eJPT Certification

Section: Web Applicaitons

08/30/2020

Learning Objectives:

* HTTP Protocol
* Burp Suite Basics

**Web Application Security:**

* There are four fundamental aspects of web application security:
  + HTTP Protocols
  + Cookies
  + Sessions
  + Same Origin Policy

**HTTP Protocol Basics:**

* How does this support my pentesting career?
  + The ability to exploit web applications and find vulnerabilities in web servers and services.
  + Web applications technology is used market-wide also by desktop or mobile applications.
* **Hypertext Transfer protocol (HTTP)** – the most used application protocol on the internet.
  + It is the client-server protocol used to transfer web pages and web application data.
  + In HTTP, the client, usually a web browser, connects to a web server such as MS IIS or Apache HTTP Server. HTTP is also used under the hood by many mobile and modern applications.
* During an HTTP communication, the client and server exchange messages.
  + The client sends requests to the server and the server sends back responses.
  + HTTP works on top of TCP protocol.
    - First a TCP connection is established and then the client sends its requests and waits for a response. The server processes the request and sends back its answer, providing a status code and appropriate data.
* To end lines in HTTP, you have to use \r (carriage return) and the \n (newline) characters.
* Every header contains a request followed by some header fields. The format is as follows: Header-name: header value.

**HTTP Requests:**

**A screenshot of a cell phone

Description automatically generated**

**HTTPS**

* HTTP Secure (HTTPS), or HTTP over SSL/TLS, is a method to run HTTP which is a clear-text protocol over SSL/TLS, a cryptographic protocol.
* Why is HTTPS important?
  + An attacker on the path cannot sniff the application layer communication.
  + An attacker on the path cannot alter the application layer data.
  + The client can tell the real identity of the server and, sometimes, vice-versa.
* A network user will be able to sniff the HTTP traffic but will not be able to read the HTTP Request headers, body, target domain, HTTP Response headers, or body.
* Network user may recognize:
  + Target IP address.
  + Target port
  + DNS or similar protocols may disclose which domain user tries resolve.
* IMPORTANT- HTTPS does not protect against web app flaws. The extra encryption layer only protects data exchanged between the client and the server. It does not protect from an attack against the application itself.
  + **Attacks such as XSS and SQL injections will still work.**

**Cookies**

Notes:

* Web applications are applications that run on web servers and accessible via web browser (chrome, edge, etc.)
* Almost every website on the internet includes some kind of intelligence in its web page
  + Intelligence could either be on a client side or server side.
* The web app world is extremely heterogeneous. Which means there are many ways to accomplish the same task, but that also means there are many ways to mess things up.