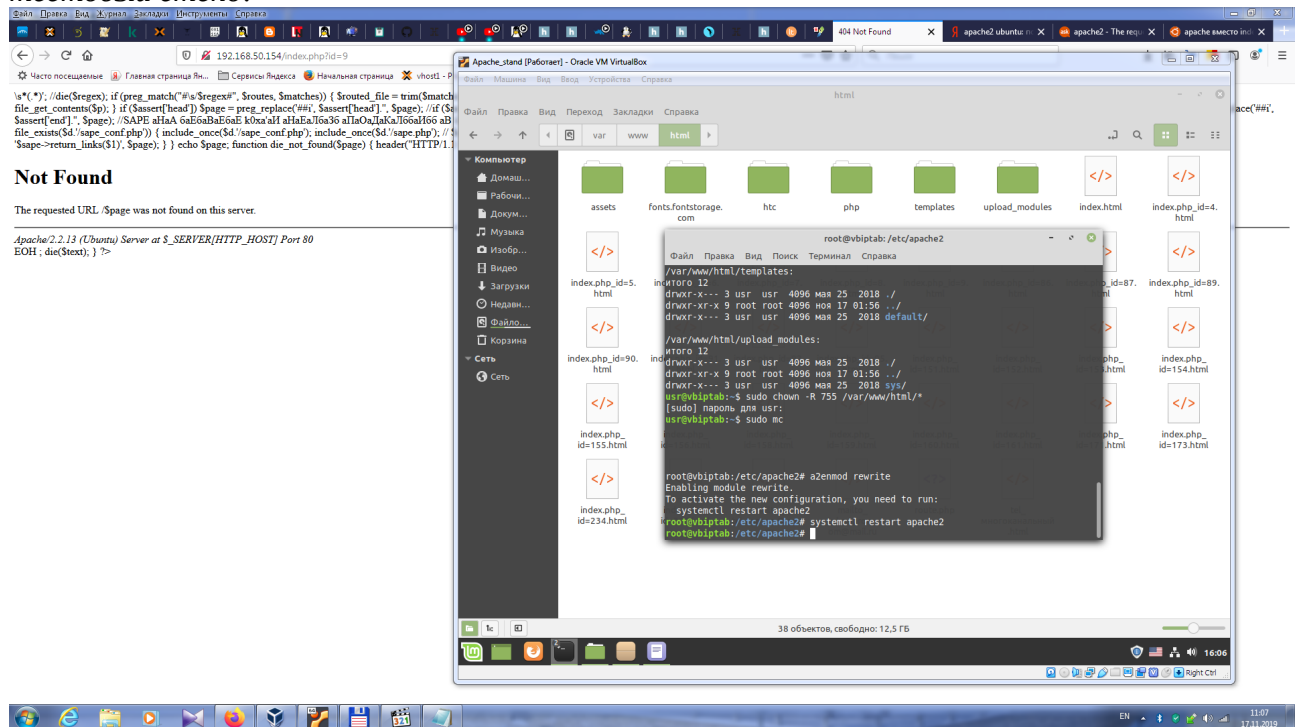


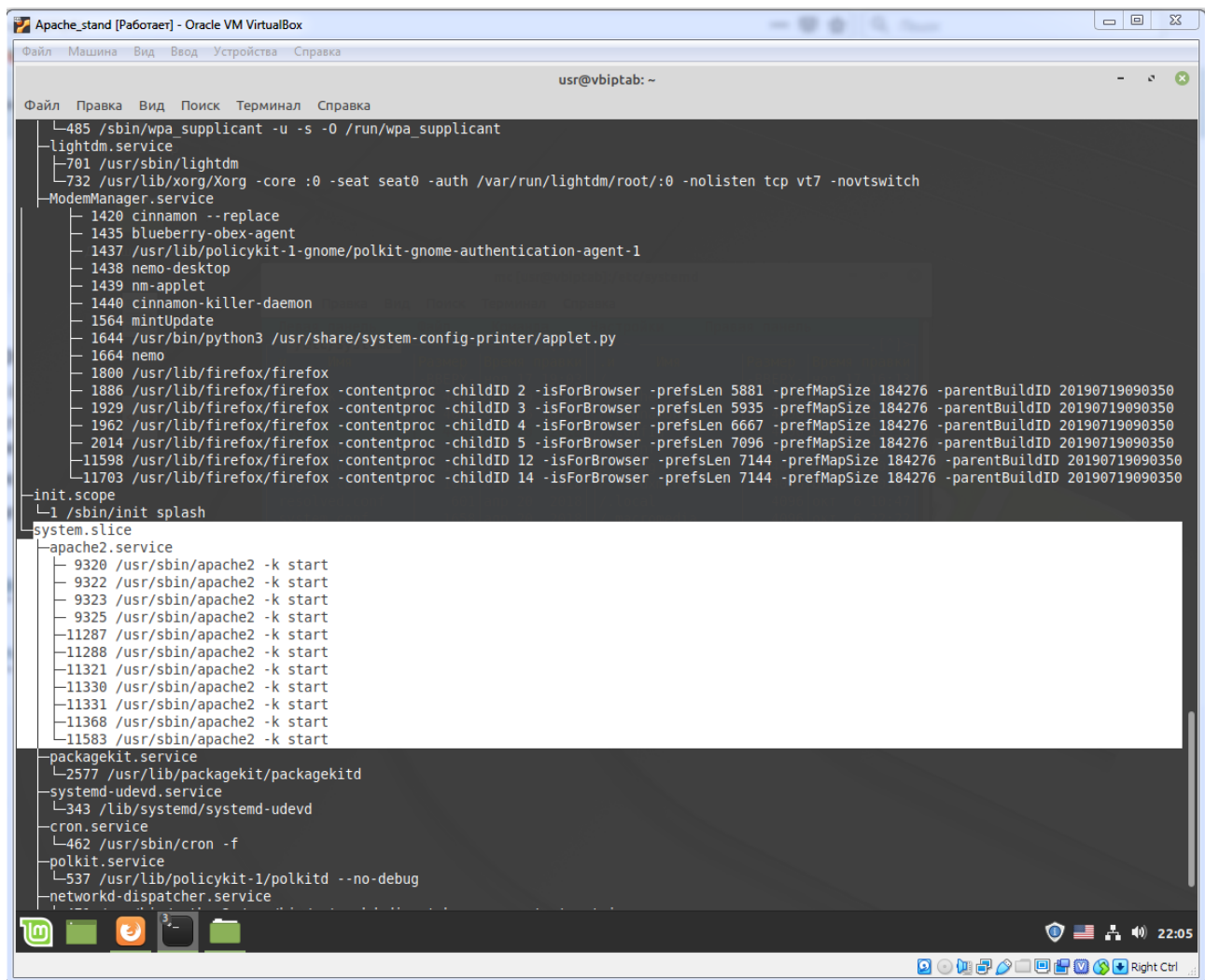
ДЗ 10

На установленный web-сервер *Apache* подключить плагины безопасности и активировать специальные настройки безопасности для внешних пользователей.

1. Подготовка

Устанавливаем, настраиваем знакомимся с веб-сервером *Apache*, разворачиваем тестовый стенд:



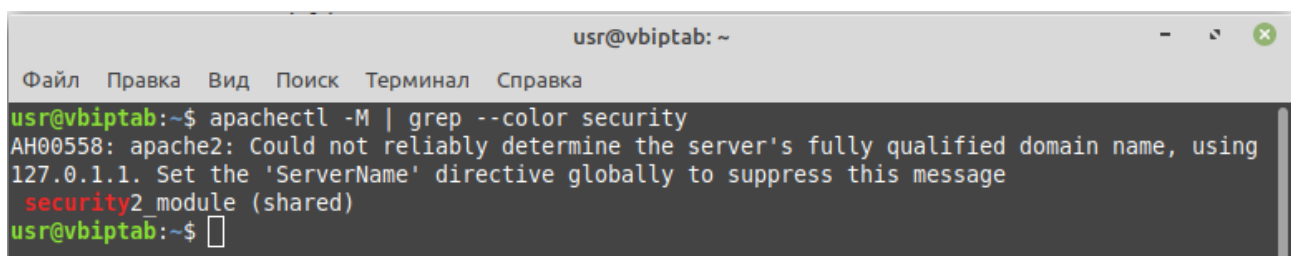


2. Установим и настроим **mod_security** на **Apache2** в **Linux Mint 19.2 "Tina"**:

`sudo apt update && sudo apt install libapache2-modsecurity`

К сожалению, данный метод установки в моём случае не выполнялся, поэтому пришлось воспользоваться запасным вариантом, и скачать установочный пакет с **pkgs.org** зато зависимости автоматом подтянулись и второй способ прошёл гладко.

`apachectl -M | grep --color security`



Установка **ModSecurity** включает в себя конфигурационный файл, который нужно переименовать:

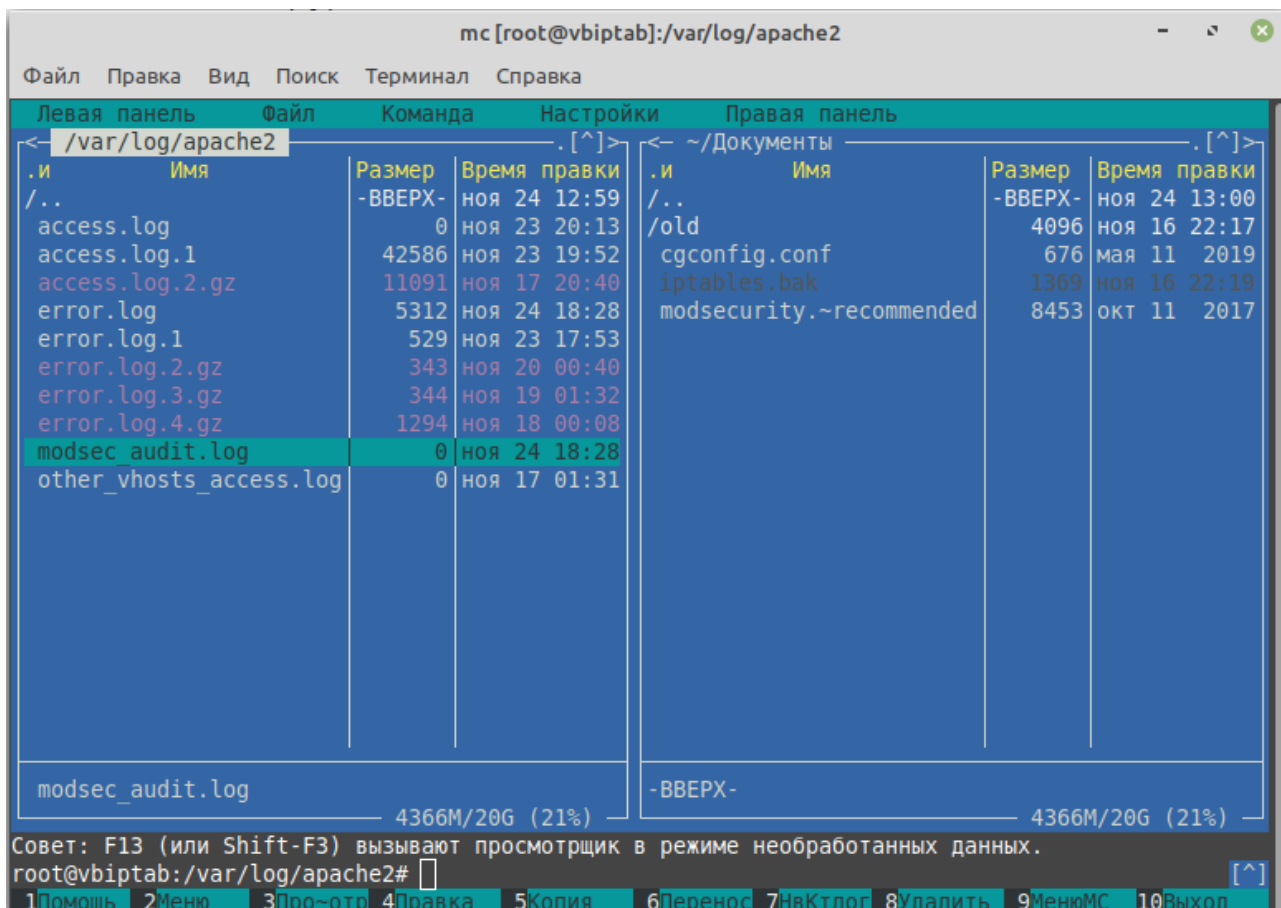
`mv /etc/modsecurity/modsecurity.conf{-recommended,}`

Затем перезапустим Apache:

```
service apache2 reload
```

```
root@vbiptab:/etc/modsecurity# mv /etc/modsecurity/modsecurity.conf{-recommended,}
root@vbiptab:/etc/modsecurity# service apache2 reload
root@vbiptab:/etc/modsecurity#
```

В каталоге логов **Apache2** будет создан новый лог-файл для **mod_security**:



3.

```
root@vbiptab:/var/log/apache2# ll modsec*.log
-rw-r----- 1 root root 0 ноя 24 18:28 modsec_audit.log
root@vbiptab:/var/log/apache2#
```

Настроим **mod_security**:

Для корректной работы установка **mod_security** «из коробки» нуждается в дополнительной настройке. Стандартный конфигурационный файл настроен на **DetectionOnly**, то есть, веб-фаервол **только отслеживает** логи, при этом **ничего не блокируя**. Чтобы изменить его поведение, отредактируем файл **modsecurity.conf**:

```
sudo mcedit /etc/modsecurity/modsecurity.conf
```

Заменяем в файле строку вида **SecRuleEngine DetectionOnly** на **SecRuleEngine On**

Примечание: при настройке **mod_security** на рабочем варианте сервера рекомендуется изменить эту директиву только после тестирования всех установленных правил.

```
mc [root@vbiptab]:/etc/modsecurity
Файл  Правка  Вид  Поиск  Терминал  Справка
/etc/modsecurity~odsecurity.conf  [----] 16 L: [ 1+ 6 7/227] *(261 /8442b) 0010 0x00A [*][X]
# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On

# -- Request body handling -----
# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "(?:application(?:/soap\+|/)|text/)xml" \
    "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"

# Enable JSON request body parser.
# Initiate JSON Processor in case of JSON content-type; change accordingly
# if your application does not use 'application/json'

1Помощь 2Сох-ить 3Блок 4Замена 5Копия 6Пер-ить 7Поиск 8Удалить 9МенюМС 10Выход
```

Директива **SecResponseBodyAccess** Отвечает за буферизацию тела ответа; ее рекомендуется включать, только если требуется обнаружение и предохранение от утечки данных. Включенная директива (**SecResponseBodyAccess On**) не только будет использовать **больше ресурсов сервера**, но **и увеличит размер лог-файла**, следовательно, ее желательно отключить. Для этого заменим «**SecResponseBodyAccess On**» на «**SecResponseBodyAccess Off**»

```
# -- Response body handling -----
# Allow ModSecurity to access response bodies..
# You should have this directive enabled in order to identify errors
# and data leakage issues.
#
# Do keep in mind that enabling this directive does increases both
# memory consumption and response latency.
#
SecResponseBodyAccess Off

# Which response MIME types do you want to inspect? You should adjust the
# configuration below to catch documents but avoid static files
# (e.g., images and archives).
#
SecResponseBodyMimeType text/plain text/html text/xml

1Помощь 2Сох-ить 3Блок 4Замена 5Копия 6Пер-ить 7Поиск 8Удалить 9МенюМС
```

Ограничим максимальный объем данных, который можно передать веб-приложению.
За это отвечают 2 директивы:

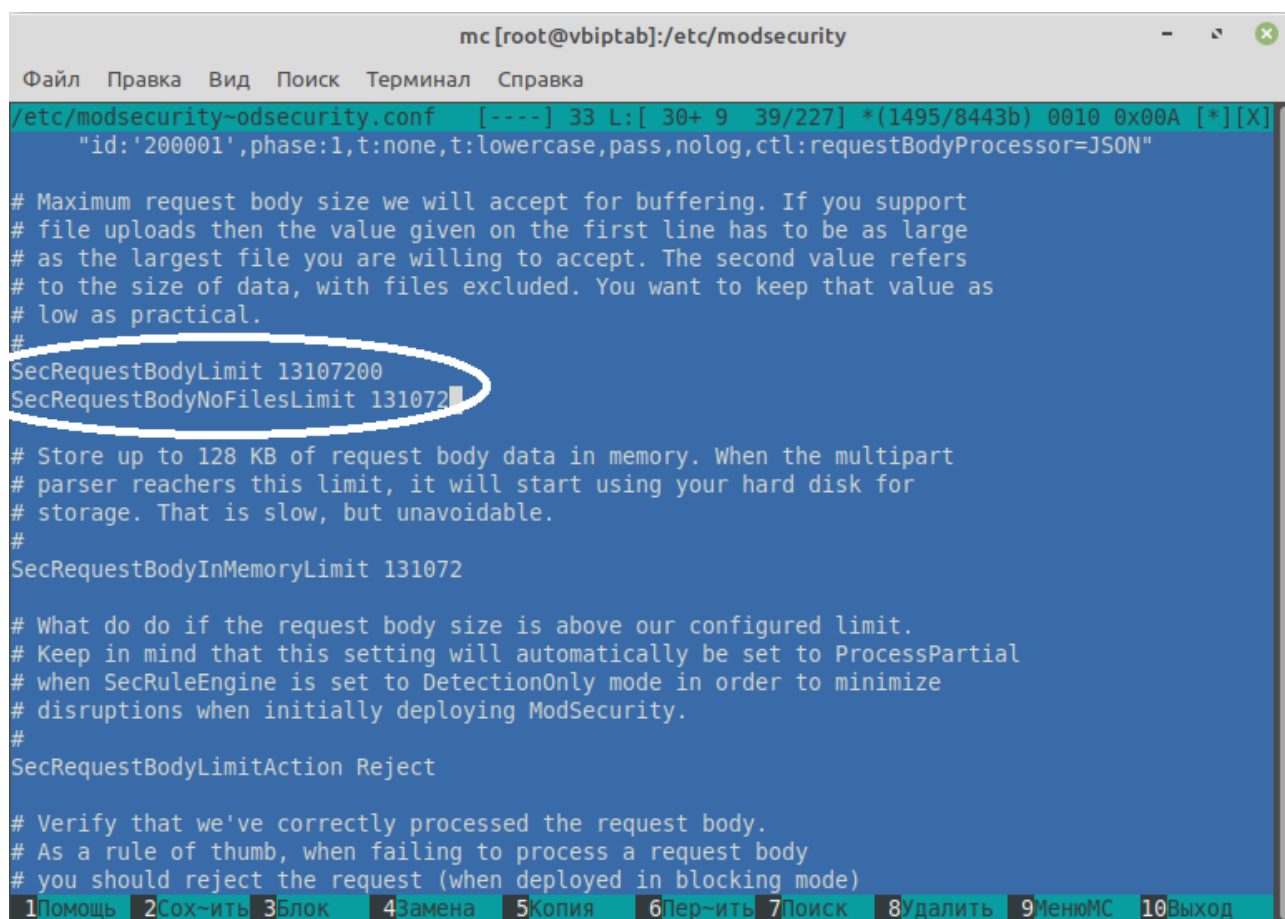
SecRequestBodyLimit
SecRequestBodyNoFilesLimit

Директива **SecRequestBodyLimit** задает максимальный размер данных **POST**. Если клиент отправляет больше данных, сервер выдаст ошибку **413 Request Entity Too Large**.
Если в веб-приложении нет механизма загрузки файлов, это значение можно существенно уменьшить. В конфигурационном файле зададим следующее:

SecRequestBodyLimit 13107200

Что равно **12.5** мегабайтам.

По-анalogии работает и директива **SecRequestBodyNoFilesLimit**. Разница только в том, что данная директива ограничивает размер данных **POST** за вычетом размера файлов.



```
mc [root@vbiptab]:/etc/modsecurity
Файл  Правка  Вид  Поиск  Терминал  Справка
/etc/modsecurity~odsecurity.conf  [---] 33 L:[ 30+ 9 39/227] *(1495/8443b) 0010 0x00A [*][X]
  "id:'200001',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=JSON"

# Maximum request body size we will accept for buffering. If you support
# file uploads then the value given on the first line has to be as large
# as the largest file you are willing to accept. The second value refers
# to the size of data, with files excluded. You want to keep that value as
# low as practical.
#
SecRequestBodyLimit 13107200
SecRequestBodyNoFilesLimit 131072

# Store up to 128 KB of request body data in memory. When the multipart
# parser reaches this limit, it will start using your hard disk for
# storage. That is slow, but unavoidable.
#
SecRequestBodyInMemoryLimit 131072

# What do do if the request body size is above our configured limit.
# Keep in mind that this setting will automatically be set to ProcessPartial
# when SecRuleEngine is set to DetectionOnly mode in order to minimize
# disruptions when initially deploying ModSecurity.
#
SecRequestBodyLimitAction Reject

# Verify that we've correctly processed the request body.
# As a rule of thumb, when failing to process a request body
# you should reject the request (when deployed in blocking mode)
1Помощь 2Сох-ить 3Блок 4Замена 5Копия 6Пер-ить 7Поиск 8Удалить 9МенюМС 10Выход
```

Примечание: данное значение обычно устанавливается по принципу **ALARP** (англ. «**as low as reasonably practicable**»), то есть, исходя из оценки риска и задействованных ресурсов).

По умолчанию в конфигурационном файле задано:

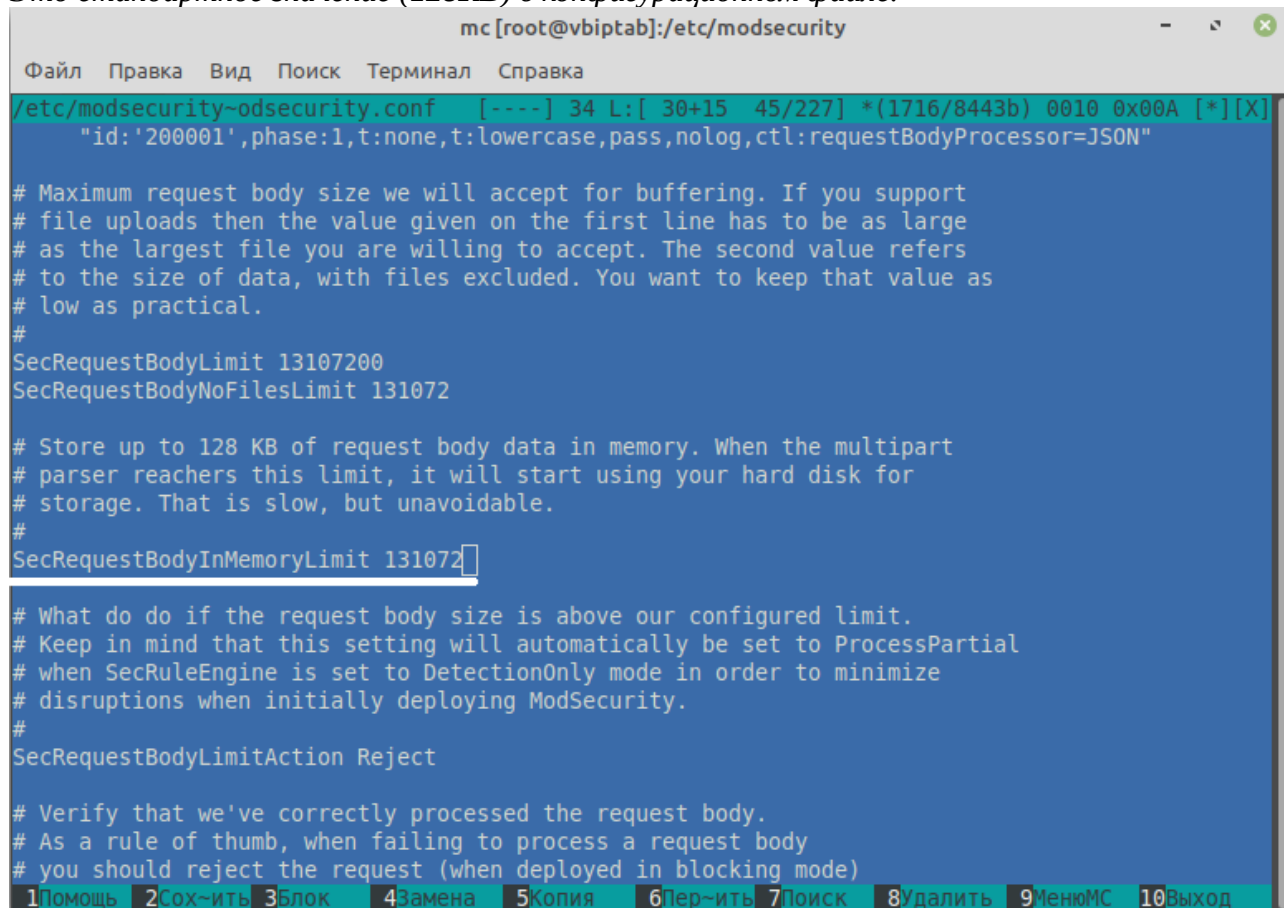
SecRequestBodyNoFilesLimit 131072

Что равно **128KB**.

В данном файле есть и еще один параметр, влияющий на производительность сервера – это **SecRequestBodyInMemoryLimit**. Этот параметр задает размер данных тела ответа, который будет помещен в RAM; остальные данные отправятся на жесткий диск (как swap). Поскольку серверы, как правило, работают на SSD, это не проблема; однако, чтобы сэкономить RAM, значение можно уменьшить.

SecRequestBodyInMemoryLimit 131072

Это стандартное значение (**128KB**) в конфигурационном файле.



```
mc [root@vbiptab]:/etc/modsecurity
Файл  Правка  Вид  Поиск  Терминал  Справка
/etc/modsecurity-odsecurity.conf  [----] 34 L:[ 30+15 45/227] *(1716/8443b) 0010 0x00A [*][X]
  "id:'200001',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=JSON"

# Maximum request body size we will accept for buffering. If you support
# file uploads then the value given on the first line has to be as large
# as the largest file you are willing to accept. The second value refers
# to the size of data, with files excluded. You want to keep that value as
# low as practical.
#
SecRequestBodyLimit 13107200
SecRequestBodyNoFilesLimit 131072

# Store up to 128 KB of request body data in memory. When the multipart
# parser reaches this limit, it will start using your hard disk for
# storage. That is slow, but unavoidable.
#
SecRequestBodyInMemoryLimit 131072

# What do do if the request body size is above our configured limit.
# Keep in mind that this setting will automatically be set to ProcessPartial
# when SecRuleEngine is set to DetectionOnly mode in order to minimize
# disruptions when initially deploying ModSecurity.
#
SecRequestBodyLimitAction Reject

# Verify that we've correctly processed the request body.
# As a rule of thumb, when failing to process a request body
# you should reject the request (when deployed in blocking mode)
1Помощь 2Сох-ить 3Блок 4Замена 5Копия 6Пер-ить 7Поиск 8Удалить 9МенюМС 10Выход
```

4. Проверим на инъекции SQL:

Прежде чем определить политику фаервола при помощи правил, попытаемся создать PHP-скрипт, уязвимый к инъекциям SQL (SQL injection).

sudo touch /var/www/tehnoprom.info/login.php

И разместим в него базовый скрипт для проверки логин скрипт PHP, как показано на рисунке ниже:

```
mc [usr@vbiptab]:/var/www/tehnoprom.info
Файл Правка Вид Поиск Терминал Справка
/var/www/tehnoprom.info/login.php [-M--] 7 L: 1+23 24/ 24] *(713 / 713b) <E0F> [*][X]
<body>
<?php
f=(isset($_POST['login']))
if ($f=='')
<----->{
<----->    $username = $_POST['username'];
<----->    $password = $_POST['password'];
<----->    $con = mysqli_connect('192.168.50.154','sa','sasa','sample');
<----->    $result = mysqli_query($con, "SELECT * FROM 'users' WHERE username='$username' AND password='$password'");
<----->    if(mysqli_num_rows($result) == 0
<----->        <----->echo 'Invalid username or password'
<----->    }.
if(mysqli_num_rows($result) == 1) echo 'Logged in A Secret forrrr you....' ;
if ($f != '')
{
<form action="" method="post">
Username: <input type="text" name="username"/><br/>
Password: <input type="password" name="password"/><br/>
<input type="submit" name="login" value="login"/>
</form>
</?php>
</body>
</html>
1 Помощь 2 Сохранить 3 Блок 4 Замена 5 Копия 6 Переместить 7 Поиск 8 Удалить 9 МенюМС 10 Выход
```

Установим и настроим MySQL, чтобы проверить работу скрипта:

```
usr@vbiptab:~$ sudo apt install mariadb-server mariadb-client
```

[sudo] пароль для usr:

Чтение списков пакетов... Готово

Построение дерева зависимостей

Чтение информации о состоянии... Готово

Будут установлены следующие дополнительные пакеты:

```
galera-3 libaiol libconfig-inifiles-perl libdbi-perl libjemalloc1
mariadb-client-10.1 mariadb-client-core-10.1 mariadb-common
mariadb-server-10.1 mariadb-server-core-10.1 mysql-common socat
```

Предлагаемые пакеты:

```
libmldbm-perl libnet-daemon-perl libsql-statement-perl mailx mariadb-test
tinyca
```

Рекомендуемые пакеты:

```
libdbd-mysql-perl libterm-readkey-perl libhtml-template-perl
```

Следующие НОВЫЕ пакеты будут установлены:

```
galera-3 libaiol libconfig-inifiles-perl libdbi-perl libjemalloc1
mariadb-client mariadb-client-10.1 mariadb-client-core-10.1 mariadb-common
mariadb-server mariadb-server-10.1 mariadb-server-core-10.1 mysql-common
```

Обновлено 0 пакетов, установлено 14 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.

Установлено или удалено не до конца 3 пакетов.

Необходимо скачать 22,7 МВ архивов.

После данной операции объем занятого дискового пространства возрастёт на 178 МВ.

Хотите продолжить? [Д/н] y

Пол:1 http://archive.ubuntu.com/ubuntu bionic/main amd64 mysql-common all 5.8+1.0.4 [7 308 B]

Пол:2 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-common all 1:10.1.43-0ubuntu0.18.04.1 [29,6 kB]

Пол:3 <http://archive.ubuntu.com/ubuntu bionic/universe amd64 galera-3 amd64 25.3.20-1> [947 kB]
Пол:4 <http://archive.ubuntu.com/ubuntu bionic/main amd64 libdbi-perl amd64 1.640-1> [724 kB]
Пол:5 <http://archive.ubuntu.com/ubuntu bionic/main amd64 libconfig-inifiles-perl all 2.94-1> [40,4 kB]
Пол:6 <http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libaiol amd64 0.3.110-5ubuntu0.1> [6 476 B]
Пол:7 <http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-client-core-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1> [4 778 kB]
Пол:8 <http://archive.ubuntu.com/ubuntu bionic/universe amd64 libjemalloc1 amd64 3.6.0-11> [82,4 kB]
Пол:9 <http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-client-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1> [5 658 kB]
Пол:10 <http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-server-core-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1> [4 960 kB]
Пол:11 <http://archive.ubuntu.com/ubuntu bionic/main amd64 socat amd64 1.7.3.2-2ubuntu2> [342 kB]
Пол:12 <http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-server-10.1 amd64 1:10.1.43-0ubuntu0.18.04.1> [5 108 kB]
Пол:13 <http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-client all 1:10.1.43-0ubuntu0.18.04.1> [28,4 kB]
Пол:14 <http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-server all 1:10.1.43-0ubuntu0.18.04.1> [28,5 kB]
Получено 22,7 MB за 7с (3 190 kB/s)
Предварительная настройка пакетов ...
Выбор ранее не выбранного пакета mysql-common.
dpkg: предупреждение: список файлов пакета «util-linux» отсутствует; предполагаем, что на данный момент у пакета нет установленных файлов (Чтение базы данных ... на данный момент установлено 297405 файлов и каталогов.)
Подготовка к распаковке .../00-mysql-common_5.8+1.0.4_all.deb ...
Распаковывается mysql-common (5.8+1.0.4) ...
Выбор ранее не выбранного пакета mariadb-common.
Подготовка к распаковке .../01-mariadb-common_1%3a10.1.43-0ubuntu0.18.04.1_all.deb ...
...
Распаковывается mariadb-common (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета galera-3.
Подготовка к распаковке .../02-galera-3_25.3.20-1_amd64.deb ...
Распаковывается galera-3 (25.3.20-1) ...
Выбор ранее не выбранного пакета libdbi-perl.
Подготовка к распаковке .../03-libdbi-perl_1.640-1_amd64.deb ...
Распаковывается libdbi-perl (1.640-1) ...
Выбор ранее не выбранного пакета libconfig-inifiles-perl.
Подготовка к распаковке .../04-libconfig-inifiles-perl_2.94-1_all.deb ...
Распаковывается libconfig-inifiles-perl (2.94-1) ...
Выбор ранее не выбранного пакета libaiol:amd64.
Подготовка к распаковке .../05-libaiol_0.3.110-5ubuntu0.1_amd64.deb ...
Распаковывается libaiol:amd64 (0.3.110-5ubuntu0.1) ...
Выбор ранее не выбранного пакета mariadb-client-core-10.1.
Подготовка к распаковке .../06-mariadb-client-core-10.1_1%3a10.1.43-0ubuntu0.18.04.1_amd64.deb ...
Распаковывается mariadb-client-core-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета libjemalloc1.
Подготовка к распаковке .../07-libjemalloc1_3.6.0-11_amd64.deb ...
Распаковывается libjemalloc1 (3.6.0-11) ...
Выбор ранее не выбранного пакета mariadb-client-10.1.
Подготовка к распаковке .../08-mariadb-client-10.1_1%3a10.1.43-0ubuntu0.18.04.1_amd64.deb ...
Распаковывается mariadb-client-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета mariadb-server-core-10.1.
Подготовка к распаковке .../09-mariadb-server-core-10.1_1%3a10.1.43-0ubuntu0.18.04.1_amd64.deb ...
Распаковывается mariadb-server-core-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета socat.


```

Подготовка к распаковке .../10-socat_1.7.3.2-2ubuntu2_amd64.deb ...
Распаковывается socat (1.7.3.2-2ubuntu2) ...
Настраивается пакет mysql-common (5.8+1.0.4) ...
Настраивается пакет mariadb-common (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета mariadb-server-10.1.
dpkg: предупреждение: список файлов пакета «util-linux» отсутствует;
предполагаем, что на данный момент у пакета нет установленных файлов
(Чтение базы данных ... на данный момент установлено 297785 файлов и каталогов.)
Подготовка к распаковке .../mariadb-server-10.1_1%3a10.1.43-
0ubuntu0.18.04.1_amd64.deb ...
Распаковывается mariadb-server-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета mariadb-client.
Подготовка к распаковке .../mariadb-client_1%3a10.1.43-0ubuntu0.18.04.1_all.deb ...
Распаковывается mariadb-client (1:10.1.43-0ubuntu0.18.04.1) ...
Выбор ранее не выбранного пакета mariadb-server.
Подготовка к распаковке .../mariadb-server_1%3a10.1.43-0ubuntu0.18.04.1_all.deb ...
Распаковывается mariadb-server (1:10.1.43-0ubuntu0.18.04.1) ...
Настраивается пакет libconfig-inifiles-perl (2.94-1) ...
Настраивается пакет libjemalloc1 (3.6.0-11) ...
Настраивается пакет socat (1.7.3.2-2ubuntu2) ...
Настраивается пакет libaiol:amd64 (0.3.110-5ubuntu0.1) ...
Настраивается пакет galera-3 (25.3.20-1) ...
Настраивается пакет libegl-mesa0:amd64 (19.0.8-0ubuntu0~18.04.3) ...
dpkg: ошибка при обработке пакета libegl-mesa0:amd64 (--configure):
 installed libegl-mesa0:amd64 package post-installation script subprocess
returned error exit status 2
Настраивается пакет libdbi-perl (1.640-1) ...
Настраивается пакет libglx-mesa0:amd64 (19.0.8-0ubuntu0~18.04.3) ...
dpkg: ошибка при обработке пакета libglx-mesa0:amd64 (--configure):
 installed libglx-mesa0:amd64 package post-installation script subprocess
returned error exit status 2
Настраивается пакет mariadb-server-core-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Настраивается пакет mariadb-client-core-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Настраивается пакет mariadb-client-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Настраивается пакет mariadb-client (1:10.1.43-0ubuntu0.18.04.1) ...
Настраивается пакет mariadb-server-10.1 (1:10.1.43-0ubuntu0.18.04.1) ...
Created symlink /etc/systemd/system/mysql.service →
/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/mysqld.service →
/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service →
/lib/systemd/system/mariadb.service.
Настраивается пакет mariadb-server (1:10.1.43-0ubuntu0.18.04.1) ...
Обрабатываются триггеры для libc-bin (2.27-3ubuntu1) ...
Обрабатываются триггеры для doc-base (0.10.8) ...
Обработка 1 добавленный файл doc-base...
Регистрация документа в scrollkeeper...
Обрабатываются триггеры для systemd (237-3ubuntu10.31) ...
Обрабатываются триггеры для man-db (2.8.3-2ubuntu0.1) ...
Обрабатываются триггеры для ureadahead (0.100.0-21) ...
usr@vbiptab:~$ sudo apt-get install software-properties-common
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие НОВЫЕ пакеты будут установлены:
 software-properties-common
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0
пакетов, и 0 пакетов не обновлено.
Установлено или удалено не до конца 3 пакетов.
Необходимо скачать 8 160 В архивов.
После данной операции объём занятого дискового пространства возрастёт на 15,4
кВ.
Пол:1 http://packages.linuxmint.com tina/upstream amd64 software-properties-
common all 1.8.8 [8 160 В]

```

Получено 8160 В за 0с (20,7 kB/s)

Выбор ранее не выбранного пакета software-properties-common.

```
usr@vbiptab:~$ sudo apt-key adv --recv-keys --keyserver
hkp://keyserver.ubuntu.com:80 0xF1656F24C74CD1D8
Executing: /tmp/apt-key-gpghome.QfbdraRqvq/gpg.1.sh --recv-keys --keyserver
hkp://keyserver.ubuntu.com:80 0xF1656F24C74CD1D8
gpg: key F1656F24C74CD1D8: 6 подписей не проверено за отсутствием ключа
gpg: ключ F1656F24C74CD1D8: импортирован открытый ключ "MariaDB Signing Key
<signing-key@mariadb.org>"
gpg: Всего обработано: 1
gpg: импортировано: 1
```

```
usr@vbiptab:~$ sudo apt update
Сущ:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Сущ:2 http://security.ubuntu.com/ubuntu bionic-security InRelease
Сущ:3 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Игн:4 http://packages.linuxmint.com tina InRelease
Сущ:5 http://archive.canonical.com/ubuntu bionic InRelease
Сущ:6 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Сущ:7 http://packages.linuxmint.com tina Release
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.
```

```
usr@vbiptab:~$ sudo apt install mariadb-server mariadb-client
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет mariadb-client самой новой версии (1:10.1.43-0ubuntu0.18.04.1).
Уже установлен пакет mariadb-server самой новой версии (1:10.1.43-0ubuntu0.18.04.1).
```

Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.

usr@vbiptab:~\$

```
usr@vbiptab:~$ sudo systemctl status mysql
[sudo] пароль для usr:
● mariadb.service - MariaDB 10.1.43 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset:
   Active: active (running) since Sun 2019-11-24 20:43:30 +05; 31min
   ago
     Docs: man:mysql(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 3897 (mysqld)
    Status: "Taking your SQL requests now..."
     Tasks: 27 (limit: 4656)
    CGroup: /system.slice/mariadb.service
           └─3897 /usr/sbin/mysqld
```

```
ноя 24 20:43:31 vbiptab /etc/mysql/debian-start[3930]: P
rocessing databases
ноя 24 20:43:31 vbiptab /etc/mysql/debian-start[3930]: i
nformation_schema
ноя 24 20:43:31 vbiptab /etc/mysql/debian-start[3930]: m
ysql
ноя 24 20:43:31 vbiptab /etc/mysql/debian-start[3930]: p
erformance_schema
ноя 24 20:43:31 vbiptab /etc/mysql/debian-start[3930]: P
hase 6/7: Checking and upgrading tables
```

```
root@vbiptab:/home/usr# mysql -u root -p
```

```

Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 10.1.43-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database sample;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> connect sample;
Connection id:      44
Current database: sample

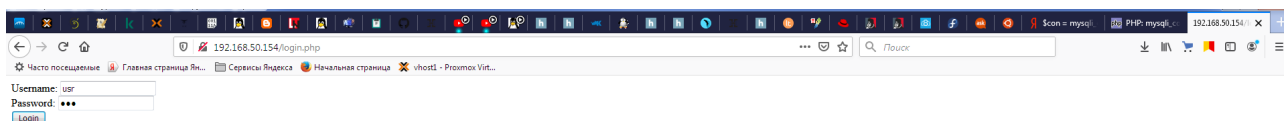
MariaDB [sample]> create table users(username VARCHAR(100),password
VARCHAR(100));
Query OK, 0 rows affected (0.02 sec)

MariaDB [sample]> insert into users values('sa','sasa');
Query OK, 1 row affected (0.10 sec)

MariaDB [sample]> insert into users values('usr','sasa1');
Query OK, 1 row affected (0.00 sec)

MariaDB [sample]> quit;
Bye
root@vbiptab:/home/usr#

```



теперь при проверке подлинности логина/пароля из БД **sample MySQL** наш скрипт должен работать.

Теперь нужно выполнить тестовую инъекцию SQL, попробовав обойти ввод учетных данных. В поле **Username** введём:

' or true --

Примечание: после символов – необходимо поставить пробел, иначе инъекция не работает.

Поле **Password** оставьте пустым и нажмите кнопку входа.

На экране появится сообщение для авторизованных пользователей – значит, инъекция сработала.

Чтобы защитить сервер от подобных атак, нужно настроить правила брандмауэра.

5. Настройка правил **mod_security**:

По умолчанию **mod_security** поставляется с базовым набором правил **CRS (Core Rule Set)**,

расположенном в каталоге: `/usr/share/modsecurity-crs/`; документацию по нему можно найти здесь: `/usr/share/doc/modsecurity-crs/`

Чтобы подгрузить эти готовые правила, нужно, **чтобы веб-сервер Apache2 читал указанные выше каталоги**. Для этого отредактируем файл **`mod-security.conf`**:

```
mcedit /etc/apache2/mods-enabled/mod-security.conf
```

В **`<IfModule security2_module>`** внесём следующие параметры:

```
Include "/usr/share/modsecurity-crs/*.conf"
Include "/usr/share/modsecurity-crs/activated_rules/*.conf"
```

Директория **`activated_rules`** аналогична директории **`Apache mods-enabled`**. Правила доступны в каталогах:

```
/usr/share/modsecurity-crs/base_rules
/usr/share/modsecurity-crs/optional_rules
/usr/share/modsecurity-crs/experimental_rules
```

Чтобы активировать правила, нужно создавать символические ссылки в каталоге **`activated_rules`**. Создадим правило для защиты от SQL-инъекции.

```
cd /usr/share/modsecurity-crs/activated_rules/
ln -s /usr/share/modsecurity-crs/base_rules/modsecurity_crs_41_sql_injection_attacks.conf .
```

Чтобы новые правила вступили в исполнение, нужно перезапустить Apache2.

```
service apache2 reload
```

Теперь, вернувшись на созданную ранее страницу входа и попробовав выполнить тестовую **SQL-инъекцию**, Если директива **`SecRuleEngine`** была включена, увидим сообщение об ошибке **`403 Forbidden`**.

Если же значение **`DetectionOnly`** не было изменено, инъекция будет успешно выполнена, но сообщение о ней **будет внесено в лог-файл `modsec_audit.log`**.

Кроме того, можно создавать собственные правила и добавить в любой конфигурационный файл модуля или разместить в каталогах **`mod_security`**, но на этом подробно останавливаться мы не будем.