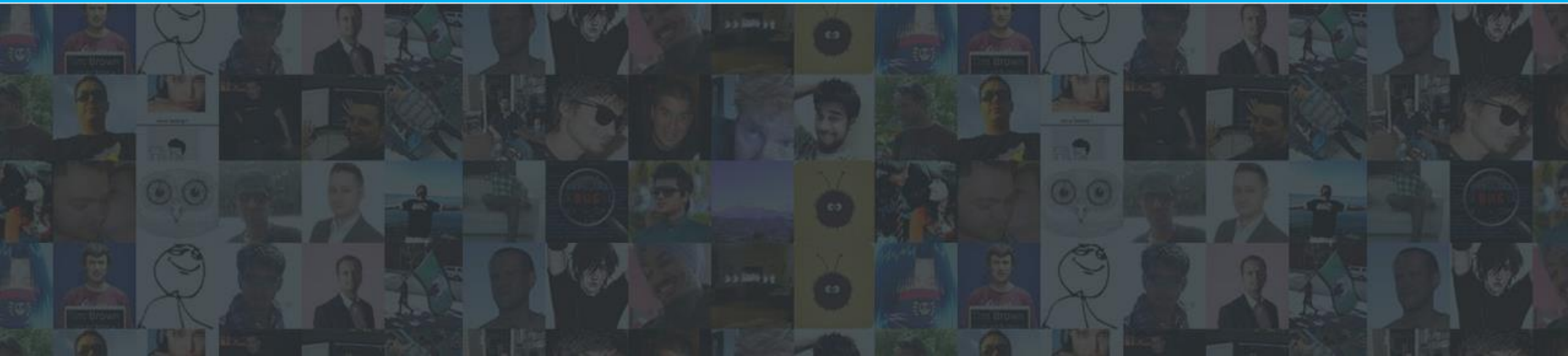
History of bounty programs

袁劲松



关于我

2010年 携程旅行网

关注应用安全、安全架构、应急响应、安全管理等

Freebuf.com

赏金漏洞历史 – 有趣的开始

赏金漏洞历史 – 有趣的开始

- 1995年 - Netscape（网景）推出第一个漏洞赏金计划
  - 1995年10月10日 一个有纪念意义的日子
  - 网景浏览器2.0beta版本安全问题
  - 50名白帽子
  - 奖品：Netscape杯子和T恤

pay-for-bugs → bounty

赏金漏洞历史 – 有趣的开始

2002年 - IDefense公司推出赏金漏洞中间人计划

- 2002年8月，安全分析监测公司iDefense推出漏洞贡献者（VCP）计划
- 赏金范围

Number of Contributions	Value per undisclosed vulnerability	Value per new exploit for previously disclosed vulnerability	Value per undisclosed vulnerability AND accompanying exploit
EVALUATION PHASE			
1-3	up to $75 US	up to $100 US	up to $200 US
REGULAR CONTRIBUTOR			
>4	up to $175 US	up to $200 US	up to $400 US

- 奖金：漏洞类型、细节、严重级别、受影响的用户数
- 2007年 首次悬赏IE7和VISTA

赏金漏洞历史 – 有趣的开始

2004年 - Mozilla Firefox浏览器推出赏金漏洞计划

- 2004年8月2日， Mozilla基金会推出赏金漏洞计划

Mozilla Security Bugs Bounty Program Launched

Monday August 2nd, 2004

The Mozilla Foundation has announced a Security Bug Bounty Program. Under the new scheme, any user who reports a critical security vulnerability in end-user Mozilla software will receive a US$500 reward. The program is being funded by Linux distributor Linspire (formerly Lindows.com) and Internet entrepreneur and space tourist Mark Shuttleworth. The Mozilla Security Bug Bounty page has more details, including the process for reporting vulnerabilities and under what circumstances a report is eligible (unfortunately for sloppy developers, you cannot claim a bounty for a bug in your own code!). Netscape has run a bug bounty program in the past, though this latest Mozilla initiative is unrelated.

In addition, the Mozilla Foundation has updated the Mozilla Security Center with tips for safe browsing and information about how Mozilla keeps you secure.

Update: The article has been rewritten to include additional information. Thanks to

- 500美元

赏金漏洞历史 – 有趣的开始

2005年 - Zero Day Initiative浮出水面

- 2005年7月23日，TippingPoint推出ZDI中间人赏金计划

- 2010年被3COM公司收购

赏金漏洞历史 – 有趣的开始

2007年 - Pwn2Own

- 2007年的CanSecWest安全会议，Dragos Ruiu发起Pwn2Own大赛
- Mac OSX漏洞
- 笔记本电脑 →10000美刀
- 2014年，85W美刀

赏金漏洞历史 – 有趣的开始

2009年 – no more free bugs

- 2009年的CanSecWest安全会议，Charlie Miller喊出口号：

赏金漏洞历史 – 有趣的开始

2010年 - Google推出针对Web应用的赏金计划

- 2010年，Chromium开源项目安全测试
- 随后推出针对网站安全性测试

*.google.com
*.youtube.com
*.blogger.com
*.orkut.com

赏金漏洞历史 – 有趣的开始

2010年 - Mozilla升级了他们的赏金计划

- 范围扩展至Web应用层面

bugzilla.mozilla.org
*.services.mozilla.com
getpersonas.com
aus*.mozilla.org
www.mozilla.com/org

www.firefox.com
www.getfirefox.com
addons.mozilla.org
services.addons.mozilla.org
versioncheck.addons.mozilla.org
pfs.mozilla.org
download.mozilla.org

- Baracuda和Deutsche Post

赏金漏洞历史 – 有趣的开始

2011年 - Facebook 白帽子计划

- 2011年8月上线，最低将支付500美元

  负责任的漏洞披露流程、可能对facebook用户造成影响的漏洞，如XSS、CSRF、远程代码执行等。

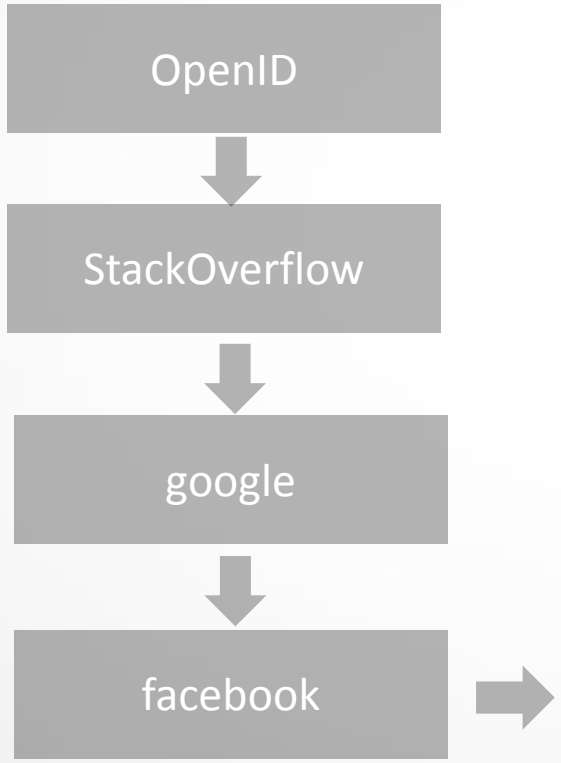
  拒绝接受朝鲜、利比亚、古巴等地提交的漏洞

- 600+白帽子
- 截止目前，共发放200万美刀奖励

facebook

赏金漏洞历史 – 有趣的开始

- Web赏金漏洞史上最高 – 单个漏洞3.5W美刀




```
__html : "\
There was an error while processing the OpenID response. \
No matching endpoint found after discovering http:\/\/www.ubercomp.com\/...(redacted)... \
<br \/><br \/> OP Endpoint mismatch. Expected http:\/\/www.ubercomp.com\/...(redacted)..., \
got http:\/\/www.ubercomp.com\/...(REDACTED).../?x=\
root:x:0:0:root:\/root:\/bin\/bash\n \
bin:x:1:1:bin:\/bin:\/sbin\/nologin\n \
daemon:x:2:2:daemon:\/sbin:\/sbin\/nologin\n \
adm:x:3:4:adm:\/var\/adm:\/sbin\/nologin\n \
lp:x:4:7:lp:\/var\/spool\/lpd:\/sbin\/nologin\n \
sync:x:5:0:sync:\/sbin:\/bin\/sync\n \
shutdown:x:6:0:shutdown:\/sbin:\/sbin\/shutdown\n \
halt:x:7:0:halt:\/sbin:\/sbin\/halt\n \
mail:x:8:12:mail:\/var\/spool\/mail:\/sbin\/nologin\n \
uucp:x:10:14:uucp:\/var\/spool\/uucp:\/sbin\/nologin\n \
operator:x:11:0:operator:\/root:\/sbin\/nologin\n \
games:x:12:100:games:\/usr\/games:\/sbin\/nologin\n \
gopher:x:13:30:gopher:\/var\/gopher:\/sbin\/nologin\n \
ftp:x:14:50:FTP User:\/var\/ftp:\/sbin\/nologin\n \
nobody:x:99:99:Nobody:\/:\/sbin\/nologin\n \
dbus:x:81:81:System message bus:\/:\/sbin\/nologin\n \
...(REDACTED)..."
        },
        "payload": null,
        "bootloadable": {},
        "ixData": []
    }, 1)
});
```

赏金漏洞历史 – 有趣的开始

2012年 – 腾讯TSRC上线

- 2012年6月上线
- 300+白帽子，5000+漏洞
- 截止目前，共发放超过250WRMB

赏金漏洞历史 – 有趣的开始

2013年 - 互联网漏洞奖金

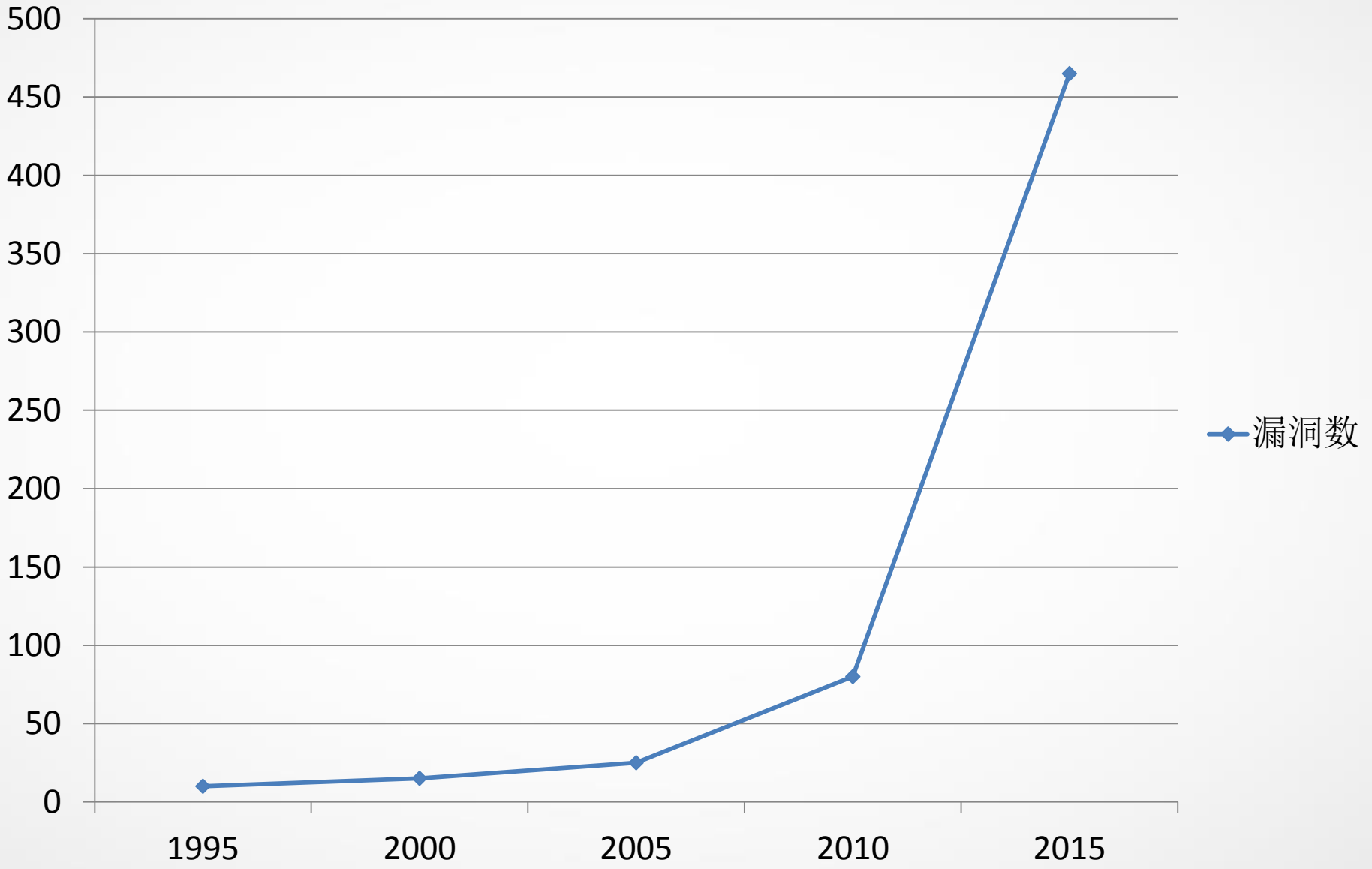
- 2013年，微软和Facebook联合发起互联网漏洞奖金

赏金漏洞历史 – 有趣的开始

2014年 - *SRC如雨后春笋

- 2014年 各互联网公司纷纷建立自己的安全应急响应中心

赏金漏洞历史 – 趋势


500
450
400
350
300
250
200
150
100
50
0
1995
2000
2005
2010
2015
漏洞数

赏金漏洞类型

赏金漏洞厂商

- 安全应急响应中心
- 第三方漏洞平台

ZDI、 iDefense VCP 、bugcrowd、hackerone、乌云、sobug、漏洞盒子

赏金漏洞类型

奖励计划

- 奖金
- 礼品
- 名声和积分

参与赏金漏洞白帽子类型

白帽子类型

- 公司从业人员
- 自由职业者
- 安全爱好者

why

- 奖金、礼品
- 名声
- 工作机会
- 挑战/娱乐

“

With many eyes all bugs are shallow !

- Linus’ Law

Heartbleed

“

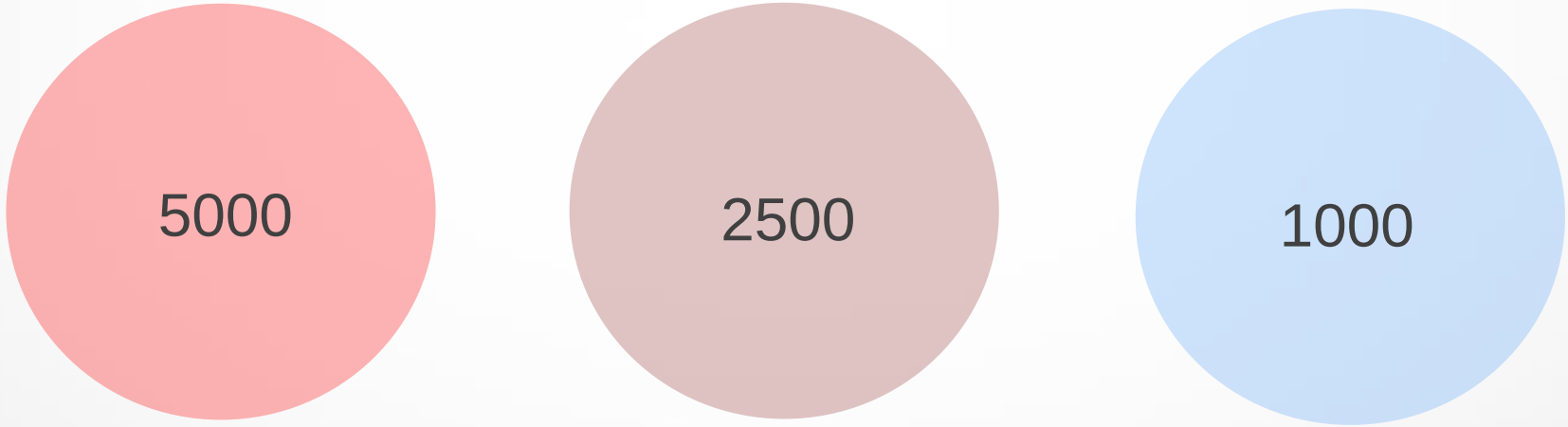
With many eyes **and the right incentive**
all bugs are shallow

- Linus’ Amended Law

赏金漏洞案例

某开源商城系统安全测试

- 赏金池 10W，1个月时间



赏金漏洞案例

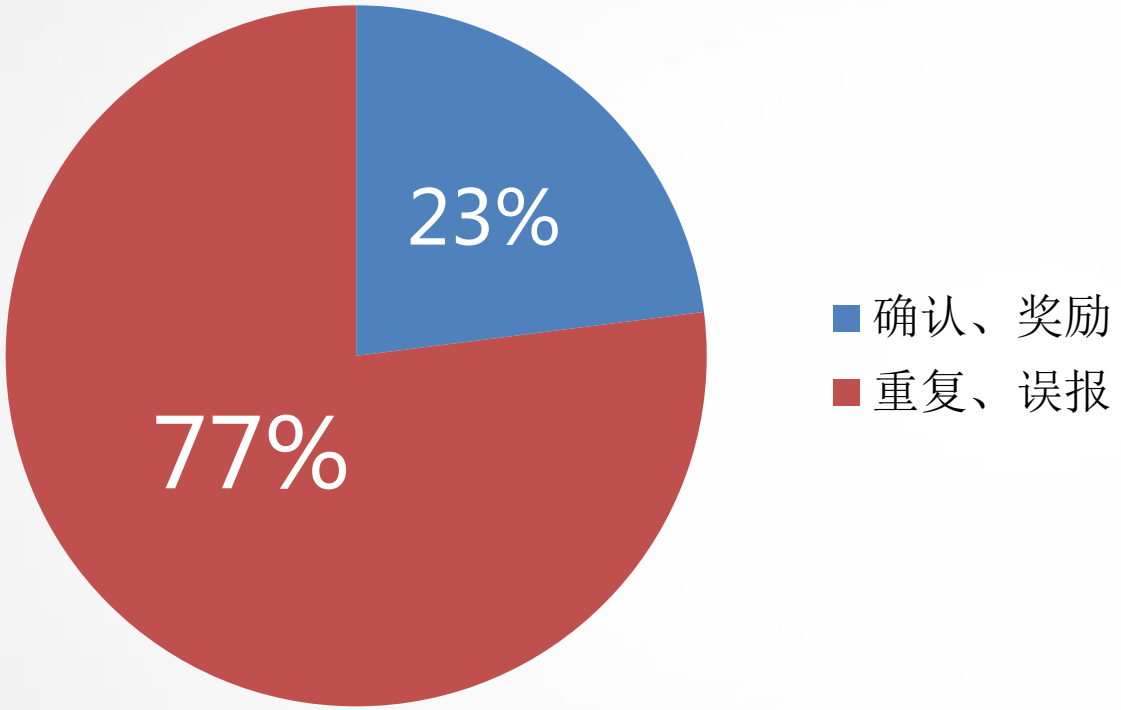
- **311**名白帽子参与了安全测试
- 提交**41**个漏洞
- **3**个严重高危漏洞

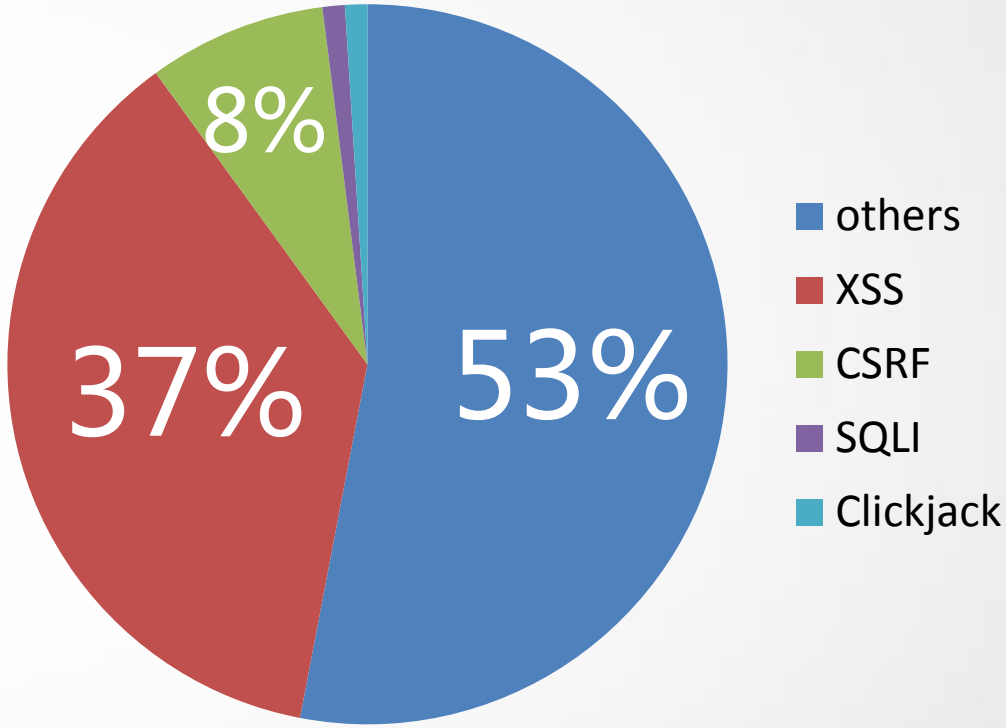
赏金漏洞案例

- 该商城系统自2006年 – 2014年，网络公布的漏洞数为：

27个

赏金漏洞案例





传统测试与赏金漏洞对比

传统测试 VS 赏金漏洞

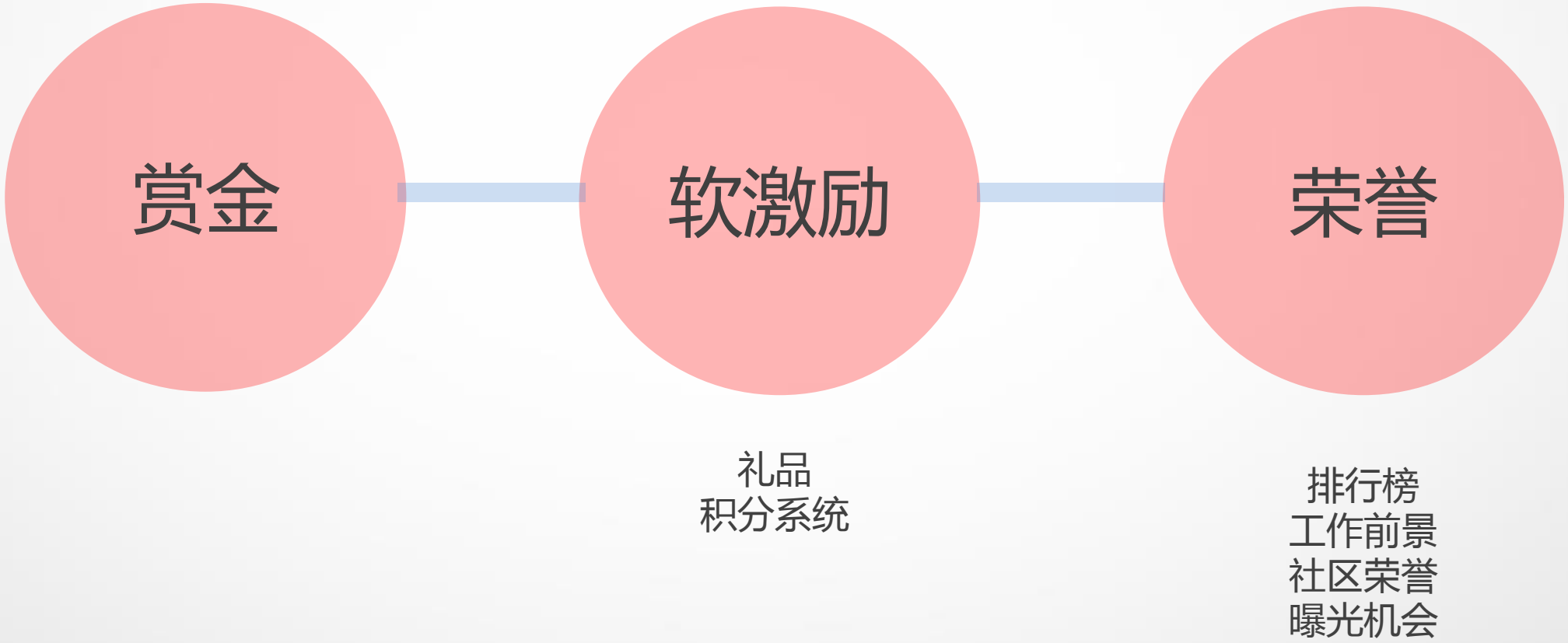
传统测试与赏金漏洞对比

	传统		赏金
覆盖面	少数测试人员		覆盖面广
资源	至项目结束	VS 渗透测试	长期
质量	漏洞成本高		不同技能、成本可控

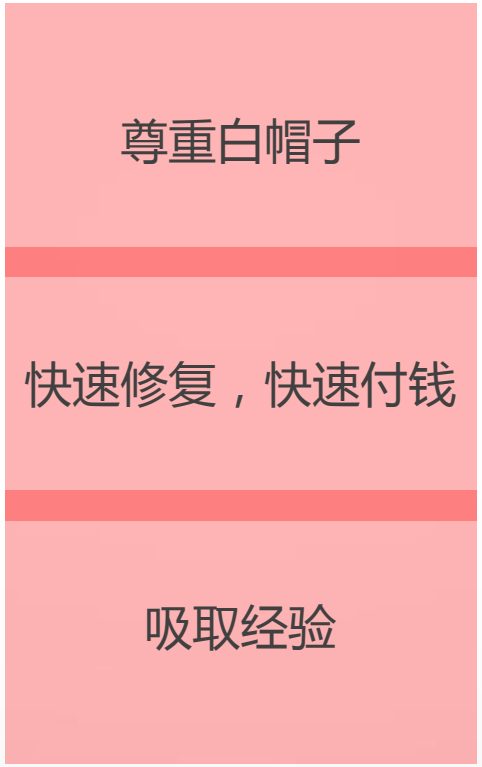
赏金漏洞的意义

- 发现未知漏洞
- 漏洞披露流程可控
- 降低成本
- 吸纳人才

如何让更多的人参与安全测试？



如何让更多的人参与安全测试？



漏洞盒子

"连接世界各地的安全研究者与白帽子"

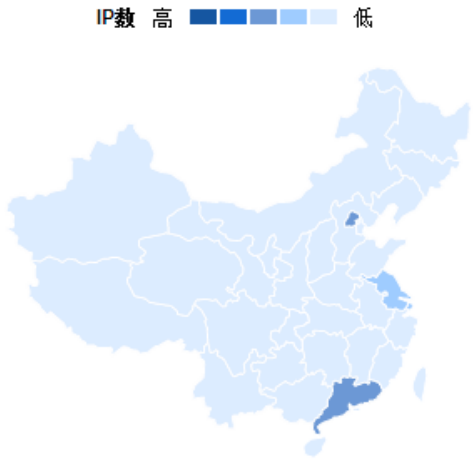
简单高效的漏洞处理平台，帮助你发现产品中潜在的安全风险

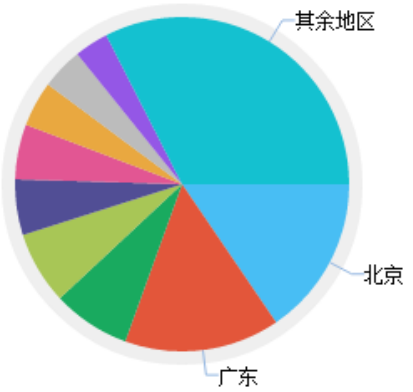
参加项目　　发起项目

漏洞盒子

漏洞盒子

- 上线一月，超过 **4000+** 全球各地白帽子
- 企业网站、内部应用、代码、移动APP程序安全测试
- 提供整套解决方案
- 完善的漏洞生命周期管理

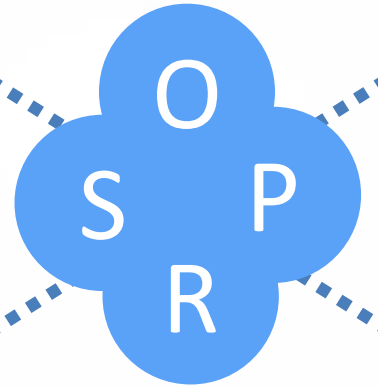




漏洞盒子-如何保障企业漏洞风险可控

对象风险控制

实名制白帽身份，确保项目参与过程不失控，无泄漏，无转手；
校验企业用户资质，确保不泄漏白帽信息，不直接与白帽接触；
签署保密合同，确保合法备案，保障双方权益；



交易风险控制

禁止安全专家与客户直接发生奖金交易，避免交易法律风险；
审核机制，确保竞争机制；

过程风险控制

对于高机密要求，由平台或客户提供堡垒机、厂商提供VPN、网络镜像测试流量，确保全程审计白帽测试行为

结果风险控制

安全专家非经客户和平台允许，对外透露测试过程和结果的任何细节。将取消其白帽资格；
客户与白帽协商定位风险级别，输出有证据，无争议的报告；

Thank You