

# BJDCTF2nd 假猪套天下第一 Writeup

原创

Tajang  于 2021-04-11 13:51:09 发布  98  收藏

分类专栏: [CTF](#) 文章标签: [php](#) [网络安全](#) [web](#) [html](#)

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/qq\\_45619909/article/details/115598085](https://blog.csdn.net/qq_45619909/article/details/115598085)

版权

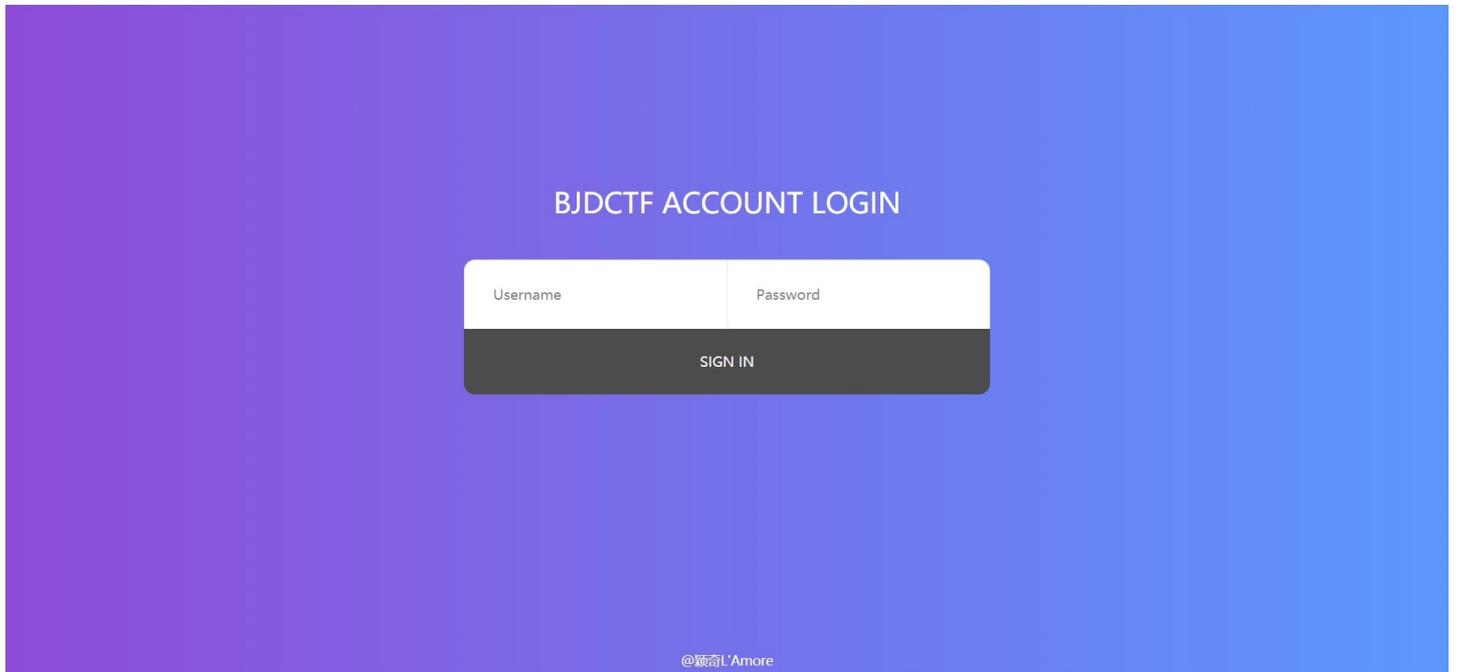


[CTF 专栏收录该内容](#)

20 篇文章 0 订阅

订阅专栏

打开靶机后是一个登录页面



我们先输入一个admin和123456试试



真调皮, 那我们什么都不输入再登录一次

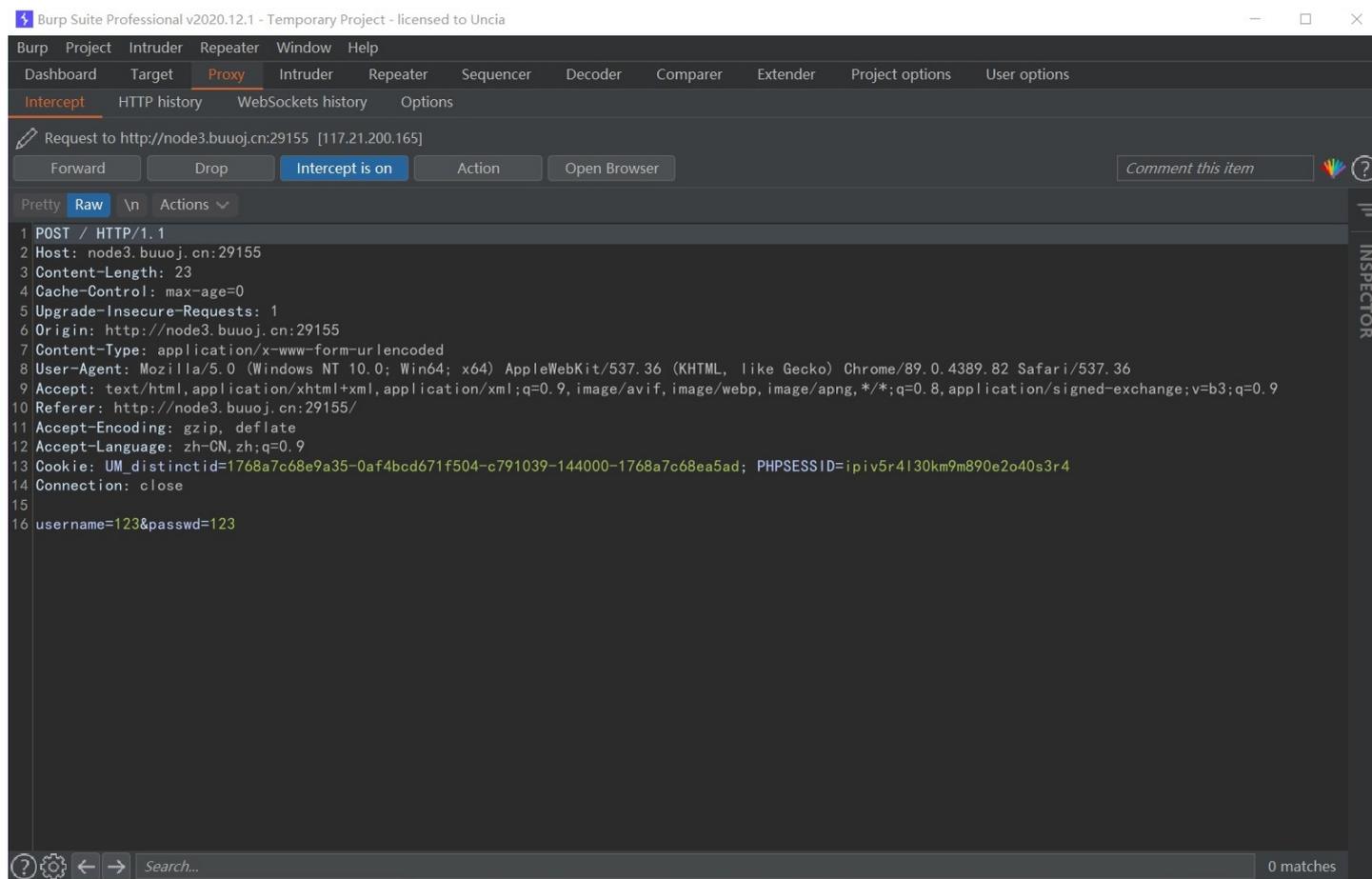
node3.buuoj.cn:29155 显示

不能为空 你登录你妈呢

确定

我真的是越来越喜欢Y1ng师傅出的题了

试了，F12，robots协议，看了网页源代码没发现什么重要内容。在一筹莫展的时候那就抓包。抓包如下：



发送到Repeater,发包。发现如下：

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-h5YGqBse-1618120221358)(https://cdn.jsdelivr.net/gh/Tajang-ctf/blog\_images/bjdtaowa5.png)]

我们可以看到右边代码里倒数第二行提示了Log1n.php页面，我们关闭代理打开网页看一下

one error occurred

@颖奇L'Amore

很粉的界面，没什么线索，再抓一次包，发送到Repeater，发包，内容如下：

The screenshot shows the Burp Suite interface with the Repeater tab active. The request is a GET to /L0g1n.php. The response is an HTML page with a pink background and a message: "Sorry, this site will be available after totally 99 years!".

```
Request
1 GET /L0g1n.php HTTP/1.1
2 Host: node3.buuoj.cn:29155
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: UM_distinctid=1768a7c68e9a35-0af4bcd671f504-c791039-144000-1768a7c68ea5ad; PHPSESSID=ipiv5r4130km9m890e2o40s3r4; time=1615644534
10 Connection: close
11
12

Response
21 height:35px;
22 line-height:35px;
23 background:#DDA0DD;
24 position:fixed;
25 bottom:0px;
26 left:0px;
27 font-size:14px;
28 color:#000;
29 text-align:center;
}
</style>
</head>
<body bgcolor="#DDA0DD">
  <center>
    <a href="https://gem-love.com/" target="_blank"><div class="botC
      @颖奇L'Amore
    </div>
  </a>
  <br>
  <br>
  <br>
  <br>
  <br>
  <br>
  <br>
  <font color=black size=32px>
    Sorry, this site will be available after totally 99 years!
```

右下角给了提示，意思是这个网站99年后才能用，这时又没头绪了，注意它的提示，99年。认真看一下包，发现header里有个time项。那我们把time项数值改很大试试。发包后返回如下：







1 x 2 x ...

Send Cancel < >

Target: http://node3.buuoj.cn:29155

### Request

Pretty Raw \n Actions

```
1 GET /L0g1n.php HTTP/1.1
2 Host: node3.buuoj.cn:29155
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Commodo 64
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: UM_distinctid=
  1768a7c68e9a35-0af4bcd671f504-c791039-144000-1768a7c68ea5ad; PHPSESSID=
  ipiv5r4l30km9m890e2o40s3r4; time=999999999999
10 Client-ip:127.0.0.1
11 Referer:gem-love.com
12 Connection: close
13
14
```

### Response

Pretty Raw Render \n Actions

```
21   line-height:35px;
22   background:#DDA0DD;
23   position:fixed;
24   bottom:0px;
25   left:0px;
26   font-size:14px;
27   color:#000;
28   text-align:center;
29 }
</style>
</head>
<body bgcolor="#DDA0DD">
  <center>
    <a href="https://gem-love.com/" target="_blank"><div class="botCe
      @颖奇L'Amore
    </div>
  </a>
  <br>
  <br>
  <br>
  <br>
  <br>
  <br>
  <br>
  <font color=black size=32px>
  no no no i think it is not the real commmodo 64, <br>
  what is the real ua for Commdo?
```

Inspector

Done 1,104 bytes | 34 millis

不是真的Commodo 64?百度一下，发现这个浏览器全称是Commodore 64,改正再来

1 Burp Suite Professional v2020.12.1 - Temporary Project - licensed to Uncia

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

1 x 2 x ...

Send Cancel < >

Target: http://node3.buuoj.cn:29155

### Request

Pretty Raw \n Actions

```
1 GET /L0g1n.php HTTP/1.1
2 Host: node3.buuoj.cn:29155
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Commodore 64
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: UM_distinctid=
  1768a7c68e9a35-0af4bcd671f504-c791039-144000-1768a7c68ea5ad; PHPSESSID=
  ipiv5r4l30km9m890e2o40s3r4; time=999999999999
10 Client-ip:127.0.0.1
11 Referer:gem-love.com
12 Connection: close
13
14
```

### Response

Pretty Raw Render \n Actions

```
ight:35px;
ne-height:35px;
ckground:#DDA0DD;
sition:fixed;
ttom:0px;
ft:0px;
nt-size:14px;
lor:#000;
xt-align:center;

21 yle>
22 >
23
24 bgcolor="#DDA0DD">
25 ter>
26 href="https://gem-love.com/" target="_blank"><div class="botCenter">
  @颖奇L'Amore
  div>
  a>
27 r>
  r>
  r>
  r>
  r>
  r>
  r>
28 ont color=black size=32px>
29 Sorry, this site is only optimized for those whose email is root@gem-love
```

Inspector

0 matches 0 matches

Done 1,097 bytes | 30 millis

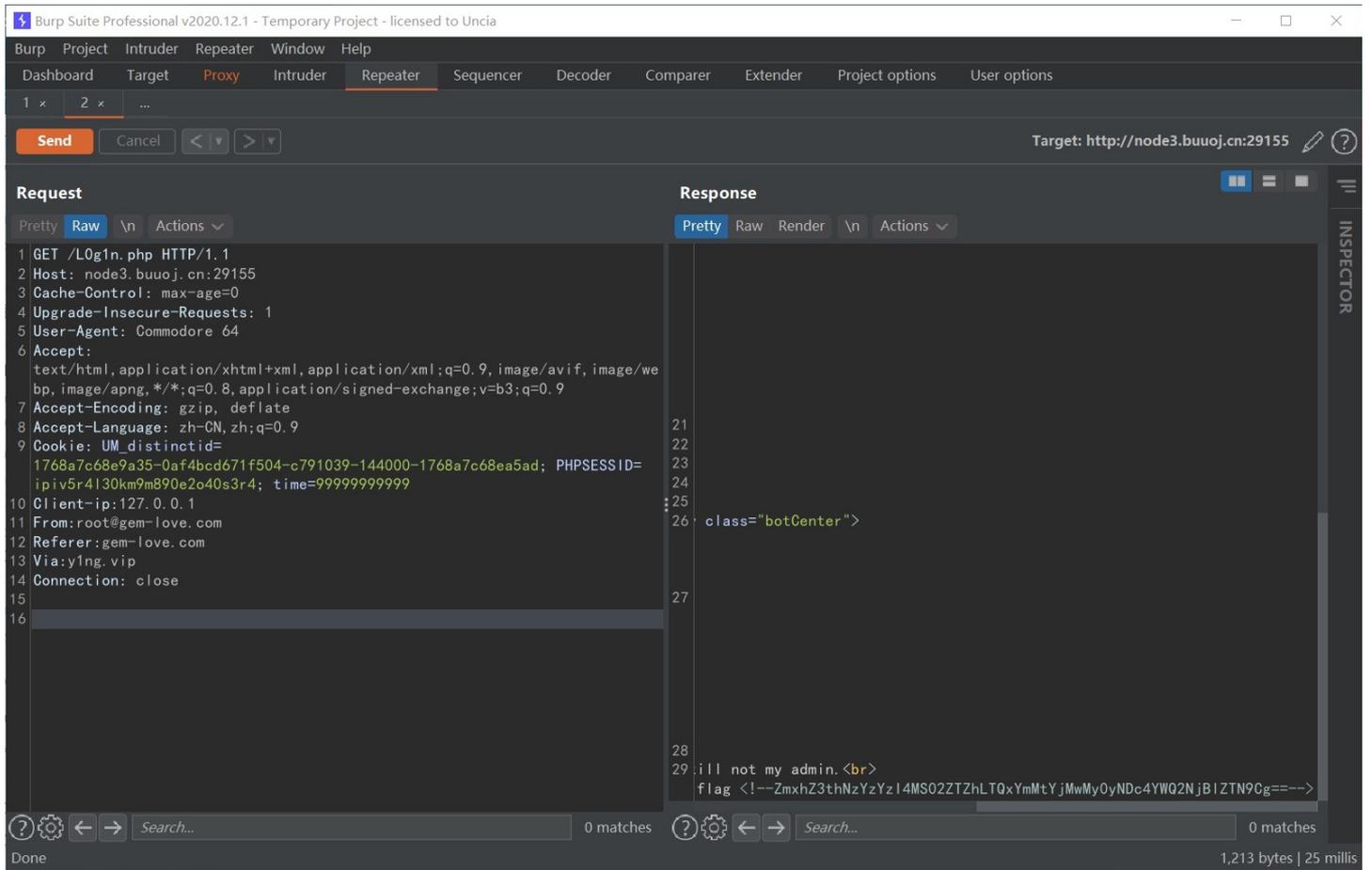
还要邮箱，在包里添加

```
From:root@gem-love.com
```

The screenshot shows the Burp Suite interface with the 'Repeater' tab active. The target is set to `http://node3.buuoj.cn:29155`. The request pane shows an HTTP GET request to `/L0g1n.php` with various headers and cookies. The response pane shows an HTML page with a message in Chinese: 'Sorry, this site is only optimized for those who use the http proxy or if you dont have the proxy, pls contact us to buy, ¥100/Month'. The response also includes CSS styles and HTML tags like `<a href="https://gem-love.com/" target="_blank"><div class="botCenter">`.

提示让我买? 开玩笑, 我身上搜不出10块钱。它说需要代理服务器地址是y1ng.vip, 那我们加个

Via:y1ng.vip



终于给了，虽然它说不给我们flag，但是后面的注释里给了一串代码，尝试使base64进行解码!

请输入要进行 Base64 编码或解码的字符

ZmxhZ3thNzYzYzI4MS02ZTZhLTQxYmMtYjMwMy0yNDc4YWQ2NjBIZlZTN9Cg==

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

flag{a763c281-6e6a-41bc-b303-2478ad660ee3}

有本事你再套几个，这题并不难主要就是考察访问头的要点。不知道的地方仍然百度了一些。希望知识积累得更多!