

Prototype implementation of Web Application Firewall stack including log analyzer

Abstract

A Web Application Firewall protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application and prevents any unauthorized data from leaving the application. Implementation of web application firewall is just not the solution for resolving the security problems that a web-based applications might have, proper configuration is required in order to make the WAF capable of identifying and blocking many of the web-app attacks. In this project, we need to implement a OWSAP WAF stack using open-source technologies like Caddy, Coraza. And logging and monitoring logs of web server using Kibana, Elasticsearch. A prototype is to be developed using the mentioned tools.

Student Prerequisites - Linux OS, knowledge of web-application architecture, Docker Containers.
Learning Outcomes: An overview of enterprise client-server web application having integration.

Academic Project Requirements:

- 1) Required No. of student(s) for academic project: 1**
- 2) Name of course with branch/discipline: B.E./B.Tech. Computer Engineering/IT/MCA**
- 3) Academic Project duration:**
 - (a) Total academic project duration: 8 Weeks**
 - (b) Student's presence at IPR for academic project work: 2 Full working Days per week**

Email to: sharad.jash@ipr.res.in[Guide's e-mail address] and project_cs@ipr.res.in [Academic Project Coordinator's e-mail address]

Phone Number: 079 -2304 [Guide's phone number]