

**Домашнее задание № 30**

***Web Application Security***

1. **Ознакомиться с основными ресурсами по web app security**
2. **Установить WAF (nginx + Modsecurity)**

* установить и протестировать запрет тестовых запросов curl
* [Nginx + Modsecurity WAF](https://opsshield.com/help/cpguard/install-modsecurity-with-nginx-on-debian-ubuntu/)
* [Smirnov nginx + modsecurity github](https://github.com/sm1lexops/Profile_challenges?tab=readme-ov-file#5-%D0%BF%D1%80%D0%B5%D0%B4%D0%BB%D0%BE%D0%B6%D0%B8%D1%82%D0%B5-%D1%81%D1%85%D0%B5%D0%BC%D1%83-%D0%B8%D0%BD%D1%82%D0%B5%D0%B3%D1%80%D0%B0%D1%86%D0%B8%D0%B8-web-application-firewall-waf-%D0%B2-%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5-%D0%BD%D0%B0%D0%BF%D0%B8%D1%88%D0%B8%D1%82%D0%B5-%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B3%D1%83%D1%80%D0%B0%D1%86%D0%B8%D1%8E-%D0%B4%D0%BB%D1%8F-%D0%B2%D0%BD%D0%B5%D0%B4%D1%80%D0%B5%D0%BD%D0%B8%D1%8F-waf-%D0%BD%D0%B0%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80-modsecurity-%D0%B2-nginx-%D0%BD%D0%B0%D0%BF%D0%B8%D1%88%D0%B8%D1%82%D0%B5-%D0%BA%D0%BE%D0%BD%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D1%8B%D0%B5-%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80%D1%8B-%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B5-%D0%B2%D1%8B-%D0%B1%D1%8B-%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B8%D0%BB%D0%B8-%D0%B2-waf-%D0%BD%D0%B0%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80-%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D0%B0%D1%86%D0%B8%D1%8F-sql-%D0%B8%D0%BD%D1%8A%D0%B5%D0%BA%D1%86%D0%B8%D0%B9-xss-%D0%B0%D1%82%D0%B0%D0%BA-%D0%B1%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%BA%D0%B0-%D0%B7%D0%B0%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85-%D0%BF%D0%B0%D1%82%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B2)

**3.\*** **Разверните** [Готовая виртуалка Ubuntu + modesecurity](https://drive.google.com/file/d/12tO5SwSu43IJprim8BafCmF-aQb9-EfM/view)

* Настройте сетевой адаптер в режиме моста (Сетевой мост/Network Bridge)
* Проверьте ip адрес виртуальной машины
* Запустите контейнер с уязвимым приложением.
* sudo **docker run -d -p 8080:80 saurav7055/xvwa**
* Теперь приложение доступно по адресу {ip сервера}:80/xvwa по всей вашей домашней сети, если нет ограничений файервола.
* Вызовите 5 различных сработок WAF Правила, применяя уязвимости в приложении
* Пришлите результат сработки, правило WAF и его ID (var/log/nginx/error.log)

Ссылки на дополнительные ресурсы

* [Отличия WAF vs IPS](https://stormwall.pro/knowledge-base/termin/waf)
* [12 Лучших WAF решений](https://dzen.ru/a/ZCrzuo293D16oGyd)
* [How to install **modesecurity** with nginx](https://www.tecmint.com/install-modsecurity-nginx-debian-ubuntu/)
* [CRS (Core Rule Set) набор правил для modesecurity](https://coreruleset.org/)
* [Встраивание modesecurity crs](https://www.netnea.com/cms/nginx-tutorial-6_embedding-modsecurity/) - [Modesecurity Wiki](https://github.com/owasp-modsecurity/ModSecurity/wiki/)
* [Готовая виртуалка Ubuntu + modesecurity](https://drive.google.com/file/d/12tO5SwSu43IJprim8BafCmF-aQb9-EfM/view)
* [Примеры WAF ByPass](https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-devteev-CC-WAF.pdf)
* [OWASP ASVS стандарт для безопасной разработки Web](https://habr.com/ru/companies/acribia/articles/519050/)
* [Xtreme Vulnerable Web Application (XVWA)](https://github.com/s4n7h0/xvwa)