make a portswigger account while you’re waiting
download burp suite community edition

Introduction to Web Servers

Batman’s Kitchen 2025

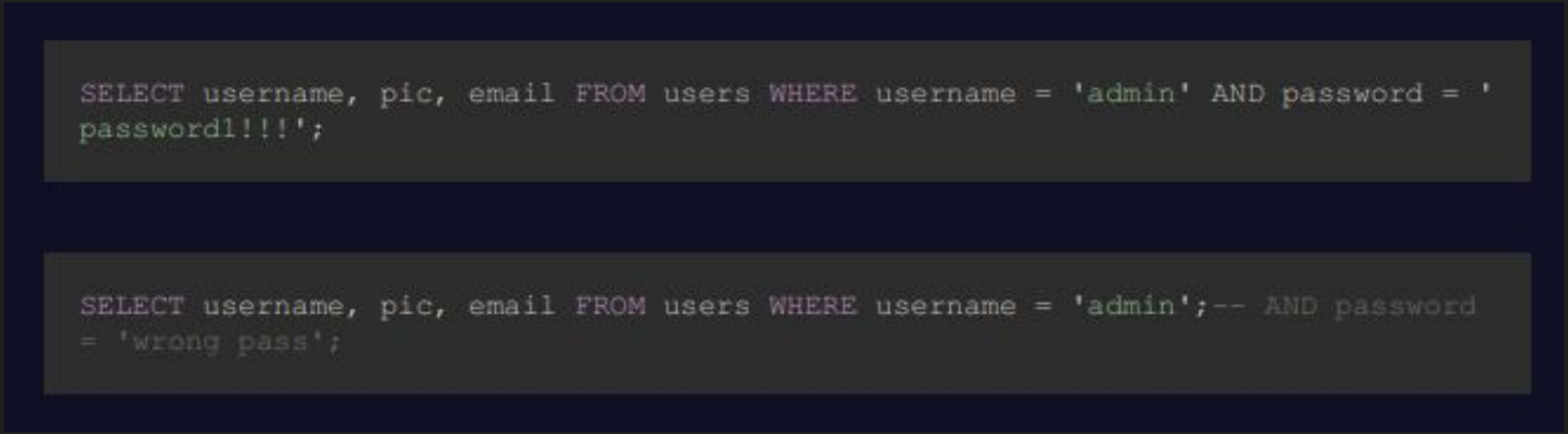
Housekeeping

Friday - AI security talk by Jono

Every tues/thurs - Mitre embedded capture the flag (reach out to @ppanic)

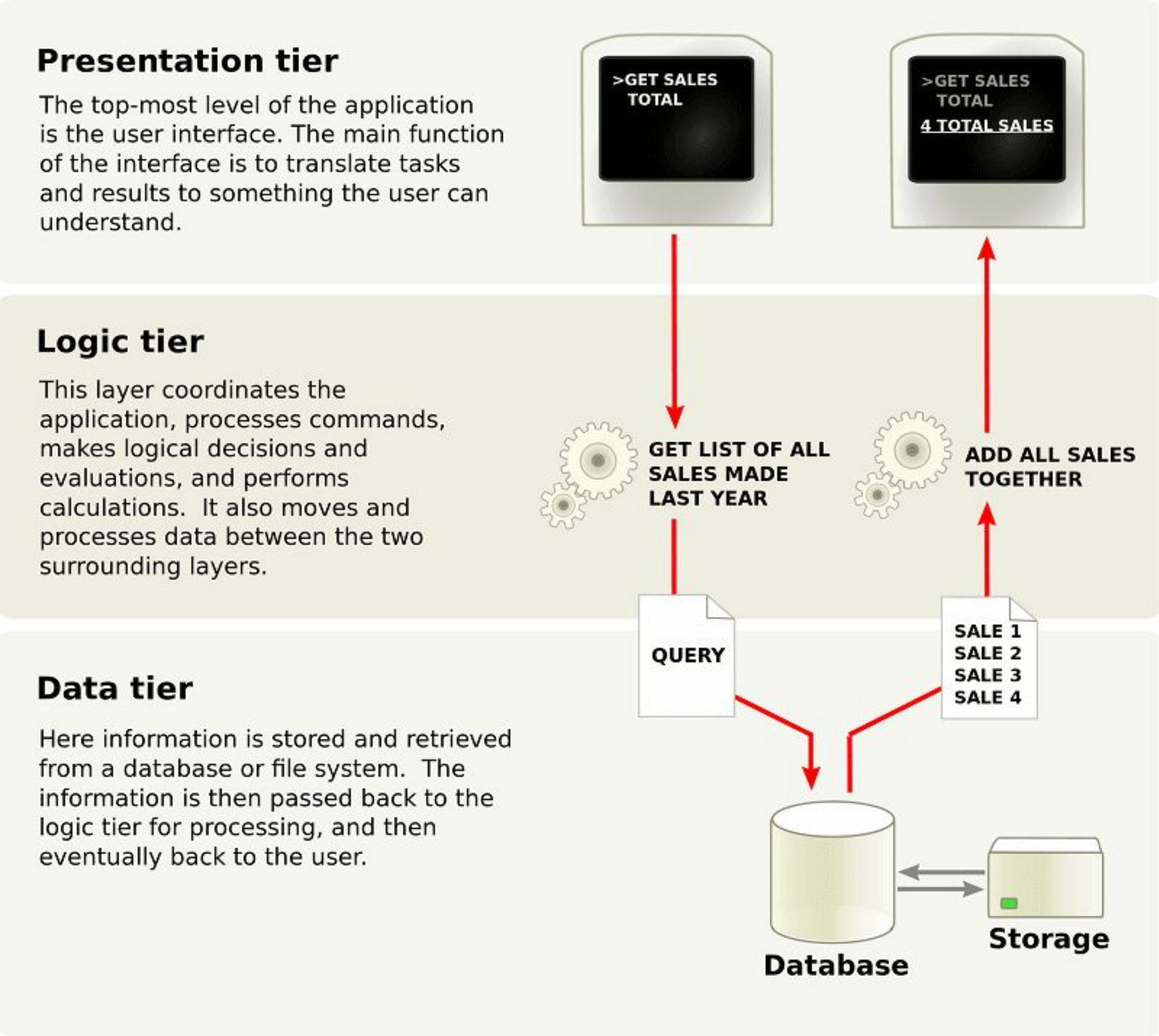
Every (mon?)/thurs - CCDC real time defense competition (reach out to @lilian4972)

Recap: SQLi



```
SELECT username, pic, email FROM users WHERE username = 'admin' AND password = '
password1!!!';
```

```
SELECT username, pic, email FROM users WHERE username = 'admin';-- AND password
= 'wrong pass';
```



Presentation tier

The top-most level of the application is the user interface. The main function of the interface is to translate tasks and results to something the user can understand.

Logic tier

This layer coordinates the application, processes commands, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers.

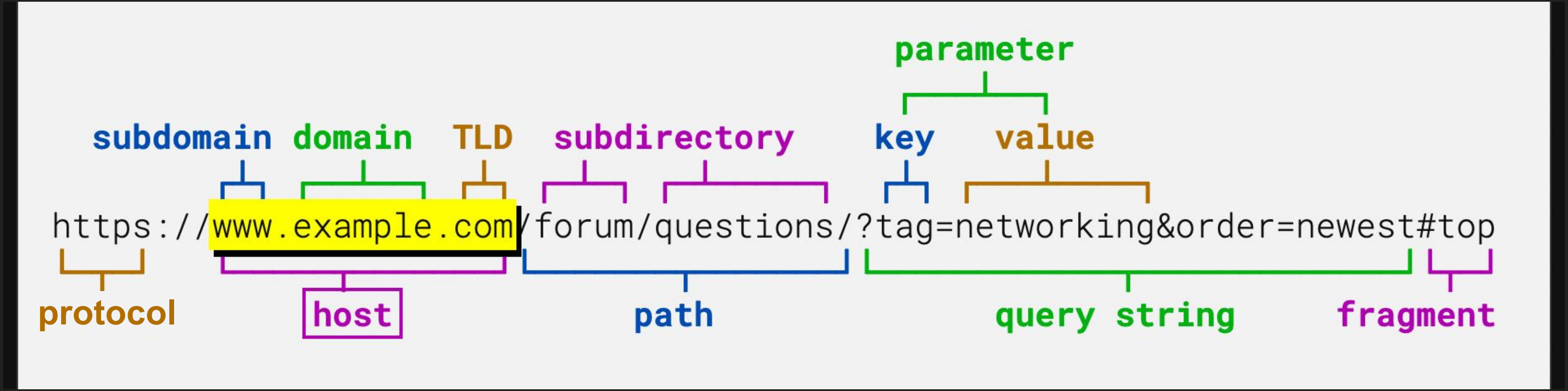
Data tier

Here information is stored and retrieved from a database or file system. The information is then passed back to the logic tier for processing, and then eventually back to the user.

src=https://en.wikipedia.org/wiki/Multitier_architecture

URL

uniform resource locator



HTTP

Hypertext transfer protocol

Requests + responses

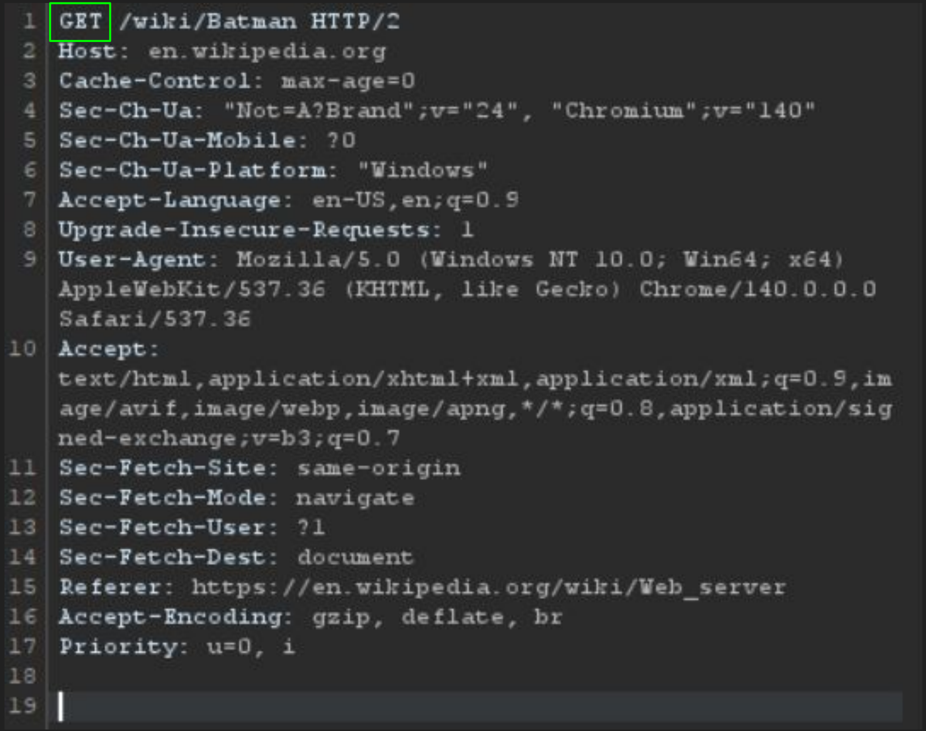
GET	The GET method requests a representation of the specified resource. Requests using GET should only retrieve data and should not contain a request content.
HEAD	The HEAD method asks for a response identical to a GET request, but without a response body.
POST	The POST method submits an entity to the specified resource, often causing a change in state or side effects on the server.
PUT	The PUT method replaces all current representations of the target resource with the request content.
DELETE	The DELETE method deletes the specified resource.
CONNECT	The CONNECT method establishes a tunnel to the server identified by the target resource.
OPTIONS	The OPTIONS method describes the communication options for the target resource.
TRACE	The TRACE method performs a message loop-back test along the path to the target resource.
PATCH	The PATCH method applies partial modifications to a resource.

src=https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Methods

GET	The GET method requests a representation of the specified resource. Requests using GET should only retrieve data and should not contain a request content.
HEAD	The HEAD method asks for a response identical to a GET request, but without a response body.
POST	The POST method submits an entity to the specified resource, often causing a change in state or side effects on the server.
PUT	The PUT method replaces all current representations of the target resource with the request content.
DELETE	The DELETE method deletes the specified resource.
CONNECT	The CONNECT method establishes a tunnel to the server identified by the target resource.
OPTIONS	The OPTIONS method describes the communication options for the target resource.
TRACE	The TRACE method performs a message loop-back test along the path to the target resource.
PATCH	The PATCH method applies partial modifications to a resource.

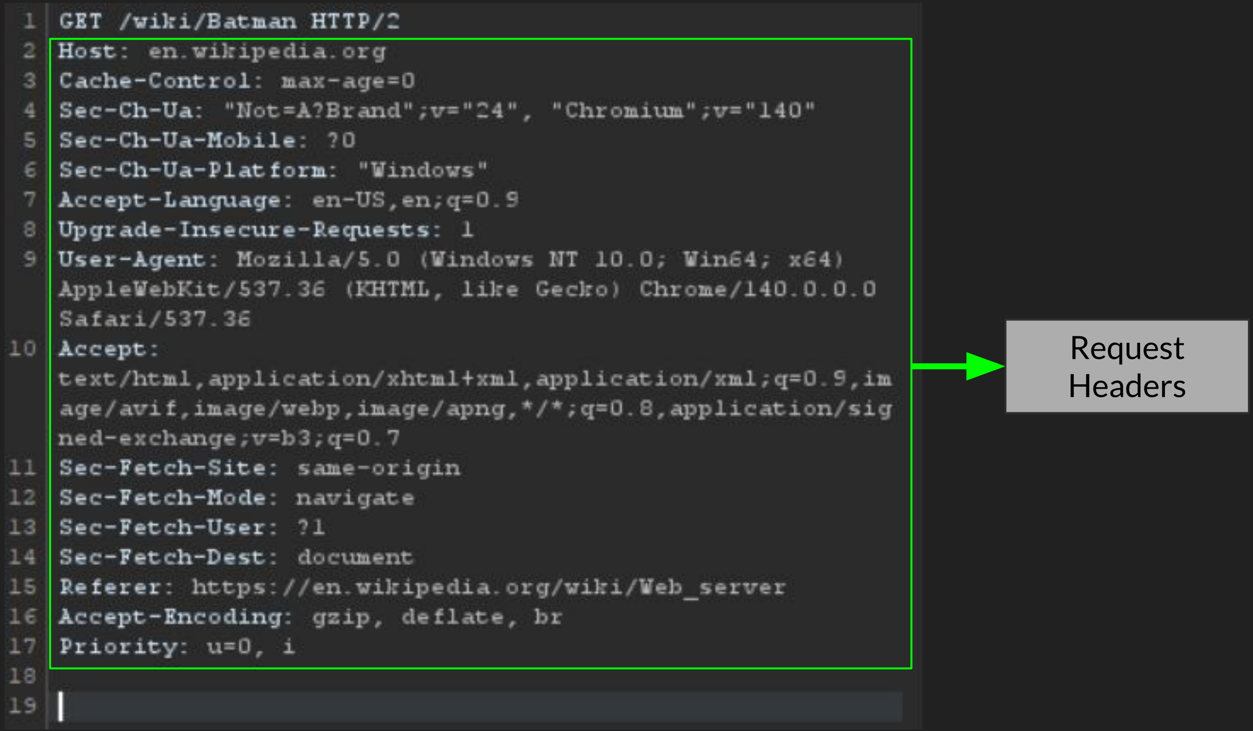
src=https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Methods

GET: https://en.wikipedia.org/wiki/Batman



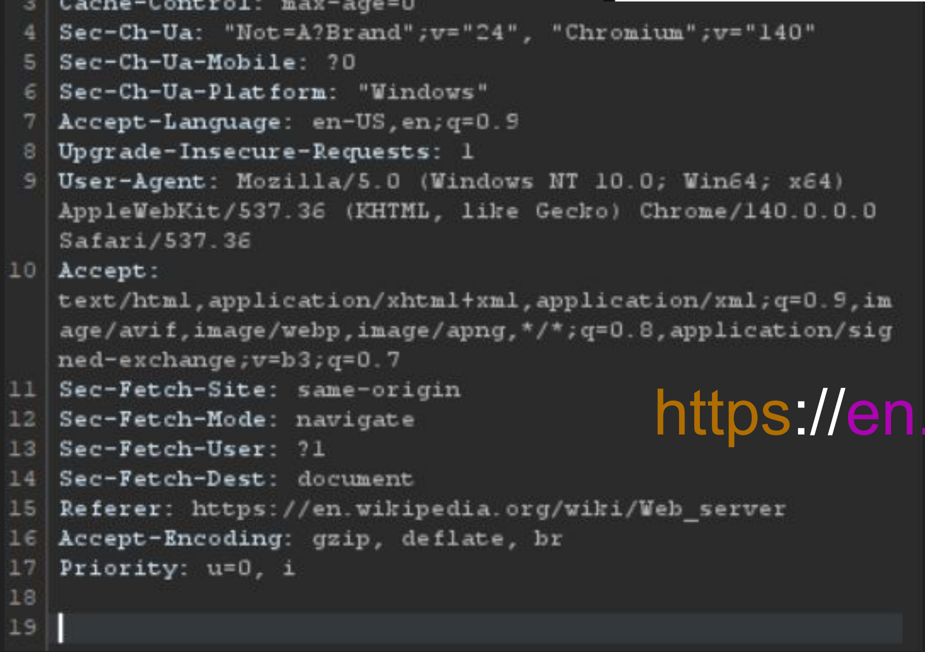
```
GET /wiki/Batman HTTP/2
Host: en.wikipedia.org
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://en.wikipedia.org/wiki/Web_server
Accept-Encoding: gzip, deflate, br
Priority: u=0, i


```

GET: https://en.wikipedia.org/wiki/Batman

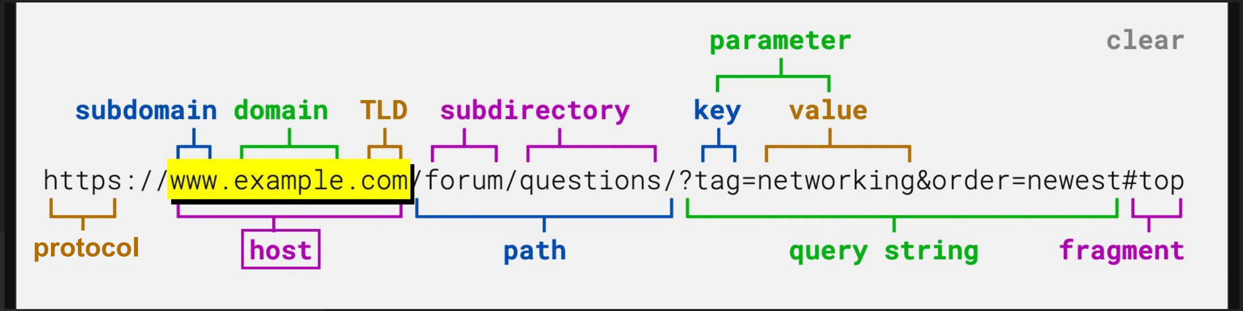


```
GET /wiki/Batman HTTP/2
Host: en.wikipedia.org
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://en.wikipedia.org/wiki/Web_server
Accept-Encoding: gzip, deflate, br
Priority: u=0, i


```

GET

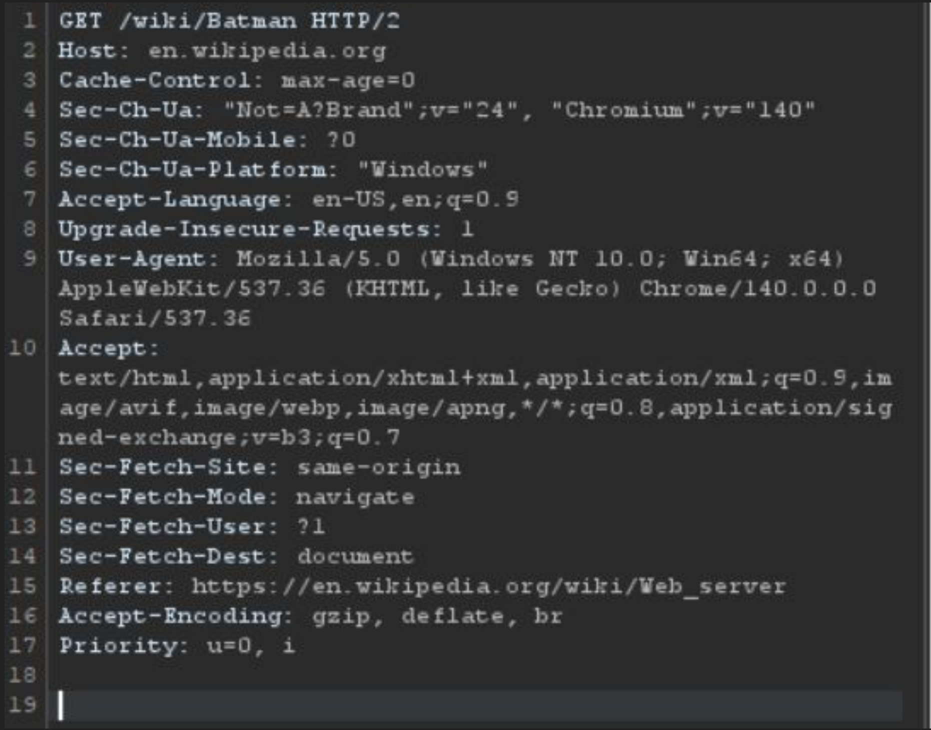


```
GET /wiki/Batman HTTP/2
Host: en.wikipedia.org
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://en.wikipedia.org/wiki/Web_server
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

```

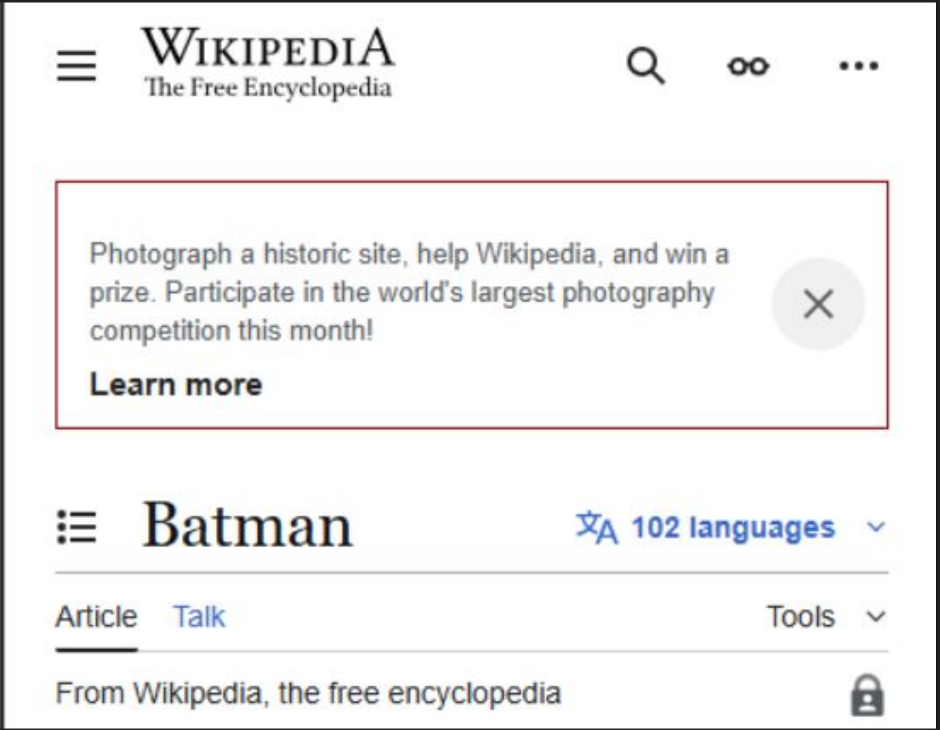


https://en.wikipedia.org/wiki/Batman

GET



```
GET /wiki/Batman HTTP/2
Host: en.wikipedia.org
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://en.wikipedia.org/wiki/Web_server
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

```



WIKIPEDIA
The Free Encyclopedia

Photograph a historic site, help Wikipedia, and win a prize. Participate in the world's largest photography competition this month!

Learn more

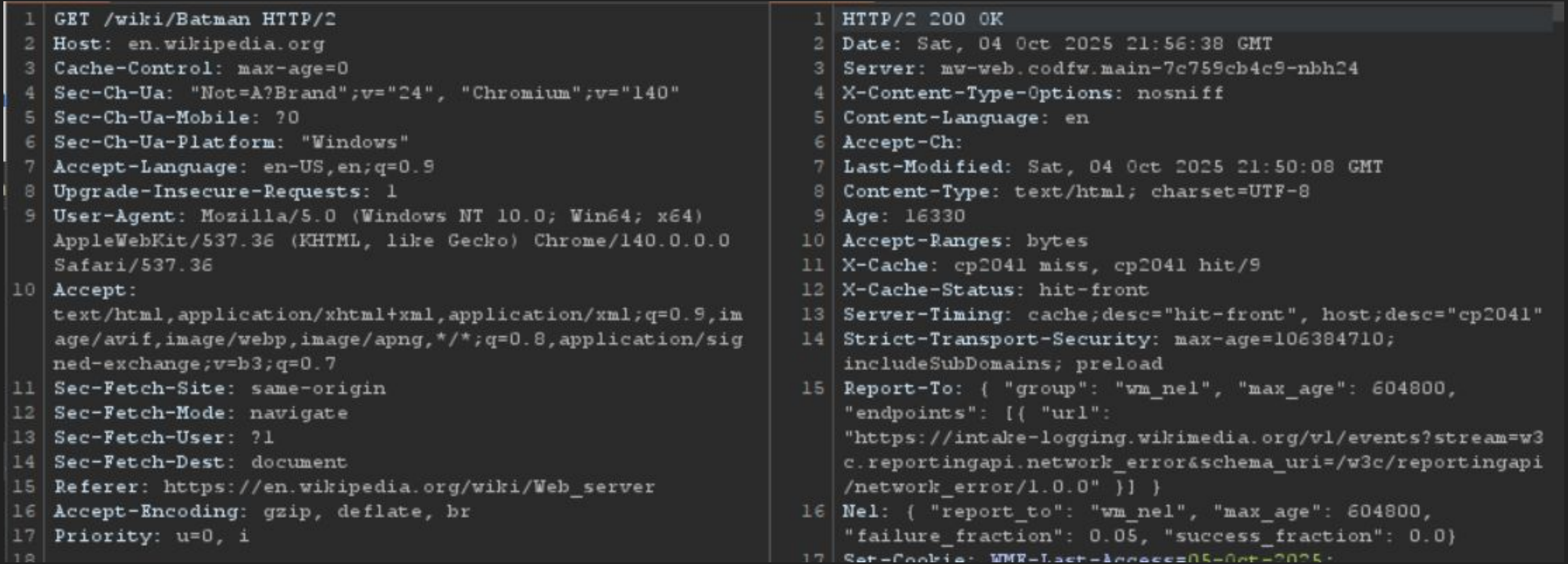
Batman

102 languages

Article Talk Tools

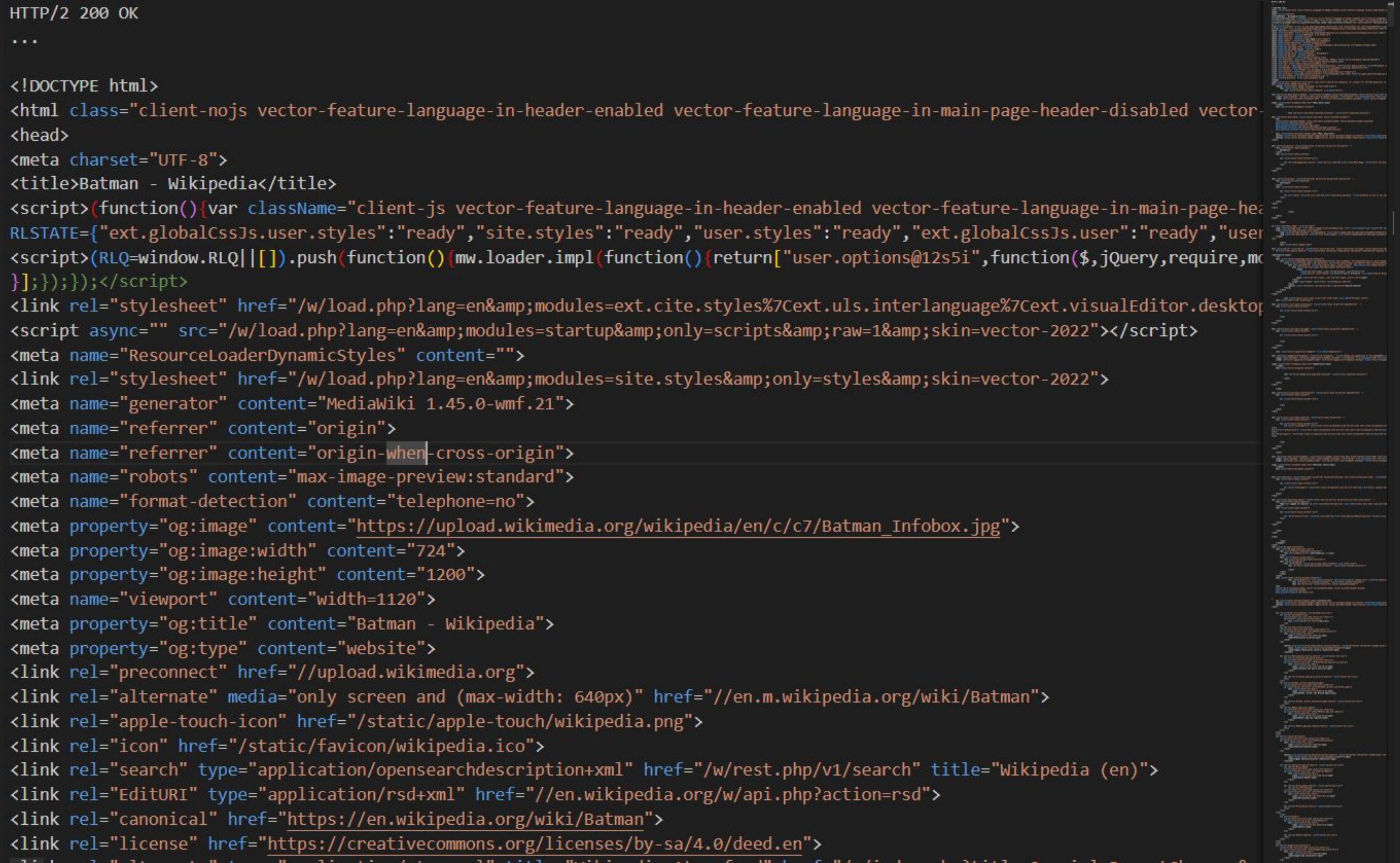
From Wikipedia, the free encyclopedia

GET



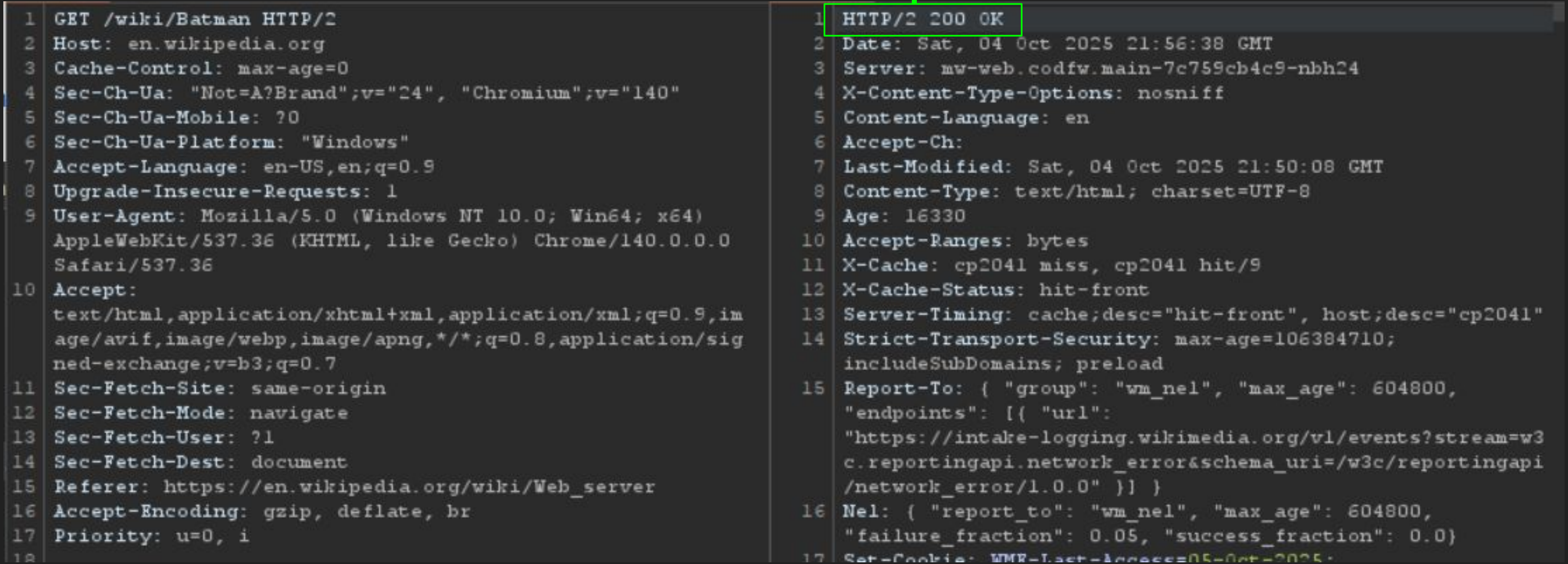
```
GET /wiki/Batman HTTP/2
Host: en.wikipedia.org
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://en.wikipedia.org/wiki/Web_server
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 200 OK
Date: Sat, 04 Oct 2025 21:56:38 GMT
Server: mw-web.codfw.main-7c759cb4c9-nbh24
X-Content-Type-Options: nosniff
Content-Language: en
Accept-Ch:
Last-Modified: Sat, 04 Oct 2025 21:50:08 GMT
Content-Type: text/html; charset=UTF-8
Age: 16330
Accept-Ranges: bytes
X-Cache: cp2041 miss, cp2041 hit/9
X-Cache-Status: hit-front
Server-Timing: cache;desc="hit-front", host;desc="cp2041"
Strict-Transport-Security: max-age=106384710; includeSubDomains; preload
Report-To: { "group": "wm_nel", "max_age": 604800, "endpoints": [{ "url": "https://intake-logging.wikimedia.org/v1/events?stream=w3c.reportingapi.network_error&schema_uri=/w3c/reportingapi/network_error/1.0.0" }] }
Nel: { "report_to": "wm_nel", "max_age": 604800, "failure_fraction": 0.05, "success_fraction": 0.0}
Set-Cookie: WMF-Last-Access=05-Oct-2025;
```



```
HTTP/2 200 OK
...

<!DOCTYPE html>
<html class="client-nojs vector-feature-language-in-header-enabled vector-feature-language-in-main-page-header-disabled vector-
<head>
<meta charset="UTF-8">
<title>Batman - Wikipedia</title>
<script>(function(){var className="client-js vector-feature-language-in-header-enabled vector-feature-language-in-main-page-hea
RLSTATE={"ext.globalCssJs.user.styles":"ready","site.styles":"ready","user.styles":"ready","ext.globalCssJs.user":"ready","user
<script>(RLQ=window.RLQ||[]).push(function(){mw.loader.impl(function(){return["user.options@12s5i",function($,jQuery,require,mo
}];});});</script>
<link rel="stylesheet" href="/w/load.php?lang=en&amp;modules=ext.cite.styles%7Cext.uls.interlanguage%7Cext.visualEditor.desktop
<script async="" src="/w/load.php?lang=en&amp;modules=startup&amp;only=scripts&amp;raw=1&amp;skin=vector-2022"></script>
<meta name="ResourceLoaderDynamicStyles" content="">
<link rel="stylesheet" href="/w/load.php?lang=en&amp;modules=site.styles&amp;only=styles&amp;skin=vector-2022">
<meta name="generator" content="MediaWiki 1.45.0-wmf.21">
<meta name="referrer" content="origin">
<meta name="referrer" content="origin-when-cross-origin">
<meta name="robots" content="max-image-preview:standard">
<meta name="format-detection" content="telephone=no">
<meta property="og:image" content="https://upload.wikimedia.org/wikipedia/en/c/c7/Batman_Infobox.jpg">
<meta property="og:image:width" content="724">
<meta property="og:image:height" content="1200">
<meta name="viewport" content="width=1120">
<meta property="og:title" content="Batman - Wikipedia">
<meta property="og:type" content="website">
<link rel="preconnect" href="//upload.wikimedia.org">
<link rel="alternate" media="only screen and (max-width: 640px)" href="//en.m.wikipedia.org/wiki/Batman">
<link rel="apple-touch-icon" href="/static/apple-touch/wikipedia.png">
<link rel="icon" href="/static/favicon/wikipedia.ico">
<link rel="search" type="application/opensearchdescription+xml" href="/w/rest.php/v1/search" title="Wikipedia (en)">
<link rel="EditURI" type="application/rsd+xml" href="//en.wikipedia.org/w/api.php?action=rsd">
<link rel="canonical" href="https://en.wikipedia.org/wiki/Batman">
<link rel="license" href="https://creativecommons.org/licenses/by-sa/4.0/deed.en">
```

GET



```
GET /wiki/Batman HTTP/2
Host: en.wikipedia.org
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://en.wikipedia.org/wiki/Web_server
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

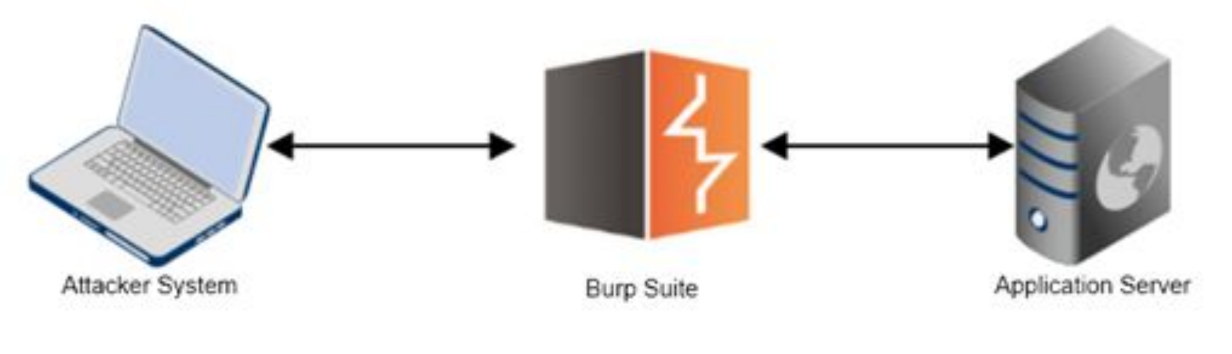
```
HTTP/2 200 OK
Date: Sat, 04 Oct 2025 21:56:38 GMT
Server: mw-web.codfw.main-7c759cb4c9-nbh24
X-Content-Type-Options: nosniff
Content-Language: en
Accept-Ch:
Last-Modified: Sat, 04 Oct 2025 21:50:08 GMT
Content-Type: text/html; charset=UTF-8
Age: 16330
Accept-Ranges: bytes
X-Cache: cp2041 miss, cp2041 hit/9
X-Cache-Status: hit-front
Server-Timing: cache;desc="hit-front", host;desc="cp2041"
Strict-Transport-Security: max-age=106384710; includeSubDomains; preload
Report-To: { "group": "wm_nel", "max_age": 604800, "endpoints": [{ "url": "https://intake-logging.wikimedia.org/v1/events?stream=w3c.reportingapi.network_error&schema_uri=/w3c/reportingapi/network_error/1.0.0" }] }
Nel: { "report_to": "wm_nel", "max_age": 604800, "failure_fraction": 0.05, "success_fraction": 0.0}
Set-Cookie: WMF-Last-Access=05-Oct-2025;
```

Response Status Code

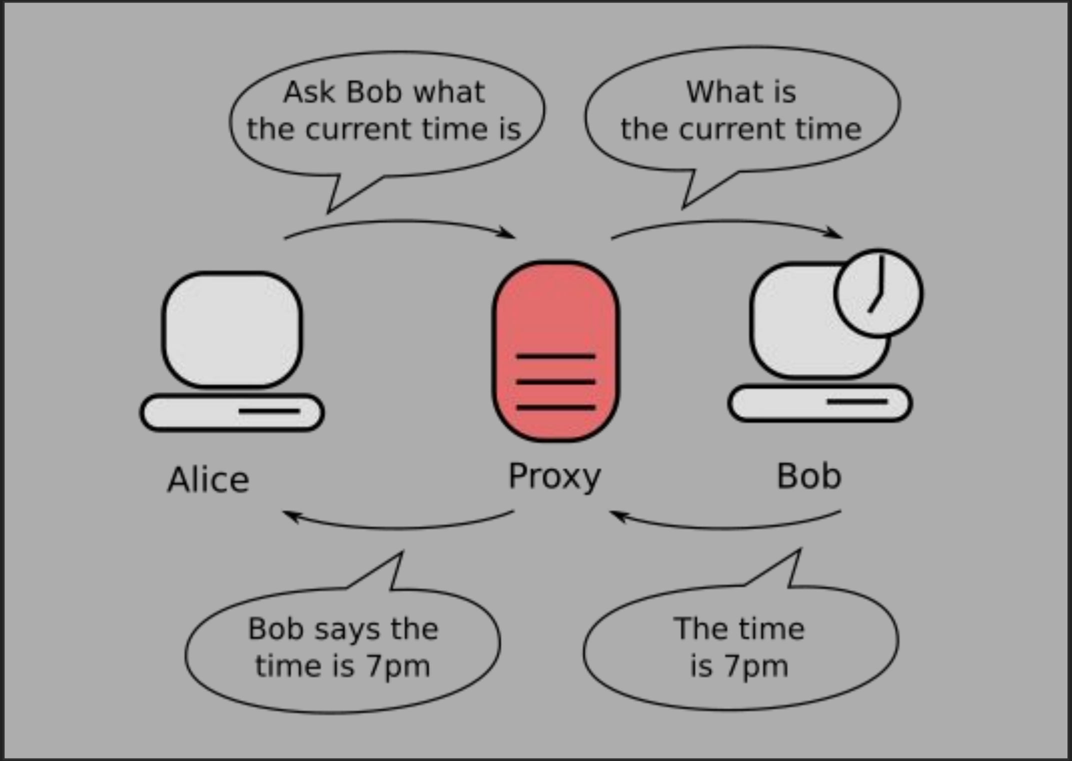
HTTP Status Codes

Informational responses	1xx
Successful responses	2xx
Redirection responses	3xx
Client error responses	4xx
Server error responses	5xx

What is Burpsuite?



What is Burpsuite?



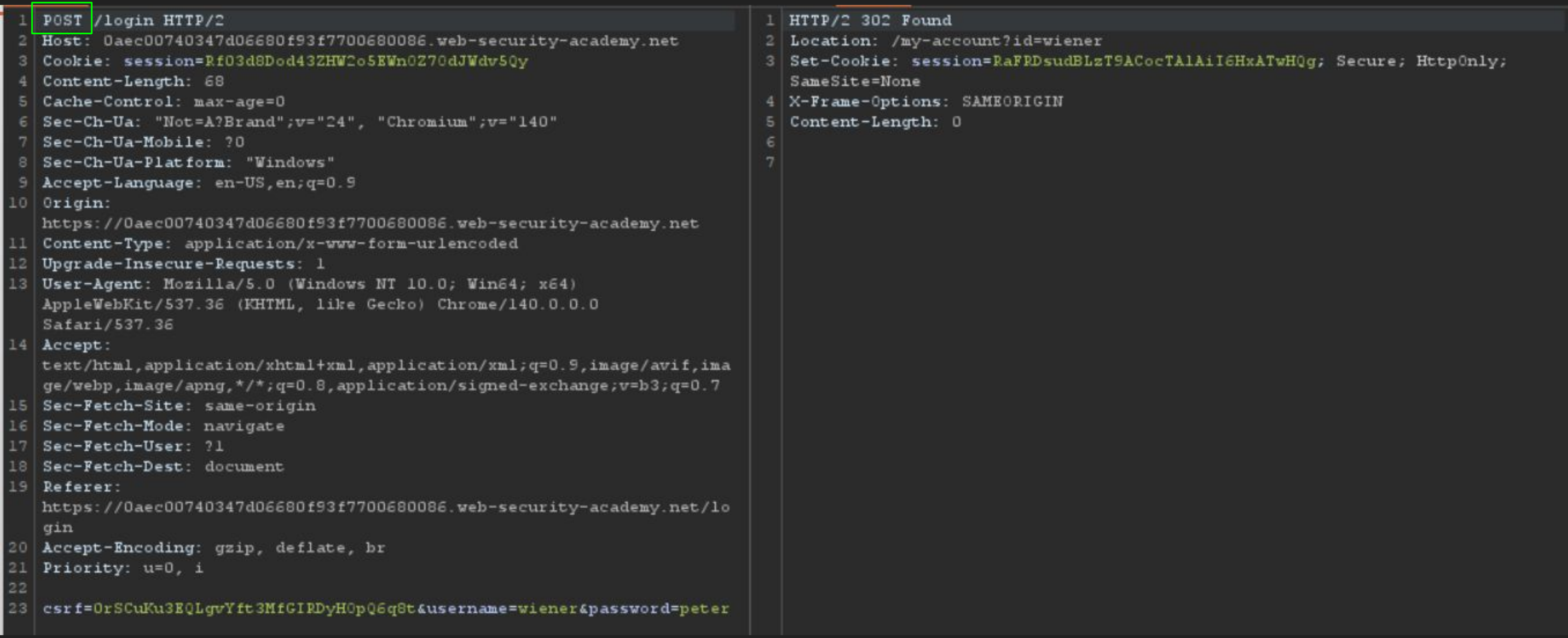
3xx - Redirection

uw.edu

4xx - client side error

https://www.washington.edu/batman

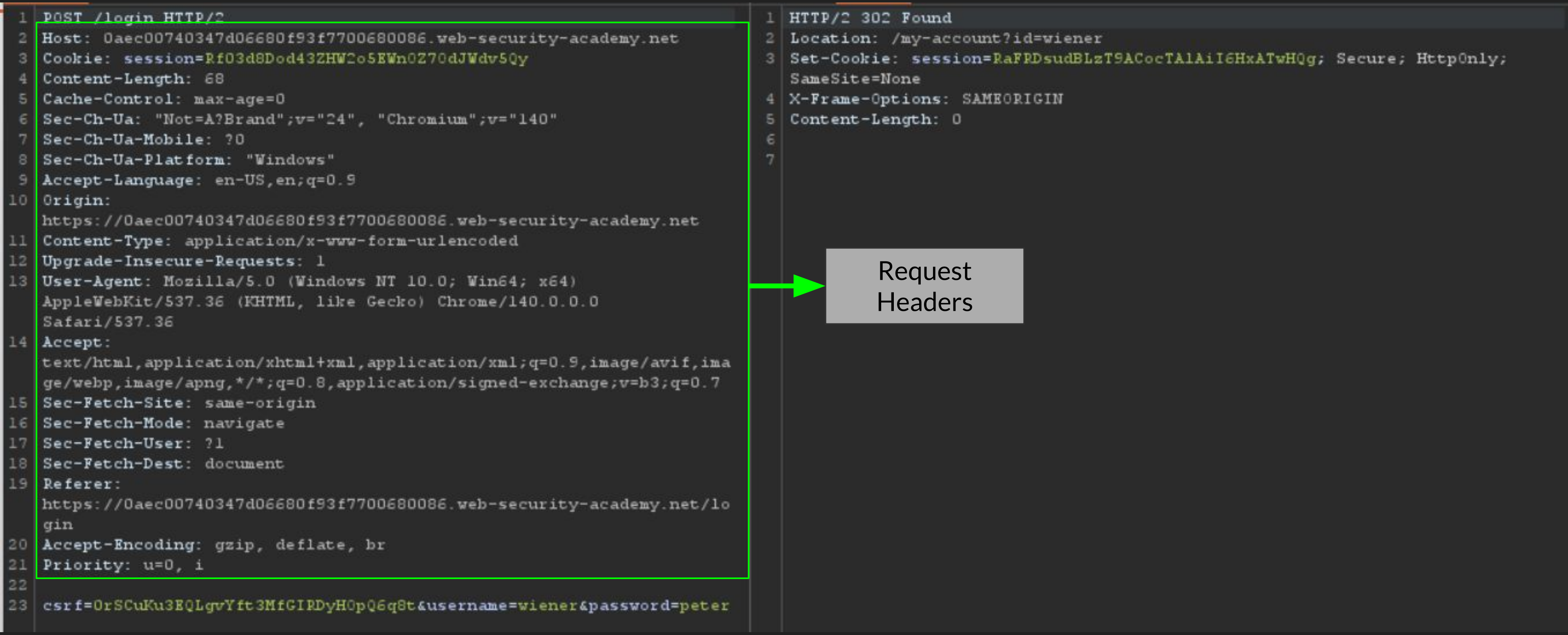
POST



```
POST /login HTTP/2
Host: 0aec00740347d06680f93f7700680086.web-security-academy.net
Cookie: session=Rf03d8Dod43ZHW2o5EWn0Z70dJWdv5Qy
Content-Length: 68
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0aec00740347d06680f93f7700680086.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aec00740347d06680f93f7700680086.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

csrf=0rSCuKu3EQLgvYft3MfGIRDyH0pQ6q8t&username=wiener&password=peter
```

```
HTTP/2 302 Found
Location: /my-account?id=wiener
Set-Cookie: session=RaFRDsudBLzT9ACocTAlAiI6HxATwHQg; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

POST

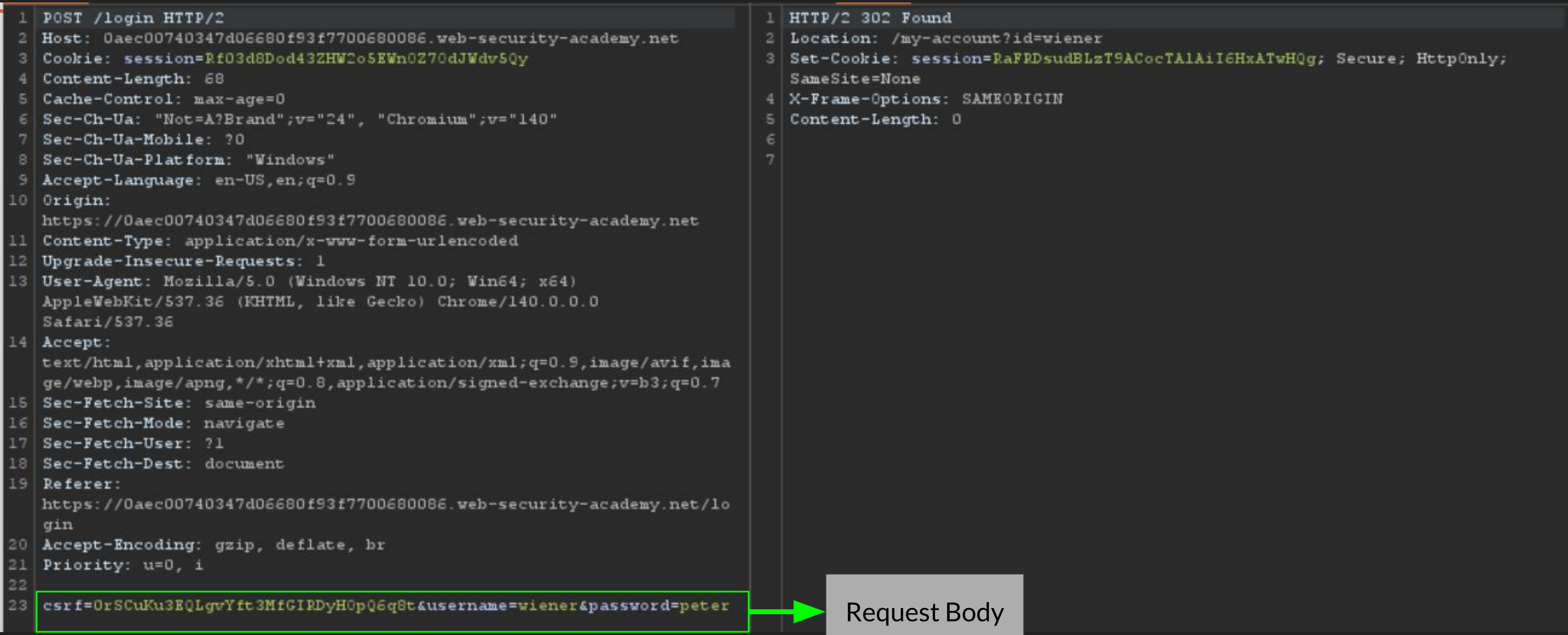


```
POST /login HTTP/2
Host: 0aec00740347d06680f93f7700680086.web-security-academy.net
Cookie: session=Rf03d8Dod43ZHW2o5EWn0Z70dJWdv5Qy
Content-Length: 68
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0aec00740347d06680f93f7700680086.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aec00740347d06680f93f7700680086.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

csrf=0rSCuKu3EQLgvYft3MfGIRDyH0pQ6q8t&username=wiener&password=peter
```

```
HTTP/2 302 Found
Location: /my-account?id=wiener
Set-Cookie: session=RaFRDsudBLzT9ACocTAlAiI6HxATwHQg; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Request Headers

POST

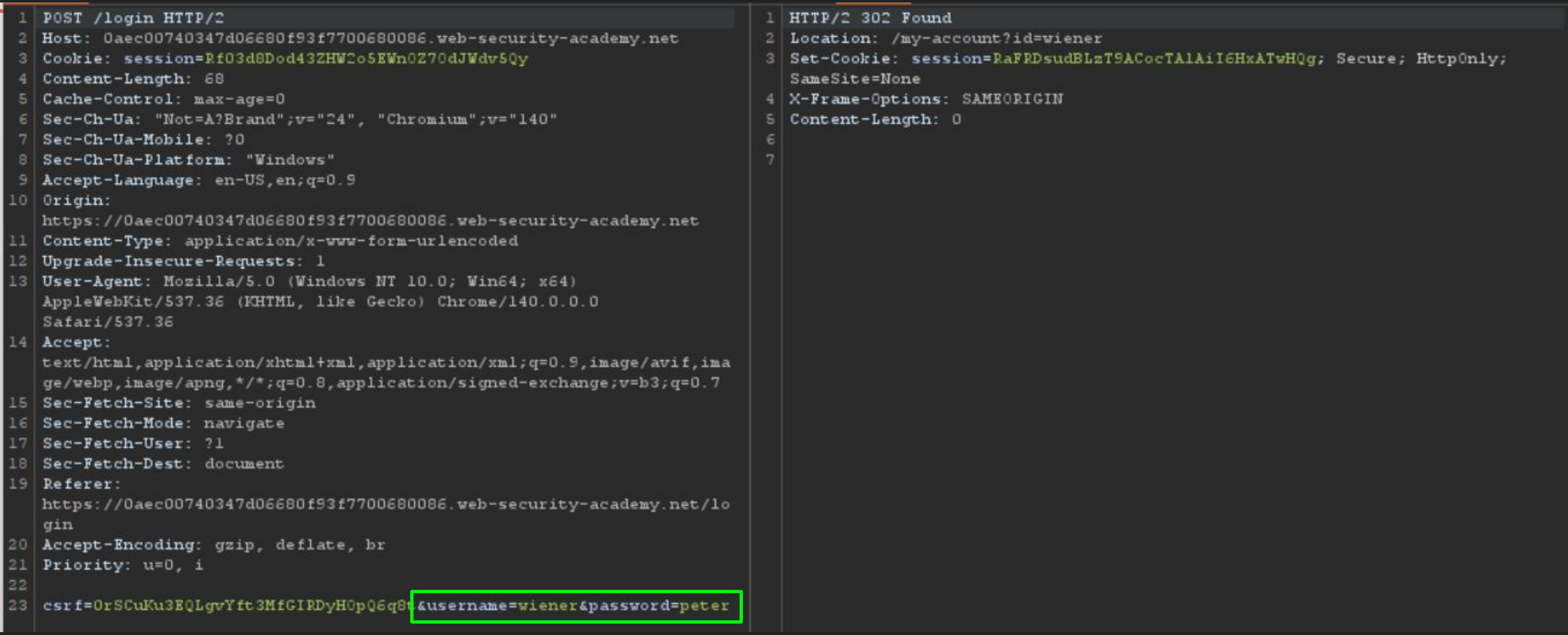


```
POST /login HTTP/2
Host: 0aec00740347d06680f93f7700680086.web-security-academy.net
Cookie: session=Rf03d8Dod43ZHW2o5EWn0Z70dJWdv5Qy
Content-Length: 68
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0aec00740347d06680f93f7700680086.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aec00740347d06680f93f7700680086.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

csrf=0rSCuKu3EQLgvYft3MfGIRDyH0pQ6q8t&username=wiener&password=peter
```

```
HTTP/2 302 Found
Location: /my-account?id=wiener
Set-Cookie: session=RaFRDsudBLzT9ACocTAlAiI6HxATwHQg; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Request Body

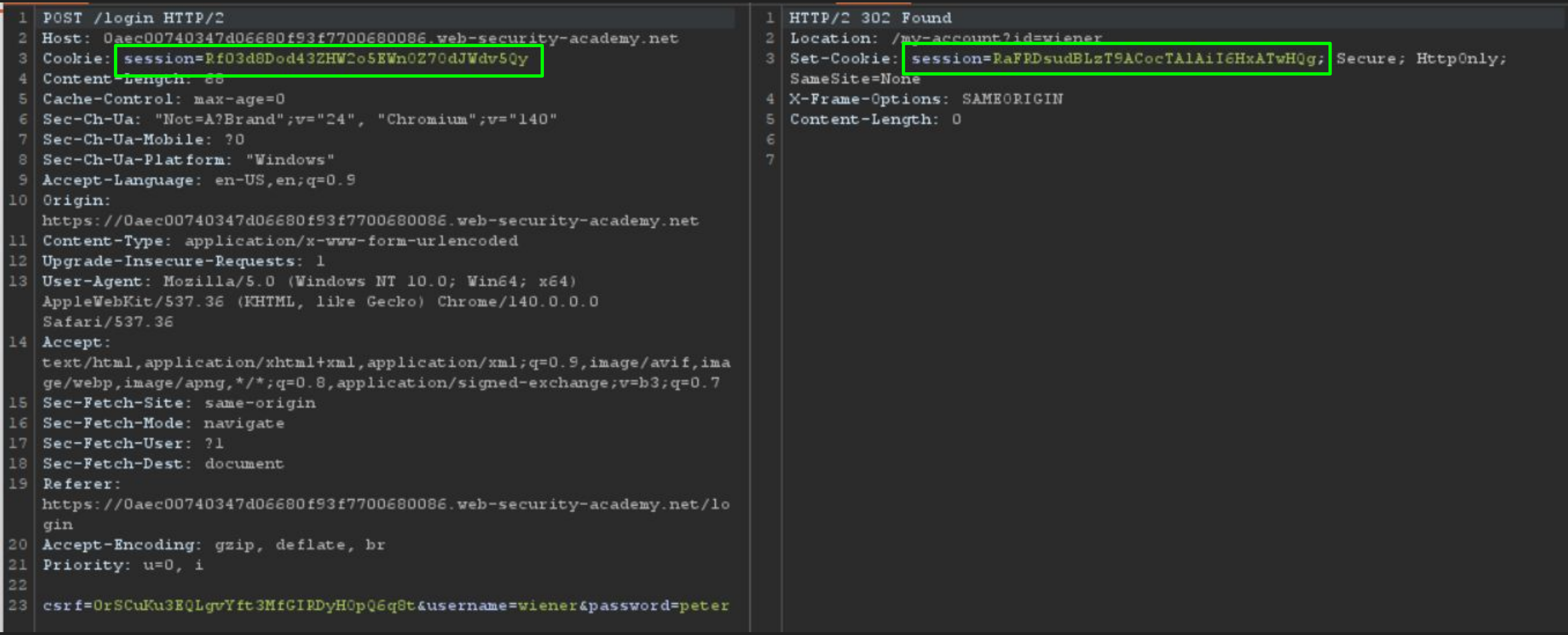
POST



```
POST /login HTTP/2
Host: 0aec00740347d06680f93f7700680086.web-security-academy.net
Cookie: session=Rf03d8Dod43ZHW2o5EWn0Z70dJWdv5Qy
Content-Length: 68
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0aec00740347d06680f93f7700680086.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aec00740347d06680f93f7700680086.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

csrf=0rSCuKu3EQLgvYft3MfGIRDyH0pQ6q8t&username=wiener&password=peter
```

```
HTTP/2 302 Found
Location: /my-account?id=wiener
Set-Cookie: session=RaFRDsudBLzT9ACocTAlAiI6HxATwHQg; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

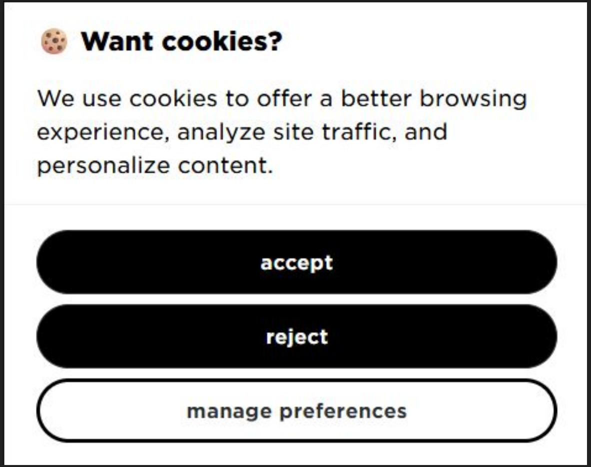
POST



```
POST /login HTTP/2
Host: 0aec00740347d06680f93f7700680086.web-security-academy.net
Cookie: session=Rf03d8Dod43ZHW2o5EWn0Z70dJWdv5Qy
Content-Length: 88
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin:
https://0aec00740347d06680f93f7700680086.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0aec00740347d06680f93f7700680086.web-security-academy.net/lo
gin
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

csrf=0rSCuKu3EQLgvYft3MfGIRDyH0pQ6q8t&username=wiener&password=peter
```

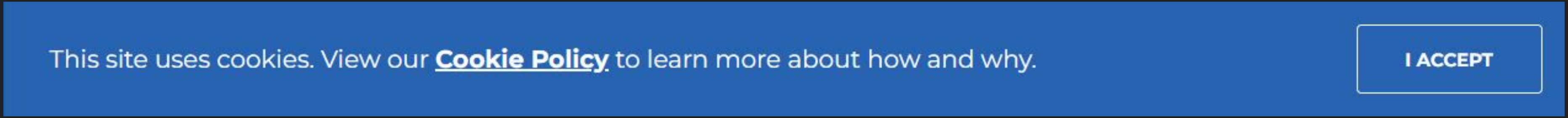
```
HTTP/2 302 Found
Location: /my-account?id=wiener
Set-Cookie: session=RaFRDsudBLzT9ACocTAlAiI6HxATwHQg; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Cookies

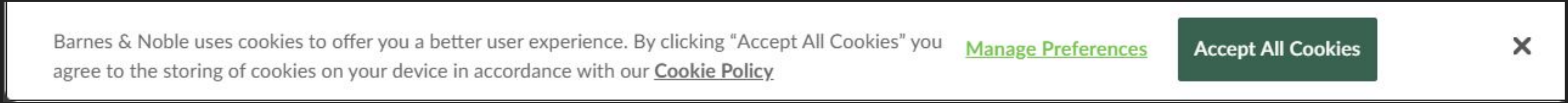


🍪 **Want cookies?**

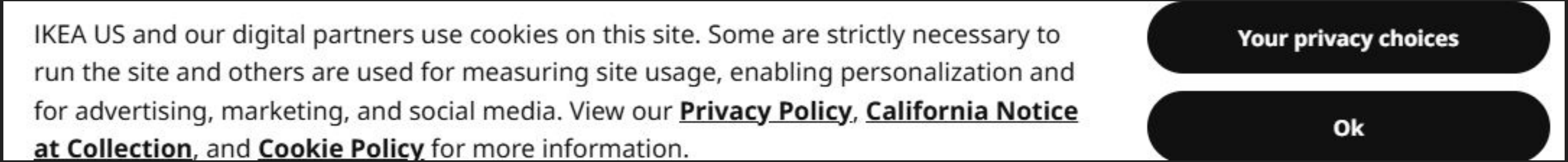
We use cookies to offer a better browsing experience, analyze site traffic, and personalize content.



This site uses cookies. View our **Cookie Policy** to learn more about how and why.

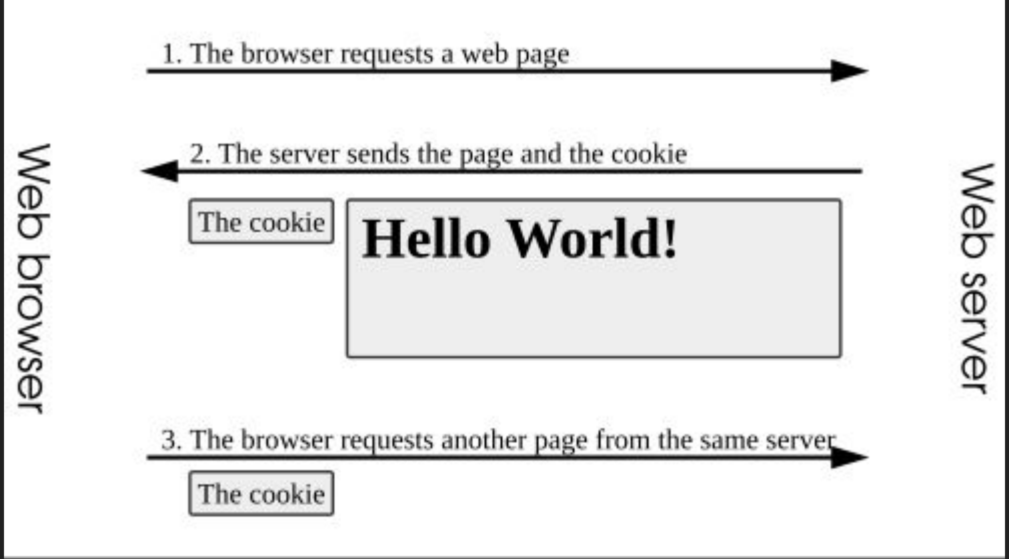


Barnes & Noble uses cookies to offer you a better user experience. By clicking “Accept All Cookies” you agree to the storing of cookies on your device in accordance with our Cookie Policy

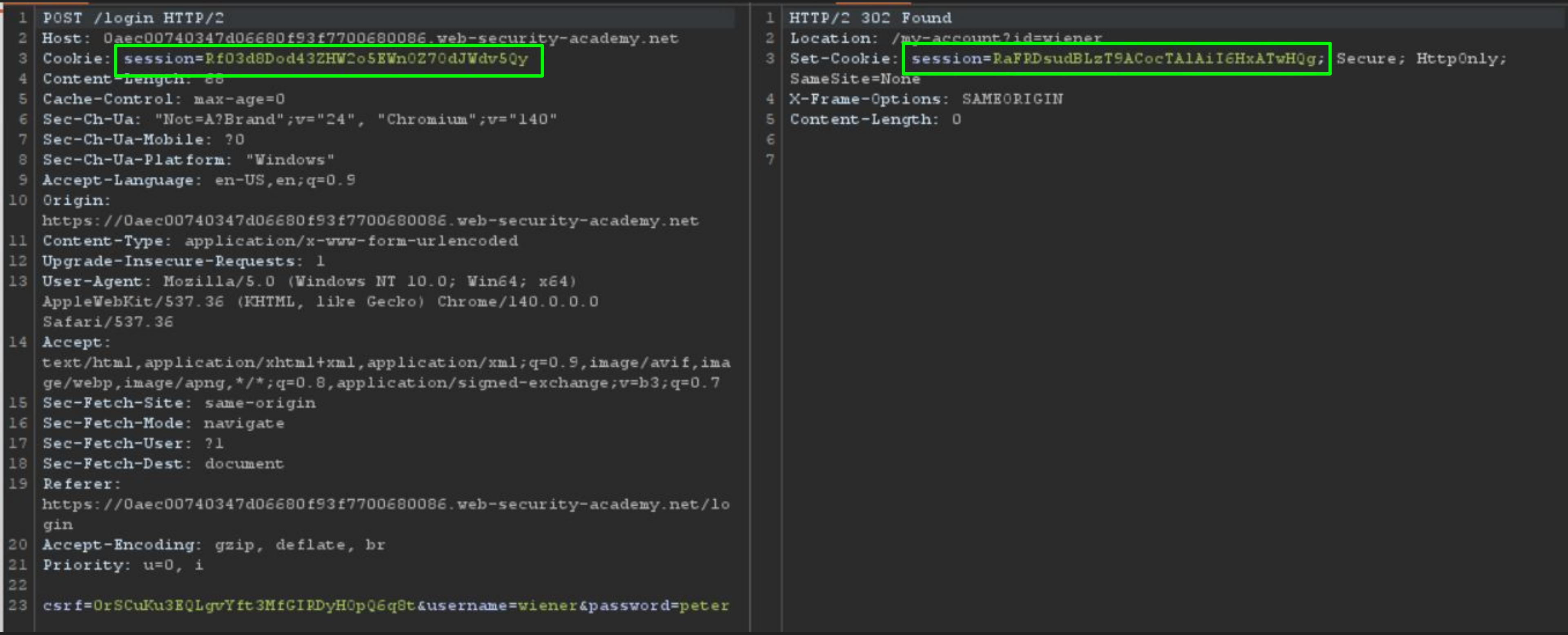


IKEA US and our digital partners use cookies on this site. Some are strictly necessary to run the site and others are used for measuring site usage, enabling personalization and for advertising, marketing, and social media. View our **Privacy Policy**, **California Notice at Collection**, and **Cookie Policy** for more information.

Cookies


Web browser
1. The browser requests a web page
2. The server sends the page and the cookie
The cookie
Hello World!
3. The browser requests another page from the same server
The cookie
Web server

POST



```
POST /login HTTP/2
Host: 0aec00740347d06680f93f7700680086.web-security-academy.net
Cookie: session=Rf03d8Dod43ZHW2o5EWn0Z70dJWdv5Qy
Content-Length: 88
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin:
https://0aec00740347d06680f93f7700680086.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0aec00740347d06680f93f7700680086.web-security-academy.net/lo
gin
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

csrf=0rSCuKu3EQLgvYft3MfGIRDyH0pQ6q8t&username=wiener&password=peter
```

```
HTTP/2 302 Found
Location: /my-account?id=wiener
Set-Cookie: session=RaFRDsudBLzT9ACocTAlAiI6HxATwHQg; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Access control: Insecure cookies / parameter

https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter

Inspect element

- Windows: ctrl + shift + i
- MacOs: cmd + shift + i

https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter

you do not need burp suite for this challenge

Doing cookies right (session ids)

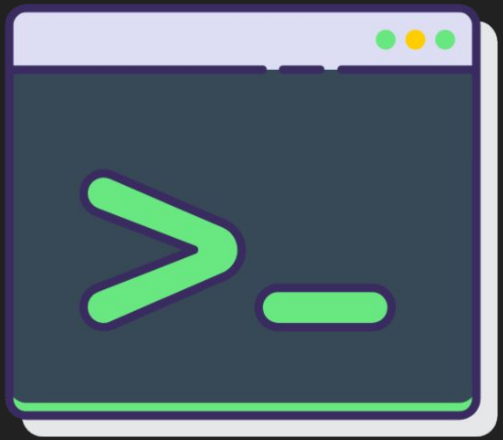
- ID Name Fingerprinting = Cookie name not obvious
- ID Length = > 128 bits
- ID Entropy = unpredictable value
- ID Value = meaningless

src: INFO 310 wi24 Reifers

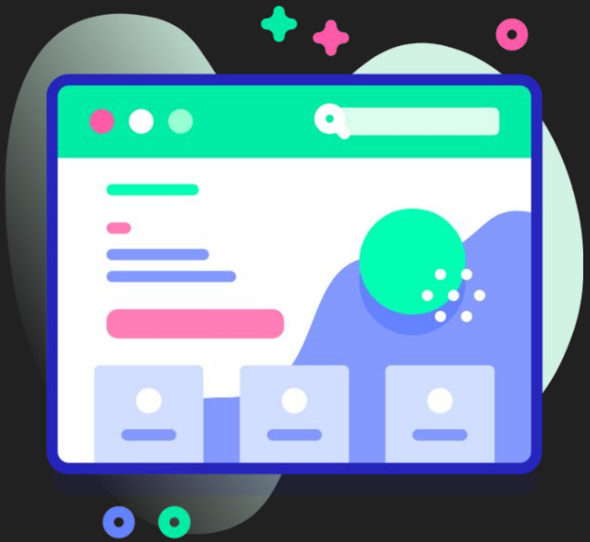
Doing cookies right (session ids)

- Secure Attribute
- HttpOnly Attribute
- SameSite Attribute
- Domain and Path Attributes
- Expire and Max-Age Attributes

src: INFO 310 wi24 Reifers



COMMAND LINE INTERFACE



GRAPHICAL USER INTERFACE

Curl

```
curl example.com
```

```
curl --path-as-is -i -s -k -X $'GET' \
    -H $'Host: en.wikipedia.org' -H $'Cache-Control: max-age=0' -H $'Sec-Ch-Ua: \"Not=A?Brand\";v=\"24\", \"Chromium\";v=\"140\"' -H $'Sec-Ch-Ua-Mobile: ?0' -H $'Sec-Ch-Ua-Platform: \"Windows\"' -H $'Accept-Language: en-US,en;q=0.9' -H $'Upgrade-Insecure-Requests: 1' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7' -H $'Sec-Fetch-Site: none' -H $'Sec-Fetch-Mode: navigate' -H $'Sec-Fetch-User: ?1' -H $'Sec-Fetch-Dest: document' -H $'Accept-Encoding: gzip, deflate, br' -H $'Priority: u=0, i' \
    $'https://en.wikipedia.org/wiki/Batman'
```

APIs

Application programming interface

Every API has four components:

1. Where is the server that's running the API? (I.e., what's the hostname?)

2. Are we allowed to access it?

3. What content does the API give us?

4. What format should the request for content be in? What format does the response come back in?

src: CSE 154 24au Wolman

https://dog.ceo/dog-api/documentation

1. Where is the server that's running the API? (I.e., what's the hostname?)

2. Are we allowed to access it?

3. What content does the API give us?

4. What format should the request for content be in? What format does the response come back in?

https://dog.ceo/dog-api/documentation

1. Where is the server that's running the API? (I.e., what's the hostname?)

   dog.ceo

2. Are we allowed to access it?

3. What content does the API give us?

4. What format should the request for content be in? What format does the response come back in?

https://dog.ceo/dog-api/documentation

1. Where is the server that's running the API? (I.e., what's the hostname?)

   dog.ceo

2. Are we allowed to access it?

   yes! no auth required

3. What content does the API give us?

4. What format should the request for content be in? What format does the response come back in?

https://dog.ceo/dog-api/documentation

1. Where is the server that's running the API? (I.e., what's the hostname?)

   dog.ceo

2. Are we allowed to access it?

   yes! no auth required

3. What content does the API give us?

   dog photos

4. What format should the request for content be in? What format does the response come back in?

https://dog.ceo/dog-api/documentation

1. Where is the server that's running the API? (I.e., what's the hostname?)

   dog.ceo

2. Are we allowed to access it?

   yes! no auth required

3. What content does the API give us?

   dog photos

4. What format should the request for content be in? What format does the response come back in?

   Request: https://dog.ceo/api/breeds/image/random Response: json

Some no auth APIs

https://pokeapi.co/api/v2/pokemon/ditto

https://http.cat/404

https://api.fbi.gov/wanted/v1/list

Take home challenges

More access control!

https://portswigger.net/web-security/file-path-traversal/lab-simple

https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references

API Security

https://portswigger.net/web-security/api-testing/lab-exploiting-api-endpoint-using-documentation

HTTP Verbs

https://play.picoctf.org/practice/challenge/132

For next wednesday…

Please have all of these set up on your device before we begin:

Burpsuite: https://portswigger.net/burp/communitydownload

Docker: https://docs.docker.com/engine/install/

OWASP Juice Shop: https://owasp.org/www-project-juice-shop/

If you need help, ask an officer!

```
docker pull bkimminich/juice-shop
```

```
docker run --rm -p 3000:3000 bkimminich/juice-shop
```