Lab 5 - Web Application Firewall (WAF)

> Secure System Development - Spring 2025

In this lab, you will practice deploying and configuring ModSecurity WAF.

- Create a `.md` step-by-step report of the actions you took with screenshots of key results.

Task 1 - Blocking SQLi with WAF

> Guide: https://github.com/owasp-modsecurity/ModSecurity/wiki/Reference-Manual-(v2.x)

1. Deploy Juice-Shop: bkimminich/juice-shop
2. Access the application at port 3000.
3. Show that you're able to login as `admin` by exploiting a SQL injection in the `email` field.
4. Deploy OWASP ModSecurity+CRS for Nginx in front of the app: owasp/modsecurity-crs:nginx
    - E.g., use a docker-compose file to run `app` and `waf` containers in the same network.
5. Access the application through the WAF at port 8080
6. Show that the previous exploit is no longer possible with default WAF configuration applied.

Task 2 - Bypassing WAF

> Reference: https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF

1. Update your exploit to bypass WAF checks.
2. Re-Configure WAF to block the updated exploit
    - i.e., add a custom rule to prevent your exploit from getting through the WAF.
3. Apply the new configuration and verify that your updated exploit no longer works.
4. Carry an automated SQLi test (e.g., using `sqlmap`) and check whether WAF blocks all attempts. Explain the results.