

Задание выполнил студент группы 2345 Романенко Кирилл

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

Создал копию ВМ. Подключился к ней по ssh

```
(kirill@kali)-[~]  
$ ssh vagrant@192.168.56.11  
vagrant@192.168.56.11's password:  
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com/  
Last login: Wed Apr 12 06:40:14 2023  
vagrant@ubuntu:~$
```

Настроил ip адрес на eth2. Выполнил apt update.

Установил пакет mod_security для apache2

```
apt install libapache2-mod-security2
```

Открыл директорию /etc/apache2/mods-enabled и отредактировал файл security2.conf

```
nano /etc/apache2/mods-enabled/ security2.conf
```

Подключил конфиги правил и конфиг для управления правилами и действиями. В открытом файле дописал:

```
Include /usr/share/modsecurity-crs/modsecurity_crs_10_setup.conf
```

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

Активировал правила для защиты от XSS

```
cd /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
```

Дописал в файл `modsecurity_crs_10_setup.conf` строки для блокирования

```
nano /usr/share/modsecurity-  
crs/activated_rules/modsecurity_crs_10_setup.conf
```

`SecDefaultAction "phase:1,deny,log"` – действие для правил фазы 1.

`SecDefaultAction "phase:2,deny,log"` – действие для правил фазы 2.

Перезагрузил Apache 2

```
service apache2 restart
```

P.S. Стандартный конфигурационный файл WAF

(`/etc/modsecurity/modsecurity.conf`) настроен на работу в режиме `DetectionOnly`, т.е. фаервол отслеживает логи, при этом ничего не блокируя.

Чтобы изменить поведение, нужно в файле

`/etc/modsecurity/modsecurity.conf` изменить директиву `SecRuleEngine` `DetectionOnly` на `SecRuleEngine On`. Прочие полезные директивы:

- `SecResponseBodyAccess` (значения «on» или «off», по умолчанию «on») – доступ к анализу тела ответа. Включение увеличит нагрузку на WAF и логи.
- `SecRequestBodyLimit` (по умолчанию 13 107 200 б, или 12,5 МБ) – максимальный размер данных POST. Если клиентом будет отправлено больше, будет ошибка 403.
- `SecRequestBodyNoFilesLimit` (по умолчанию 131 072 б, или 128 КБ) – ограничивает размер данных POST за вычетом размера файлов.