

## 逐鹿中原



## 极客之光

首届RealWorld国际(郑州)网络安全大赛

远程控制车灯、轻松拿到QQ登录凭证……

# 网络竞技,很炫很酷有点神秘 其实就在我们身边

本报讯(记者 覃岩峰 张竞昶 王翠/文 宋晔 李焱/图) 远程控制车灯、轻松拿到QQ登录凭证……每当一道道比赛题目被破解,选手们忍不住击掌相庆,观众们发出一片欢呼,现场气氛被炫酷的网络攻防术推向一个又一个高潮。

“我们出的题目虽然有难度,但都有战队解出来,这让我们感到欣慰。”长亭科技首席安全研究员、联合创始人杨坤说,从题量和难易度来说,这次比赛是成功的。比赛是一个全新赛制的尝试,跟线上赛相比,这些题目的解决时间都耗费比较长,需要选手们深挖才能得到真实的破解效果。



## 首支成功破题队伍 抓住漏洞攻入目标路由器

比赛首日下午4时3分,来自俄罗斯的LCBC战队成为第一个解题成功的队伍,拿到第一个500分。

“我们在路由器的网络协议程序里编写了一个扩展,这个扩展里面有一个漏洞,攻击者利用这个漏洞入侵到目标路由器,拿到了最高权限。”杨坤介绍,由于路由器一般是公司或者家用网络的网关,所有漏洞破解后,接到这个路由器上的所有设备的数据均可以被监听和篡改。

“就像刚刚演示的一样,选手破解成功后,我们在自己的电脑上输入大赛的官网,出现的界面已经变成了选手写下的网页。”杨坤说,“打个比方比如你输入的是百度的网址,而实际上登录的则是他们想让你登录的网站。”



## “吃饭、睡觉、攻破、重复”强队连闯“三道关”

“吃饭、睡觉、攻破、重复”——Eat Sleep Pwn Repeat战队2017年世界排名第2,累计获得9次国际CTF大赛冠军,实力强悍。战队成员通力合作,连闯“三道关”。在破解“The Last Guardian”题目时,经过台下的不断验算,队伍来到舞台上从正式

开始到攻破耗时不足1分钟,成为首个攻破该题的战队。战队制作了一个恶意网页,当网络“受害人”浏览该网页时,只要登录过一次,“受害人”的QQ、微博、博客等网络登录凭证均可被轻易盗取,一系列网络攻击展示让现场观众叹为观止。

## 赢得比赛,需要经验专长加运气

“传统的CTF比赛参加过很多次,但这样的线下比赛是第一次参加。”PPP战队一名队员说,网络安全技术更迭很快,郑州这次的大赛有很多创新的地方,希望能多举办这样的比赛,给全球极客提供交流切磋的机会。

对于获得冠亚季军的三支战队,杨坤认为,这些战队都是国际顶尖战队,除了现场参赛的队员,还有远程的队员援助,能够取得最终成绩,是他们的经验和专长使然。比如,冠军俄罗斯LCBC战队的队员中,有

很多都是工作多年的安全专家,经验丰富,有大量的实战经验,在解决实际场景这一类的题上有特别优势。亚军中国台湾的217战队中,有一个队员非常擅长web安全方面的题目,在网站安全方向是顶级的安全员,在此类题中贡献不少。第三名德国的Eat Sleep Pwn Repeat战队,他们挖掘一些未知的漏洞经验,取得了超出预期的效果。

当然除了实力,杨坤认为,比赛成绩还需要选手们克服时差,以及在选题中的“运气”。

## ■战队专访

## So Cool! 明年还想参加

本报讯(记者 张竞昶 覃岩峰)昨日下午5时,比赛刚刚落幕,记者专访了两位队员。

一个说:“So Cool! 感觉特别棒!”

一个说:“我们会离自己的榜样和目标越来越远。”

## PPP战队: 感觉特别棒! 团队收获很多

“So Cool! 感觉特别棒! 如果明年还有这样的赛事,我还要参加!”在这次大赛中,PPP战队以1806分的总成绩取得了第四名,尽管没有斩获前三名稍感遗憾,但团队成员们依然很开心、兴奋。经历了48小时不眠不休的高强度奋战,大家始终情绪饱满。

PPP战队源自美国卡内基梅隆大学,其成员来自美国、加拿大、新加坡、瑞士、中国等多个国家。2017年世界排名第3名、2016年世界排名第3名,累计获得国际CTF大赛冠军40次……在网络安全大赛领域,PPP战队可谓强者中的强者,比赛结束后,PPP

战队队长Bo Robert Xiao在接受采访时表示,这是他们第一次参加Real World大赛,与传统的CTF竞赛相比,这种基于真实世界软件的全新CTF赛制难度大一些。比赛伊始,由于不适应新赛制,团队很久都没有人得分,几个小时之后,才开始陆续解决问题,之后越来越顺手。

“跟平时参加的比赛构成不太一样,传统的CTF更像Puzzle,Real World更现实,一些类似Pwn赛的漏洞破解场景,平时根本没有机会接触,经过这次大赛,团队收获了很多。”对于比赛结果,Bo Robert Xiao很乐观,“别急,再给我们点儿时间!”

## r3kapiq战队: 我们会离榜样和目标越来越近

r3kapiq战队,2018年新成立的中国战队,是由新锐战队Eur3kA与老牌CTF战队Flappypig战队组成的联合战队,累计获得国际大赛前5名3次,此次派出10人出战,现场5人,场外支持5人,最终以1235分的战绩取得了第5名。

“我们的战队很‘新’,但经验一点儿也不少,今年4月第一次参加国际大赛以来,在很多国内外大赛中都取得了不错的成绩。”r3kapiq战队的队长李冠成是北京大学的研三学生,在他看来,作为当今广为流传的一种网络竞技形式,传统的CTF(夺旗赛)有很多特点和优势,但考察的知识和技巧不一定适用

于真实软件攻防场景。此次RealWorld国际(郑州)网络安全大赛在延续传统CTF赛事命题灵活、难度可控的基础上,结合了只有在Pwn赛中才能体验到的攻防技术应用,虚拟空间的网络安全技术与真实世界相连,参赛体验特别好,对队员个人技术的提高有很大的帮助。

李冠成说,此次大赛,他们发挥得不是特别理想,一些成员完全没有接触过这种新赛制,今后,会加强这方面的学习,提高能力,“我们跟世界顶级强队的差距不小,未来的路还很长。我相信,通过不断的学习和实践,我们会离自己的榜样和目标越来越近。”