Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1: Выполните установку **mod_security** (из репозиториев Debian) в копию ВМ, на которой установлены пакеты для работ (DVWA, XVWA и т.д.).

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

Использовался один из VPS сервисов, который по хорошему должны были бы предоставить GB, но был арендован за свои кровные. Подключился к ней по ssh.

Произведена настройка и установка пакета mod_security для Apache2

#apt update.
#apt install libapache2-mod-security2

В директории **/etc/apache2/mods-enabled** редактируется файл конфига **security2.conf**

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

Подключение конфигов правил и конфигов для управления правилами и действиями.
В сам файл конфига дописывается:

Include /usr/share/modsecurity-crs/modsecurity_crs_10_setup.conf
Include "/usr/share/modsecurity-crs/activated_rules/.conf"*

Далее активируются правила защиты от XSS атак.

#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

Дописываются 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.

Перезагрузка Apache2

#service apache2 restart

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

Для изменения поведения, необходимо 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.