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?

```
The HTTP request and response process occurs within the client-server
architecture. CLient (such as web browser) sends a request to the server
(such as web browser) using the HTTP protocol.The request typically includes
information such as the requested resource (such as a web page),headers, and
other metadata. This client-server architecture is the basic model for how
web applications and services work over the internet, with the client making
requests and the server responding with the requested information.
```

2. What are the parts of an HTTP request?

```
1. Request line: This includes the HTTP method (such as GET or POST), the
   URI (Uniform Resource Identifier) of the requested resource, and the
   HTTP version.
2. Headers: These provide additional information about the request, such
   as the user agent (which identifies the client making the request),
   accepted languages and encodings, and cookies.
3. Request body (optional): This contains additional data that the client
   wants to send to the server, such as form data or a file upload. This
   part is only used for some HTTP methods, such as POST and PUT
```

3. Which part of an HTTP request is optional?

```
The request body. Used for sending additional data to the server and is not
required for all types of HTTP requests.
```

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

```
1. Status Line: The first line of an HTTP response contains the status
   line, which includes the HTTP protocol version< a three-digit status
   code, and a brief textual description of the status code.
2. Response Headers: usually contains one or more headers that provide
   additional information about the response, such as the content type,
   content encoding, cache control directives and much more.
3. Message Body: actual content of the HTTP response. Could be an HTML
   page, image file, JSON object, or any kind of data that the client
   requested from the server. Message body is separated from the headers
   by a blank line.
```

5. Which number class of status codes represents errors?

```
4xx class of status codes
400 Bad Request
401 Unauthorized
403 Forbidden
404 Not Found
405 Method Not Allowed
```

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

```
1. GET: use to retrieve a resource from the server.
2. POST: used to submit data to the server
```

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

```
1. POST: used to submit data to be processed to a specified resource
2. PUT: upload data to a specified resource
3. PATCH: partially update a resource on a server
```

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

```
It is in the body of the request. The type of data in the body is indicated
by the “Content-Type” header.
```

9. In which part of an HTTP response does the browser receive the web code to

generate and style a webpage?

```
The body of the response. The body of the response contains the HTML code, CSS stylesheets, JavaScript code, and any other resources (images, videos, or audio files) needed to render the webpage.
```

Using curl

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

```
- Automation. Curl can be used to automate tasks that require fetching data from a web browser or sending data to a web browser.
- Command-line interface. Curl is a command line tool that can be easily integrated into scripts or used from the command line.
- Speed. Curl can be faster than a web browser because it doesn't have to render HTML, CSS, or JavaScript. This can be especially useful for downloading large files or fetching data from API's.
- Debugging. Curl provides detailed information about the HTTP request and response, which can be useful for debugging network or server issues.
- Cross-platform compatibility. Curl is available on a wide range of platforms, including Windows, macOS, Linux, and Unix, so it can be used in a variety of environments.
    ● Curl is a command-line tool that is designed for specific use cases, and it may not provide the same user-experience as a web browser. Curl does not support rendering images or running complex client-side JavaScript, therefore may not be suitable for tasks such as browsing websites or interacting with web applications.
```

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

```
-x or --request
```

12. Which `curl` option sets request headers?

```
-H or --header
```

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

```
-i or --include
```

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

```
HTTP OPTIONS request method
```

Sessions and Cookies

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

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

Answer: The ‘Set-Cookie’ response header sends a cookie to the client
```

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

```
GET /cart HTTP/1.1
Host: www.example.org
Cookie: cart=Bob

Answer: The ‘Cookie’ request header will continue the client’s session
```

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
```

17. What is the request method?

```
POST
```

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

```
The header Upgrade-Insecure-Requests: 1 express the client's preference for
an encrypted response
```

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

```
No. Request doesn't have a user session associated with it.
```

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

```
Login credentials. Barbara&password=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]
```

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 with it?

```
Yes. SessionID=5
```

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

```
It's most likely to look like how the page is configured.
```

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

```
Set-Cookie: SESSID=8toks; httponly
```

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?

```
Load balancer technology
```

Deploy and Test a Container Set

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

```
Dockers
```

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

```
yaml
```

Databases

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

```
SELECT <column name> FROM customers;
```

32. 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> (column1, column2, column3) VALUES (value1,
‘value2’, value3)
```

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

```
It would delete the table.
```

Optional Additional Challenge 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]
```