HGAME 2022 Week2 writeup by X1aoba1

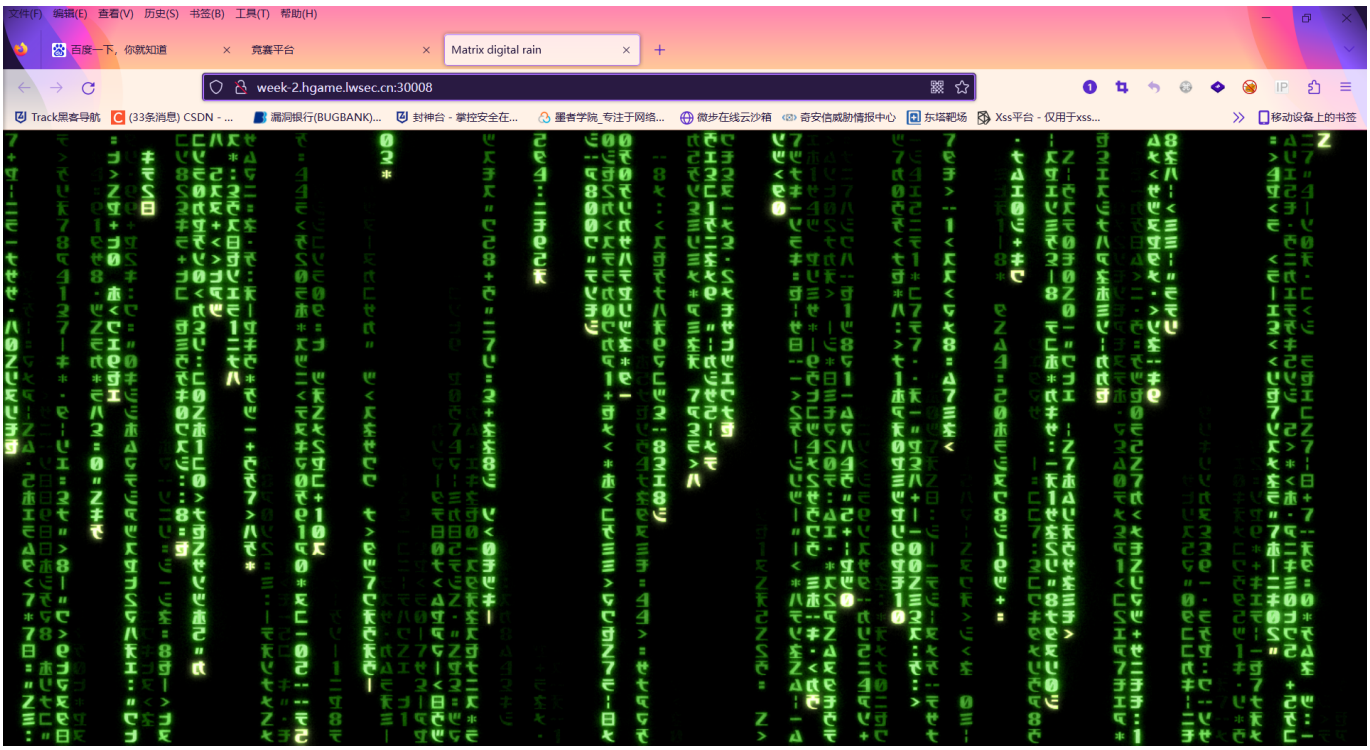
Table of Contents

WEB

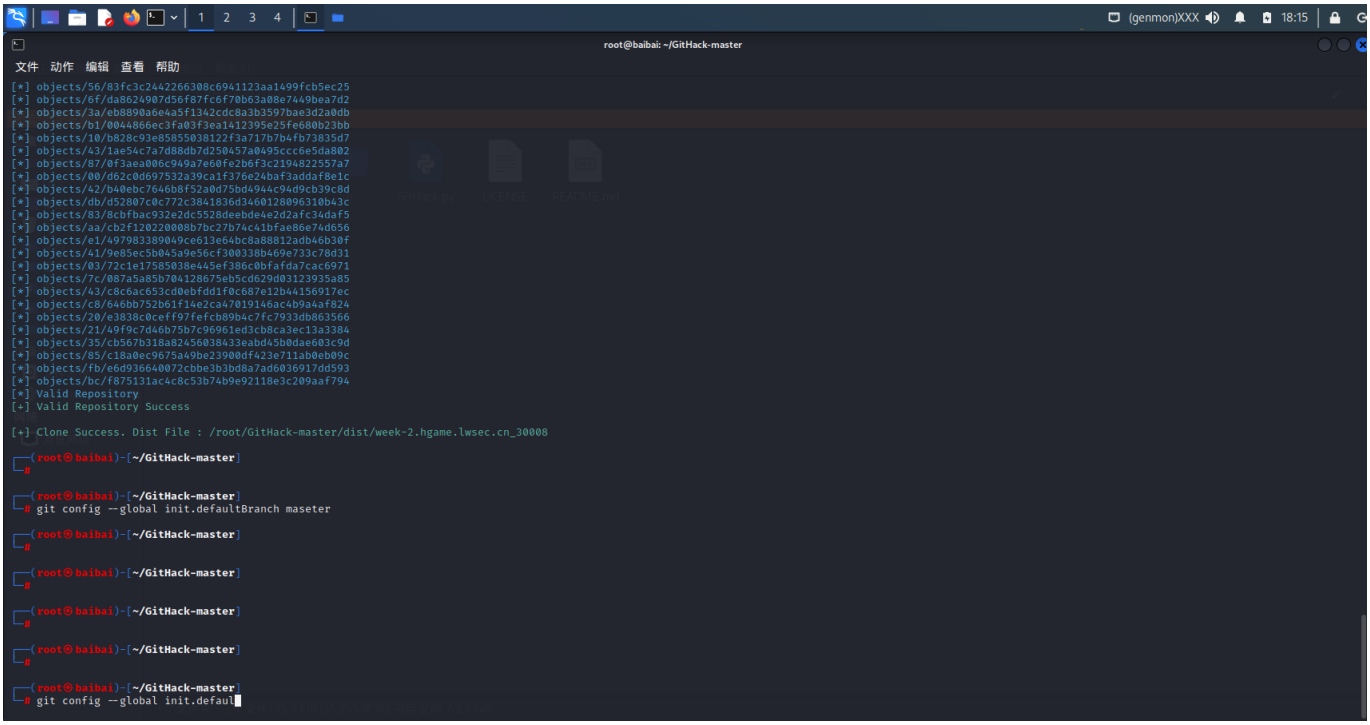
Git Leakage

看题目名字，知道是git文件泄露

打开题目环境

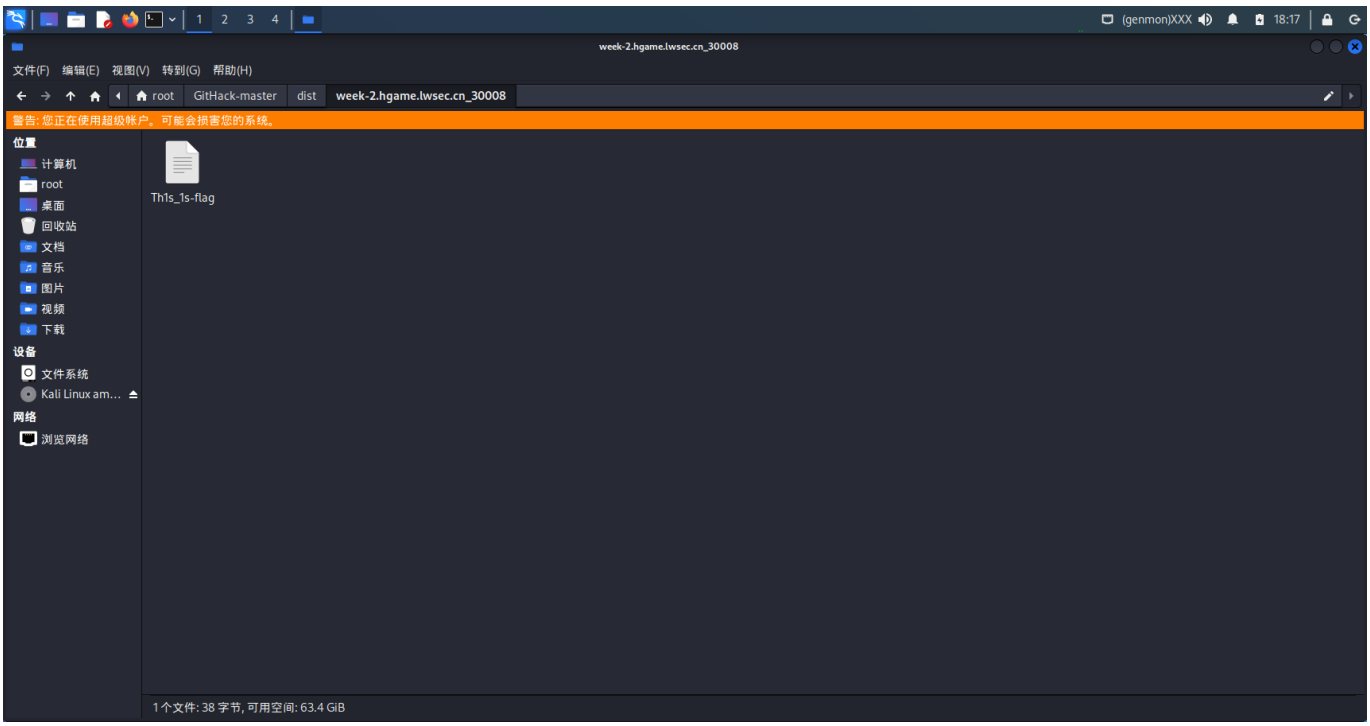


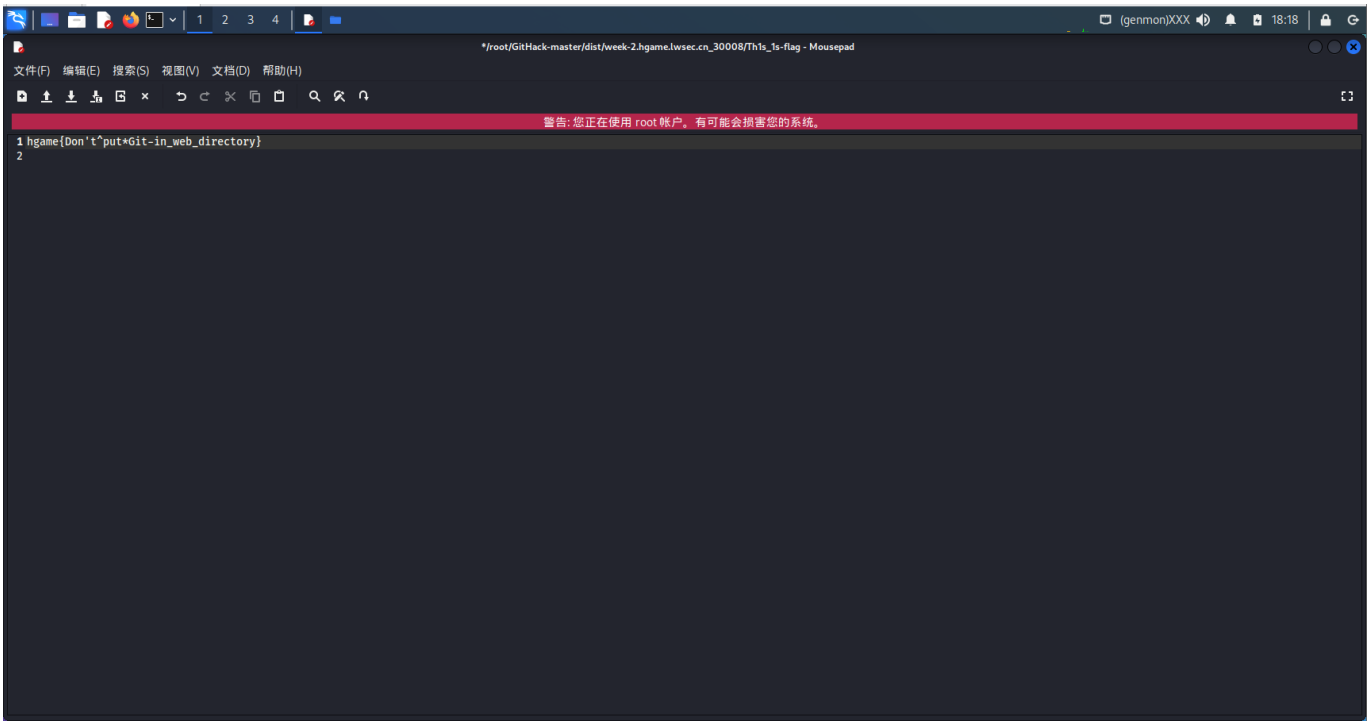
使用GitHack来下载.git文件



之前做过一些题目要进行日志的对比，来获取Flag，这次尝试之后，无果

然后抱着好奇的心态打开了.git文件的下载路径，发现了不得了的东西

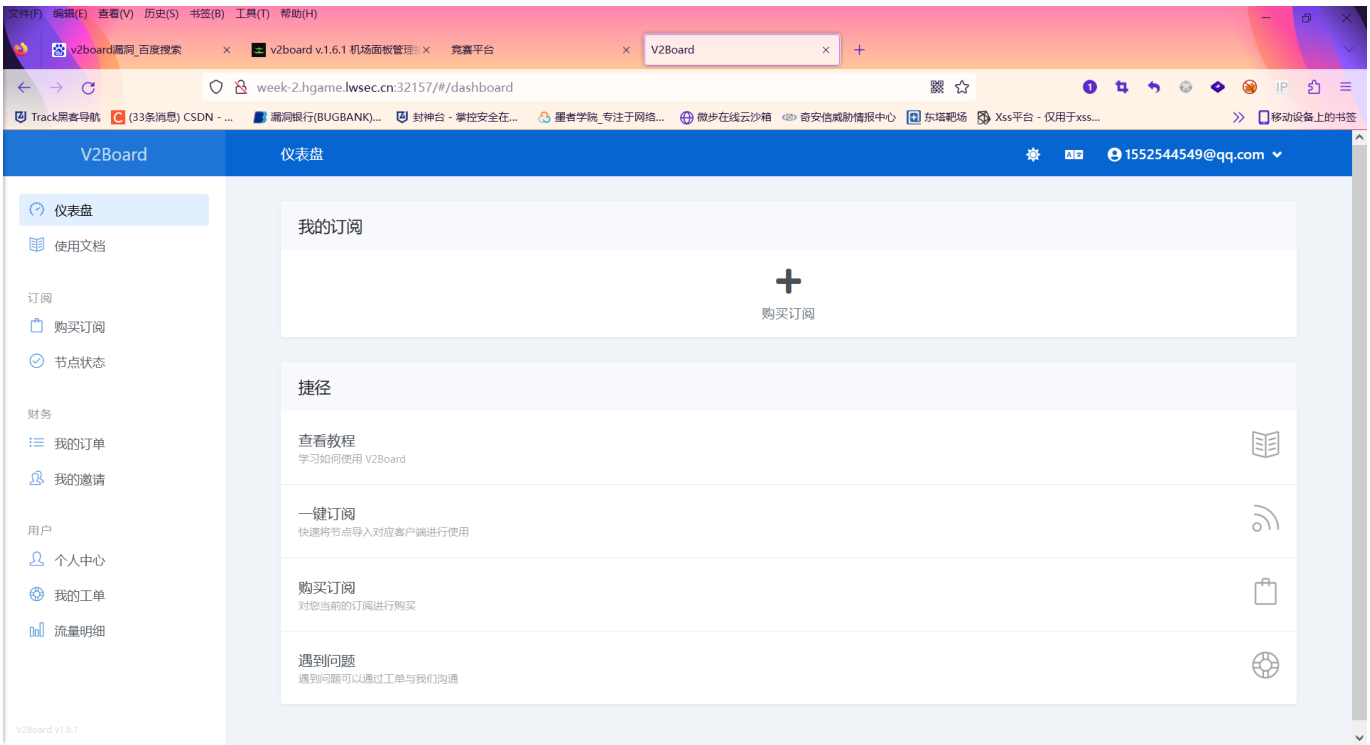




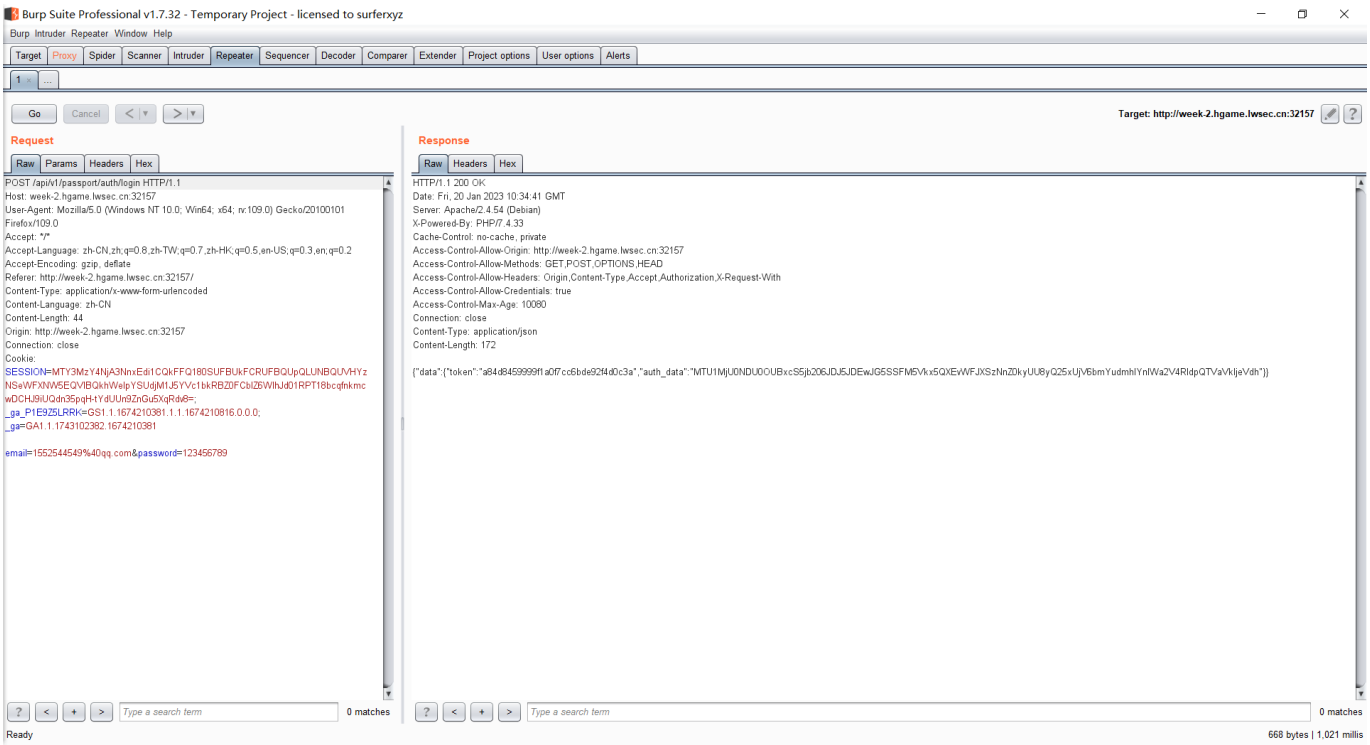
v2board

这道题是22年12月份爆出来的v2board的越权漏洞，漏洞成因是authorization使用redis缓存后没有对普通用户和管理员做鉴权，导致普通用户登录成功后可以直接请求管理员的接口

先伪造邮箱注册一个用户，将自己的authorization写入redis缓存



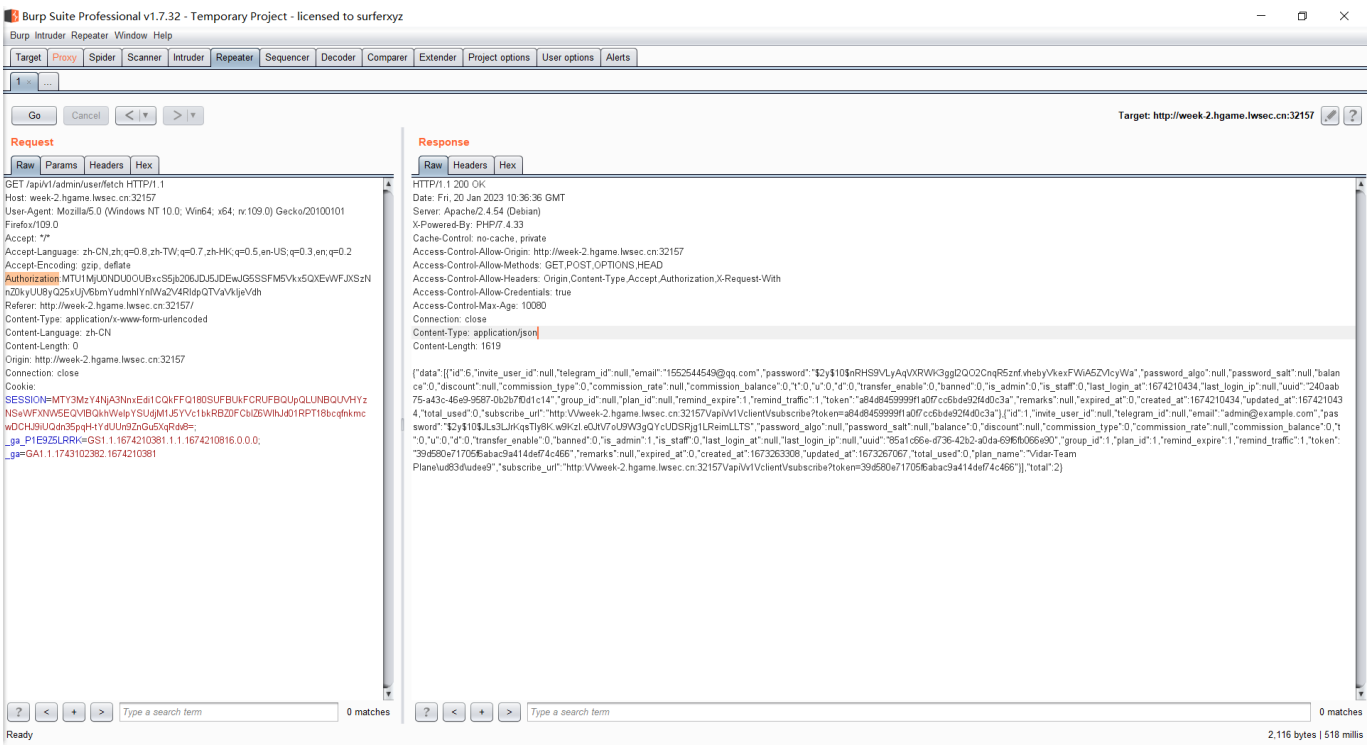
Bp抓包



将得到的auth_data保存下来

然后可以调用接口/api/v1/admin/user/fetch来获取用户信息，实现越权

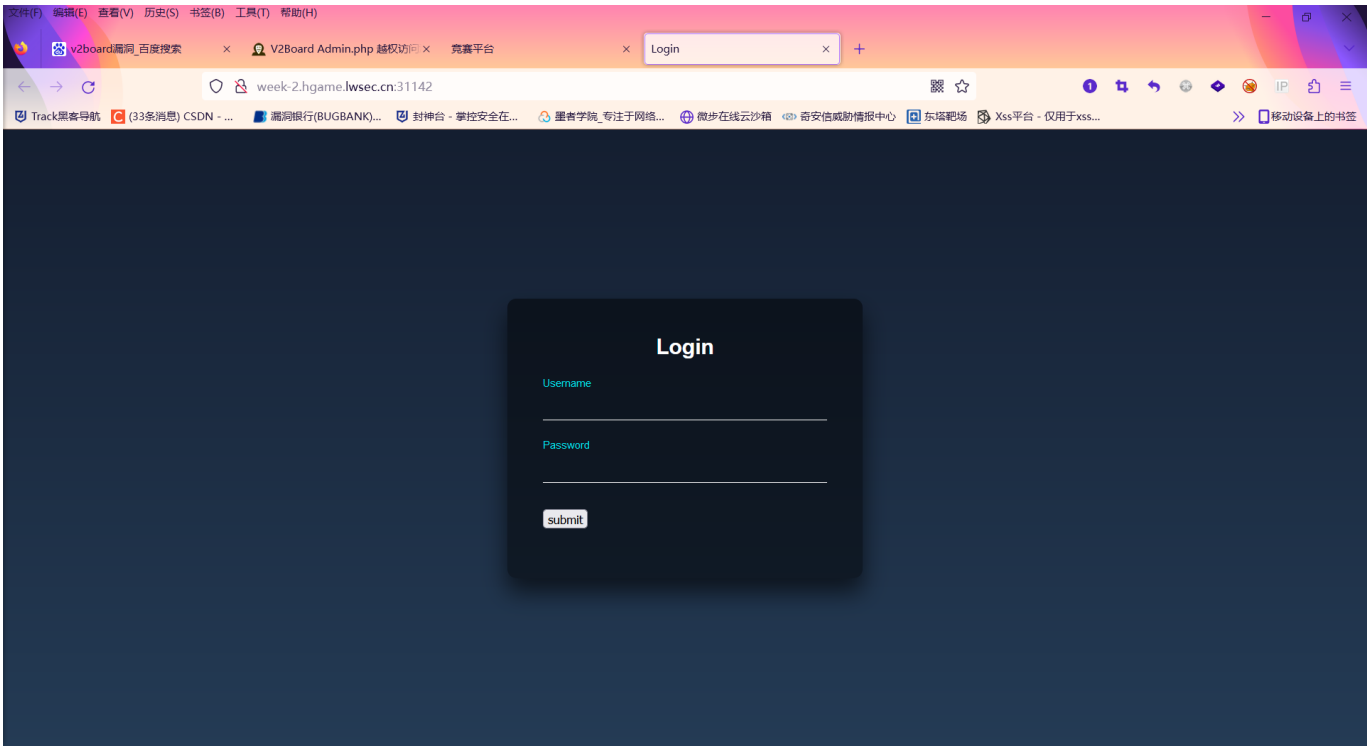
注意：要在消息头中添加Authorization字段，值为之前获取到的auth_data



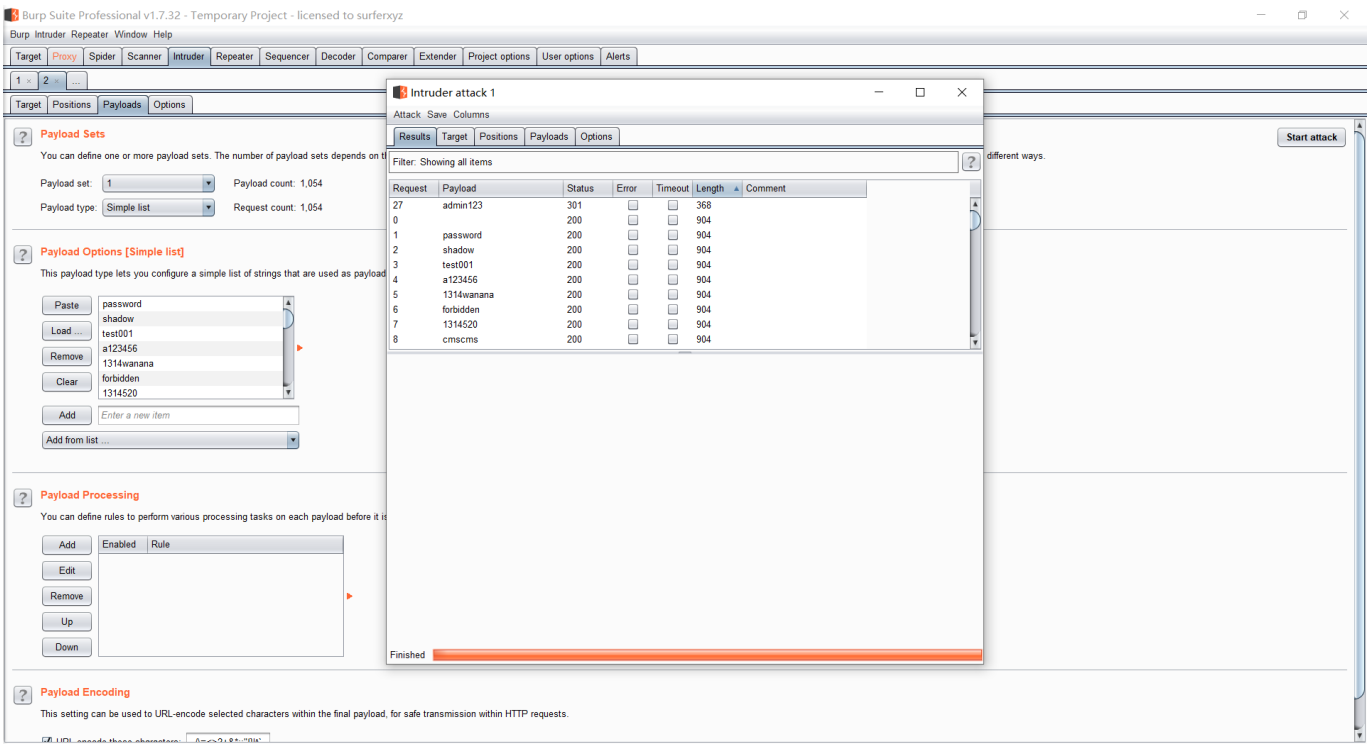
发现admin用户的token，按照Flag格式提交

Search Commodity

题目上说有弱口令爆破，打开环境

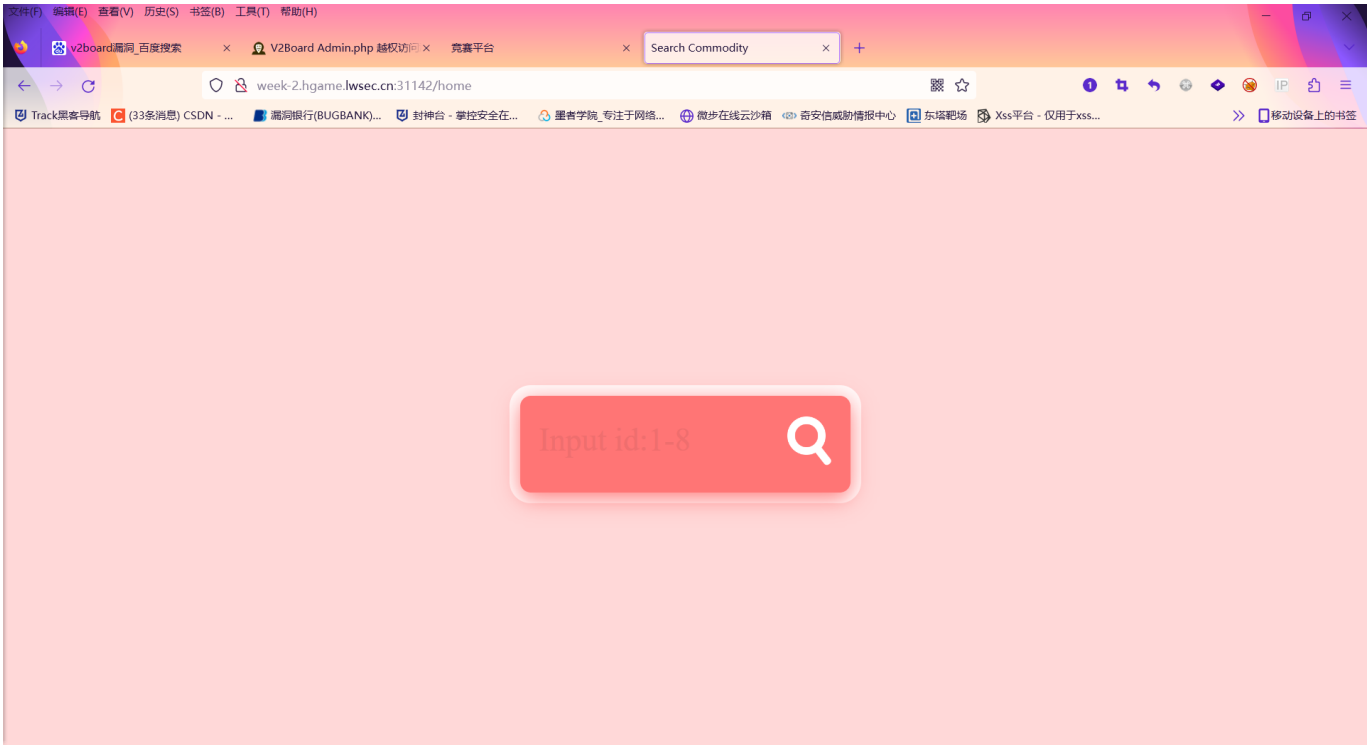


Bp抓包，开始爆破，用户名已经知道了



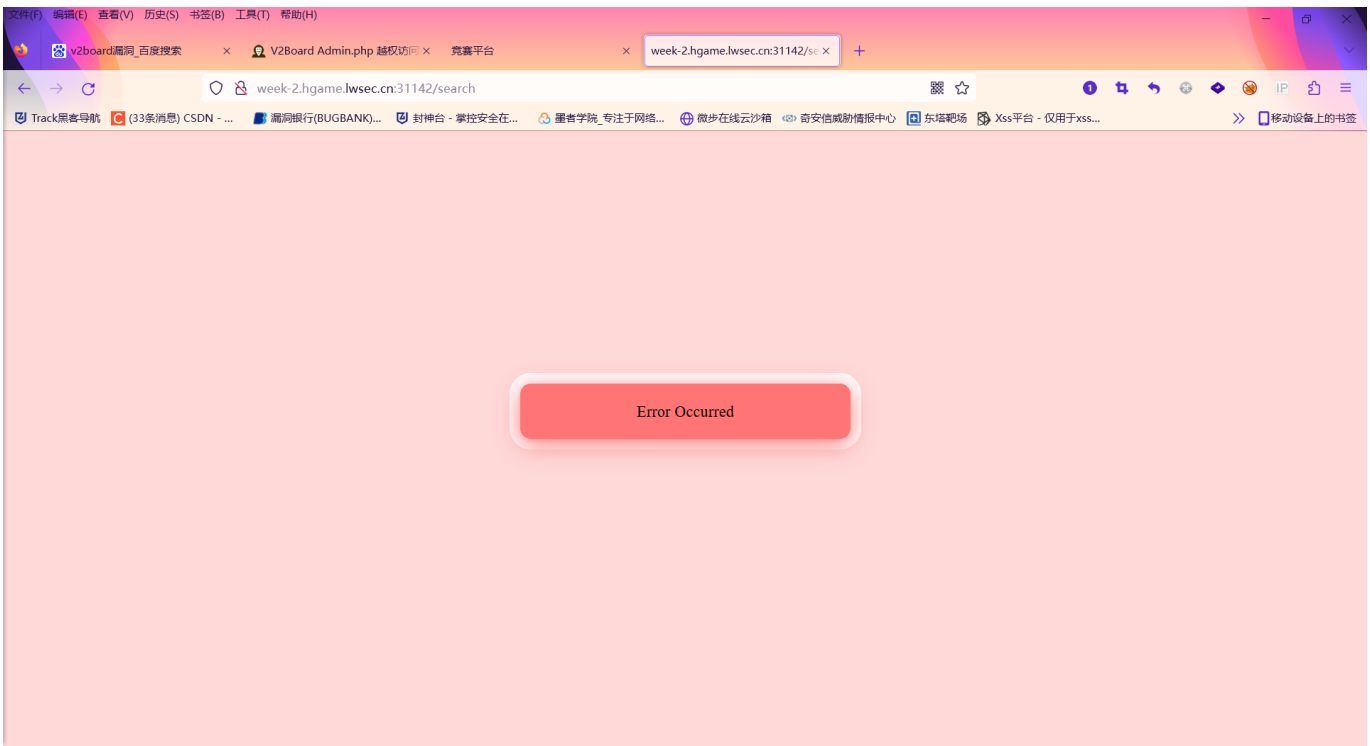
发现密码为admin123

登录进去



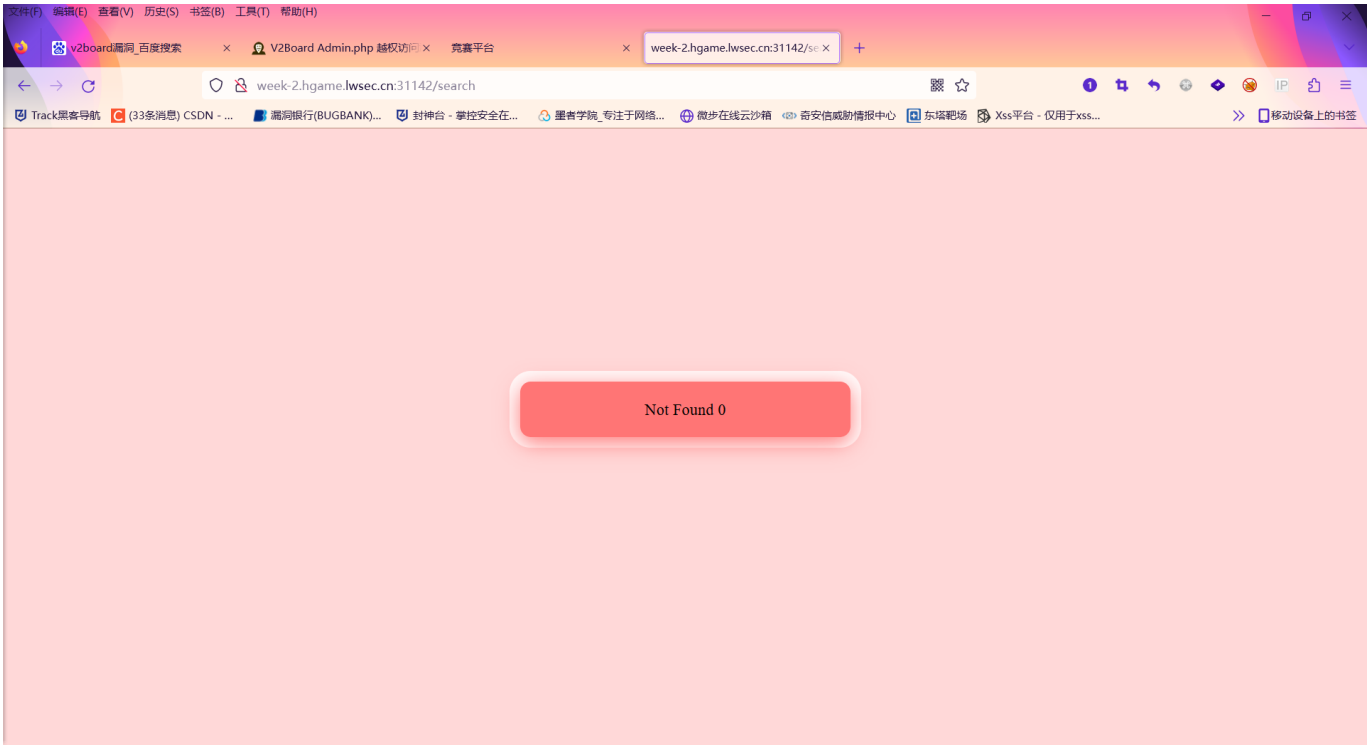
感觉是一道SQL注入题，开始尝试寻找注入点

使用‘ “ ’）”）来闭合，都报错，且报错无具体信息

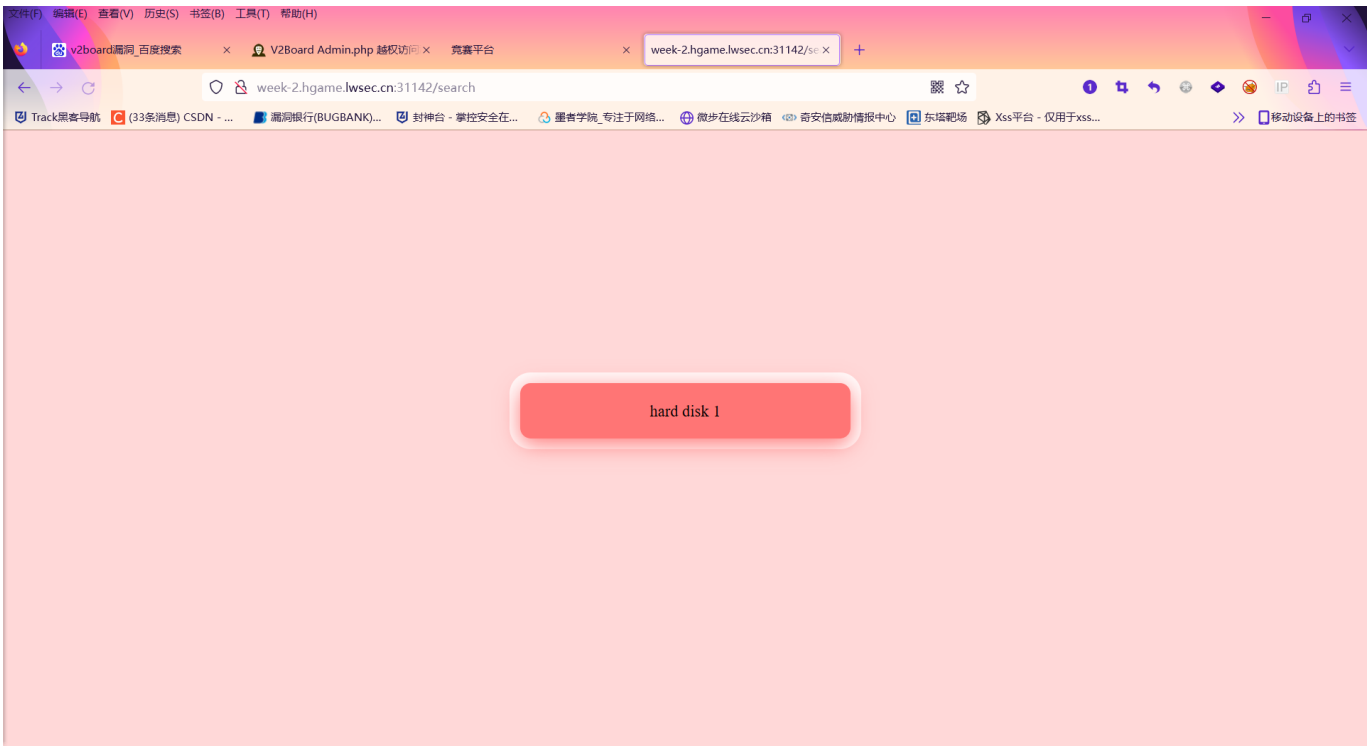


看来是整型注入

输入1 and 1=1 回显正常，输入1 and 1=2 回显也正常，都是Not found 0



然后尝试输入1 and，发现返回了查询成功的页面



waf应该是黑名单，发现之后就替换成空字符，可以来信息探测，判断哪些被过滤掉了

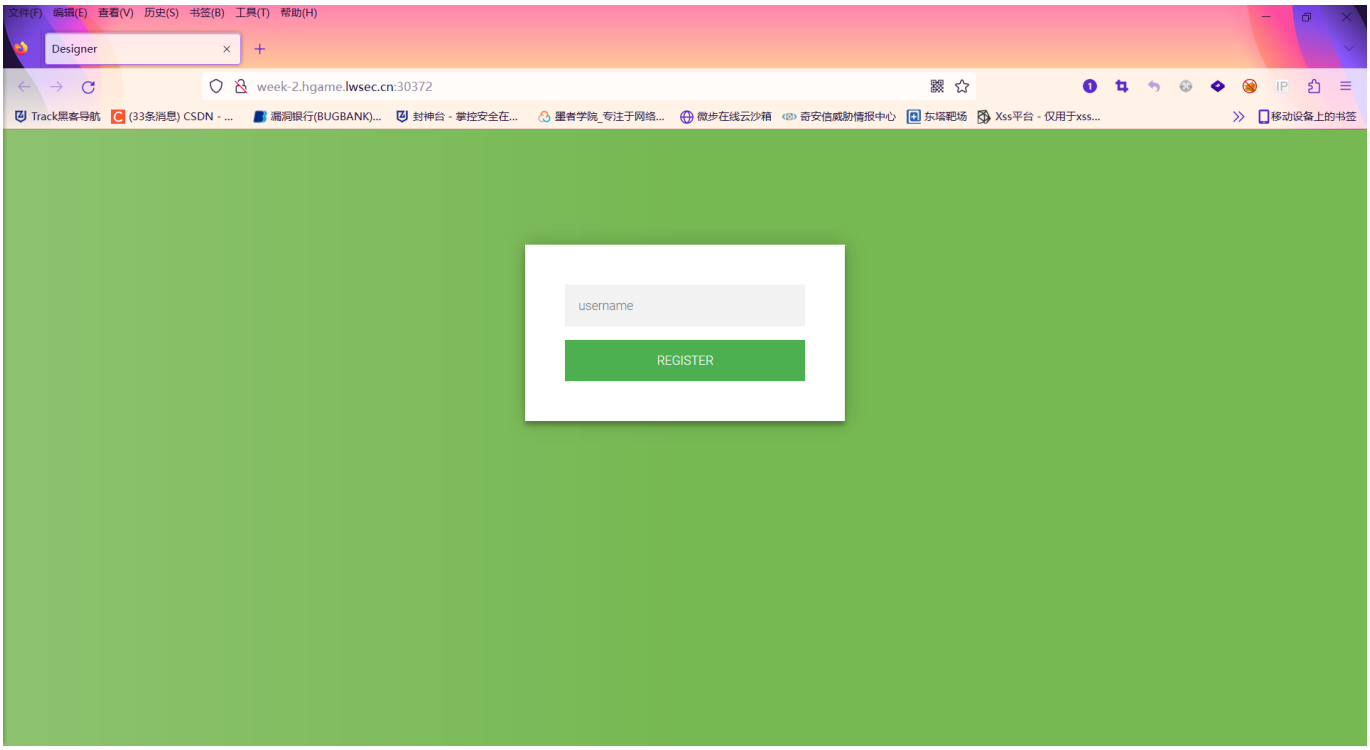
发现or union select 都被过滤掉了

然后无论怎样尝试注入，都是返回错误界面

SQL注入还是卡住了

Designer

打开题目环境



这个username试了一下，可以随便输，登录进去之后就是设计按钮的页面，看不出来什么

题目还给了一个源码，下载审一下

```
app.post("/user/register", (req, res) => {
  const username = req.body.username
  let flag = "hgame{fake_flag_here}"
  if (username == "admin" && req.ip == "127.0.0.1" || req.ip == "::ffff:127.0.0.1") {
    flag = "hgame{true_flag_here}"
  }
  const token = jwt.sign({ username, flag }, secret)
  res.json({ token })
})
```

这里本来以为有眉目了，结果发现上大当（不是

```
app.get("/button/preview", (req, res) => {
  const blacklist = [
    /on/i, /localStorage/i, /alert/, /fetch/, /XMLHttpRequest/, /window/, /location/, /document/
  ]
  for (const key in req.query) {
    for (const item of blacklist) {
      if (item.test(key.trim()) || item.test(req.query[key].trim())) {
        req.query[key] = ""
      }
    }
  }
  res.render("preview", { data: req.query })
})

app.listen(9090)
```

这里发现了可疑的函数，功能应该是按钮的预览

然后再结合之前的页面

猜测应该是存储型XSS漏洞，来获取admin的信息

在网上找了很多XSS漏洞的讲解，最后还是没有把题给做出来

可能思路是错的