| 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?

| Web-based Client-Server |
| --- |

1. What are the parts of an HTTP request?

| Parts of a HTTP GET Request are:   * Request line * Headers * Whitespace * Request body (which is optional) |
| --- |

1. Which part of an HTTP request is optional?

| Request body |
| --- |

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

| Well.. there are four parts.   * Status line * Headers * Whitespace * Response body |
| --- |

1. Which status-code number class represents errors?

| 400 codes |
| --- |

1. What are the two most common request methods for a security professional to encounter?

| GET and POST requests |
| --- |

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

| POST |
| --- |

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

| Request body |
| --- |

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

| Response body |
| --- |

### Using cURL

1. What are the advantages of using curl over the browser?

| Per the information from the StudentGuide:  Cybersecurity professionals need to be able to quickly test HTTP requests in a way that can be automated, but also allows them to make adjustments as they work.  In a security context, we can use curl to send customized HTTP requests that allow security professionals to:   * Test web server security configurations. * Ensure web servers don't leak sensitive data through their HTTP responses. * Verify that servers only respond to certain request types. * Look for vulnerabilities on a web server. |
| --- |

1. Which curl option changes the request method?

| -X |
| --- |

1. Which curl option sets request headers?

| -H, --header <header/@file>  This passes custom header(s) to server |
| --- |

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

| -I, --head  This show document info only |
| --- |

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

| Options |
| --- |

### Sessions and Cookies

I had to get more information for the following two questions, because 1) I wasn’t sure what was being asked since there were answers already in the answer blocks and 2) I was thinking set-cookie was used as a persistent cookie and not a session. So, I used the following site to help understand: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

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

| HTTP/1.1 200 OK  Content-type: text/html  Set-Cookie: cart=Bob  Set-cookie: cart=Bob Set-cookie headers is a part of the response that is sent back from the server to the client |
| --- |

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

| GET /cart HTTP/1.1  Host: www.example.org  Cookie: cart=Bob  Cookie: cart=Bob  This is a continuation of the previous response, as with every subsequent request to the server, the browser is sending the stored cookies back to the server using the Cookie header. |
| --- |

### 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 |
| --- |

1. What is the request method?

| POST |
| --- |

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

| Upgrade-Insecure-Requests: 1 |
| --- |

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

| No  However, if we go by a very loose definition, we could argue yes, since the connection is “keep-alive”, which in essence means that the current TCP connection/session is kept alive until it’s closed. But a specific user? No. |
| --- |

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

| Barbara’s credentials   * username=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] |
| --- |

1. What is the response status code?

| 200 OK |
| --- |

1. What web server is handling this HTTP response?

| Apache |
| --- |

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

| Yes  SessionID=5 |
| --- |

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

| text/html |
| --- |

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

| I do not believe we covered this in class… however, I went to the following site for education: <https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html>  X-Frame-Options: DENY   * Avoid click jacking and their content isn’t embedded into another site   X-XSS-Protection: 1; mode=block   * Enables XSS filtering. Rather than sanitizing the page, the browser will prevent rendering of the page if an attack is detected.   X-Content-Type: NoSniff   * Prefents browsers from guessing the media type, which is known as MIME sniffing. If this is is allowed, it could allow a browser to transfer non-executable content into executable.   According to the OWASP site, the other items they consider part of the security request headers are:   * Content-Type * Strict-Transport-Security * Set-Cookie * Server |
| --- |

### Monoliths and Microservices

1. What are the individual components of microservices called?

| Front-end Server, which is responsible for the interaction between the user and the systems  Back-end Server, which executes business logic and is the intermediary between the front end and the database  Database, which is used to store the information |
| --- |

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

| Application Programming Interface (API) on the back-end server.  I’m presuming this is what you are looking for since an API can be written/coded/set-up to do what is needed. It can write to a Database (in such a case as an employee needing to update inventory on their Database). But it can also be used to update other services and systems (at the same time, or separate). |
| --- |

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

| Load Balancer |
| --- |

### Deploying and Testing a Container Set

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

| Docker Compose |
| --- |

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

| YAML, or .yml |
| --- |

### Databases

1. Which type of SQL query would you use to view all of the information within a table called customers?

| SELECT \* FROM customers; |
| --- |

1. 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, ...); |
| --- |

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

| It will delete the entire table |
| --- |

### Bonus Activity: The Cookie Jar

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

| No, there was no obvious confirmation. However, there was also no error. |
| --- |

**Question 2**: How many items exist in this file?

| 3 |
| --- |

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

| Yes, but you have to scroll up to see the information. |
| --- |

**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.

| Yes. The output that we received from the curl command (curl --cookie ./ryancookies.txt <http://localhost:8080/wp-admin/index.php>) is showing all the .html code that was used to create the page. If you know how to read it, you can find the information that you are looking for. |
| --- |

**Question 5**: What happens this time?

| It still gives you the .html code, but gives you the ‘Cheatin’” page. |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.