ISC 2019 第七届互联网安全大会

WCTF赛事回顾与实践型人才培养的探索

郑文彬

360集团首席安全技术官

小鹅助理

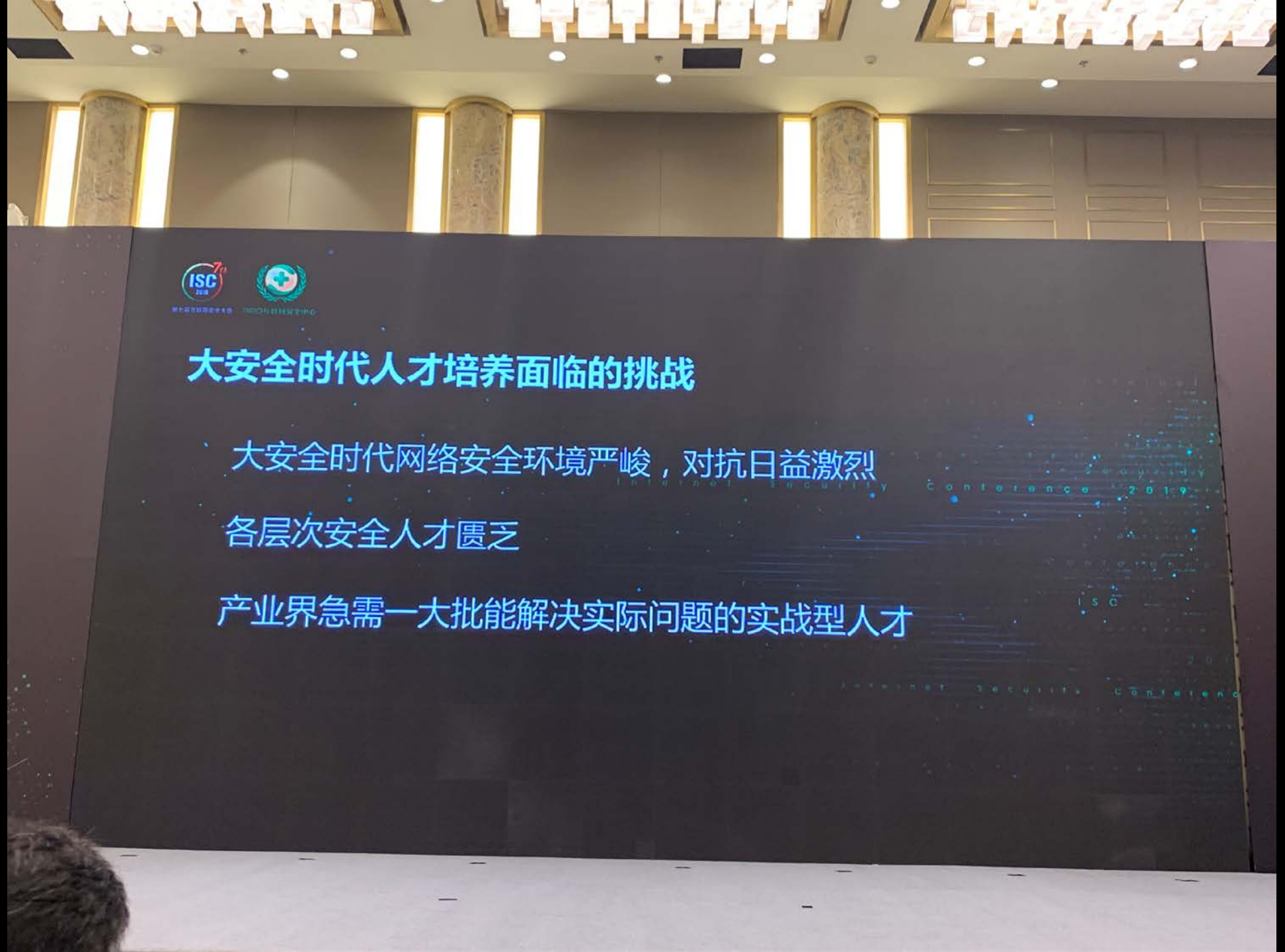
扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费

门票


ISC
MJ0011
360集团首席安全技术官
360Vulcan Team 创始人


ISC
WCTF赛事回顾与实战型人才培养的探索
彭峙酿 360核心安全

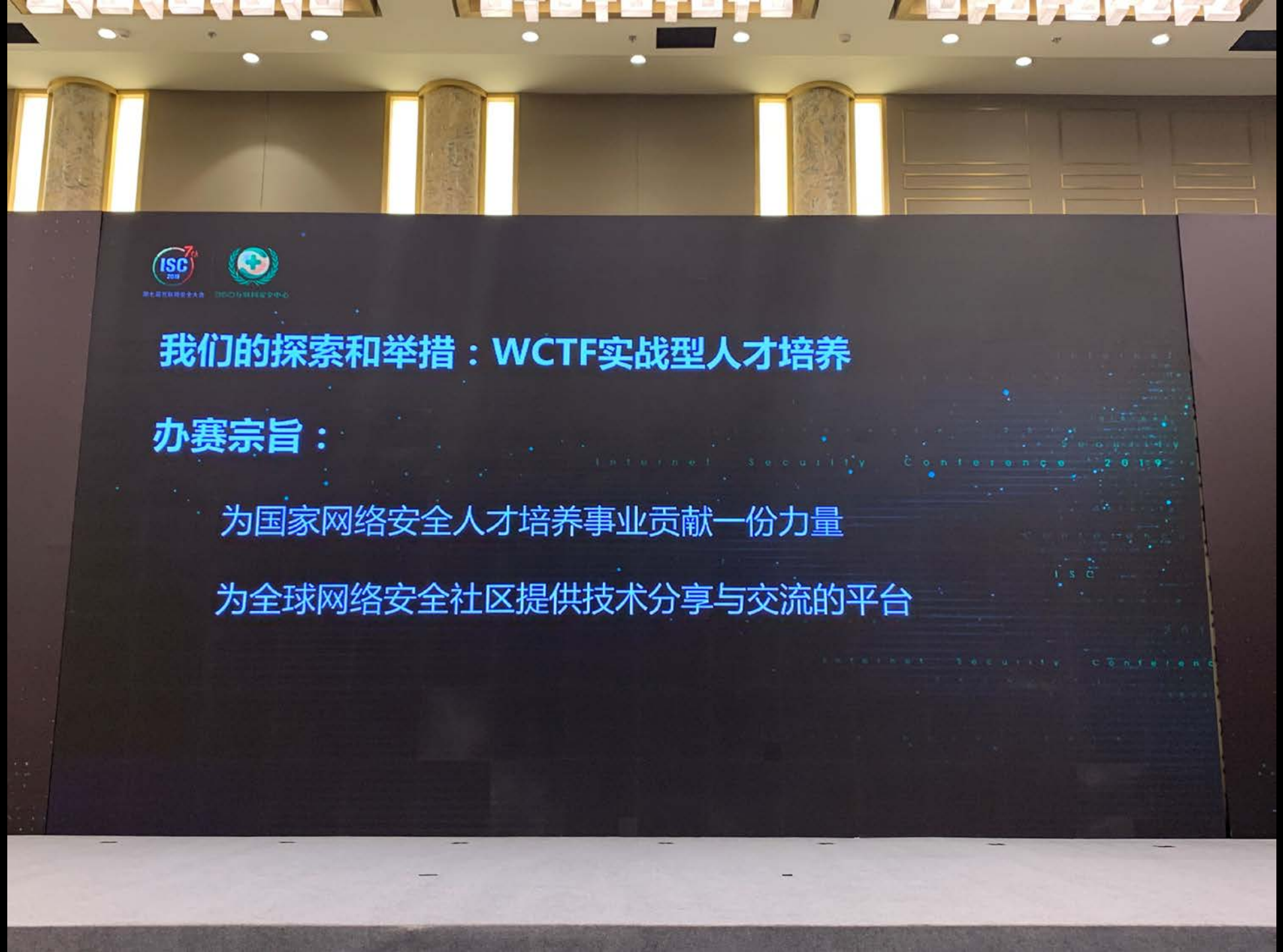

大安全时代人才培养面临的挑战
大安全时代网络安全环境严峻，对抗日益激烈
各层次安全人才匮乏
产业界急需一大批能解决实际问题的实战型人才


高校的信息安全人才培养情况
培养学科基础
实践能力和实战技术缺乏
科研导向
技术对抗落后


高校的信息安全人才培养情况
培养学科基础
实践能力和实战技术缺乏
科研导向
技术对抗落后
需要补充各种实训手段

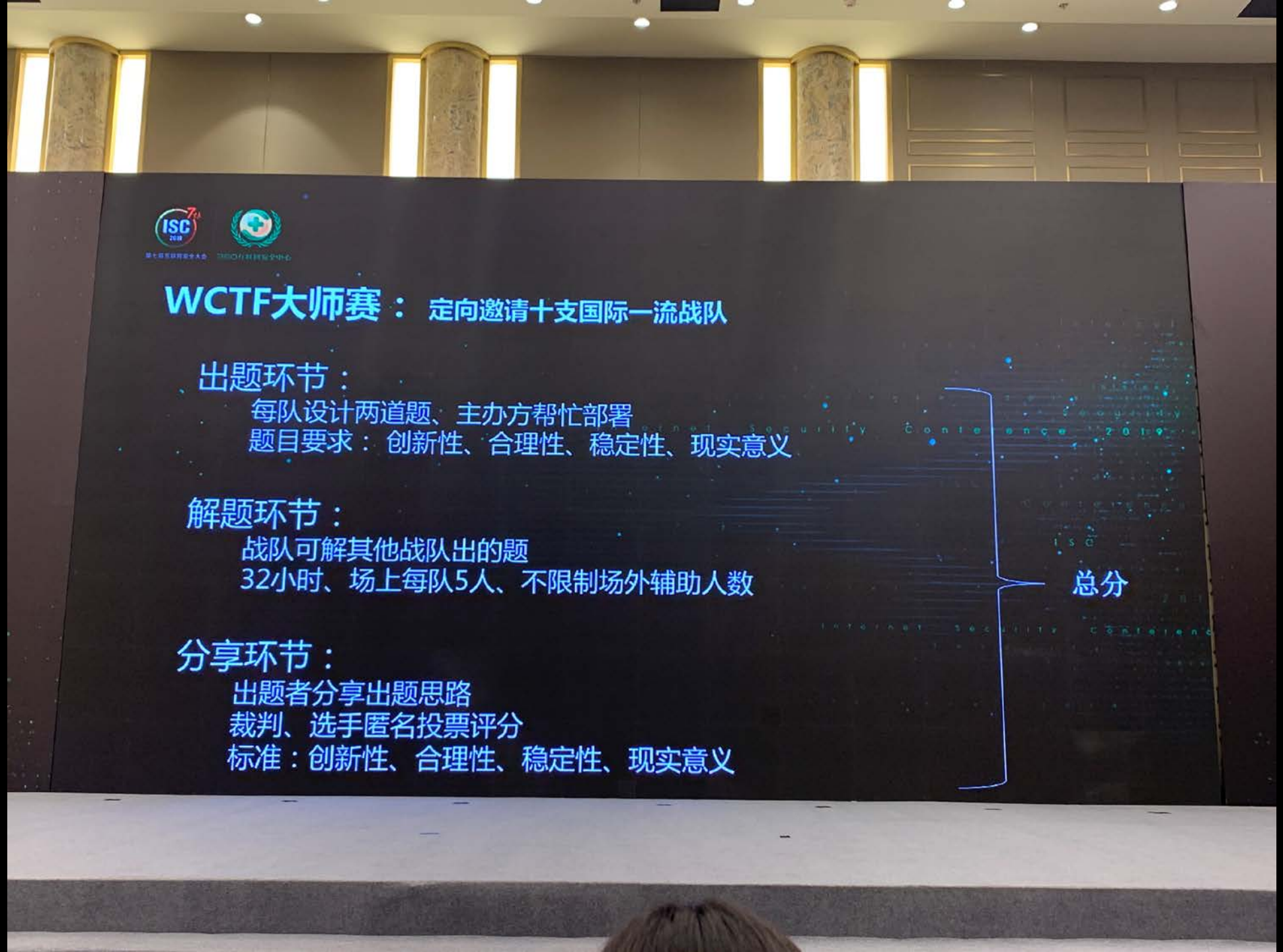

现有各类竞赛的成效与不足
成效：
赛事丰富
关注度高
参与度强
提升学生
兴趣和实
践能力
培养出了
一批优秀
人才

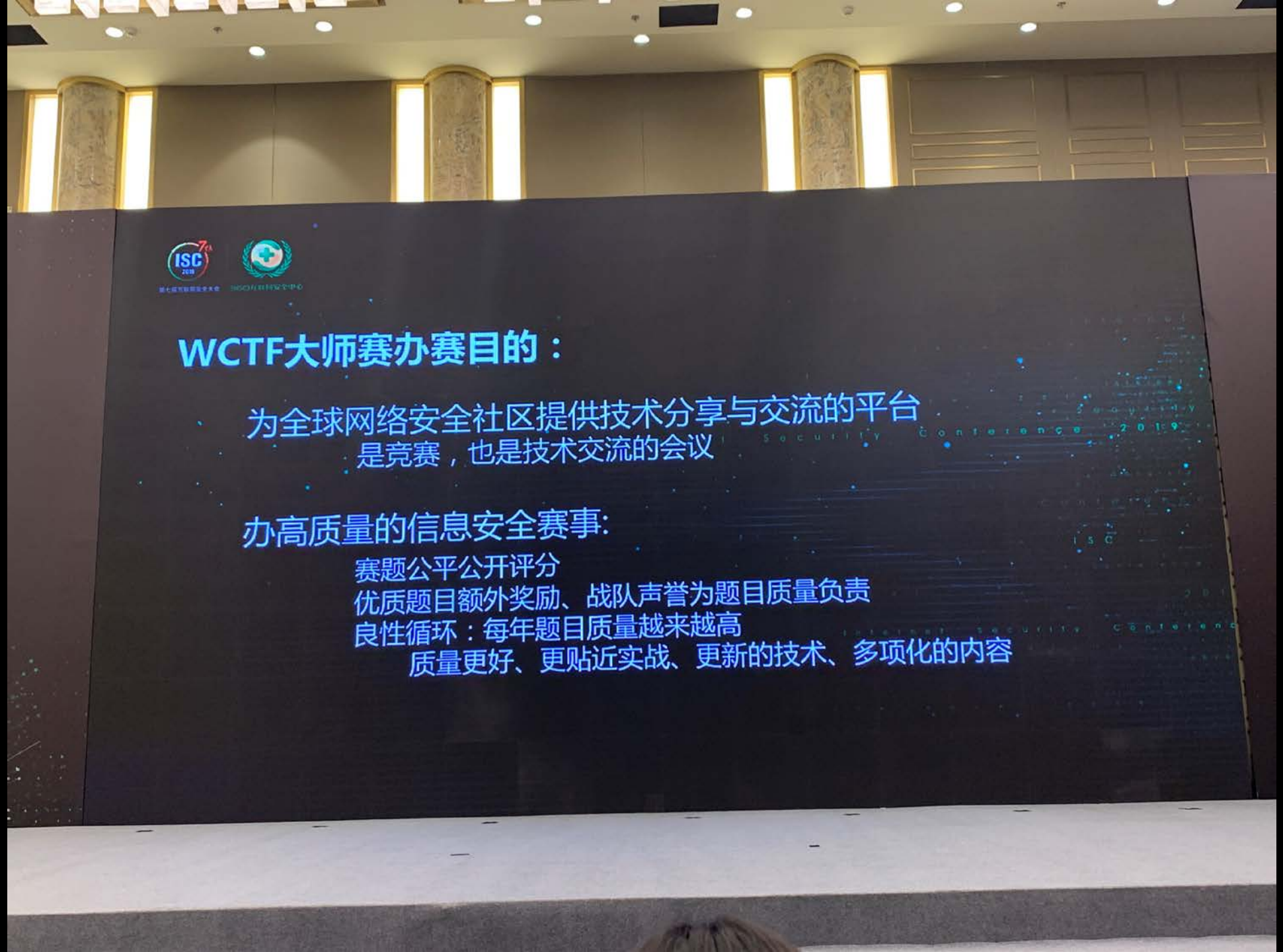

现有各类竞赛
成效：
赛事丰富
关注度高
参与度强
提升学生
兴趣和实
践能力
培养出了
一批优秀
人才
不足：
质量参差不齐
内容同质化严
重
与工业界实际
需求存在差距
时效性落后
缺乏技术的分
享和交流
选手易遇到瓶
颈


我们的探索和举措：WCTF实战型人才培养
办赛宗旨：
为国家网络安全人才培养事业贡献一份力量
为全球网络安全社区提供技术分享与交流的平台

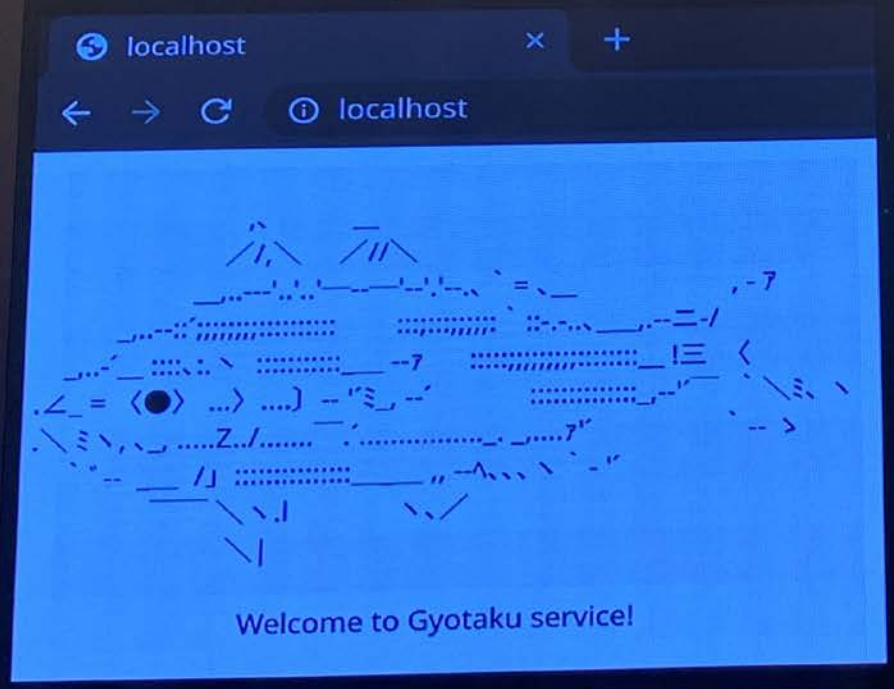

WCTF赛制介绍：
大师赛: 面向国际一流战队
新锐赛: 面向国内高校战队
线上赛: 面向全球安全社区


WCTF大师赛： 定向邀请十支国际一流战队
出题环节：
每队设计两道题、主办方帮忙部署
题目要求： 创新性、合理性、稳定性、现实意义
解题环节：
战队可解其他战队出的题
32小时、场上每队5人、不限制场外辅助人数
分享环节：
出题者分享出题思路
裁判、选手匿名投票评分
标准：创新性、合理性、稳定性、现实意义


WCTF大师赛： 定向邀请十支国际一流战队
出题环节：
每队设计两道题、主办方帮忙部署
题目要求： 创新性、合理性、稳定性、现实意义
解题环节：
战队可解其他战队出的题
32小时、场上每队5人、不限制场外辅助人数
分享环节：
出题者分享出题思路
裁判、选手匿名投票评分
标准：创新性、合理性、稳定性、现实意义
总分

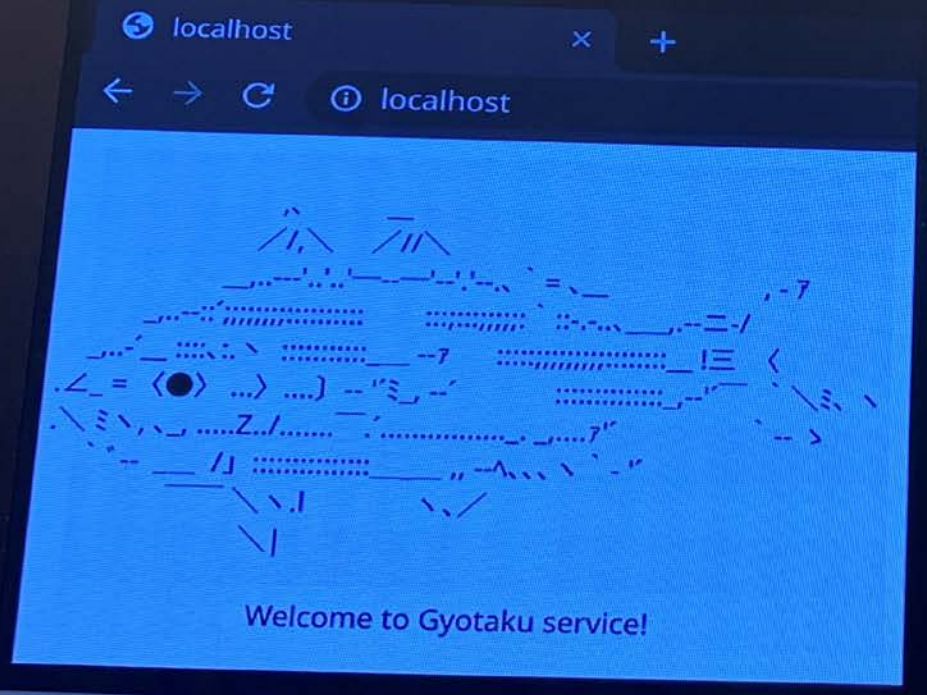

WCTF大师赛办赛目的：
为全球网络安全社区提供技术分享与交流的平台
是竞赛，也是技术交流的会议
办高质量的信息安全赛事:
赛题公平公开评分
优质题目额外奖励、战队声誉为题目质量负责
良性循环：每年题目质量越来越高
质量更好、更贴近实战、更新的技术、多项化的内容

精彩赛题回顾： Gyotaku The Flag（TokyoWesterns）



鱼拓服务： 存储用户提交的数据
没有漏洞，如何窃取数据？

精彩赛题回顾： Gyotaku The Flag（TokyoWesterns）



鱼拓服务： 存储用户提交的数据

- There is no XSS
- There is no SQL
- There is no command execution
- There is no SSRF
- There is no buffer overflow
- There is no LFI
- There is no HTML
- There is no ... implementation

没有漏洞，如何窃取数据？

精彩赛题回顾： Gyotaku The Flag（TokyoWesterns）

没有漏洞，如何窃取数据？

全新的Windows侧信道攻击手段:
- 内容审计器可能导致信息泄露
- 杀毒软件 Windows Defender

杀毒软件会删除病毒文件：

s=f(secret,user_input)

-> 被删除 -> s=病毒

-> 未删除 -> s≠病毒

精彩赛题回顾： Gyotaku The Flag (TokyoWesterns)

2019 Pwnies Award 提名：

AV + Javascript engine + EICAR

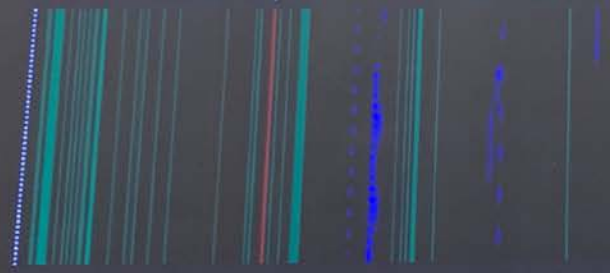
Credit: @icchy

"No implementation, no bugs?" PROVEN FALSE.

At a Chinese CTF, Japanese hacker @icchy briefly presented a cool technique for using Windows Defender (or any other AV) as an oracle, based on Microsoft's (hilarious) inclusion of a working Javascript engine and using the EICAR string as a trigger. He literally owned a CTF flag that had no implementation.


精彩赛题回顾： TPM2137 (Dragon Sector)
RadomSemi™
Engineering Your Budget
TPM2137
Secure Passkey Verification
OVERVIEW
Offering the best balance of cyber and price, the TPM2137 offers a simple yet secure solution for password and secret checking in your application.
RadomSemi™ offers full customizability on the password that the device verifies, as long as the password is exactly 8 characters.
FEATURES
Industry standard UART idle-high receive-only interface at 115200 baud.
Single 12MHz clock source.
Simple 'ok'/'wrong' LED output pins, active low.
Based on Truly Unhackable™ FPGA Technology.
Refer to the TPM2137 Secure Passkey
FPGA bitstream
可信赖平台模块(TPM)
不可破解？
FPGA真的安全吗？

精彩赛题回顾： TPM2137 (Dragon Sector)



硬件逆向和开源EDA工具的例子

硬件实现并不一定安全

FPGA比特流可以被导出，硬件可以被逆向

呼吁安全社区更多关注硬件安全

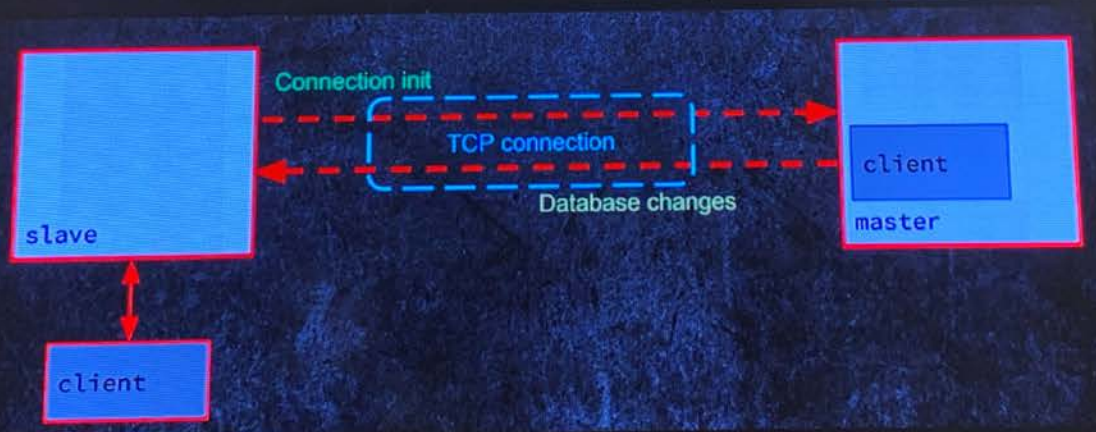

精彩赛题回顾： TPM2137 (Dragon Sector)
Videos
Gynvael's HACKING LIVESTREAM
2:27:41
Hacking Livestream #85: Solving TPM2137 from Master WCTF
GynvaelEN
YouTube - Jul 24, 2019
Gynvael's HACKING LIVESTREAM
2:16:31
Hacking Livestream #86: Solving TPM2137 from Master WCTF
GynvaelEN
YouTube - 7 days ago
Gynvael's HACKING LIVESTREAM
Hacking Livestream #86: Solving TPM2137 from Master WCTF
GynvaelEN
YouTube - 7 days ago

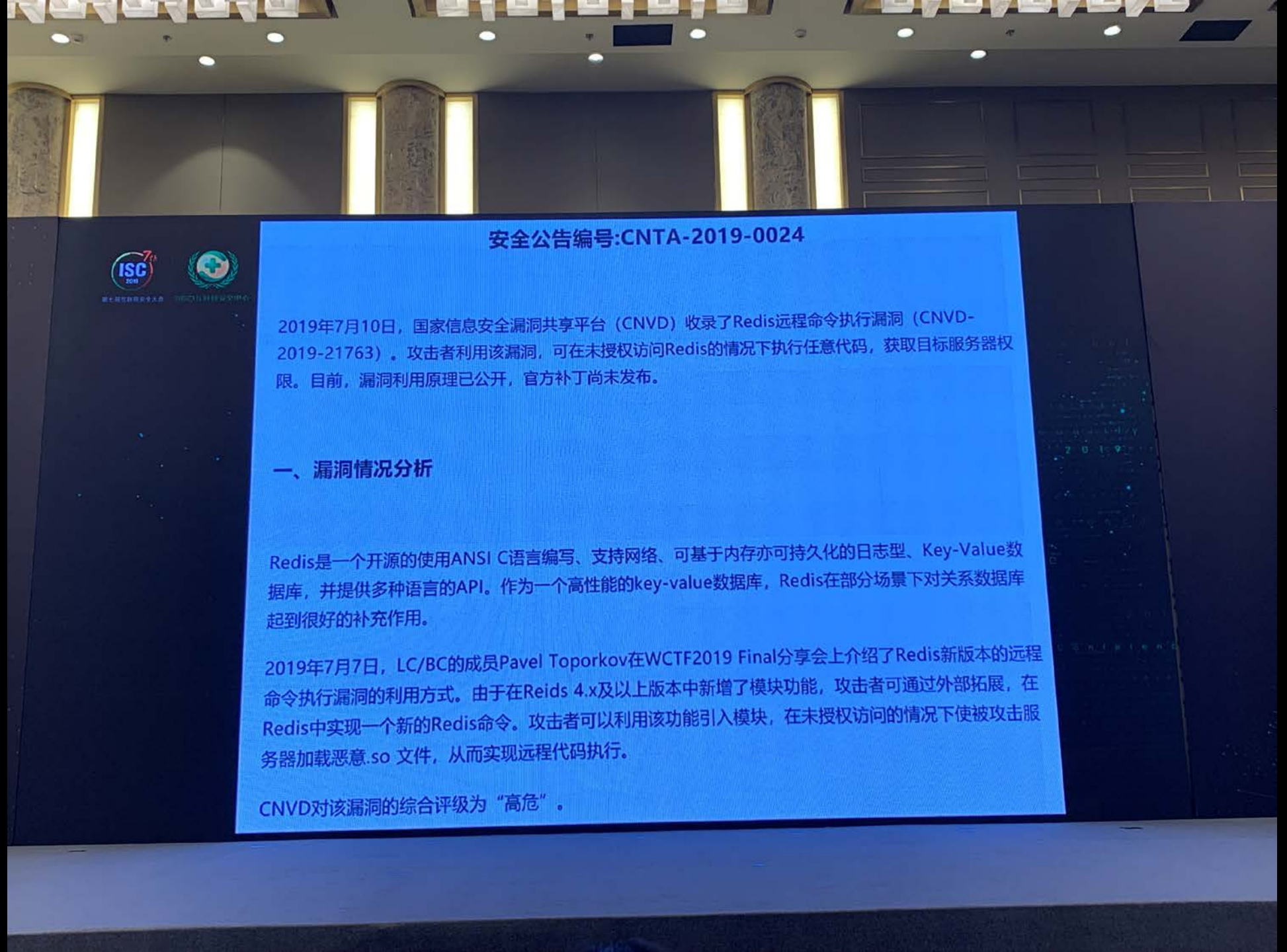
精彩赛题回顾： P door (LCBC)

Php反序列化+Redis远程代码执行新技术

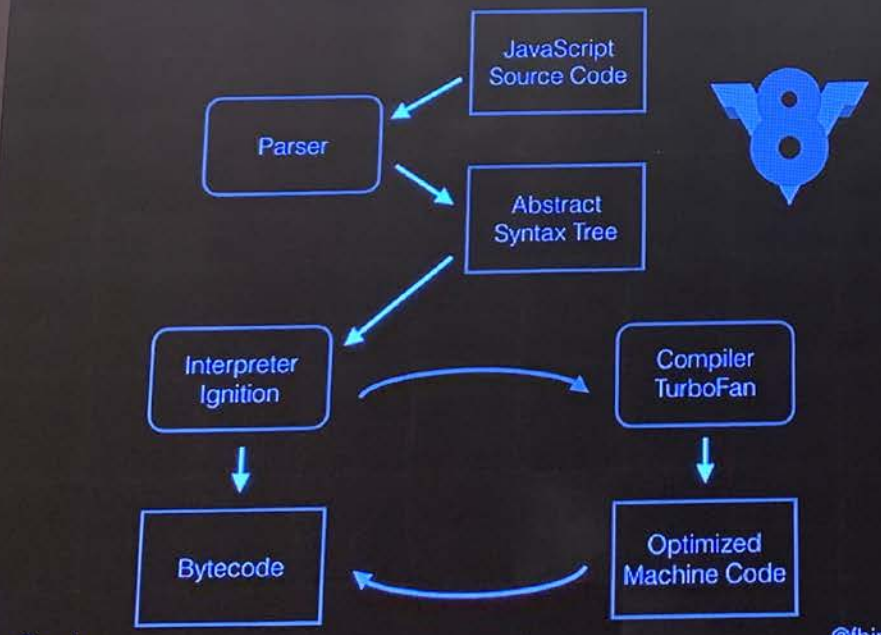
Php反序列化精妙构造

Redis主从备份实现远程代码执行




安全公告编号:CNTA-2019-0024
2019年7月10日，国家信息安全漏洞共享平台（CNVD）收录了Redis远程命令执行漏洞（CNVD-2019-21763）。攻击者利用该漏洞，可在未授权访问Redis的情况下执行任意代码，获取目标服务器权限。目前，漏洞利用原理已公开，官方补丁尚未发布。
一、漏洞情况分析
Redis是一个开源的使用ANSI C语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value数据库，并提供多种语言的API。作为一个高性能的key-value数据库，Redis在部分场景下对关系数据库起到很好的补充作用。
2019年7月7日，LC/BC的成员Pavel Toporkov在WCTF2019 Final分享会上介绍了Redis新版本的远程命令执行漏洞的利用方式。由于在Reids 4.x及以上版本中新增了模块功能，攻击者可通过外部拓展，在Redis中实现一个新的Redis命令。攻击者可以利用该功能引入模块，在未授权访问的情况下使被攻击服务器加载恶意.so 文件，从而实现远程代码执行。
CNVD对该漏洞的综合评级为“高危”。

精彩赛题回顾： Browser Training (ESPR)



浏览器漏洞入门:
Chrome v8引擎

当前热门漏洞研究方向
编译优化

Google

@fhinkel

精彩赛题回顾： Browser Training (ESPR)

```
void DependentCode::InstallDependency(Isolate* isolate,
                                      const MaybeObjectHandle& code,
                                      Handle<HeapObject> object,
                                      DependencyGroup group) {

#if 0
  Handle<DependentCode> old_deps(DependentCode::GetDependentCode(object),
                                 isolate);
  Handle<DependentCode> new_deps =
      InsertWeakCode(isolate, old_deps, group, code);
  // Update the list head if necessary.
  if (!new_deps.is_identical_to(old_deps))
    DependentCode::SetDependentCode(object, new_deps);
#endif
}
```

```
arr = [1.1, 1.2, 1.3]; arr.x = 2;
function foo(idx) {
  arr[idx] = 8.691694759794e-311;
}
foo(0);
%OptimizeFunctionOnNextCall(foo);
arr[0x100000] = 1.23; // 改变元素类型
foo(0x080000); //越界写
```

编译依赖移除、多样化漏洞利用技术


精彩赛题回顾： Browser Training (ESPR)
ZERCON
Ignition Bytecode
Ignition is a register machine.
安全会议上进行了类似议题分享
赛题形式展现，赛后再讲解
另一种形式的技术分享

最佳赛题： 6502 (Shellphish)

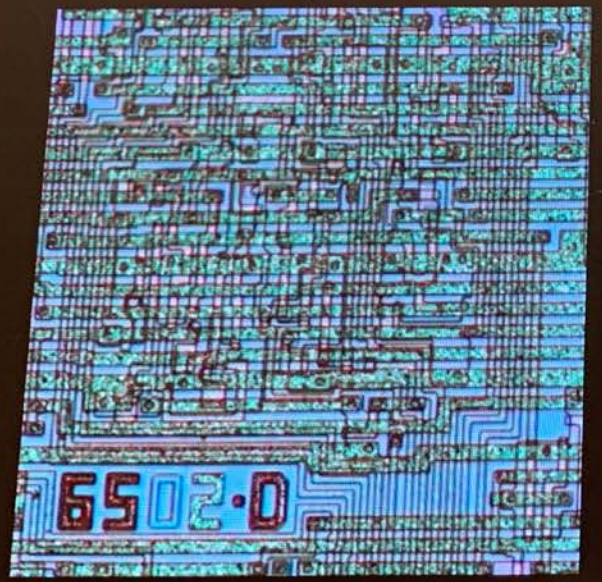
还记得他们吗？

最佳赛题： 6502 (Shellphish)

还记得他们吗？

文曲星、AppleII电脑、任天堂红白机

最佳赛题： 6502 (Shellphish)



6502CPU

软件模拟CPU：极客情怀

漏洞与算法： 精密结合

专注、深入探索


最佳赛题： 6502 (Shellphish)
BEST CHALLENGE
Challenge: 6502
349.46
Shellphish
BEST CHALLENGE
$ 5000
BEST CHALLENGE
Challenge: 6502
349.46
Shellphish


WCTF2019大师赛排名：
NO1 中国台湾217战队
2016WCTF的冠军队伍，来自中国台湾的217今年再下一城，经过三天的激烈比拼，成功破解10道题目，斩获2135分拿下2019WCTF冠军王者宝座，并获得50000美元奖励！
NO2 波兰Dragon Sector战队
来自谷歌安全中心的波兰Dragon Sector战队在本届WCTF中拿下3个首杀，共解出8道题目，以1923分的优秀战绩获得2019WCTF亚军及30000美金奖励！
NO3 中国r3kapig战队
来自中国的r3kapig战队共夺得7面战旗，经过分享问答PK环节，最终斩获1671个积分成为2019WCTF季军，并获得20000美元奖励！


WCTF新锐赛： 邀请十支国内高校战队
赛前培训：
走进校园，技术分享
解题环节：
同场竞技：大师赛赛题
定向提高：360的赛题
赛后分享：
大师赛分享会
360安全团队分享会
晋级：
新锐赛冠军获邀参与来年大师赛


WCTF新锐赛特点：
为国家网络人才培养事业贡献一份力量
特点：
提供与国际战队同场竞技、交流的舞台：认识不足，学习优点
高质量、多样化的赛题，帮助新人进一步提高能力，突破瓶颈
与360安全团队交流：了解和走进工业界


WCTF2019分享照片：
走进北航
时间：2019.5.18 13:30
地点：北京航空航天大学主M 201教室
主要内容
走进成信大
时间：2019.5.23 13:30
主要内容
走进西电
时间：2019.6.4 14:30
主要内容

WCTF2019新锐赛排名：


WCTF2019新锐赛排名：
The First Bonus 120 + 30
The Second Bonus 120 + 20
The Third Bonus 120 + 10
Solved 120
Additional Challenge 100 + 30/20/10
Challenge Maker
Update: 2019-07-05 18:02:56
Ranking Teams Score
1 NESE 960
2 SixStar 610
3 bluevehale 600
4 Tianshu 480
5 KapOk 470
6 lancet 460
7 Syclover 370
8 L-team 350
9 vidar 340
10 RedBud 280
+30
+10
+10
+30
+20
+20
+30
+30


WCTF线上赛： 面向全球安全社区
大师赛题目+360制定题目
开放、共享
对新手友好
促进信息安全技术的普及推广


WCTF线上赛： 面向全球安全社区
大师赛题目+360制定题目
开放、共享
对新手友好
促进信息安全技术的普及推广


WCTF2019线上赛排名：
Scoreboard
Place Team CTF points
1 Whitzard 850.000
2 Plaid Parliament of Pwning 650.000
3 $wag 640.000
4 C4T BuT S4D 640.000
5 OpenToAll 630.000
6 Venom 610.000
7 Balsn 600.000
8 mhackeroni 510.000
9 Azure Assassin Alliance 480.000
10 BurpFiction 480.000


WCTF培养实战型人才培养
质量参差不齐
内容同质化严重
与工业界实际需求存在差距
时效性落后
缺乏技术的分享和交流
选手易遇到瓶颈
高质量赛题
多样化内容
贴近工业界需求
高时效性
重分享与交流
帮助选手突破瓶颈


未来展望：
与时俱进、不断改进
开放合作

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票