eJPT Certification

Section: Web Applications- Burp Suite

08/30/2020

**Tools:**

* Burp Suite

**How does this support my pentesting career?**

* Web application analysis
* Finding vulnerabilities
* Attacks
* Burp Suite is one of the most used pentesting tools

**Intercepting Proxies**

* Intercepting proxies is a tool that enables you to analyze and modify any request, and any response exchanged between an HTTP client and a server.
* Most common web app proxies are:
  + The intercepting proxy feature of Burp Suite
  + ZAP
    - An alternative proxy interceptor from burp suite
* Intercepting proxy should not be confused with a proxy server. Proxy servers filter all the traffic coming from the internal network. Intercepting proxies intercepts browser traffic which enables pentesters to analyze and manipulate data.

**Burp Proxy**

* Intercept requests and responses between your browser and the web server.
* Build request manually
* Crawl a website by automatically visiting every page in a website.
* Fuzz web applications by sending them patterns of valid and invalid inputs to test their behavior.
* Burp allows you to intercept and modify requests coming from your browser before they are sent to a remote server.
  + You can modify the header and the body of a message by hand or automatically.

**Burp Repeater**

* Lets you manually build raw HTTP requests.
  + Burp Repeater provides you with:
    - Syntax highlighting
    - Raw and rendered responses
    - Integration with other Burp tools

Notes

* Follow burp proxy configuration slides and try out configuration on kali.
* Try building a request in burp repeater