Sasha Shahidi

Week 14 Homework: Web Development

HTTP Requests and Responses

Answer the following questions about the HTTP request and response process.

1. What type of architecture does the HTTP request and response process occur in?
   Client-server architecture

2. What are the different parts of an HTTP request?
   Request line, request header, and request body

3. Which part of an HTTP request is optional?
   Request body

4. What are the three parts of an HTTP response?
   Status line, response headers, and response body

5. Which number class of status codes represents errors?
   400 and 500 range

6. What are the two most common request methods that a security professional will encounter?
   GET and POST

7. Which type of HTTP request method is used for sending data?
   POST

8. Which part of an HTTP request contains the data being sent to the server?
   Request body

9. In which part of an HTTP response does the browser receive the web code to generate and style a web page?
   Response body

Using curl

Answer the following questions about curl:

10. What are the advantages of using curl over the browser?
    It is more flexible and you can make changes while transferring the data.

11. Which curl option is used to change the request method?

    -x

12. Which curl option is used to set request headers?

    -h

13. Which curl option is used to view the response header?

    -i

14. Which request method might an attacker use to figure out which HTTP requests an HTTP server will accept?

    Options or GET

Sessions and Cookies

Recall that HTTP servers need to be able to recognize clients from one another. They do this through sessions and cookies.

Answer the following questions about sessions and cookies:

Which response header sends a cookie to the client?

HTTP/1.1 200 OK
Content-type: text/html

15. Set-Cookie: cart=Bob

    Set-Cookie

Which request header will continue the client's session?

GET /cart HTTP/1.1
Host: www.example.org

16. Cookie: cart=Bob

    Cookie

Example HTTP Requests and Responses

Look through the following example HTTP request and response and answer the following questions:

HTTP Request

```
POST /login.php HTTP/1.1
Host: example.com
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/80.0.3987.132 Mobile Safari/537.36

username=Barbara&password=password
```

17. What is the request method?
    POST

18. Which header expresses the client's preference for an encrypted response?
    Upgrade-Insecure-Requests: 1

19. Does the request have a user session associated with it?
    There is no user session associated with the request

20. What kind of data is being sent from this request body?
    Login information

HTTP Response

```
HTTP/1.1 200 OK
Date: Mon, 16 Mar 2020 17:05:43 GMT
Last-Modified: Sat, 01 Feb 2020 00:00:00 GMT
Content-Encoding: gzip
Expires: Fri, 01 May 2020 00:00:00 GMT
Server: Apache
Set-Cookie: SessionID=5
Content-Type: text/html; charset=UTF-8
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type: NoSniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block

[page content]
```

21. What is the response status code?
    200

22. What web server is handling this HTTP response?
    Apache

23. Does this response have a user session associated to it?
    Yes, SessionID=5

24. What kind of content is likely to be in the [page content] response body?
    Text/html

25. If your class covered security headers, what security request headers have been included?
    Strict-Transport-Security: max-age=31536000; includeSubDomains

Monoliths and Microservices

Answer the following questions about monoliths and microservices:

26. What are the individual components of microservices called?
    Services

27. What is a service that writes to a database and communicates to other services?
    API's

28. What type of underlying technology allows for microservices to become scalable and have redundancy?
    Containers

Deploying and Testing a Container Set

Answer the following questions about multi-container deployment:

29. What tool can be used to deploy multiple containers at once?
    Docker

30. What kind of file format is required for us to deploy a container set?
    .yaml / .yml

Databases

31. Which type of SQL query would we use to see all of the information within a table called customers?
    SELECT * FROM customers

32. Which type of SQL query would we use to enter new data into a table? (You don't need a full query, just the first part of the statement.)

    INSERT INTO

33. Why would we never run DELETE FROM <table-name>; by itself?

    It will delete all data from the tables

Bonus Challenge Instructions: The Cookie Jar

Step 1:

I followed the steps and created two new users in the Wordpress sysadmin account with the credentials listed: Amanda and Ryan.

Step 2:

1. Using your browser, log into your WordPress site as your sysadmin account and navigate to localhost:8080/wp-admin/users.php, where we previously created the user Ryan. Examine this page briefly. Log out.

I see the accounts for Amanda, Ryan, and sysadmin, with their email addresses, roles, and number of posts.

2. Using your browser, log into your Ryan account and attempt to navigate to localhost:8080/wp-admin/index.php. Note the wording on your Dashboard.

It shows the Dashboard of the Wordpress account.

3. Attempt to navigate to localhost:8080/wp-admin/users.php. Note what you see now.

It says that I am not allowed to browse users.

Step 3:

1. Construct a curl request that enters two forms: "log={username}" and "pwd={password}" and goes to http://localhost:8080/wp-login.php. Enter Ryan's credentials where there are placeholders.

Question: Did you see any obvious confirmation of a login? (Y/N)

YES

2. Construct the same curl request, but this time add the option and path to save your cookie: --cookie-jar ./ryancookies.txt. This option tells curl to save the cookies to the ryancookies.txt text file.

3. Read the contents of the ryancookies.txt file.

Question: How many items exist in this file?

2

Step 4:

1. Craft a new curl command that now uses the --cookie option, followed by the path to your cookies file. For the URL, use http://localhost:8080/wp-admin/index.php.

 Question: Is it obvious that we can access the Dashboard? (Y/N)

 NO

2. Press the up arrow on your keyboard to run the same command, but this time, pipe | grep Dashboard to the end of your command to return all instances of the word Dashboard on the page.

 Question: Look through the output where Dashboard is highlighted. Does any of the wording on this page seem familiar? (Y/N) If so, you should be successfully logged in to your Editor's dashboard.

 NO

Step 5:

Finally, write a curl command using the same --cookie ryancookies.txt option, but attempt to access http://localhost:8080/wp-admin/users.php.

 Question: What happens this time?

 The command did not take me to the users page in Wordpress.