# 知了堂网安培训 “输入密码获取flag“ writeup “有时候某些看似不起眼的小文件，或许会有大作用“

原创

晴天咩咩 于 2021-06-16 16:02:41 发布 117 收藏 1

分类专栏： CTF 文章标签： 安全 信息安全 加密解密 php

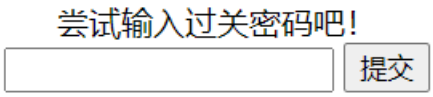


本文链接：https://blog.csdn.net/qq_35694424/article/details/117959289

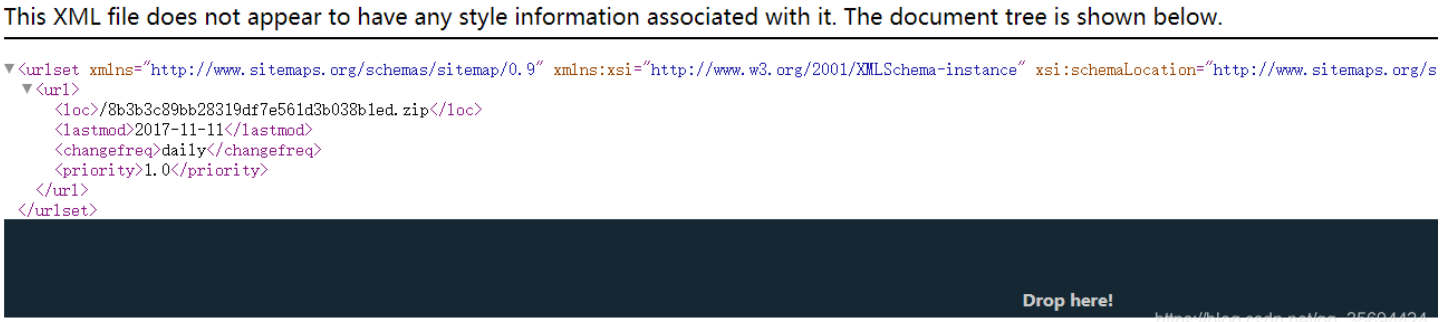


> 题目描述:有时候某些看似不起眼的小文件，或许会有大作用。

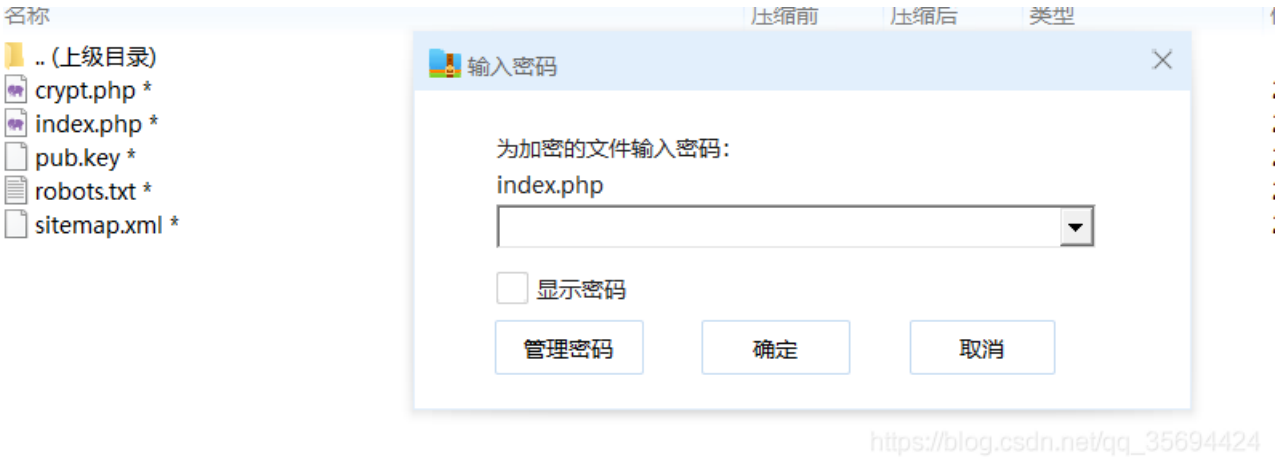
进入题目,发现一个web页面,根据提示扫描后台文件,得到sitemap.xml




访问得到如下信息




访问`8b3b3c89bb28319df7e561d3b038b1ed.zip`文件得到加密的后台文件




爆破无果,必须得到密钥才行.随后发现返回html中存在两行注释

```
<!DOCTYPE html>
<html lang="en">
<head>
        <meta charset="UTF-8">
        <title>输入密码获取flag</title>
        <script>
                window.document.oncontextmenu = function(){
                        return false;
                }
                document.onkeydown = function(){
                        if(window.event && window.event.keyCod
                                event.keyCode=0;
                                event.returnValue=false;
                        }
                }
        </script>
</head>
<body>
        <center>
                尝试输入过关密码吧!
                <form action="" method="post">
                        <input type="text" name="t">
                        <input type="submit">
                </form>
                        </center>
        <!--d360b102f09e82aaf214aa97d3b0c2b1-->
        <!--RSA-->
</body>
</html>
```



以为密码是那串MD5的原像,但是解密后仍然不对,这里存脑洞,最后得到密码就是这个MD5值,随后解压压缩包.得到如下文件

```php
<?php
 include 'crypt.php';
 include 'xxx.php'; //flag文件
 if(isset($_POST['t'])){
  $an = $_POST['t'];
  if(encrypt($an)==="2659271827191d241d1f1f5a25251d19"){
   echo "You win! flag is:".$flag;
  }else{
   echo "Ooops!!!Your answer is wrong!";
  }
 }
?>
```

分析逻辑可以知道通过encrypt函数加密t,检验是否密文等于2659271827191d241d1f1f5a25251d19,通过查阅php手册发现并没有encrypt这个函数,所以该函数存在与crypt.php包中.

打开crypt.php文件发现是二进制文件,但是php为脚本语言不存在编译故推测该文件被加密过,考虑到文件夹下还有pub.key文件,提取公钥后发现n为2048位,e为65537是安全参数,不存在破解方法.


尝试将n直接分解可以得到两个素数,那么可以得到rsa私钥d,从而解密

| | Result: |
|---|---|
| digits | number |
| 617 (show) | 1876228833...81<617> = 250527704258269<15> · 7489107197...49<602> |

解密脚本如下

```python
from Crypto.Util.number import *
from Crypto.PublicKey import RSA

key = RSA.import_key(open("./pub.key", "rb").read())
n = key.n
e = key.e
c = open('crypt.php', 'rb').read()
c = bytes_to_long(c)

p = 74891071972884336452892671945839935839027130680745292701175368094445819328761543101567760612778187287503041052186054409602799660254304070752542327616415127619185118484301676127655806327719998855075907042722072624352495417865982621374198943186383488123852345021090112675763096388320624127451586578874243946255833495297552979177208715296225146999614483257176865867572412311362252398105201644557511678179053171328641678681062496129308882700731534684329411768904920421185529144505494827908706070460177001921614692189821267467546120600239688527687872217881231173729468019623441005792563703237475678063375349
q = n // p
assert(p * q == n)
d = inverse(e, (p-1) * (q-1))
print(long_to_bytes(pow(c,d,n)))
```

结果如下

```
10179@ChrisMBookPro  Downloads  8b3b3c89bb28319df7e561d3b038b1ed  3.7.5  & "C:/Program Files/Python37/python.exe" c:/Users/10179/Downloads/8b3b3c89bb28319df7e561d3b038b1ed/exp.py
b'\x02\xdf(\x97\xc6sk6$\xe4\x81\xa2/V\x8awzj\x05\xca{8\xb1\xf7\xd9G\x7f?\x12\x9e\x8a\xe0\xaf\x988SC\x8dg\x81\xde\x97N\x049\x1c\xcb\xc5\xd0H\x00function encrypt($data){\r\n\t$str="";\r\n\t$a = strrev(str_rot13($data));\r\n\tfor($i=0;$i<strlen($a);$i++){\r\n\t\t$b = ord($a[$i])+10;\r\n\t\t$c = $b^100;\r\n\t\t$e = sprintf("%02x", $c);\r\n\t\t$str.=$e;\r\n\t}\r\n\treturn $str;\r\n}'
```

将代码格式化后如下

```php
function encrypt($data) {
    $str="";
    $a = strrev(str_rot13($data));
    for ($i=0;$i<strlen($a);$i++) {
        $b = ord($a[$i])+10;
        $c = $b^100;
        $e = sprintf("%02x", $c);
        $str.=$e;
    }
    return $str;
}
```



根据代码写出解密函数,随后得到明文

```python
import codecs
c = bytes.fromhex('2659271827191d241d1f1f5a25251d19')
m = ''
for i in c:
    t = i ^ 100
    t = t - 10
    m += chr(t)
m = codecs.encode(m[::-1], "rot13" )
print('answer: ', m)
```

问题 输出 终端 调试控制台

```
10179@ChrisMBookPro Downloads 8b3b3c89bb28319df7e561d3b038b1ed 3.7.5 &
Users/10179/Downloads/8b3b3c89bb28319df7e561d3b038b1ed/exp.py
b'\x02\xdf(\x97\xc6sk6$\xe4\x81\xa2/V\x8awzj\x05\xca{8\xb1\xf7\xd9G\x7f?\x12\x9e\x8a\xe
b\xc5\xd0H\x00function encrypt($data){\r\n\t$str="";\r\n\t$a = strrev(str_rot13($data))
\t$b = ord($a[$i])+10;\r\n\t\t$c = $b^100;\r\n\t\t$e = sprintf("%02x", $c);\r\n\t\t$str
answer:  fb774ddb6bf9e938
10179@ChrisMBookPro Downloads 8b3b3c89bb28319df7e561d3b038b1ed 3.7.5
```



提交明文最后得到flag

尝试输入过关密码吧!

提交

You win! flag is:flag{023299564b0db47d5f3e476a254d0c21}

完整代码

```
from Crypto.Util.number import *
from Crypto.PublicKey import RSA

key = RSA.import_key(open("./pub.key", "rb").read())
n = key.n
e = key.e
c = open('crypt.php', 'rb').read()
c = bytes_to_long(c)

p = 74891071972884336452892671945839935839027130680745292701175368094445819328761543101567760612778187287503041052186054409602799660254304070752542327616415127619185118484301676127655806327719998855075907042722072624352495417865982621374198943186383488123852345021090112675763096388320624127451586578874243946255833495297552979177208715296225146999614483257176865867572412311362252398105201644557511678179053171328641678681062496129308882700731534684329411768904920421185529144505494827908706070460177001921614692189821267467546120600239688527687872217881231173729468019623441005792563703237475678063375349
q = n // p
assert(p * q == n)
d = inverse(e, (p-1) * (q-1))
print(long_to_bytes(pow(c,d,n)))

import codecs
c = bytes.fromhex('2659271827191d241d1f1f5a25251d19')
m = ''
for i in c:
    t = i ^ 100
    t = t - 10
    m += chr(t)
m = codecs.encode(m[::-1], "rot13" )
print('answer: ', m)
```