Write Up

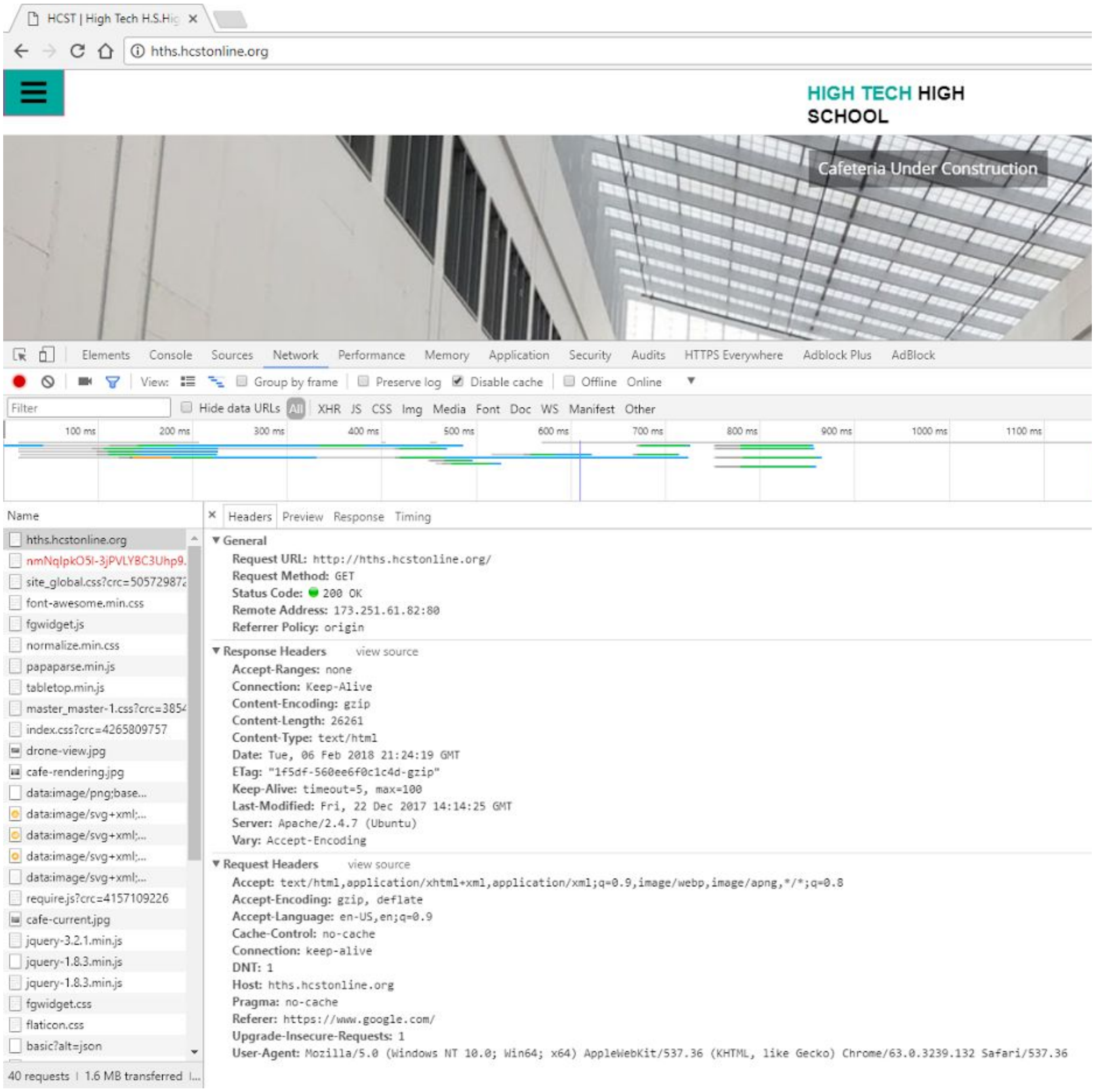
A request method is a format for an HTTP request that indicates the intent the request has. For example, a GET request attempts to retrieve data from a source but a POST request submits data into a source for storage or some sort of server-side feedback. These methods have different structures for how these methods should be sent and appear differently in HTTP code.

Response headers are HTTP headers coming to a client from a server in response to an HTTP request. These headers often have information such as the authentication methods, cookies, CORS restrictions, or allowed content types. They allow the client to gain insight to the quality of their requests and can often have data for the client to process.

Request headers are HTTP headers going from a client to a server attached to an HTTP request. These headers give the server information about the client in order for the server to respond appropriately but do not describe any data in the body of the request according to Mozilla's glossary[1].

[1] https://developer.mozilla.org/en-US/docs/Glossary/Request_header

Existing Webpage Screenshot - http://hths.hcstonline.org/



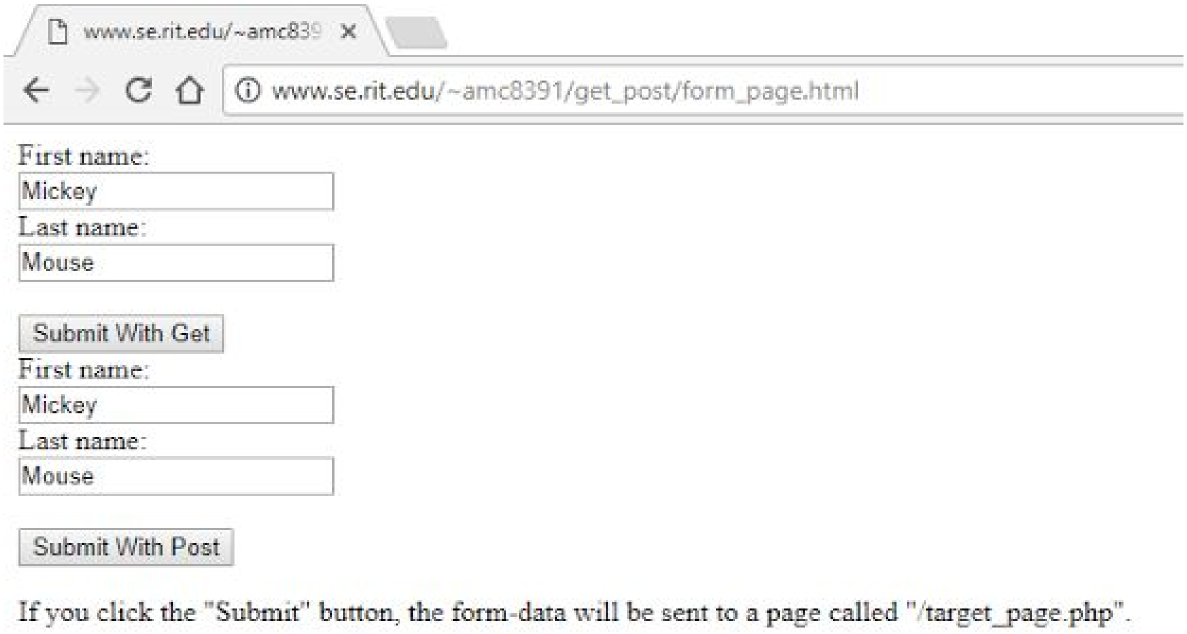
Name

```
hths.hcstonline.org
nmNqlpkO5I-3jPVLYBC3Uhp9.
site_global.css?crc=50572987
font-awesome.min.css
fgwidget.js
normalize.min.css
papaparse.min.js
tabletop.min.js
master_master-1.css?crc=3854
index.css?crc=4265809757
drone-view.jpg
cafe-rendering.jpg
data:image/png;base...
data:image/svg+xml;...
data:image/svg+xml;...
data:image/svg+xml;...
data:image/svg+xml;...
require.js?crc=4157109226
cafe-current.jpg
jquery-3.2.1.min.js
jquery-1.8.3.min.js
jquery-1.8.3.min.js
fgwidget.css
flaticon.css
basic?alt=json
```

40 requests | 1.6 MB transferred |...

```
▼ General
   Request URL: http://hths.hcstonline.org/
   Request Method: GET
   Status Code: ● 200 OK
   Remote Address: 173.251.61.82:80
   Referrer Policy: origin
▼ Response Headers     view source
   Accept-Ranges: none
   Connection: Keep-Alive
   Content-Encoding: gzip
   Content-Length: 26261
   Content-Type: text/html
   Date: Tue, 06 Feb 2018 21:24:19 GMT
   ETag: "1f5df-560ee6f0c1c4d-gzip"
   Keep-Alive: timeout=5, max=100
   Last-Modified: Fri, 22 Dec 2017 14:14:25 GMT
   Server: Apache/2.4.7 (Ubuntu)
   Vary: Accept-Encoding
▼ Request Headers     view source
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
   Accept-Encoding: gzip, deflate
   Accept-Language: en-US,en;q=0.9
   Cache-Control: no-cache
   Connection: keep-alive
   DNT: 1
   Host: hths.hcstonline.org
   Pragma: no-cache
   Referer: https://www.google.com/
   Upgrade-Insecure-Requests: 1
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
```

Pre Submission Page - http://www.se.rit.edu/~amc8391/get_post/

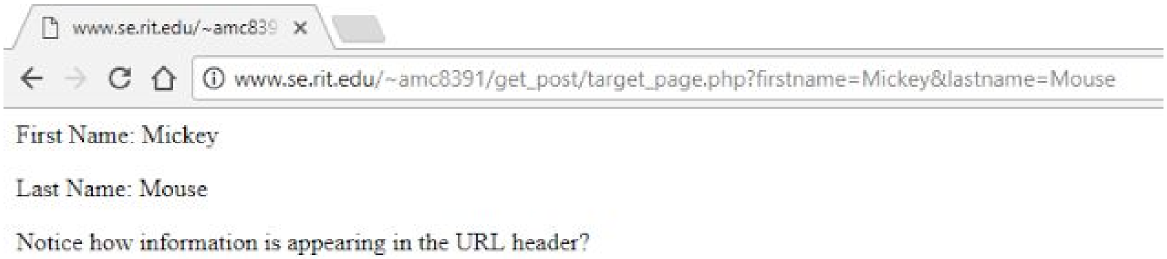


First name:
Mickey
Last name:
Mouse

First name:
Mickey
Last name:
Mouse

If you click the "Submit" button, the form-data will be sent to a page called "/target_page.php".

Post Submission Page (using GET)

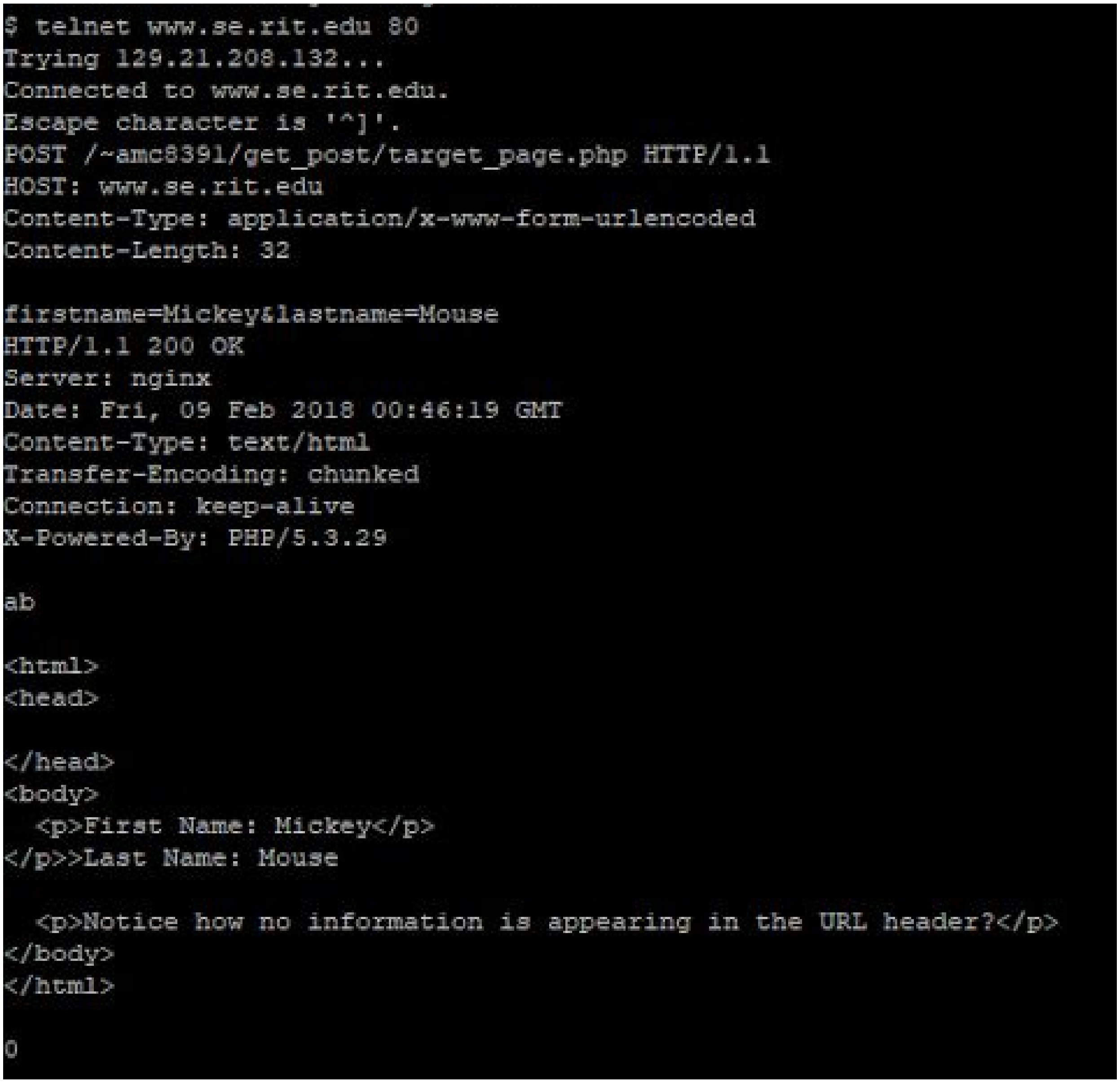

www.se.rit.edu/~amc839
www.se.rit.edu/~amc8391/get_post/target_page.php?firstname=Mickey&lastname=Mouse

First Name: Mickey

Last Name: Mouse

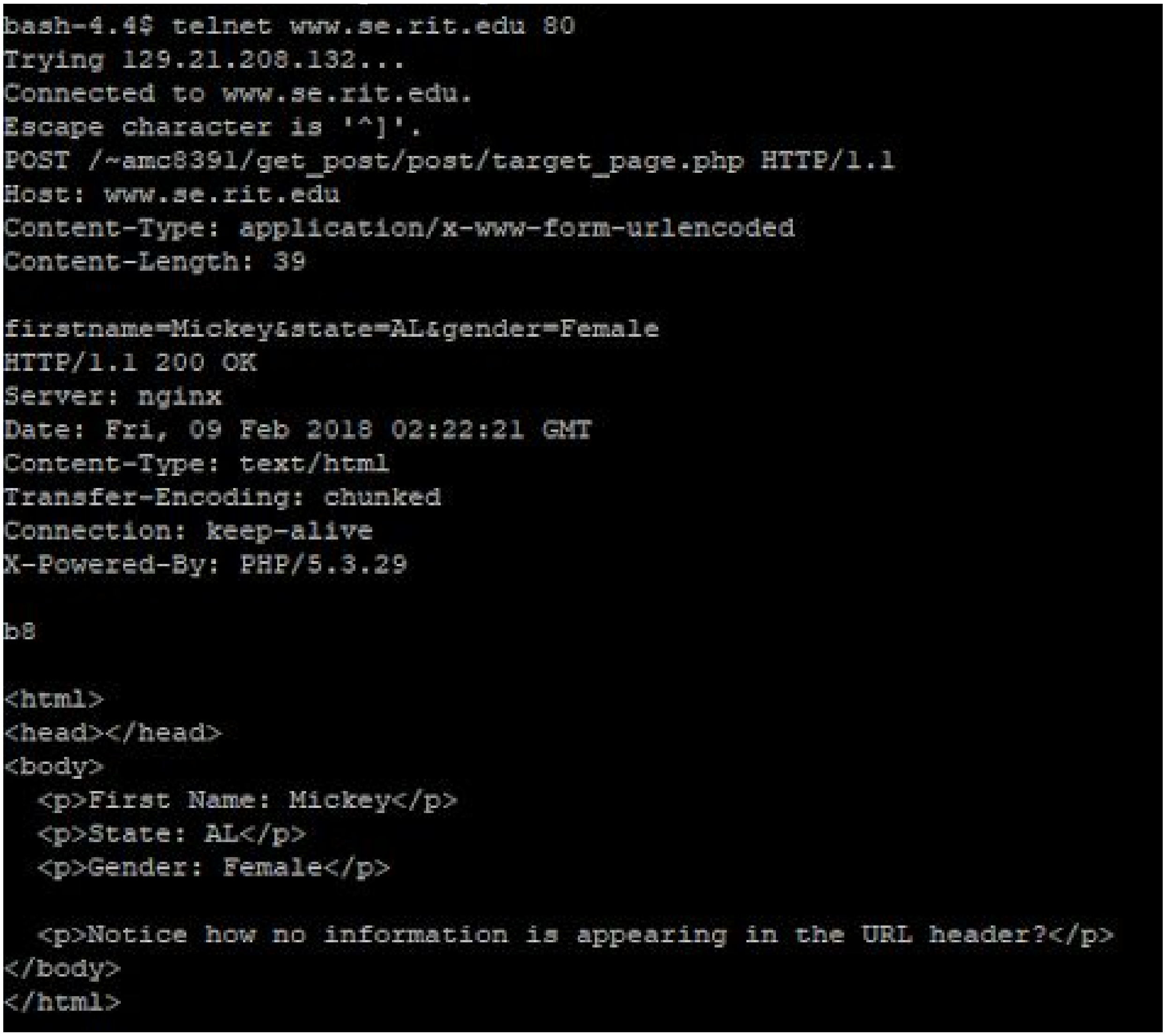
Notice how information is appearing in the URL header?

Telnet GET



```
$ telnet www.se.rit.edu 80
Trying 129.21.208.132...
Connected to www.se.rit.edu.
Escape character is '^]'.
POST /~amc8391/get_post/target_page.php HTTP/1.1
HOST: www.se.rit.edu
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

firstname=Mickey&lastname=Mouse
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 09 Feb 2018 00:46:19 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.29

ab

<html>
<head>

</head>
<body>
  <p>First Name: Mickey</p>
</p>>Last Name: Mouse

  <p>Notice how no information is appearing in the URL header?</p>
</body>
</html>

0
```

Telnet POST



```
bash-4.4$ telnet www.se.rit.edu 80
Trying 129.21.208.132...
Connected to www.se.rit.edu.
Escape character is '^]'.
POST /~amc8391/get_post/post/target_page.php HTTP/1.1
Host: www.se.rit.edu
Content-Type: application/x-www-form-urlencoded
Content-Length: 39

firstname=Mickey&state=AL&gender=Female
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 09 Feb 2018 02:22:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.29

b8

<html>
<head></head>
<body>
  <p>First Name: Mickey</p>
  <p>State: AL</p>
  <p>Gender: Female</p>

  <p>Notice how no information is appearing in the URL header?</p>
</body>
</html>
```

Telnet Commands

GET	`telnet www.se.rit.edu 80`
	`GET /~amc8391/get_post/get/target_page.php?firstname=Mickey&state=AL&gender=Female HTTP/1.1`
	`HOST: www.se.rit.edu`

POST	`POST /~amc8391/get_post/post/target_page.php HTTP/1.1`
	`Host: www.se.rit.edu`
	`Content-Type: application/x-www-form-urlencoded`
	`Content-Length: 39`
	
	`firstname=Mickey&state=AL&gender=Female`