



Cybersecurity

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?

Client - Server. Client requests over http to the web server. Web server queries the application server. Application server sends data from database server. The requested information makes its way back to the client → Database → Application Server → Web Server → Client.

2. What are the parts of an HTTP request?

- 1) Command :Get, head, post etc (request line). Can contain query parameters.
- 2) Header: Identifies and validates user
- 3) Whitespace: Indicates end of request
- 4) Body

3. Which part of an HTTP request is optional?

Body

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

- 1) Status line. Contains response status code
- 2) Header. Contains additional information about the response

3) Response body. Contains resource requested by the client and all of the web code.

5. Which status-code number class represents errors?

400 (client errors) and 500 (server errors)

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

GET and POST

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

POST is the most typical. You could also say PUT sends data, since it'll "update or replace resources" which would require data being sent/

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

The header.

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

The response body.

Using cURL

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

- 1) Can easily find status code in http responses.
- 2) Can test web server security configurations.
- 3) Still possible to access a web server that does not have a website with nav links or a visual UI
- 4) It's much better for security audits on web servers

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

Curl --request POST. Specify using the request modifier then write the desired method.

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. You would want to know the communication options for the HTTP server.

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
```

The set-cookie header.

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

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

Cart HTTP/1.1

A persistent connection is the default on HTTP/1.1 requests.

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.

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

Since the connection has “keep-alive” specified, there is a TCP connection in place. On HTTP 1.1 the client can send requests and receive answers from the server any number of times. This connection and series of requests and responses could be considered the user’s session.

If the question specified, “is there a user session id” the answer would be no. I am contrasting this to question 23.

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

The user is entering Barbara and password into a form using the information specified in the content type header.

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, it was a success.

22. What web server is handling this HTTP response?

Apache

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

Yes, the session id=5

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

Text

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

Strict transport security, X-Content-Type, X-Frame-Options and X-XSS-Protection

Monoliths and Microservices

26. What are the individual components of microservices called?

The components are separated into their own individual machines that each run a “service”. A service is generally accepted as a portion of a stack, or an individual component of a microservice.

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

Product API

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

The replication of identical components into containers. You could say the technology is called containerization.

Deploying and Testing a Container Set

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

Docker Compose

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

.yml

Databases

31. Which type of SQL query would you use to view all of the information within 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 customers
```

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

It will delete the entire table.