Cybersecurity

Module 12 Challenge Submission File

Web Development

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

HTTP Requests and Responses

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

```
It is based on a client/server architecture where the web browsers. Act like
http clients and the web server acts as the server.
```

2. What are the parts of an HTTP request?

```
An http request contains the fallowing parts: Request line, headers,
Whitespace, and Request Body (optional).
```

3. Which part of an HTTP request is optional?

```
The request body.
```

4. What are the three parts of an HTTP response?

```
The three parts are Status line, Headers, Whitespace, Response Body.
```

5. Which number class of status codes represents errors?

```
400-499 Indicate client errors, meaning the client sent an improperly
formatted request.
500-599 Indicates server errors, meaning the server application failed
somehow.
```

6. What are the two most common request methods a security professional encounters?

```
GET and POST
```

7. Which type of HTTP request method is used to send data?

```
The PUT request method is used to send data.
```

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

```
The POST method is used and often causing a change in the state or side
effect on the server.
```

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

```
That would be located in the content-type or the body of the response.
```

Using curl

10. What are the advantages of using `curl` over the browser?

```
The command-line tool curl allows security professionals to quickly test
HTTP requests in a way that can be automated and allows them to make quick
adjustments. This also means we can test web server security configurations,
ensure web servers don't leak sensitive data, and look for vulnerabilities
on a web server.
```

11. Which `curl` option changes the request method?

```
Curl -X <method>
```

12. Which `curl` option sets request headers?

```
Curl -H <header/@file>
```

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

```
Curl -i
```

14.

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

```
curl -v -X OPTIONS
```

Sessions and Cookies

16. Which response header sends a cookie to the client?

```
HTTP/1.1 200 OK
Content-type: text/html
Set-Cookie: cart=Bob

The header that sends cookies to the client is the set-cookie. Alson with
the session info that contains the response.
```

17. Which request header will continue the client's session?

```
GET /cart HTTP/1.1
Host: www.example.org
Cookie: cart=Bob
Connection: Keep-Alive
```

Example HTTP Requests and Responses

Use the following sample HTTP request and response to answer the questions in this section:

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
```

18. What is the request method?

```
POST
```

19. Which header expresses the client's preference for an encrypted response?

```
The connection type and upgrade-insecure-request headers.
```

20. Does the request have a user session associated with it?

```
Login
```

21. What kind of data is being sent from this request body?

```
Username and password
```

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]
```

22. What is the response status code?

```
OK 200
```

23. What web server is handling this HTTP response?

```
apache
```

24. Does this response have a user session associated with it?

```
Yes the sessionID is 5
```

25. What kind of content is likely to be in the [page content] response body?

```
A commpresses gzip file.
```

26. If your class covered security headers, what security request headers have been included?

```
Strict-Transport-Security: max-age=31536000
```

Monoliths and Microservices

27. What are the individual components of microservices called?

```
services
```

28. What is a service that writes to a database and communicates to other services?

```
APIs
```

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

```
Load balancer technology
```

Deploy and Test a Container Set

30. What tool can you use to deploy multiple containers at once?

```
docker-compose-ip
```

31. What kind of file format is required to deploy a container set?

```
yamal
```

Databases

32. Which type of SQL query would you use to view all the information in a table called `customers`?

```
ELECT column_name FROM customers
```

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

```
INSERT INTO table_name (column_1, column_2, column_3) VALUES (value_1,
'value_2', value_3)
```

34. Why would you never run `DELETE FROM <table-name>;` by itself?

- It will delete the entire table there is no select statement.

Bonus Activity: The Cookie Jar

Question 1: Did you see any obvious confirmation of a login? (Y/N)

```
[Enter answer here]
```

Question 2: How many items exist in this file?

```
[Enter answer here]
```

Question 3: Is it obvious that you can access the dashboard? (Y/N)

```
[Enter answer here]
```

Question 4: 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.

```
[Enter answer here]
```

Question 5: What happens this time?

```
[Enter answer here]
```