Fundamentals of Computer Security

Web Applications

Lab 2

Contents

- Web application Basic Protection

- Database Connectivity

- Setting up Web Application Firewalls

Basic Web Security

❖ Call rate limit

❖ Optional: Blocking IPs

❖ Part1.pdf

❖ You will need two machines: 1 ubuntu with nginx and attacker (kali)

Database Connectivity (homework)

❖ Setup your web server with a database connectivity (any application works).

❖ Setup an authentication to DB using one of the following methods:

  ❖ Basic, Digest, Certificate

❖ Protect the service from brute force attacks.

Firewalls & IDS/IPS

- ❖ Protect your application using two of the following tools:

- ❖ Network Firewalls; Snort, Suricata

- ❖ Web Application Firewalls; IronBee, WebKnight, Shadow Daemon

- ❖ Honeypots; Glastopf, WebTrap, honeyhttpd

  - ❖ https://github.com/paralax/awesome-honeypots

  - ❖ https://owasp.org/www-community/Web_Application_Firewall

OWASP

❖ Describe OWASP Top 10 in your own words.

Open Web Application Security Project:
Https://owasp.org