eJPT Certification

Section: Web Applications- Burp Suite

09/30/2020

**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

**Overview**

* **Proxy** - What allows us to funnel traffic through Burp Suite for further analysis
* **Target** - How we set the scope of our project. We can also use this to effectively create a site map of the application we are testing.
* **Intruder** - Incredibly powerful tool for everything from field fuzzing to credential stuffing and more
* **Repeater** - Allows us to 'repeat' requests that have previously been made with or without modification. Often used in a precursor step to fuzzing with the aforementioned Intruder
* **Sequencer** - Analyzes the 'randomness' present in parts of the web app which are intended to be unpredictable. This is commonly used for testing session cookies
* **Decoder** - As the name suggests, Decoder is a tool that allows us to perform various transforms on pieces of data. These transforms vary from decoding/encoding to various bases or URL encoding.
* **Comparer** - Comparer as you might have guessed is a tool we can use to compare different responses or other pieces of data such as site maps or proxy histories (awesome for access control issue testing). This is very similar to the Linux tool diff.
* **Extender** - Similar to adding mods to a game like Minecraft, Extender allows us to add components such as tool integrations, additional scan definitions, and more!
* **Scanner** - Automated web vulnerability scanner that can highlight areas of the application for further manual investigation or possible exploitation with another section of Burp. This feature, while not in the community edition of Burp Suite, is still a key facet of performing a web application test.

**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

Burp Intruder

1. ***Sniper*** - The most popular attack type, this cycles through our selected positions, putting the next available payload (item from our wordlist) in each position in turn. This uses only one set of payloads (one wordlist).

2. ***Battering Ram*** - Similar to Sniper, Battering Ram uses only one set of payloads. Unlike Sniper, Battering Ram puts every payload into every selected position. Think about how a battering ram makes contact across a large surface with a single surface, hence the name battering ram for this attack type.

3. ***Pitchfork*** - The Pitchfork attack type allows us to use multiple payload sets (one per position selected) and iterate through both payload sets *simultaneously*. For example, if we selected two positions (say a username field and a password field), we can provide a username and password payload list. Intruder will then cycle through the combinations of usernames and passwords, resulting in a total number of combinations equalling the smallest payload set provided.

4. ***Cluster Bomb*** - The Cluster Bomb attack type allows us to use multiple payload sets (one per position selected) and iterate through all combinations of the payload lists we provide. For example, if we selected two positions (say a username field and a password field), we can provide a username and password payload list. Intruder will then cycle through the combinations of usernames and passwords, resulting in a total number of combinations equalling usernames x passwords. *Do note, this can get pretty lengthy if you are using the community edition of Burp.*

Notes

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