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 Client-Server architecture.
```

2. What are the parts of an HTTP request?

```
An HTTP request is made up of 3 major components. 1) The request line, which
includes the method, URI and HTTP version. 2) The Headers, which includes
information like host, user-agent, types of acceptable media that can be
processed, content-type, authorization and cookies. 3) The Body, which is
primarily used by the client when using POST or PUT methods.
```

3. Which part of an HTTP request is optional?

```
The Body of an HTTP request is optional.
```

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

```
An HTTP response is made up of a Status Line, Header, & Body. The status
line contains the HTTP Version, a Status Code and an explanation of the
status code. The Header contains Content-type and length, Server
information, Date and Cookies. The body is where any requested data by the
client is sent by the server.
```

5. Which number class of status codes represents errors?

```
The 400’s represent errors.
```

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?

```
POST and PUT.
```

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

```
The message body usually contains the data being sent.
```

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

```
The response body contains the necessary code to style and generate the
webpage.
```

Using curl

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

```
There are instances where we need to access a web server that has no website
or visual UI. Containers are an example of a resource that needs a command
line tool to send and receive HTTP requests from. curl allows us to do this.
```

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

```
-X
```

12. Which `curl` option sets 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 what HTTP requests an HTTP server will accept?

```
OPTIONS
```

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 ← this 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 ← this 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?

```
Upgrade-Insecure-Requests: 1
```

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

```
No cookie has been assigned yet.
```

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

```
Login information for a user named “Barbara” with the 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 OK
```

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?

```
text/html
```

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

```
X-Content-Type: NoSniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
```

Monoliths and Microservices

26. What are the individual components of microservices called?

```
Each component is called a service.
```

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

```
This is called an API.
```

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

```
Modularity.
```

Deploy and Test a Container Set

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

```
Docker
```

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 * 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
```

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

```
Let’s say we are querying a table named “emails”, the command DELETE FROM
emails will remove the entire table.
```

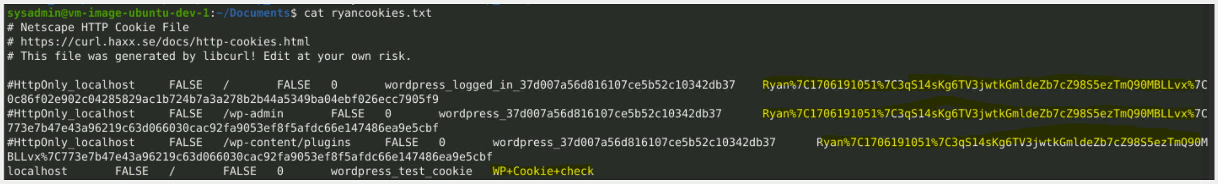
Optional Additional Challenge Activity: The Cookie Jar

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

```
There is no obvious confirmation of a login.
```

Question 2: How many items exist in this file?

```
We see 3 cookies for Ryan and one test cookie.
```



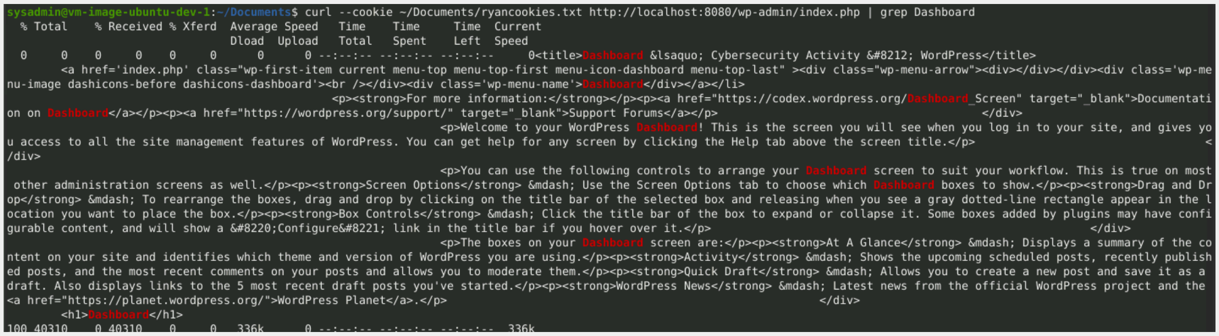
```
sysadmin@vm-image-ubuntu-dev-1:~/Documents$ cat ryancookies.txt
# Netscape HTTP Cookie File
# https://curl.haxx.se/docs/http-cookies.html
# This file was generated by libcurl! Edit at your own risk.

#HttpOnly_localhost     FALSE   /       FALSE   0       wordpress_logged_in_37d007a56d816107ce5b52c10342db37    Ryan%7C1706191051%7C3qS14sKg6TV3jwtkGmldeZb7cZ98S5ezTmQ90MBLLvx%7C
0c86f02e902c04285829ac1b724b7a3a278b2b44a5349ba04ebf026ecc7905f9
#HttpOnly_localhost     FALSE   /wp-admin       FALSE   0       wordpress_37d007a56d816107ce5b52c10342db37      Ryan%7C1706191051%7C3qS14sKg6TV3jwtkGmldeZb7cZ98S5ezTmQ90MBLLvx%7C
773e7b47e43a96219c63d066030cac92fa9053ef8f5afdc66e147486ea9e5cbf
#HttpOnly_localhost     FALSE   /wp-content/plugins     FALSE   0       wordpress_37d007a56d816107ce5b52c10342db37      Ryan%7C1706191051%7C3qS14sKg6TV3jwtkGmldeZb7cZ98S5ezTmQ90M
BLLvx%7C773e7b47e43a96219c63d066030cac92fa9053ef8f5afdc66e147486ea9e5cbf
localhost       FALSE   /       FALSE   0       wordpress_test_cookie   WP+Cookie+check
```

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

```
The dashboard is not obviously accessible.
```

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.

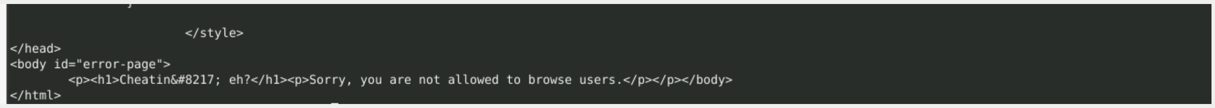
```
It appears as if we are successfully logged in to the Editor’s dashboard.
```



```
sysadmin@vm-image-ubuntu-dev-1:~/Documents$ curl --cookie ~/Documents/ryancookies.txt http://localhost:8080/wp-admin/index.php | grep Dashboard
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0<title>Dashboard &lsaquo; Cybersecurity Activity &#8212; WordPress</title>
        <a href='index.php' class="wp-first-item current menu-top menu-top-first menu-icon-dashboard menu-top-last" ><div class="wp-menu-arrow"><div></div></div><div class='wp-me
nu-image dashicons-before dashicons-dashboard'><br /></div><div class='wp-menu-name'>Dashboard</div></a></li>
                                                 <p><strong>For more information:</strong></p><p><a href="https://codex.wordpress.org/Dashboard_Screen" target="_blank">Documentati
on on Dashboard</a></p><p><a href="https://wordpress.org/support/" target="_blank">Support Forums</a></p>                                        </div>
                                                                <p>Welcome to your WordPress Dashboard! This is the screen you will see when you log in to your site, and gives yo
u access to all the site management features of WordPress. You can get help for any screen by clicking the Help tab above the screen title.</p>                                <
/div>
                                                                <p>You can use the following controls to arrange your Dashboard screen to suit your workflow. This is true on most
 other administration screens as well.</p><p><strong>Screen Options</strong> &mdash; Use the Screen Options tab to choose which Dashboard boxes to show.</p><p><strong>Drag and Dr
op</strong> &mdash; To rearrange the boxes, drag and drop by clicking on the title bar of the selected box and releasing when you see a gray dotted-line rectangle appear in the l
ocation you want to place the box.</p><p><strong>Box Controls</strong> &mdash; Click the title bar of the box to expand or collapse it. Some boxes added by plugins may have confi
gurable content, and will show a &#8220;Configure&#8221; link in the title bar if you hover over it.</p>                                                        </div>
                                                                <p>The boxes on your Dashboard screen are:</p><p><strong>At A Glance</strong> &mdash; Displays a summary of the co
ntent on your site and identifies which theme and version of WordPress you are using.</p><p><strong>Activity</strong> &mdash; Shows the upcoming scheduled posts, recently publish
ed posts, and the most recent comments on your posts and allows you to moderate them.</p><p><strong>Quick Draft</strong> &mdash; Allows you to create a new post and save it as a
draft. Also displays links to the 5 most recent draft posts you've started.</p><p><strong>WordPress News</strong> &mdash; Latest news from the official WordPress project and the
<a href="https://planet.wordpress.org/">WordPress Planet</a>.</p>                                                               </div>
        <h1>Dashboard</h1>
100 40310    0 40310    0     0   336k      0 --:--:-- --:--:-- --:--:--  336k
```

Question 5: What happens this time?

```
We get this message denying us access to users.
```



```
                        </style>
</head>
<body id="error-page">
        <p><h1>Cheatin&#8217; eh?</h1><p>Sorry, you are not allowed to browse users.</p></p></body>
</html>
```