南邮CG-CTF—Web writeup第一部分

原创

Senimo_ 于 2019-08-02 20:29:41 发布 1167 收藏 3

分类专栏： 各CTF平台 Writeup 文章标签： 南邮CG CTF writeup web

本文链接：https://blog.csdn.net/weixin_44037296/article/details/98235643

南邮CG-CTF—Web writeup第一部分

南邮CG-CTF链接

签到题1

Web 10pt

这一定是最简单的

题目地址

进入页面后，显示：“**key在哪里？**”，查看网页源码，得到**key**：

```
<a style="display:none">nctf{flag_admiaanaaaaaaaaaaa}</a>
```

md5 collision

Web 20pt

题目地址

```
//网页源码已经给出
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if (isset($a)) {
    if ($a != 'QNKCDZO' && $md51 == $md52) {
        echo "nctf{*****************}";
    } else {
        echo "false!!!";
    }
} else {
    echo "please input a";
}
```

分析代码：传入变量“**a**”的值不等于`'QNKCDZO'`，进行**md5加密**后与“**md51**”相等，即等于`'QNKCDZO'`进行**md5加密**的值。

```
QLTHNDT   //加密后
0e405967825401955372549139051580
```

在地址栏中构造**GET**传参,得到**flag**：`nctf{md5_collision_is_easy}`

```
http://chinalover.sinaapp.com/web19/?a=QLTHNDT
```

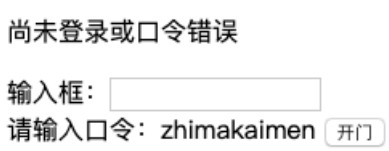
知识点：“!=”和“==”比较漏洞

通过“**!=**”和“**==**”比较漏洞我们可以绕过md5比较，即在比较时，**PHP**会把每一个以“**0e**”开头的哈希值都解释为“**0**”，所以如果两个不同的密码经过哈希以后，其哈希值都是以“**0e**”开头的，那么**PHP**将会认为他们相同，即为“**0**”

签到2

Web 15pt

题目地址



尝试输入口令，但发现被限制了字符长度，查看网页源代码：

```
<p>输入框：<input type="password" value="" name="text1" maxlength="10"><br>
 请输入口令：zhimakaimen
```

将“**<input>**”标签中的“**maxlength**”属性删除或修改为“**11**”，提交后得到**flag**

flag is:nctf{follow_me_to_exploit}

输入框：
请输入口令：zhimakaimen 开门

这题不是WEB

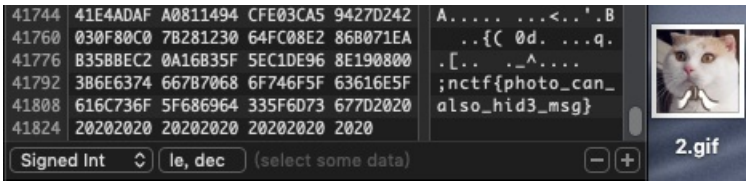
Web 25pt

真的，你要相信我！这题不是WEB

题目地址

答案又是啥。。 

将**gif**图下载到本地，在**HEX**类编辑器中打开，在最后隐藏着**flag**：



层层递进

Web 25pt
黑客叔叔p0tt1的题目 欢迎大家关注他的微博
题目地址

题目为层层递进，通过**F12**中**Sources**功能，查看网站的包含情况，发现到可疑地址：`SO.html`，查看发现相似可以地址，最后在`404.html`源码中得到**flag**（竖排插入在标签中）：

```
<script src="./js/jquery-n.7.2.min.js"></script>
<script src="./js/jquery-c.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-{.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-h.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-a.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-l.7.2.min.js"></script>
<script src="./js/jquery-4.7.2.min.js"></script>
<script src="./js/jquery-g.7.2.min.js"></script>
<script src="./js/jquery-}.7.2.min.js"></script>
-->
```

AAencode

Web 25pt
javascript aaencode
题目地址

编码有点问题，暂时无法做。

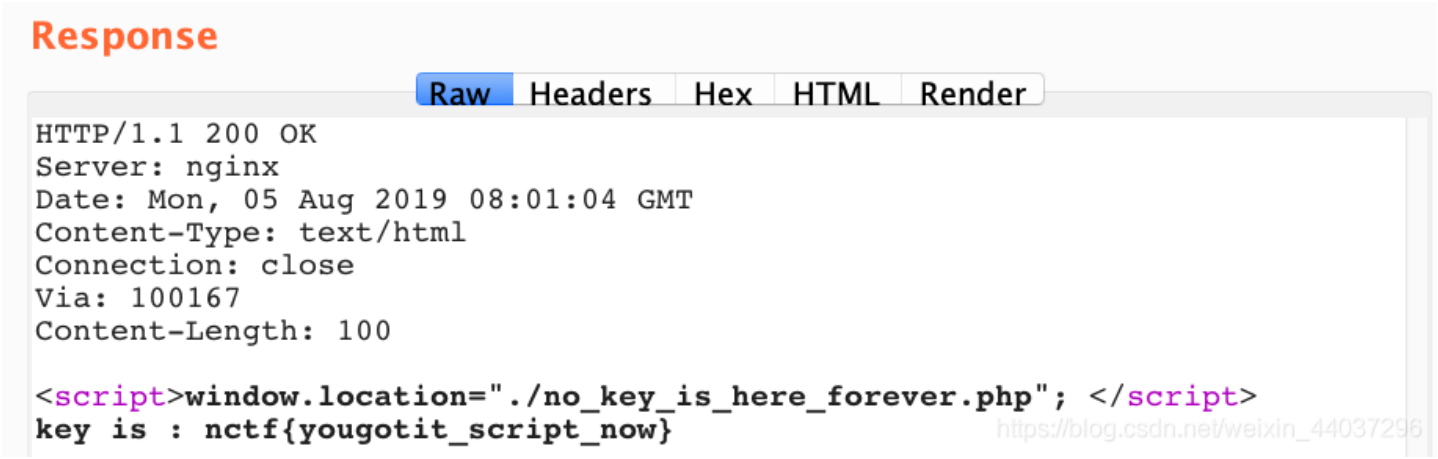
单身二十年

Web 20pt
这题可以靠技术也可以靠手速！ 老夫单身二十年，自然靠的是手速！
题目地址

进入页面后显示：“到这里找key”，查看网页源码：

```
<body>
    <a href="./search_key.php">_到这里找key__</a>
</body>
```

点击链接后跳转到新页面：“**这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神**”，观察到**URL**地址结尾不是之前的链接：`no_key_is_here_forever.php`，怀疑出现跳转，使用**Burp Suite**抓取第一次跳转的数据包，**Send to Repeater**后，发送数据包，在**Response**中得到**flag**：



php decode

Web 25pt

见到的一个类似编码的shell，请解码

```
<?php
function CLsI($ZzvSWE)
{
    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));
    for ($i = 0; $i < strlen($ZzvSWE); $i++) {
        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);
    }
    return $ZzvSWE;
}

eval(CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```

经过了gzinflate和base64_decode加密，通常将eval改为echo即可实现解密，在线调试PHP代码，运行后得到**flag**：`nctf{gzip_base64_hhhhhh}`

文件包含

Web 25pt

没错 这就是传说中的LFI

题目地址

进入页面后显示链接**click me? no**，点击后在地址栏传入了变量赋值语句：`?file=show.php`，页面显示**test123**，根据提示为**文件包含漏洞**，根据**PHP伪协议**尝试构造如下**Payload**：`?file=php://filter/read=convert.base64-encode/resource=index.php`，将**index.php**的源码经过**Base64编码**输出：

```
PGh0bWw+CiAgICA8dGl0bGU+YXNkZjwvdGl0bGU+CiAgICAKPD9waHAKCWVycm9yX3JlcG9ydGluZygwKTsKCWlmKCEkX0dFVFtmaWxlXSl7ZWNo
byAnPGEgaHJlZj0iLi9pbmRleC5waHA/ZmlsZT1zaG93LnBocCI+Y2xpY2sgbWU/IG5vPC9hPic7Cn0KJGZpbGUgPSAkX0dFVFsnZmlsZSddOwoJ
KHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3RyKCRmaWxlLCJk
YXRhIikpewoJCWVjaG8gIk9oIG5vISI7CgkJZXhpdCgpOwoJfQoJaW5jbHVkZSgkZmlsZSk7IAovL2ZsYWc6bmN0ZntlZHVsY25pX2VsaWZfbGFj
b2xfc2lfc2lodH0KCj8+CjwvaHRtbD4=
```

将输出的Base64在线解码，得到源码：

```
<html>
<title>asdf</title>

<?php
error_reporting(0);
if (!$_GET[file])
{
    echo '<a href="./index.php?file=show.php">click me? no</a>';
}
$file = $_GET['file'];
if (strstr($file, "../") || stristr($file, "tp") || stristr($file, "input") || stristr($file, "data")) {
    echo "Oh no!";
    exit();
}
include($file);
//flag:nctf{edulcni_elif_lacol_si_siht}

?>
</html>
```

flag已给出：`nctf{edulcni_elif_lacol_si_siht}`

单身一百年也没用

Web 30pt

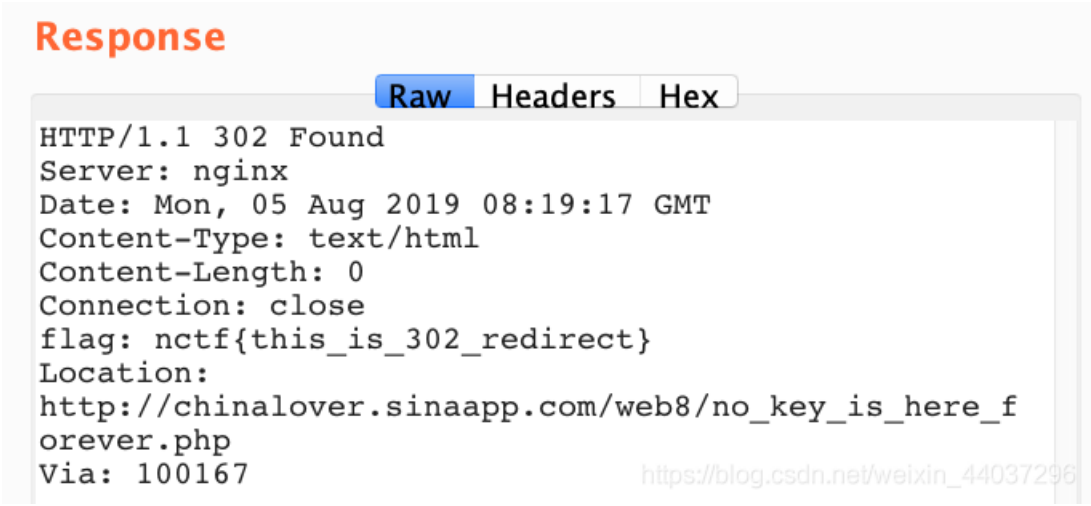
是的。。这一题你单身一百年也没用

题目地址

进入页面后显示：“**到这里找key**”，查看网页源码：

```
<body>
    <a href="./index.php">_到这里找key__</a>
</body>
```

点击链接后跳转到新页面：“**这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神**”，观察到**URL**地址结尾不是之前的链接：`no_key_is_here_forever.php`，怀疑出现跳转，使用**Burp Suite**抓取第一次跳转的数据包，**Send to Repeater**后，发送数据包，在**Response**中得到**flag**：



Dowenload～！

Web 25pt

想下啥就下啥别下音乐，不骗你，试试下载其他东西

题目地址

COOKIE

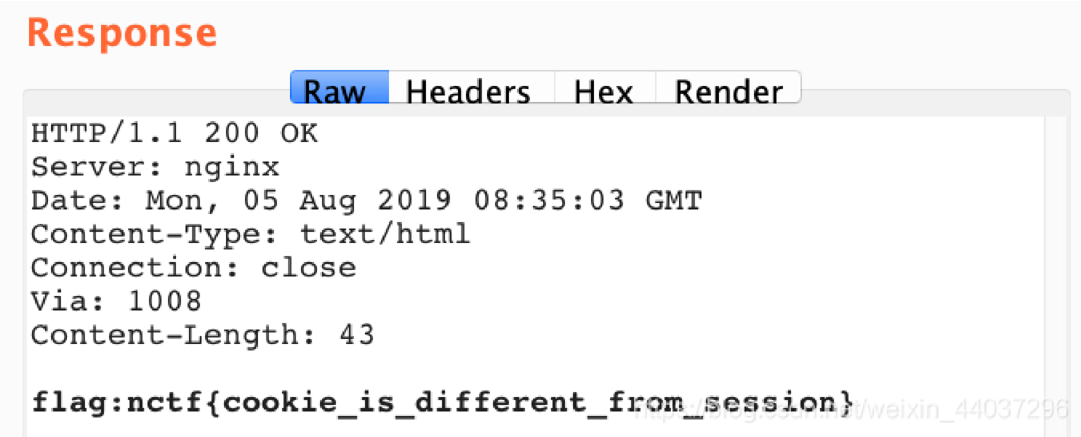
Web 25pt

COOKIE就是甜饼的意思~

TIP: 0==not

题目地址

进入网页后显示空白，使用**Burp Suite**抓取数据包，**Send to Repeater**后，发送数据包，在**Response**中提示：`Set-Cookie: Login=0`，在**Request**中添加请求头信息：`Cookie: Login=1`，发送数据包后，在**Response**中得到**flag**：



MYSQL

Web 30pt

不能每一题都这么简单嘛 你说是不是？

题目地址

进入页面后显示：“**Do you know robots.txt?** 百度百科”

提示为“**robots.txt**”，访问后得到：

```
鍒お寮€濹津紝flag涓嶅湪杩欏紝杩欒釜鏂囦欢鐨勭敤閫旂粡鐪嬭繃浜嗗紵
鍦–TF姣旇禌涓紝杩欒釜鏂囦欢寰€寰€瀛樻斁鐫€鎻愮ず淇℃伅

TIP:sql.php

<?php
if ($_GET[id]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT, SAE_MYSQL_USER, SAE_MYSQL_PASS);
    mysql_select_db(SAE_MYSQL_DB);
    $id = intval($_GET[id]);
    $query = @mysql_fetch_array(mysql_query("select content from ctf2 where id='$id'"));
    if ($_GET[id] == 1024) {
        echo "<p>no! try again</p>";
    } else {
        echo($query[content]);
    }
}
?>
```

分析代码：将传入的**id**的值转换为整型，带入到数据库查询，但在**if**语句的时候还是比较的原来输入的**id**值。

令**id**值的指数部分等于`1024`，小数部分任意取值，在地址栏构造GET传参：

```
http://chinalover.sinaapp.com/web11/sql.php?id=1024.01
```

得到**flag**：`nctf{query_in_mysql}`

注：**intval()** 函数通过使用指定的进制 **base** 转换（默认是十进制），返回变量的 integer 数值。

GBK Injection

Web 50pt

题目地址

/x00

Web 30pt

题目有多种解法，你能想出来几种？

题目地址

```
view-source:
<?php
if (isset ($_GET['nctf'])) {
    if (@ereg("^[1-9]+$", $_GET['nctf']) === FALSE)
        echo '必须输入数字才行';
    else if (strpos($_GET['nctf'], '#biubiubiu') !== FALSE)
        die('Flag: ' . $flag);
    else
        echo '骚年，继续努力吧啊~';
}
```

分析代码：通过**GET**方式传入变量**nctf**的值，且只能输入**1-9**的数字，且变量必须包含“**#biubiubiu**”。
因为**ereg()函数存在NULL**截断漏洞，导致了正则表达式被绕过，所以可以使用`%00`截断正则表达式的匹配，所以在地址栏构造**GET**传参：`?nctf=1%00%23biubiubiu`，访问后，得到**flag**：`flag:nctf{use_00_to_jieduan}`。

注：ereg()函数用指定的模式搜索一个字符串中指定的字符串,如果匹配成功返回true,否则,则返回**false**。搜索字母的字符是大小写敏感的。

bypass again

Web 30pt

依旧是弱类型

来源 hctf

题目地址

```
<?php
if (isset($_GET['a']) and isset($_GET['b'])) {
    if ($_GET['a'] != $_GET['b'])
        if (md5($_GET['a']) == md5($_GET['b']))
            die('Flag: ' . $flag);
        else
            print 'Wrong.';
}
```

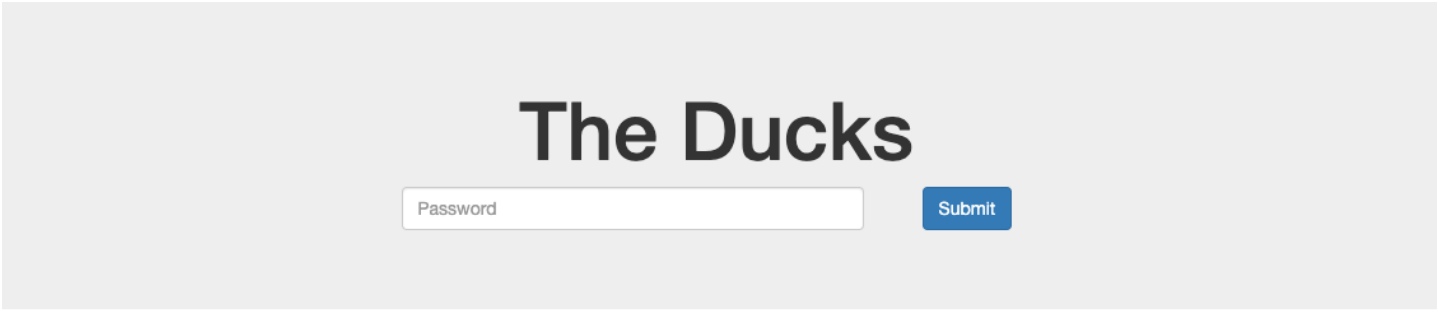
分析代码：传入变量**a**和变量**b**，两个变量的值不相等，但**md5加密**后的值相等。
同之前“**md5 collision**”题的知识点一样，通过“**==**”比较漏洞我们可以绕过md5比较，构造如下传参：`?a=QNKCDZO&b=QLTHNDT`，访问后得到**flag**：`nctf{php_is_so_cool}`

变量覆盖

Web 40pt

听说过变量覆盖么？

题目地址

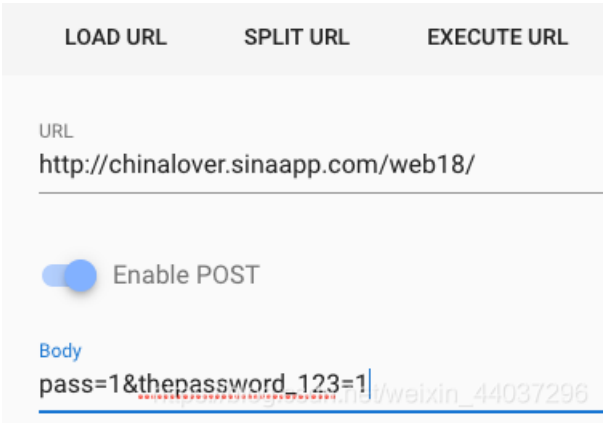


source at /source.php

先访问/source.php

分析代码：文件通过**POST**传输进来的值通过extrace()函数处理，判断变量**pass** 和变量**thepassword_123**的值是否相等。

不知道变量**thepassword_123**的值，但可以通过**extrace()函数变量覆盖漏洞重新给变量thepassword_123**赋值，通过**Google Chrome的插件HackBar**构造如下赋值：`pass=1&thepassword_123=1`



注：**extract()** 函数从数组中将变量导入到当前的符号表。

PHP是世界上最好的语言

Web 30pt

听说PHP是世界上最好的语言

题目地址