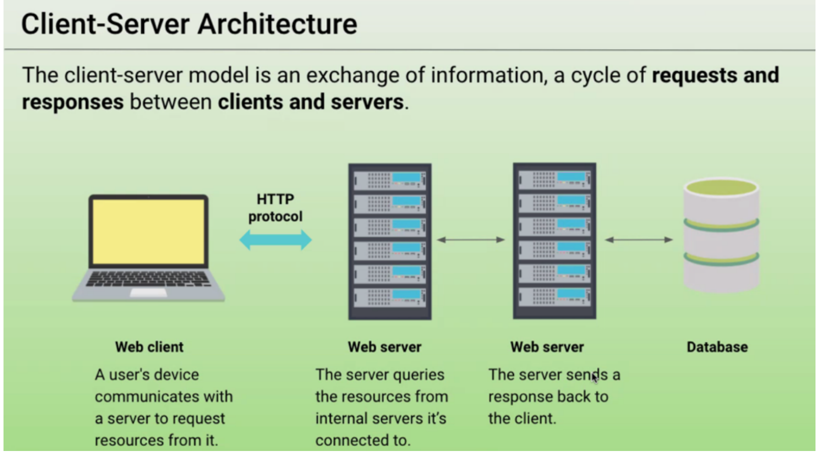
Week 14 Homework: Web Development

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?

Answer: Client-Server



Client-Server Architecture

The client-server model is an exchange of information, a cycle of **requests and responses** between **clients and servers**.

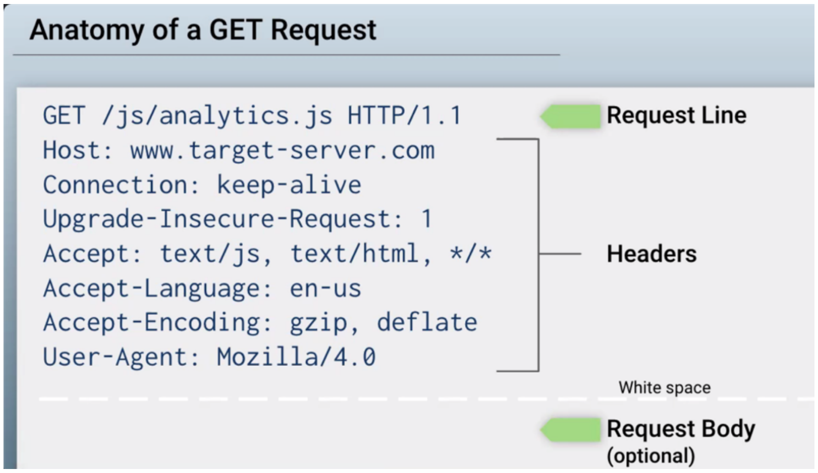
HTTP protocol
Web client
A user's device communicates with a server to request resources from it.
Web server
The server queries the resources from internal servers it's connected to.
Web server
The server sends a response back to the client.
Database

2. What are the different parts of an HTTP request?

Answer: Request line, header(s) and the body of the request

3. Which part of an HTTP request is optional?

Answer: The body of the request

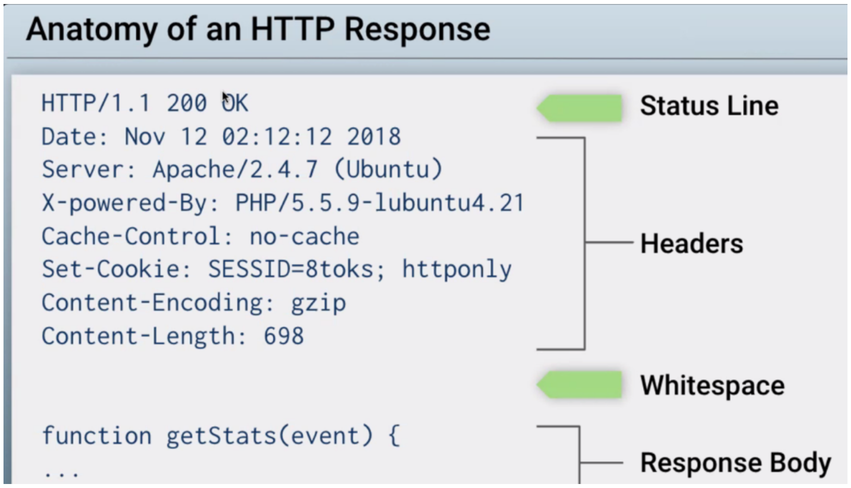


Anatomy of a GET Request

```
GET /js/analytics.js HTTP/1.1
Host: www.target-server.com
Connection: keep-alive
Upgrade-Insecure-Request: 1
Accept: text/js, text/html, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
```

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

Answer: Status Line, Header(s) and the body of the response



Anatomy of an HTTP Response

```
HTTP/1.1 200 OK
Date: Nov 12 02:12:12 2018
Server: Apache/2.4.7 (Ubuntu)
X-powered-By: PHP/5.5.9-lubuntu4.21
Cache-Control: no-cache
Set-Cookie: SESSID=8toks; httponly
Content-Encoding: gzip
Content-Length: 698


function getStats(event) {
...
```

Status Line

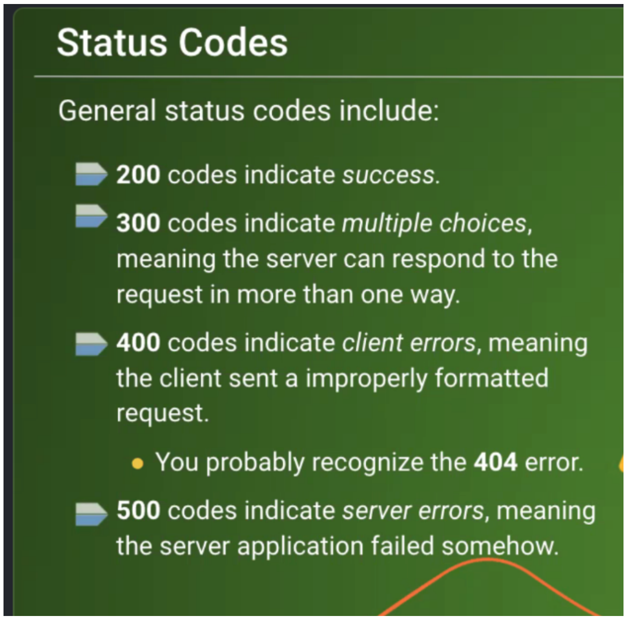
Headers

Whitespace

Response Body

5. Which number class of status codes represents errors?

Answer: 4xx are a client error and then 5xx are a server error



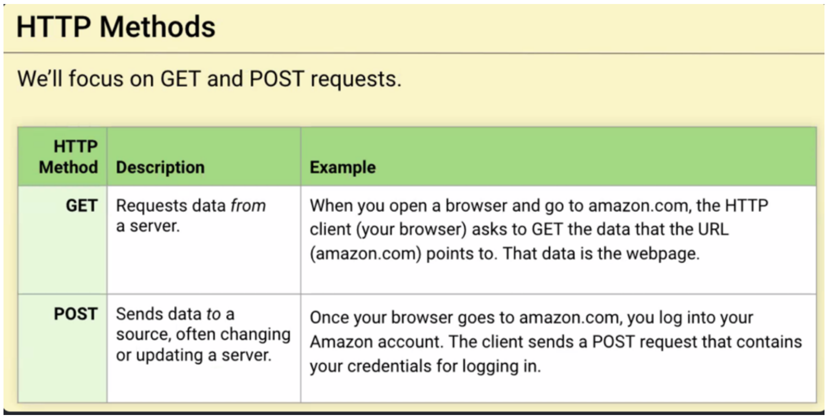
Status Codes

General status codes include:

- **200** codes indicate *success*.
- **300** codes indicate *multiple choices*, meaning the server can respond to the request in more than one way.
- **400** codes indicate *client errors*, meaning the client sent a improperly formatted request.
  - You probably recognize the **404** error.
- **500** codes indicate *server errors*, meaning the server application failed somehow.

6. What are the two most common request methods that a security professional will encounter?

Answer: GET and POST



HTTP Methods

We'll focus on GET and POST requests.

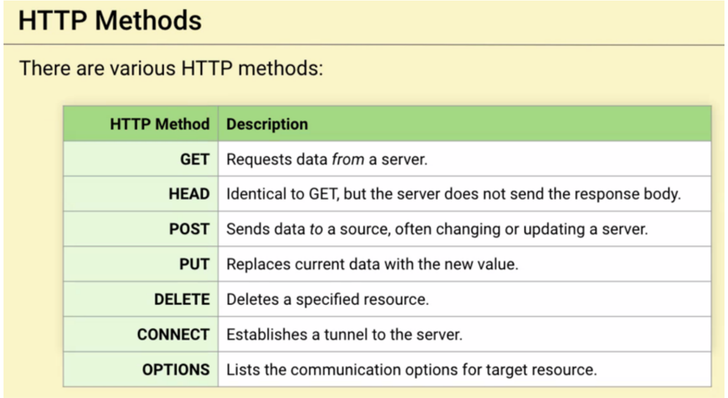
HTTP Method	Description	Example
GET	Requests data *from* a server.	When you open a browser and go to amazon.com, the HTTP client (your browser) asks to GET the data that the URL (amazon.com) points to. That data is the webpage.
POST	Sends data *to* a source, often changing or updating a server.	Once your browser goes to amazon.com, you log into your Amazon account. The client sends a POST request that contains your credentials for logging in.

7. Which type of HTTP request method is used for sending data?

Answer: POST

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

Answer: PUT



HTTP Methods

There are various HTTP methods:

HTTP Method	Description
GET	Requests data *from* a server.
HEAD	Identical to GET, but the server does not send the response body.
POST	Sends data *to* a source, often changing or updating a server.
PUT	Replaces current data with the new value.
DELETE	Deletes a specified resource.
CONNECT	Establishes a tunnel to the server.
OPTIONS	Lists the communication options for target resource.

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

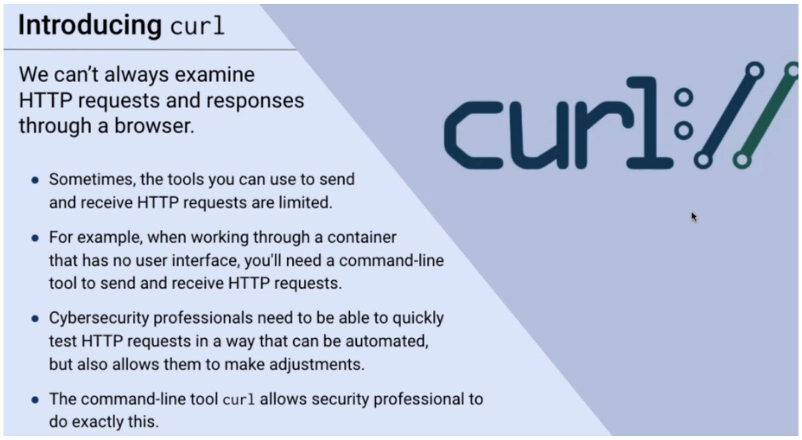
Answer:

Using curl

Answer the following questions about curl:

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

Answer: A big advantage for security professionals in utilizing the curl command vs a browser is to quickly test HTTP requests in a way that they can be automated, but also allows them to make adjustments. And browsers have limited tools to send and receive HTTP requests.



Introducing `curl`

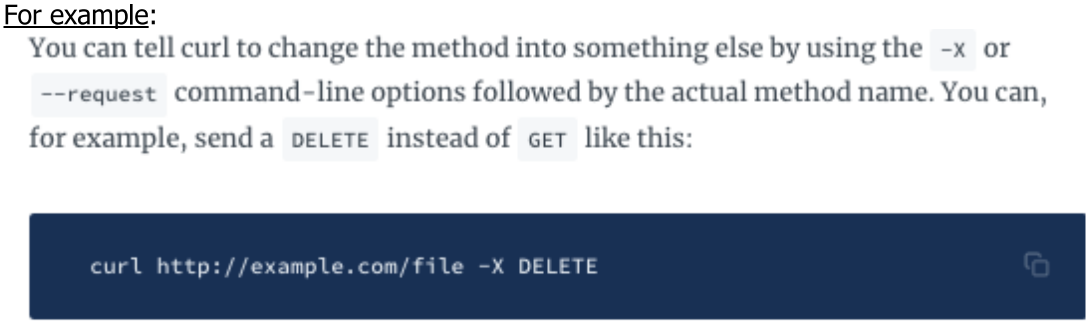
We can't always examine HTTP requests and responses through a browser.

- Sometimes, the tools you can use to send and receive HTTP requests are limited.
- For example, when working through a container that has no user interface, you'll need a command-line tool to send and receive HTTP requests.
- 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.
- The command-line tool `curl` allows security professional to do exactly this.

11. Which curl option is used to change the request method?

Answer: --request or -x

For example:



You can tell curl to change the method into something else by using the `-X` or `--request` command-line options followed by the actual method name. You can, for example, send a `DELETE` instead of `GET` like this:

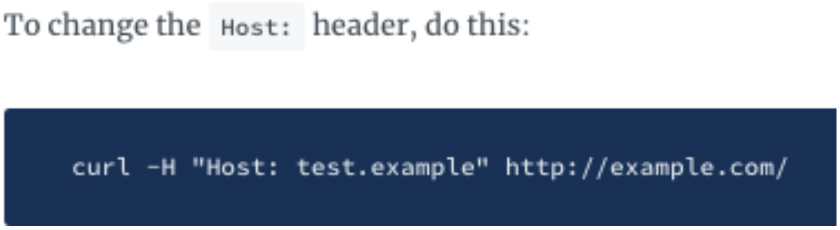
```
curl http://example.com/file -X DELETE
```

https://everything.curl.dev/http/requests

12. Which curl option is used to set request headers?

Answer: --header or -H

For example:



To change the `Host:` header, do this:

```
curl -H "Host: test.example" http://example.com/
```

https://everything.curl.dev/http/requests

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

Answer: -D

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

Answer: GET

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
```

Answer: Set-Cookie: cart=Bob

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

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

Answer: Cookie: cart=Bob

Example HTTP Requests and Responses

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
```

Answer: username=Barbara&password=password

17. What is the request method?

Answer: POST /login.php HTTP/1.1

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

Answer: Upgrade-Insecure-Requests:

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

Answer: No, just logging in and is the first step after you have logged in you should get a cookie.

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

Answer: Username and password (Request Body)

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?

Answer: 200 OK

22. What web server is handling this HTTP response?

Answer: Apache

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

Answer: Set-Cookie: SessionID=5

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

Answer: Content-Type: text/html; charset=UTF-8; which is telling the browser how to handle the content.

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

Answer: Several headers that deal with security within this HTTP Response including the following:

Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type: NoSniff
X-Frame-Options: DENY
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?

Answer: Microservice Architecture (MSA) where there are 8 core components

1. Clients
2. Identity Providers
3. API Gateway
4. Messaging Formats
5. Databases
6. Static Contents
7. Management
8. Service Directory
   https://www.optisolbusiness.com/insight/8-core-components-of-microservice-architecture

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

Answer: API Gateway
https://www3.dbmaestro.com/blog/microservices-and-databases-the-main-challenges

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

Answer: Virtual Operating System Environments assist in allowing microservices to become scalable and have redundancy while utilizing such technology as containers "Docker". https://cloudacademy.com/blog/microservices-architecture-challenge-advantage-drawback/

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?

Answer: There are a variety of tools that could be utilized such as Docker, CloudSlang, Fleet, Kiubernetes, Marathon, Nomad, OpenVZ, Packer, Solaris or Swarm.

Reference: https://mindmajix.com/open-source-containerization-devops-tools

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

Answer: The type of file format required to deploy a Docker container is 1, 2, 2.x and 3.x. There are currently several versions of the Compose file.

Reference: https://docs.docker.com/compose/compose-file/

Databases

31. Which type of SQL query would we use to see all of the information within a table called `customers`?

Answer: SELECT * FROM customers

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.)

Answer: INSERT INTO

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

Answer: If you run that command you would delete the entire table.