Questions

HTTP Requests and Responses

1. What type of architecture does the HTTP request and response process occur in?
   a. Client/Server Architecture
2. What are the different parts of an HTTP request?
   a. From this website:
      i. Request Line
      ii. Set of Headers
      iii. Body (optional)
3. Which part of an HTTP request is optional?
   a. The body (see above source)
4. What are the three parts of an HTTP response?
   a. From this website:
      i. Status Line
      ii. Set of Headers
      iii. Body
5. Which number class of status codes represents errors?
   a. 400
6. What are the two most common request methods that a security professional will encounter?
   a. GET and POST
7. Which type of HTTP request method is used for sending data?
   a. POST or PUT
8. Which part of an HTTP request contains the data being sent to the server?
   a. The body
9. In which part of an HTTP response does the browser receive the web code to generate and style a web page?
   a. The body

Using “curl”

10. What are the advantages of using “curl” over the browser?
    a. I took the following from the 14.1 class slides:
        i. It allows for quick and easy automation of HTTP requests while allowing for adjustments.
        ii. “curl” can be used on the command line which makes it very useful if you’re working in an environment that has no GUI.
11. Which “curl” option is used to change the request method?
    a. From the “curl” man pages:
        i. The “-X” option
12. Which “curl” option is used to set request headers?
    a. From the “curl” man pages:
        i. The “-H” option
13. Which “curl” option is used to view the response header?
    a. From the “curl” man pages:
        i. The “-v” option
14. Which request method might an attacker use to figure out which HTTP requests an HTTP server will accept?
    a. The OPTIONS method

Sessions and Cookies

15. Which response header sends a cookie to the client?
    a. Set-Cookie
16. Which request header will continue the client's session?
    a. Cookie → I think this is the answer the question is looking for given the example request that contained the “Cookie” header. However, see the following:
        i. I think this question could be a little more specific given you could say the “Keep-Alive” header could be used to continue a client session. Perhaps the question could read, “which request header will return to a client session?”
        ii. Technically, cookies aren’t the only way to maintain HTTP sessions. This question implies cookies are only used and required for sessions.

Example HTTP Requests and Responses

HTTP Request

17. What is the request method?
    a. POST
18. Which header expresses the client's preference for an encrypted response?
    a. Upgrade-Insecure-Requests
19. Does the request have a user session associated with it?
    a. No
20. What kind of data is being sent from this request body?
    a. Username & Password

HTTP Response

21. What is the response status code?

    a. 200
22. What web server is handling this HTTP response?
    a. Apache
23. Does this response have a user session associated with it?
    a. Yes
24. What kind of content is likely to be in the [page content] response body?
    a. HTML code
25. If your class covered security headers, what security request headers have been included?
    a. Strict-Transport-Security
        i. See this webpage: https://docs.spring.io/spring-security/site/docs/4.2.x/reference/html/headers.html
    b. X-Content-Type
        i. See this webpage: https://docs.spring.io/spring-security/site/docs/4.2.x/reference/html/headers.html#headers-content-type-options
    c. X-Frame-Options
        i. See this webpage: https://docs.spring.io/spring-security/site/docs/4.2.x/reference/html/headers.html#headers-frame-options
    d. X-XSS-Protection
        i. See this webpage: https://docs.spring.io/spring-security/site/docs/4.2.x/reference/html/headers.html#headers-xss-protection

Monoliths and Microservices

26. What are the individual components of microservices called?
    a. According this source and many others:
        i. Clients
        ii. Identity Providers
        iii. API Gateway
        iv. Messaging Formats
        v. Databases
        vi. Static Content
        vii. Service Discovery
27. What is a service that writes to a database and communicates to other services?
    a. A Service API
28. What type of underlying technology allows for microservices to become scalable and have redundancy?
    a. Containers

Deploying and Testing a Container Set

29. What tool can be used to deploy multiple containers at once?
    a. Docker Compose
30. What kind of file format is required for us to deploy a container set?
    a. YAML

Databases

31. Which type of SQL query would we use to see all of the information within a table called “customers”?
    a. Well, I don’t know that I would call it a query “type” but I would use the “SELECT” SQL command.
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.)
    a. Again, I wouldn’t call it a “type”. I would use the “INSERT” SQL command.
33. Why would we never run “DELETE FROM <table-name>;” by itself?
    a. That SQL statement would delete the entire “<table-name>” table thus deleting all records in the table.

Bonus Challenge: The Cookie Jar

Step 3: Using Forms and a Cookie Jar

“curl” command: `curl --form "log=Ryan" --form "pwd=123456" http://localhost:8080/wp-login.php --verbose`

- **Question:** Did you see any obvious confirmation of a login? (Y/N)
    - I didn’t see any obvious confirmation of a login. However, I did see some “Set-Cookie” headers. I can’t imagine these would be set in the event of a failed login.

New “curl” command: `curl --cookie-jar ./ryan-cookies.txt --form "log=Ryan" --form "pwd=123456" http://localhost:8080/wp-login.php --verbose`

- **Question:** How many items exist in this file?
    - Three cookies exist in the file.

Step 4: Log In Using Cookies

“curl” command: `curl --cookie ./ryan-cookies.txt http://localhost:8080/wp-admin/index.php`

- **Question:** Is it obvious that we can access the Dashboard? (Y/N)
    - It’s not obvious but after some painful scanning of the “curl” output I found text that indicated we successfully accessed the dashboard.

“curl” command: `curl --cookie ./ryan-cookies.txt http://localhost:8080/wp-admin/index.php | grep Dashboard`

- **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.
    - Yes, it contains the text on the user’s Dashboard’s help sections.

Step 5: Test the “users.php” Page

“curl” command:

```
curl --cookie ./ryan-cookies.txt http://localhost:8080/wp-admin/users.php --verbose
```

- **Question:** What happens this time?
    - First, including the “verbose” option gives us the HTTP response code of “403 Forbidden” which indicates the user doesn’t have access to the resource requested. Second, some of the HTML includes the text, “sorry, you are not allowed to browse users.” This also indicates the user doesn’t have access to the URL.