

二向箔-百日打卡writeup 1-5

原创

beirry 于 2021-12-02 15:08:26 发布 976 收藏

分类专栏: [二向箔安全-百日打卡](#) 文章标签: [web安全](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/beirry/article/details/121677385>

版权

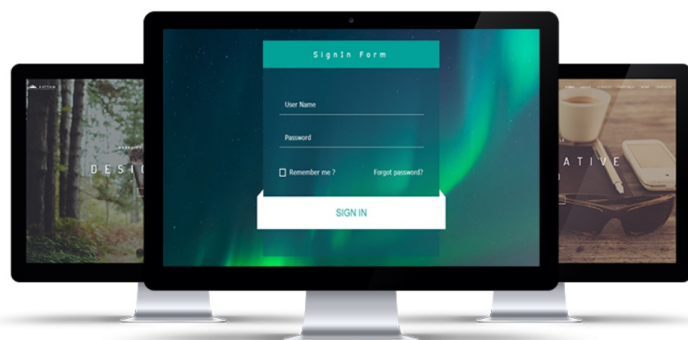


[二向箔安全-百日打卡](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

NO.1

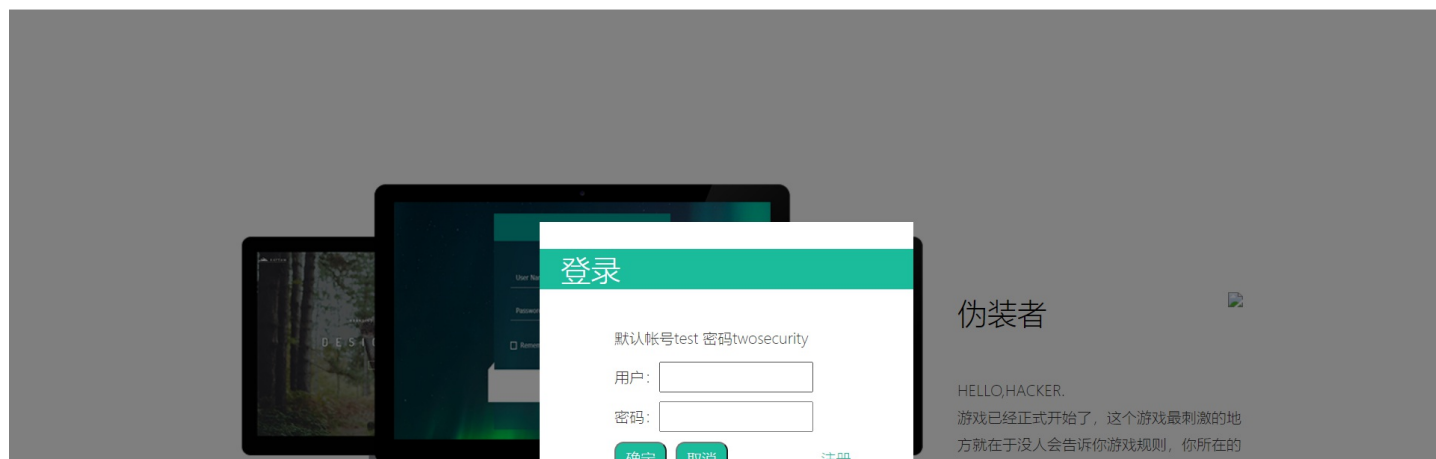


伪装者

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

点击提示按钮, 可以看到我们需要以admin登录



就是一个真实的网页入口，该怎么做，发挥你的想象。

CSDN @beiry

此处已经有一个默认账号了，还有一个注册按钮，尝试先登录默认账号。



伪装者

本练习的目的是找到一种以用户“admin”登录的方法 您目前登录为test!

[退出](#)

```
名称 名称 X 标头 预览 响应 启动器 时间 Cookie  
home GET /ker/home HTTP/1.1  
Host: rimovni.exeeye.run  
Connection: keep-alive  
Cache-Control: max-age=0  
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.exeeye.run/ker/index  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: cookie=test
```

CSDN @beiry

通过观察，看到cookie中有test字样，将test修改成admin，再刷新。



伪装者

恭喜您目前登录为admin! two(j_like_cookie)

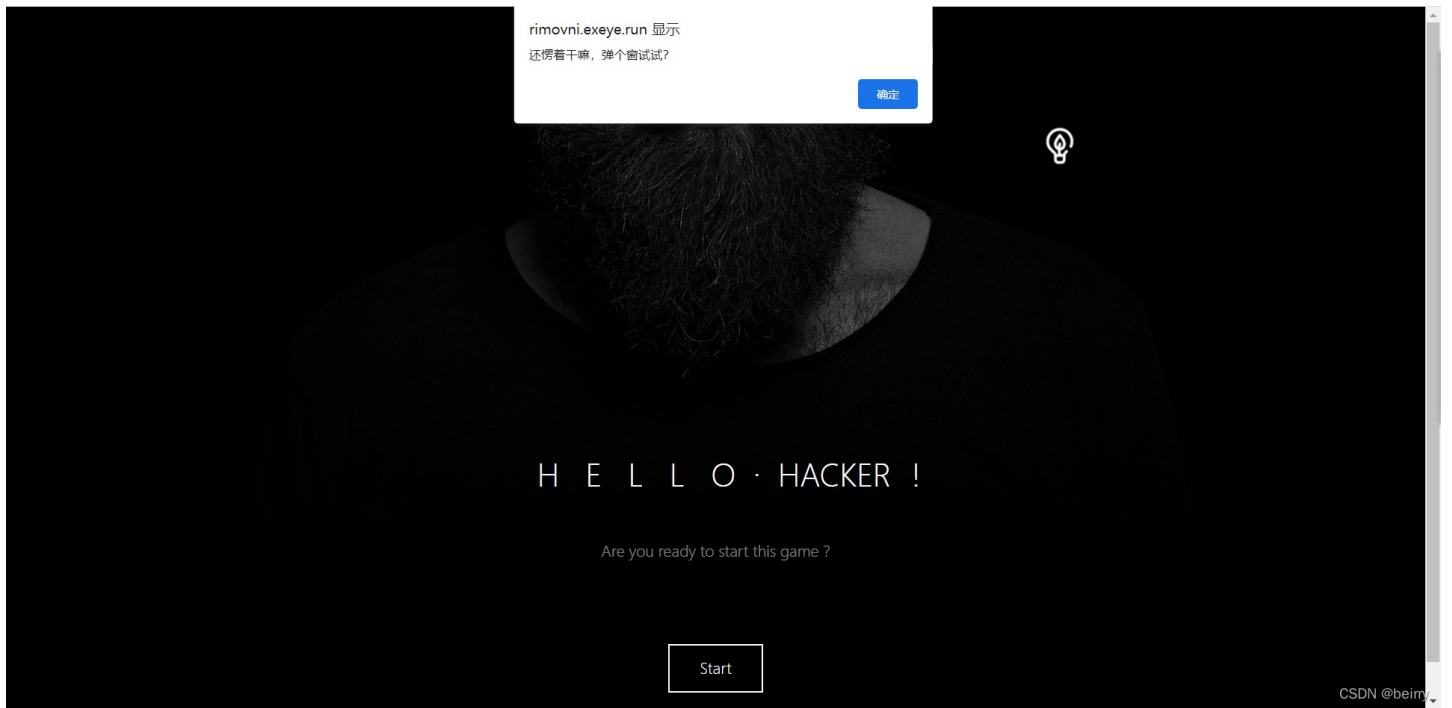
```
名称 名称 X 标头 预览 响应 启动器 时间 Cookie  
home GET /ker/home HTTP/1.1  
Host: rimovni.exeeye.run  
Connection: keep-alive  
Cache-Control: max-age=0  
sec-ch-ua: "Google Chrome";v="95", "Chromium";v="95", "Not A Brand";v="99"  
sec-ch-ua-mobile: ?0  
sec-ch-ua-platform: "Windows"  
Upgrade-Insecure-Requests: 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.exeeye.run/ker/index  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: cookie=admin
```

CSDN @beiry

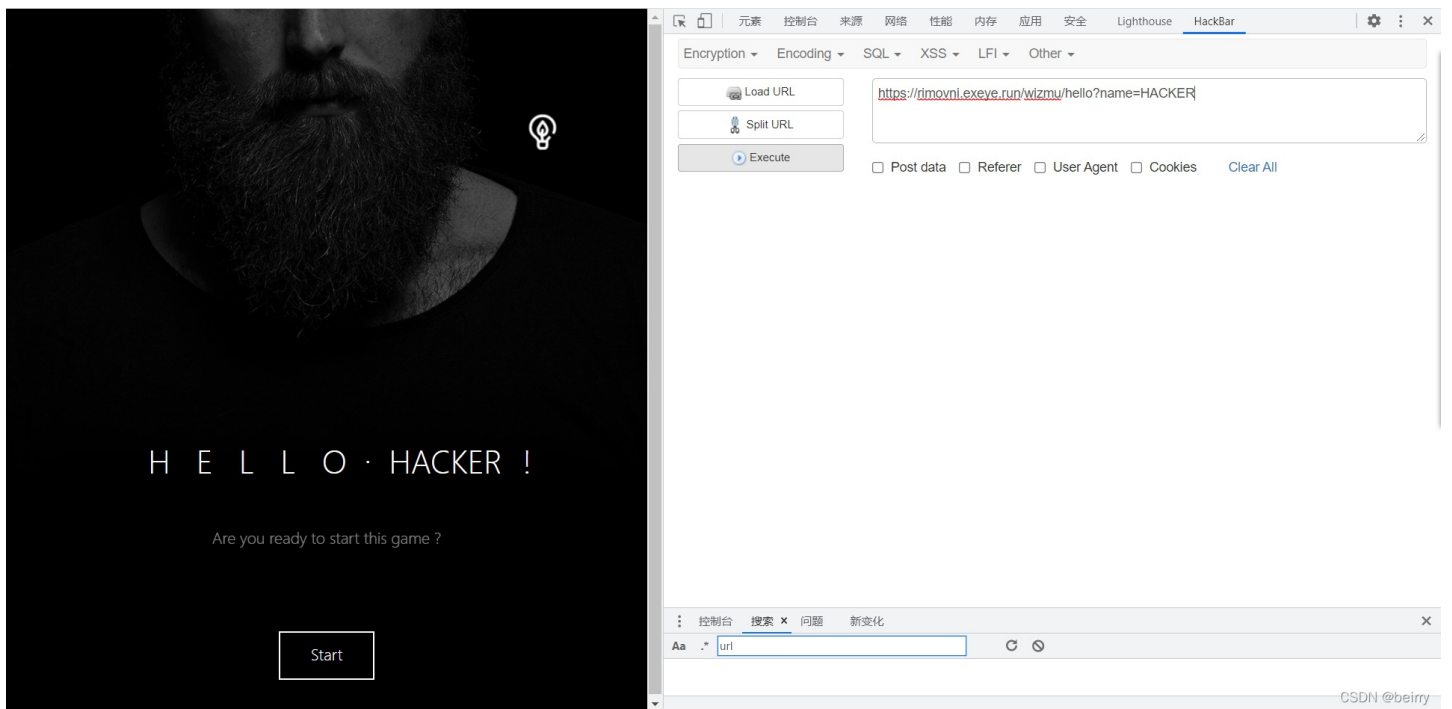
登录成功!

NO.2

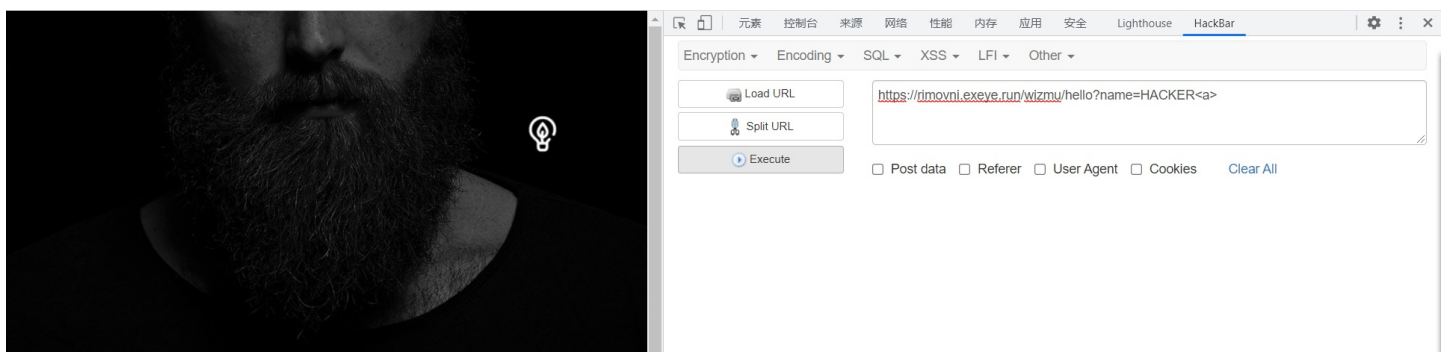
点击小灯泡，显示提示让我们弹个窗，很显然就是告诉我们这个是以xss攻击的靶场。

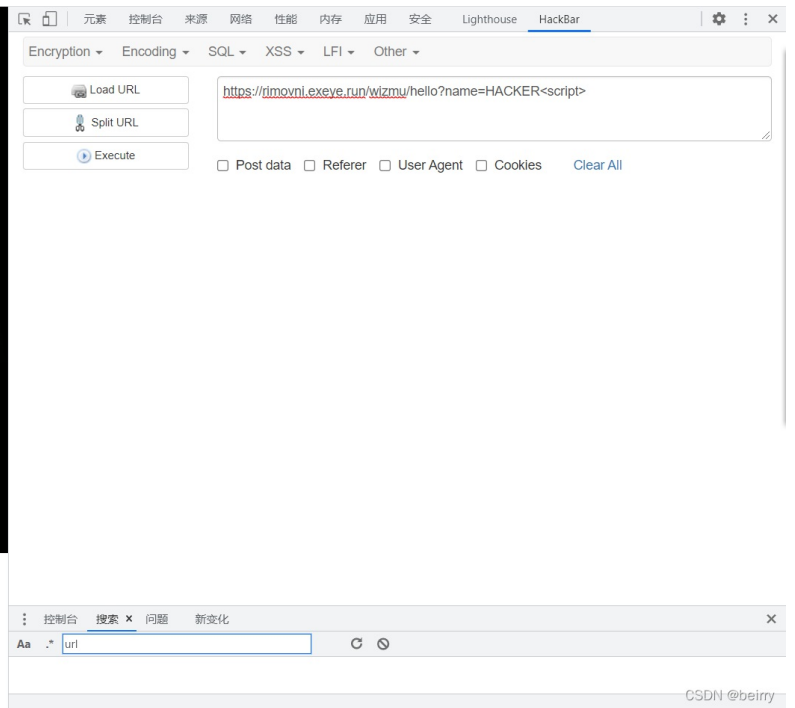
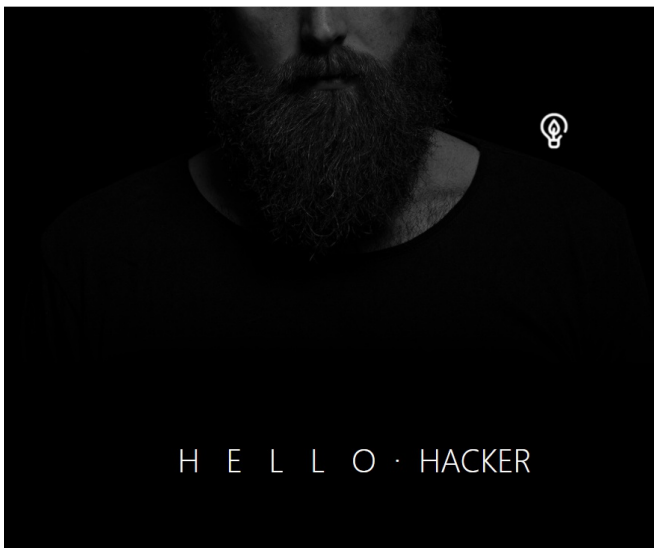
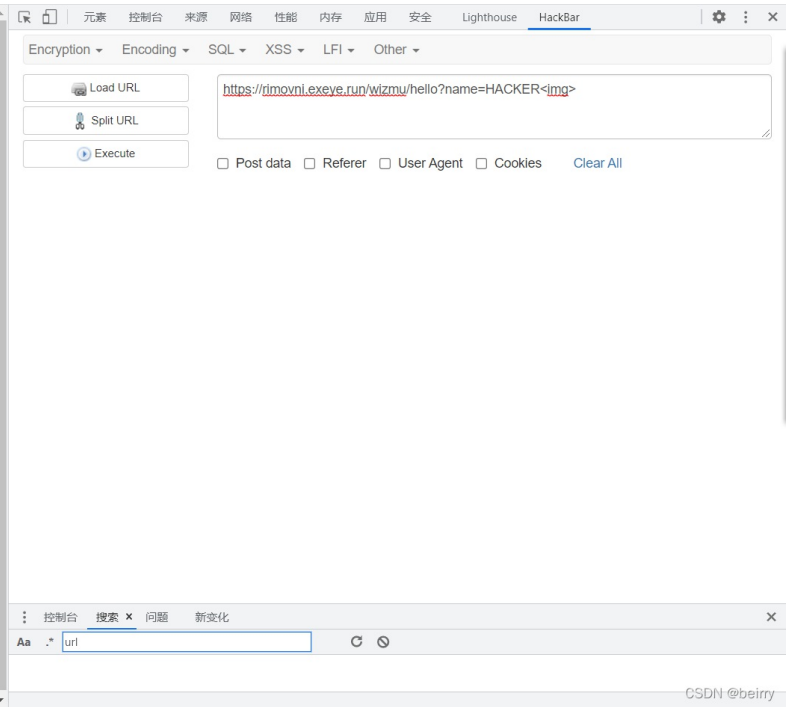
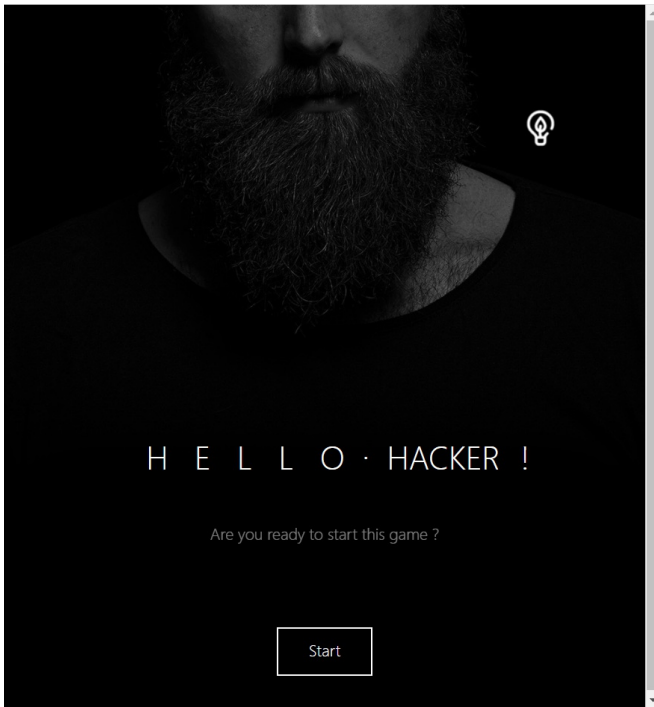
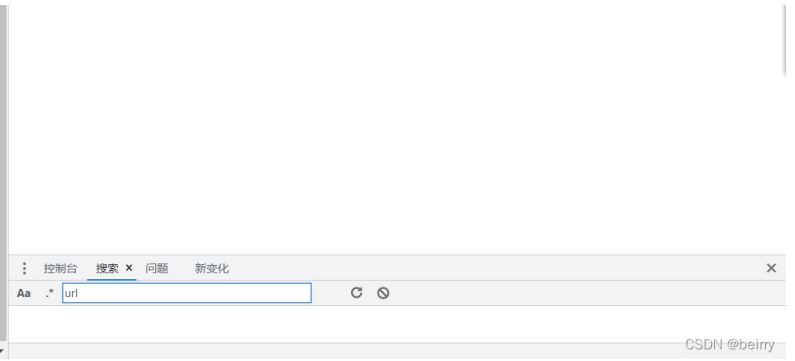
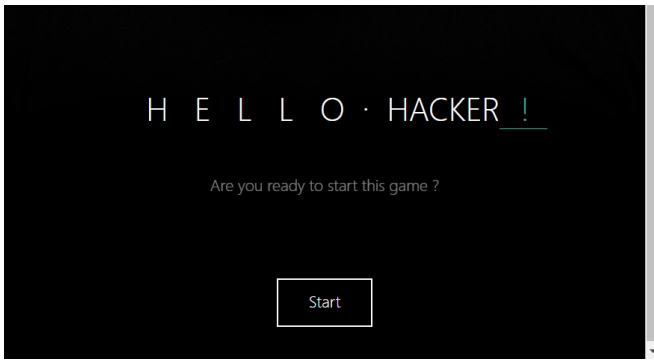


在URL中可以看到有name的参数值，一般测试xss语句，从标签开始测试，看哪些被过滤了。



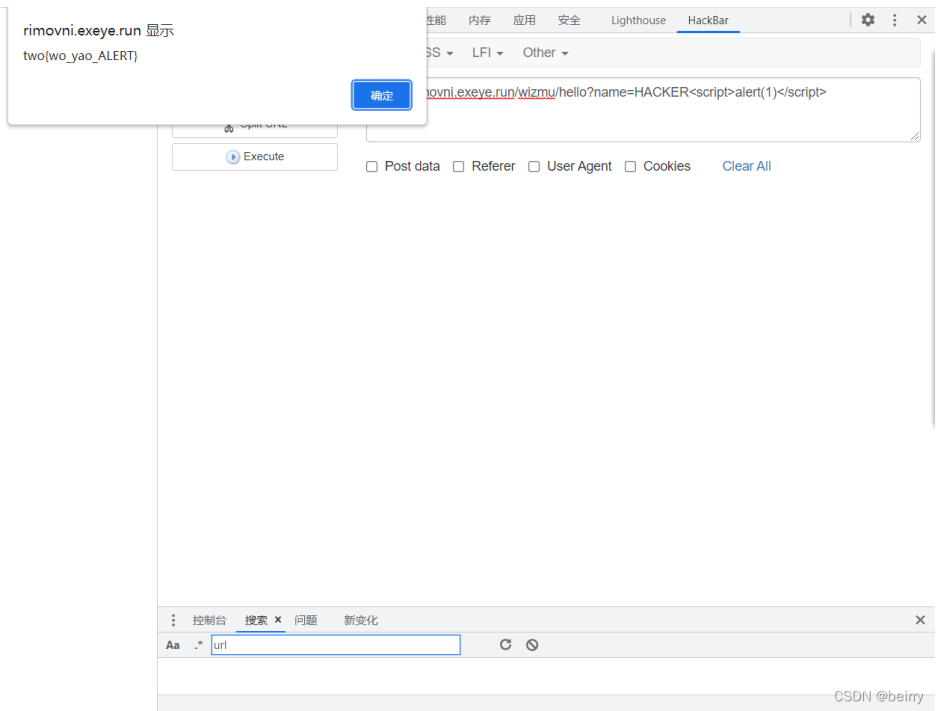
大部分情况下<a>，标签不容易被过滤，<script>易被过滤，所以在尝试xss时，可以先从<a>，测试。





可以看到这里并没有对用户输入做任何过滤，则可以直接使用弹窗语句

```
<script>alert(1)</script>
```



得到flag

NO.3

根据提示可以知道，我们输入值后点击生成链接。应该会有一个<a>标签。

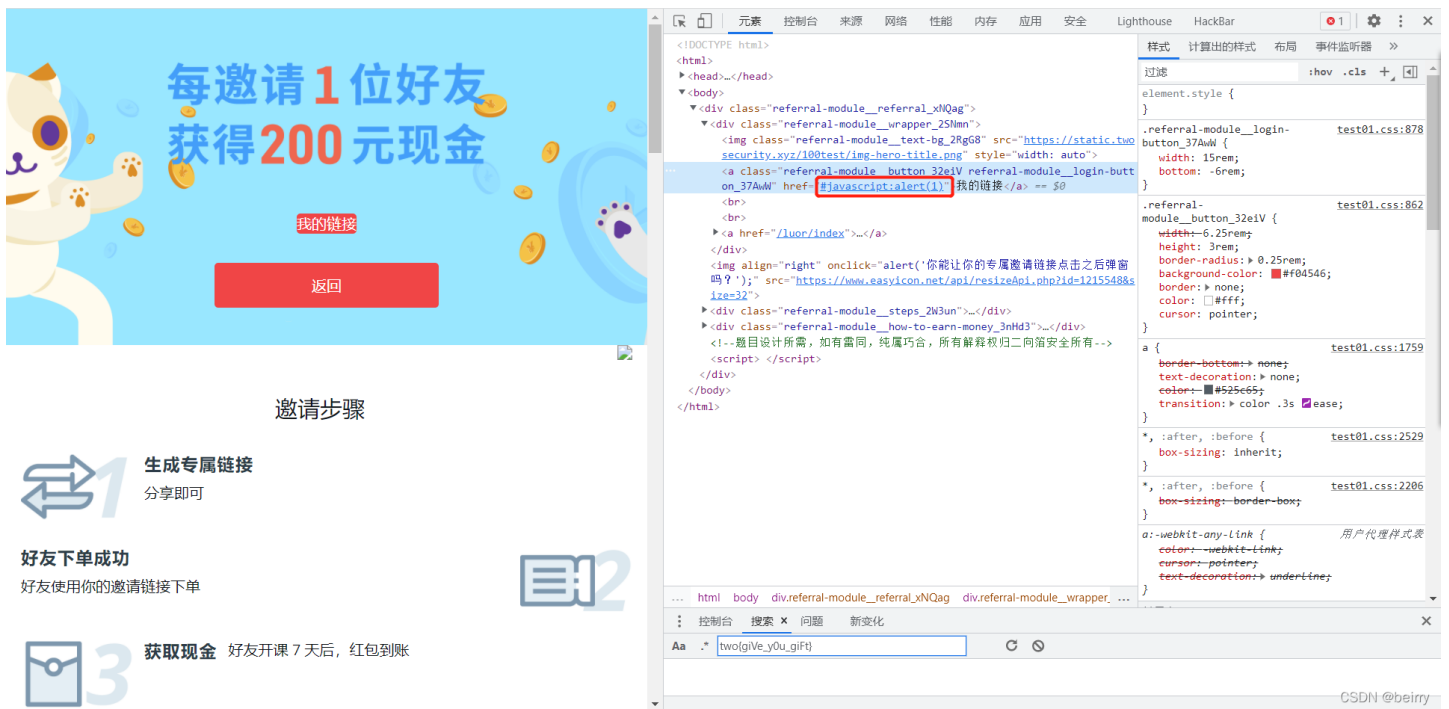


邀请步骤



CSDN @beiry

尝试写入 `javascript:alert(1)` ,点击后没反应，查看源代码发现在我们输入的值前有一个#



则尝试闭合href，在后面添加onclick来触发。

```
" onclick="alert(1)
```



邀请步骤



CSDN @beirry



邀请步骤

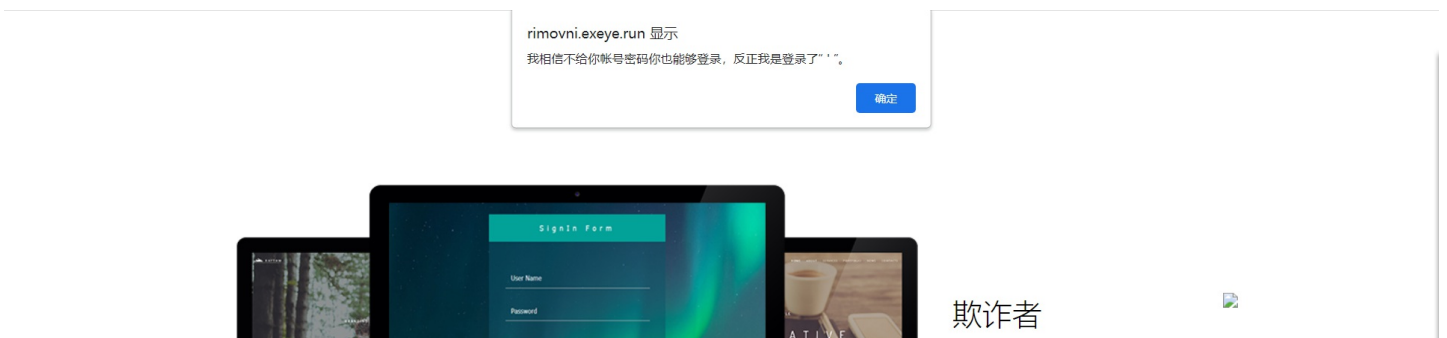
https://rimovni.exeve.run/luor/welcome#



CSDN @beirry

NO.4

登录页面可以从三个方面考虑，第一个是爆破，第二个是万能密码，第三个就是修改cookie值。





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。

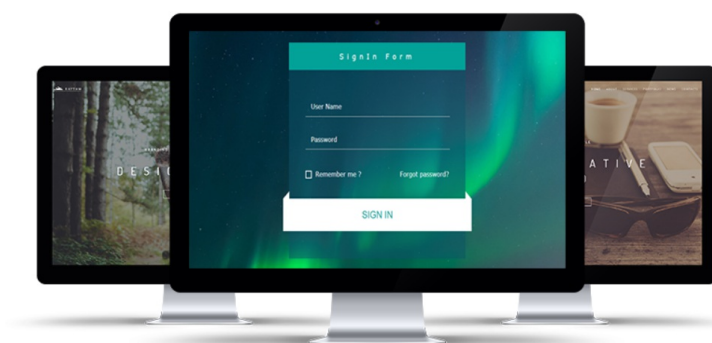
CSDN @beirry

尝试先用万能密码, 账号输入admin, 密码输入 ' or 1#



CSDN @beirry

登录成功



欺诈者

恭喜你登录成功!
two(LoGin_suCcessFu1y)

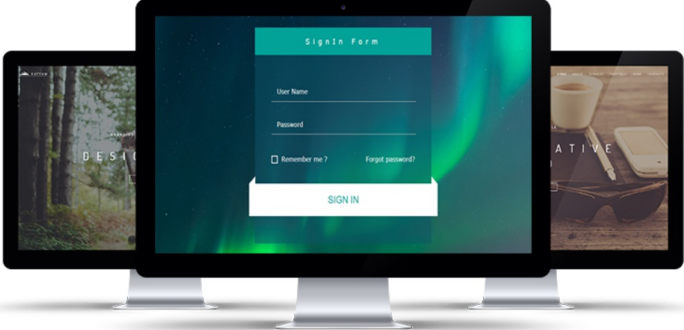
CSDN @beirry

NO.5

又是登录页面

rimovni.exeye.run 显示
找到一种以用户“admin”登录的方法，给你一块饼干。

确定



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

给了一个默认账号，那么可以先考虑修改cookie值的方法

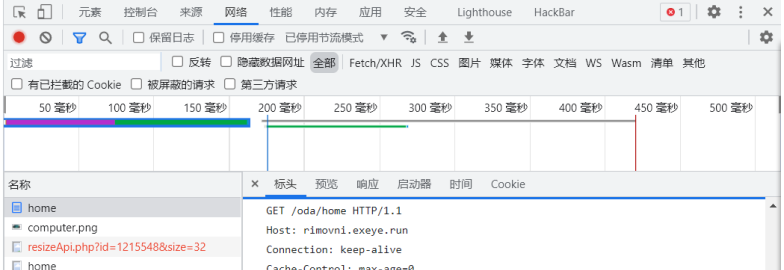


伪装者

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

观察cookie值，发现是有32位字符组合而成，那么根据特征猜测可能是md5值

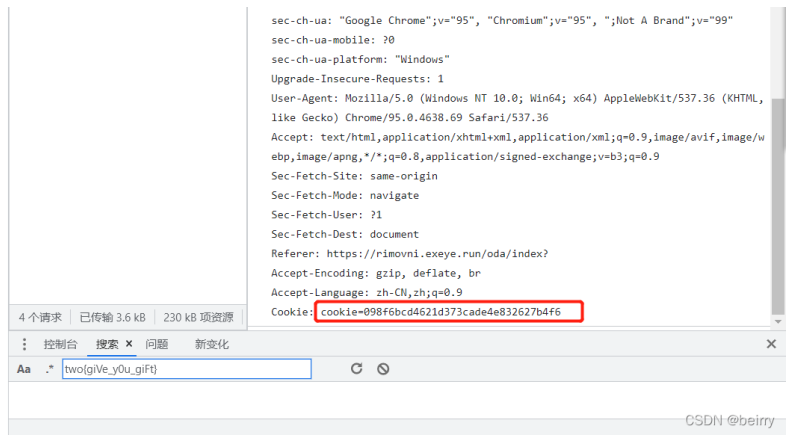


CSDN @beirry



伪装者

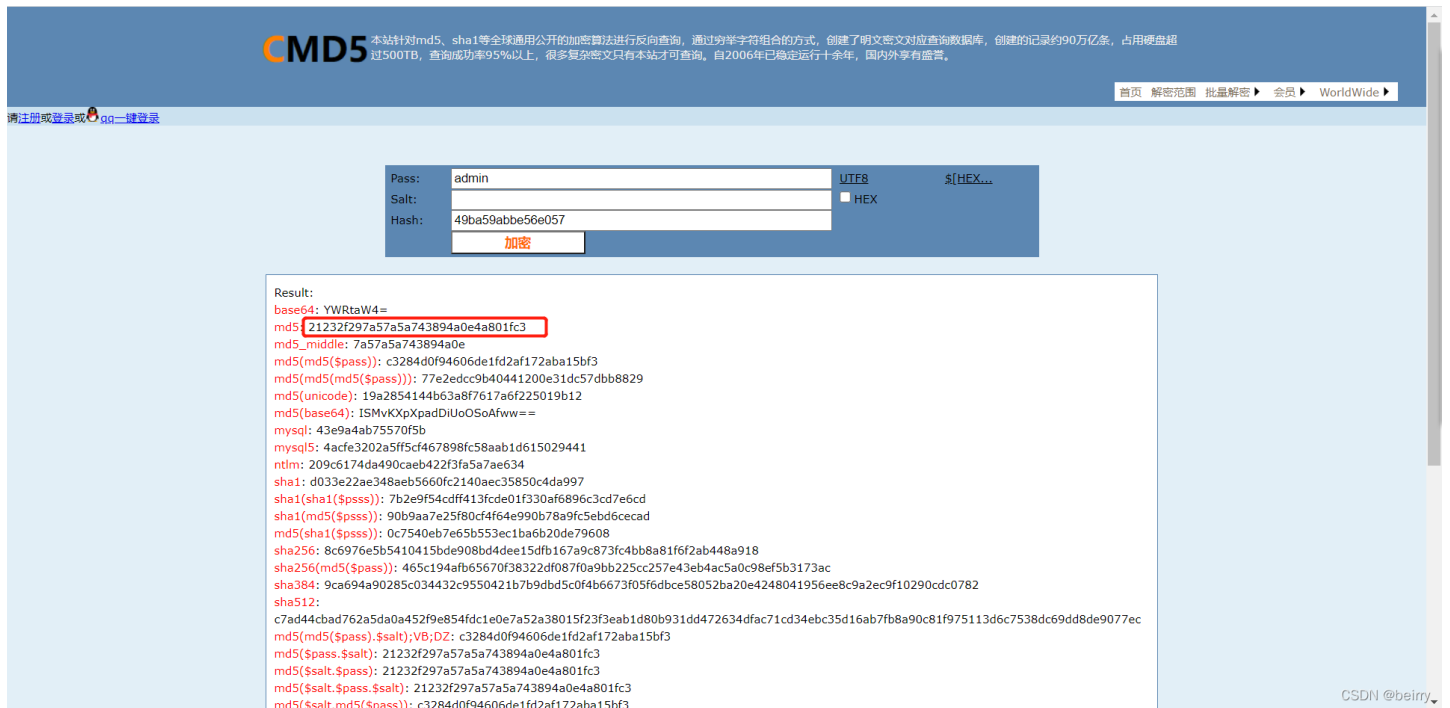
欢迎! [退出](#)



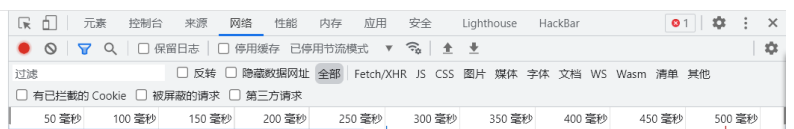
将这串字符用md5解码, 解出来可以看到是test, 也就是我们默认账号



那么我们将admin用md5编码



将这串字符覆盖到cookie上, 刷新页面





伪装者

欢迎 admin! two(cookie_md5_hahaha)

名称 X 标头 预览 响应 启动器 时间 Cookie

home
computer.png
resizeApi.php?id=1215548&size=32
home

```
GET /oda/home HTTP/1.1
Host: rimovni.exeye.run
Connection: keep-alive
Cache-Control: max-age=0
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/oda/index?
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: cookie=21232f297a57a5a743894a0e4a881fc3
```

4 个请求 | 已传输 3.6 kB | 230 kB 项资源

控制 搜索 X 问题 新变化

Aa .* two(giVe_y0u_giFt)

CSDN @beiry