eJPT Certification

Section: Web Attacks

09/14/2020

**Learning Objectives**

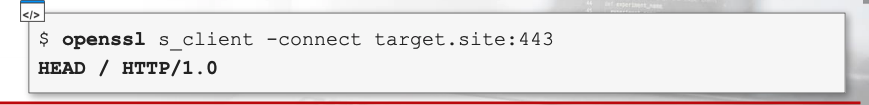
* How to approach web applications as a penetration tester
* Fundamental attacks against web applications

**Web Server Fingerprinting**

* Why is this important?
  + Knowledgeable of targets
  + Ability to use exploitation tools at their best
  + Ability to search for the right public exploit.
* Misconfigured web servers can be the open door to the whole network infrastructure.
* When fingerprinting a web server we are trying to detect the following:
  + The daemon providing the web server service, i.e. IIS, Apache, nginx, etc.
  + Its version
  + The OS of the machine hosting the server
* **Manual Web Server fingerprinting with Netcat**
  + Netcat
    - Very popular tool
    - Known as TCP/IP Swiss army knife
    - Can be used on both clients and servers
    - Can be used as a client to send manual requests to the web server.
      * This activity is called “banner grabbing”
      * To grab a banner you have to connect to a listening daemon and then read the banner it sends back to your client.

A screenshot of a cell phone

Description automatically generated

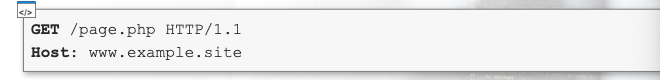
* When writing a request to the web server it must be in UPPERCASE. Request is case sensitive.
* Netcat cannot be used to connect to HTTPS daemons because it does not perform any encryption.
* **Fingerprinting with Open SSL**
  + If you want to connect to an HTTPS web server to perform manual fingerprinting you can use the OpenSSL command line tool.
  + <https://www.openssl.org/>
* **A screenshot of a cell phone

  Description automatically generatedFingerprinting with Httprint**

**A picture containing sitting, table, food

Description automatically generated**

**HTTP Verbs**

* Why is this important?
  + Ability to manually exploit a misconfigured web server
  + The covered attacks can also be used against embedded devices
  + Ability to create a custom PHP shell
* The most common HTTP methods:
  + GET
    - GET is used to request a resource. When a user wants to open a web page, the browser sends a GET Request.
    - **A screenshot of a cell phone

      Description automatically generated**You can also pass in arguments to the web app.­
  + POST
    - **A screenshot of a cell phone

      Description automatically generated**POST is used to submit HTML form data. POST parameters must be in the message body.
  + HEAD
    - **A close up of a device

      Description automatically generated**HEAD is similar to GET. HEAD asks for just the headers of the response instead of the response body.
  + PUT
    - PUT is used to upload a file to the server.

**A screenshot of a cell phone

Description automatically generated**

* + DELETE
    - DELETE is used to remove a file from the server; this is another feature that must be configured wisely as a misused DELETE leads to a denial of service and data loss.

**A screenshot of a cell phone

Description automatically generated**

* + OPTIONS
    - OPTIONS is used to query the web server for enabled HTTP verbs.

A screenshot of a social media post

Description automatically generated

* **REST APIs**
  + Stands for *Representational State Transfer Application Programming Interface*
  + Often referred to as “web services” or just “APIs”
  + Rely heavily on almost all HTTP Verbs
  + Common for apps to use “PUT” to save data but not files.
  + PUT method
    - Can be easy to confuse a REST APIs PUT method, which just creates a new content with a PUT method that allows us to create an arbitrary file.
    - A screenshot of a cell phone

      Description automatically generatedAfter create a PUT request you should try and look for the file you just created.
* Pentesters must enumerate the available HTTP methods or verbs available on the web server.
  + To do this you can send an options message with Netcat. See example below:

A screenshot of a social media post

Description automatically generated

* Exploiting DELETE
  + To exploit DELETE you just need to specify the file you want to delete. For Example:

A screenshot of a cell phone

Description automatically generated

Exploiting PUT

* A screenshot of a cell phone

  Description automatically generatedIn order to exploit the PUT method you need to know the size of the file you want to upload to the web server. To accomplish this you can use the Unix utility wc (word counter) with the -m parameter to how long, in bytes the payload is.
* A screenshot of a cell phone

  Description automatically generatedNow you can use the size of the payload to build your PUT message. For Example:
* **Uploading a PHP Shell with PUT**

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

**Directories and Files Enumeration**

* Why is it important?
  + Find and utilize testing features
  + Exploit information saved in backup or old files
  + Find hidden resources
* Enumeration
  + Helps us find hidden resources that often contain:
    - New and untested features
    - Backup files
    - Testing information
    - Developer’s notes
* There are two ways to enumerate resources:
  + Prue brute-force
  + Dictionary attacks
* Brute-force enumeration
  + Simple; try every possible combination of characters
    - However, very inefficient
* Dictionary-based Enumeration
  + Faster and more precise method to enumerate resources is to list the common file names, directory names, and file extensions.
    - A screenshot of a cell phone

      Description automatically generatedExample: common backup file names are : .bak, .old, .txt, .xxx
* Enumerating Web Resources with Dirbuster
  + Enumeration automation tool.
  + This is a very common web enumeration tool
  + Java application
  + To use you it you set at target (site URL you wish to test)
  + Choose your attack of preference (brute force or dictionary attack)