STI MEI/MIEBOM 2022/2023

Practical Exercises #8

Secure a website with ModSecurity

1. Install and configure a testing website with Apache2
2. Install ModSecurity module for Apache and ModSecurity OWASP CRS
3. Enable ModSecurity CRS in ModSecurity (if not enabled)
4. Enable ModSecurity in the website virtual host (it not enabled)
5. Perform attacks on the website (suggestion: use a browser or “curl” as the client), examples: XSS, SQLi, remote execution
6. Analyze requests responses and logs to confirm the attacks were blocked
7. Identify the CRS rules that blocked the attacks and analyze them (rules structure and actions).
8. Reconfigure the virtual host to ignore the CRS rules that blocked the XSS attach, repeat the attack and compare the results and logs
9. Reconfigure the virtual host ModSecurity to mode DetectionOnly, repeat the attacks and compare the results and logs.

Goals

Web Application Firewall with ModSecurity

Materials

- OWASP
- OWASP WSTG Project
- ModSecurity
- ModSecurity CRS