Questions

Before you work through the questions below, please create a new file and record your answers there. This will be your homework deliverable.

HTTP Requests and Responses

Answer the following questions about the HTTP request and response process.

1. What type of architecture does the HTTP request and response process occur in?
    a. This occurs as part of Client-server Architecture. This is a component of OSI layer 7 also known as the “Application Layer.”
2. What are the different parts of an HTTP request?
    a. The HTTP request is composed of three different parts:
        i. The Request Line
        ii. The Request Header
        iii. The Request Body

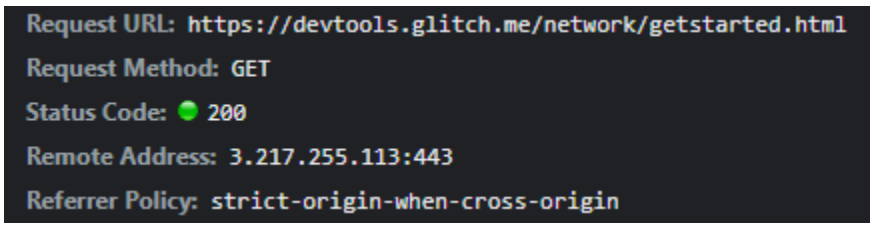
The **Request Line** is the very first line of the HTTP request and is also composed of three parts.

1. The HTTP method used

2. The request URI (Uniform Resource Identifier)

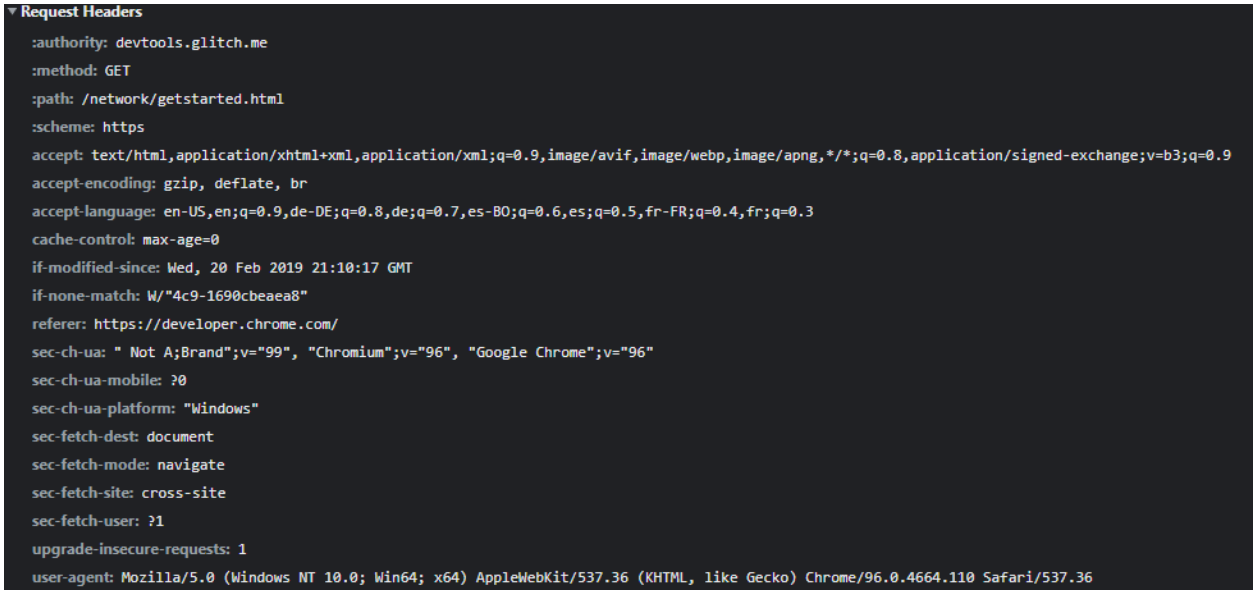
3. The HTTP protocol Version

Here is an example:



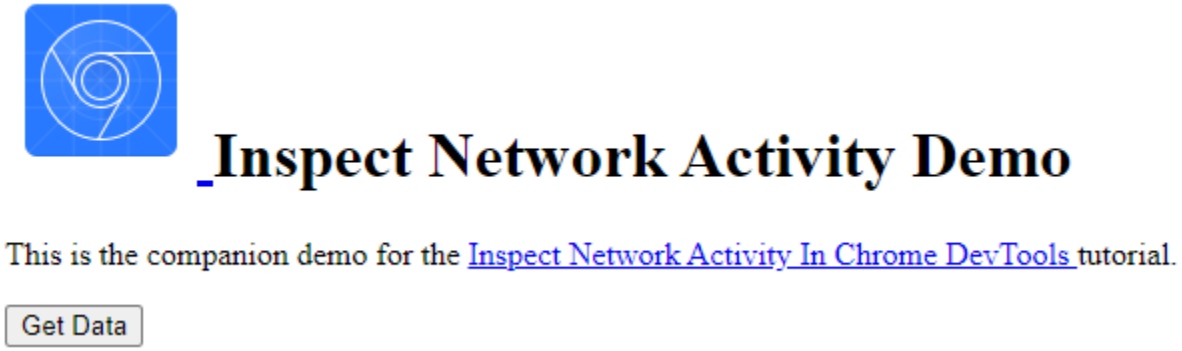
The **Request Header** provides information about the request’s context in order for the server to tailor a response to the request.

Here is an example:



The **Request Body** is data sent by the client to the requester's API (Application Programming Interface). In turn a **Response Body** is the information the requester's API sends back to the client.

Here is an example:



3. Which part of an HTTP request is optional?
    a. The **Request Body** is optional

4. What are the three parts of an HTTP response?
    a. An HTTP response is comprised of these three components:
        i. Status Line - describing the message
        ii. Header - containing attributes
        iii. Body (optional) - containing data

Here's an example:

```
HTTP/1.1 200 OK
Server: nginx/1.9.2
Date: Thu, 12 Mar 2020 06:02:20 GMT
Content-Type: text/html
Content-Length: 12905
Last-Modified: Wed, 01 Jan 2020 17:09:18 GMT
Connection: close
ETag: "5e0cd23e-3269"
Accept-Ranges: bytes
```

5. Which number class of status codes represents errors?
    a. 400 codes indicate client errors
    b. 500 codes indicate server errors

6. What are the two most common request methods that a security professional will encounter?
    a. GET and POST are the two most common
        i. **GET** method requests ask for data from a server in order to retrieve data
        ii. **POST** method requests send data to a specified location/resource
        iii. Other methods such as HEAD, PUT, DELETE, CONNECT, OPTIONS, TRACE, and PATCH exist as well but are not as frequently used depending on the situation

7. Which type of HTTP request method is used for sending data?
    a. **POST** is used to send data to a server with the purpose of creating and/or updating a resource

8. Which part of an HTTP request contains the data being sent to the server?
    a. The Request Body **POST** request sends data to the server

9. In which part of an HTTP response does the browser receive the web code to generate and style a web page?
    a. The Response Body data receives it along with the response

Using curl

Answer the following questions about curl:

10. What are the advantages of using curl over the browser?
    a. Curl is free, and can be used on most command lines for the purpose of
        i. Authentication

ii. HTTP post
iii. SSL connections
iv. Proxy support
v. FTP uploads
vi. Saving URL to file
vii. Downloading

11. Which curl option is used to change the request method?
    a. This can be done using the flags: -X or --request

12. Which curl option is used to set request headers?
    a. The flags used are -H, or --header

13. Which curl option is used to view the response header?
    a. The flags used here are -i, or --include

14. Which request method might an attacker use to figure out which HTTP requests an HTTP server will accept?
    a. An attacker could likely use a **GET** request as it requests data from a server and can be used to determine which HTTP requests that the server will accept
    b. **OPTIONS** is another likely method as it has the capability to list out the communication options of the target resource

Sessions and Cookies

Recall that HTTP servers need to be able to recognize clients from one another. They do this through sessions and cookies.

Answer the following questions about 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** sends a cookie to the client which appears to be cart=Bob

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

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

- The **cookie** itself will continue the client's session as they navigate through the website

Example HTTP Requests and Responses

Look through the following example HTTP request and response and answer the following questions:

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?
    a. **POST**
18. Which header expresses the client's preference for an encrypted response?
    a. Upgrade-Insecure-Requests: 1

19. Does the request have a user session associated with it?
    a. Not yet as the session is not reestablished since this appears to be the initial request and no session ID is specified

20. What kind of data is being sent from this request body?
    a. Login credentials of the user specifying a username of “Barbara” and a password of “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?
    a. The response code is **200** meaning successful
22. What web server is handling this HTTP response?
    a. **Apache**
23. Does this response have a user session associated with it?
    a. Yes it does, **Set-Cookie: SessionID=5**

24. What kind of content is likely to be in the [page content] response body?
    a. Content type specifies (**Content-Type: text/html)** so most like the website itself with a detailed webpage

25. If your class covered security headers, what security request headers have been included?
    a. HTTP Script Transport Security (HSTS) - Strict-Transport-Security: max-age=31536000; includeSubDomains
    b. X-Content-Type-Options HTTP - X-content-Type: NoSniff
    c. X-Frame-Options HTTP - X-Frame-Options: DENY
    d. Cros Site Scripting Protection (X-XSS) - X-XSS-Protection: 1;mode=block

Monoliths and Microservices

Answer the following questions about monoliths and microservices:

26. What are the individual components of microservices called?
    a. There are 8 core components of Microservices, they are as follows:
        i. Clients
        ii. Identity Providers
        iii. API Gateway
        iv. Messaging Formats
        v. Databases
        vi. Static Content
        vii. Management
        viii. Service Discovery

27. What is a service that writes to a database and communicates to other services?
    a. API: Application Programming Interface
28. What type of underlying technology allows for microservices to become scalable and have redundancy?
    a. Containers allow for microservices to be both scalable and redundant. This is used in conjunction with a Load Balancer

Deploying and Testing a Container Set

Answer the following questions about multi-container deployment:

29. What tool can be used to deploy multiple containers at once?
    a. **Docker Compose** can be used as a tool to deploy multiple containers
        i. This is used with *docker-compose up* and *docker-compose down* to start the containers and stop them, respectively
30. What kind of file format is required for us to deploy a container set?
    a. *YAML* file

Databases

31. Which type of SQL query would we use to see all of the information within a table called customers?
    a. **SELECT statements**
        i. SELECT * FROM Customers WHERE Last_Name='Test';

32. Which type of SQL query would we use to enter new data into a table? (You don't need a full query, just the first part of the statement.)
    a. **INSERT INTO**
        i. INSERT INTO CUSTOMERS (field1, field2, …) VALUES ('a', 'b', …)

33. Why would we never run DELETE FROM <table-name>; by itself?
    a. This would delete the entire table since it does not have a specified "where" clause