360

www.360.cn

STARTING FROM PANGOLIN

Zwell

- Pangolin
- JSky
- www.iiScan.com -> webscan.360.cn
- NOSEC.lTD. Founder
- 360 Web security Department Supervisor

- Pangolin Details
- Web security situation in China
- Web security testing
- Demo

What is Pangolin?

- SQL injection pen-test tool
- 100,000 users
- Fast
- Easy to use

- Charset
- Database support
- Auto-keyword
- Union-based
- Error-based
- GET/POST/Co
- File operation
- Cmd operation
- Fast Dump

- Google hacking
- Privilege Escalation
- emote data
- WAF
- Customizable headers
- Authentication
- MD5 crack

So many…

```
//right1和right2取交集R0
r0 = LCS(std::wstring(right1), std::wstring(right2));
//right1和wrong1取right1特有部分R1
r1 = LeftPart(std::wstring(right1), std::wstring(wrong1));
//right2和wrong2取right2特有部分R2
r2 = LeftPart(std::wstring(right2), std::wstring(wrong2));
//R0和R1交集R3
r3 = LCS(r0, r1);
//R2和R3交集就是关键字结果
r4 = LCS(r2, r3);
```

LeftPart: SES DIFF

- Char translate
- HPP
- GET with POST parameters

Bypass WAF ：Char translate

- Space to TAB
- Space to /**/ or %09 or +
- select to sElEcT
- select to se%lec%t
- ‘string’ to 0xAAAAAA
- String to %AA%AA%AA

- http://www.blackhat.com/docs/webcast/bh webcast28-balduzzi.pdf
- http://www.google.com/search?q=italy&q= china

Bypass WAF ：GET with POST parameters

- http://www.80sec.com/?p=244

```
< %
Response.Write “Request:” & Request(“t”)
% >
```

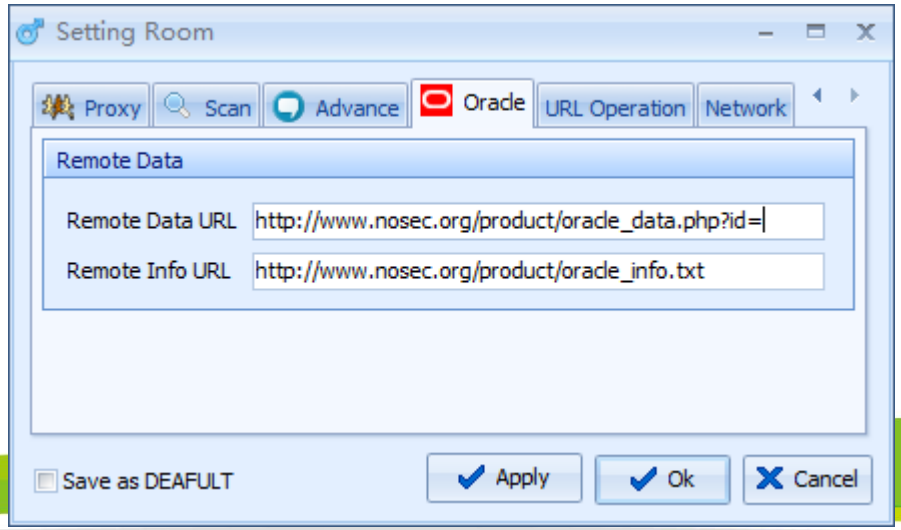
```
GET /1.asp HTTP/1.1
Host: 192.168.239.129
Content-Length: 34
Content-Type: application/x-www-form-urlencoded

t=’/**/or/**/1=1–
```

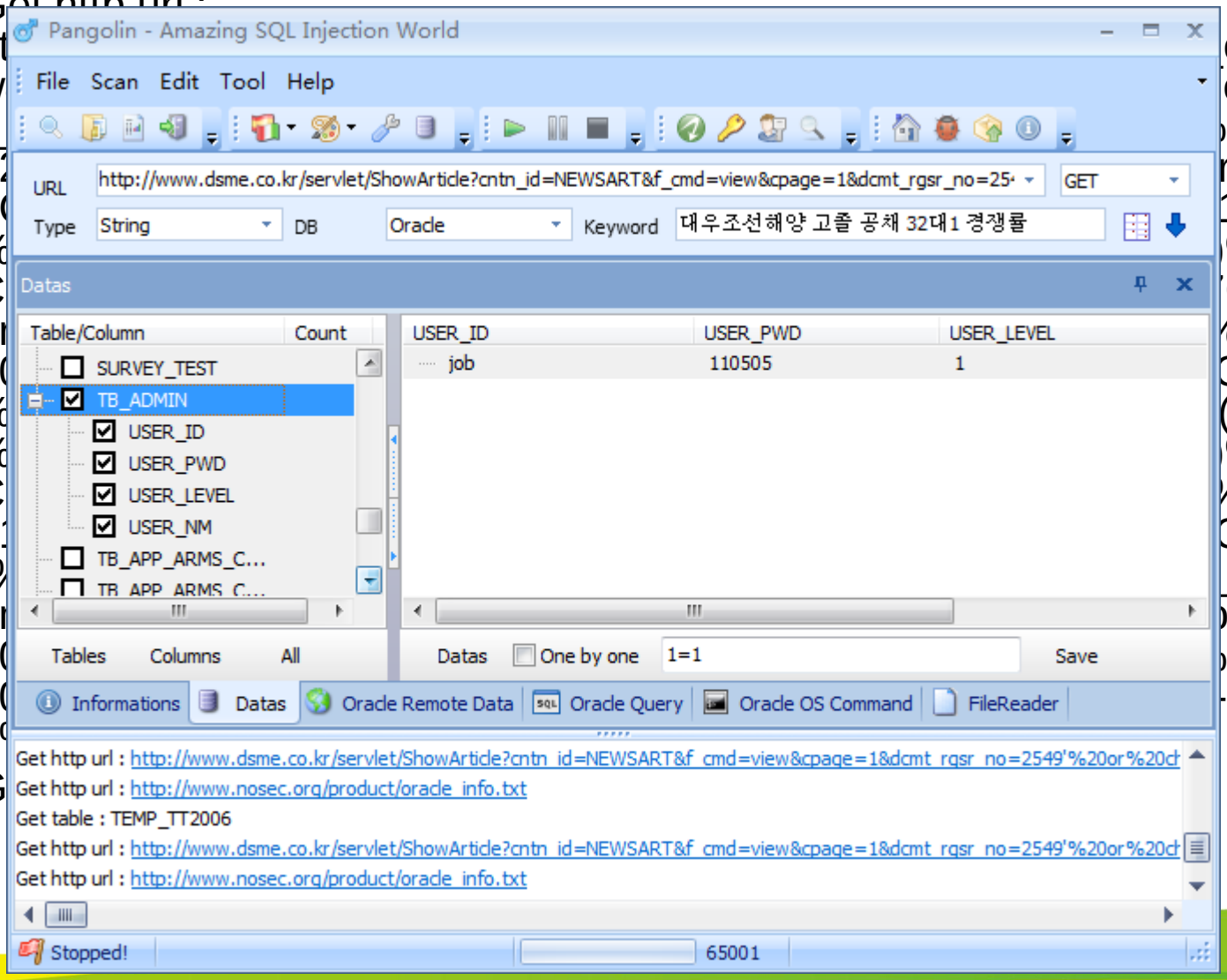
```
Request:’/**/or/**/1=1–
```

- PHP filter code: preg_match('/(and|or|union|where|limit|group by|select)/i', $id)
- Filtered injection: 1 || (select substr(gruop_concat(user_id),1,1) user from users) = 1
- Bypassed injection: 1 || 1 = 1 into outfile 'result.txt' Bypassed injection: 1 || substr(user,1,1) = 'a'

- <?php$txt=fopen("oracle_info.txt","w");$id='0';if(isset($_REQUEST['id'])){$id=$_REQUEST['id'];}fwrite($txt,$id);fclose($txt);?>
- 给出流程图



- Got http url :



- G

- Mysql injection with error
- Mysql injection with bit shifting
- And so much more……
- We need you to join us……

- Pangolin Details
- Web security situation in China
- Web security testing
- Demo

- Wooyun.org
- 80sec.com
- 80vul.com

What web site feel?

- Trojan horse
- Tamper
- Black link
- Backdoor
- DDoS
- Phishing

- Tamper
  - Sexing and Gambling
  - SEO
  - Show off
  - Reactionary
  - Trojan horse
- Search Engir

zlhl 黑链同盟
www.zlhl.org
中国最大的黑链交易平台

黑链同盟 | 黑链文章 | 网站seo技术 | 黑链代码

套餐	PR1	PR2	PR3	PR4	PR5	PR6	原价	特惠价
A	3	3	4	3	-	-	36元	20元
B	-	-	8	5	-	-	49元	35元
C	-	-	6	5	2	-	63元	45元
D	-	-	5	4	2	2	85元	65元
E	-	-	-	8	5	-	90元	70元
F	-	-	-	6	5	2	110元	90元
G	-	-	-	-	10	3	145元	110元
H	客户自己制定各PR网站数量						另议	

链接单价:PR1=1元/月 PR2=2元/月 PR3=3元/月 PR4=5元/月 PR5=10元/月 PR6=15元/月 PR7=30元/月

黑链SEO网
www.heilianseo.com 真正最好的黑链

黑链首页 | 黑链代码 | 黑链SEO

多重黑链组合套餐供站长选择:

方案组	PR值	网站数量	服务价格/时间	质量	购买
混一色	PR3+PR4	各5个共10个	35元/一个月 季付80元	稳如泰山	购买
清一色	PR3	10个	25元/一个月 季付60元	稳如泰山	购买
绿一色	PR4	10个	45元/一个月 季付108元	稳如泰山	购买
双龙会	PR5+PR6	各5个	80元/一个月 季付190元	稳如泰山	购买
小三元	PR3+PR4+PR5	各5个共15个	65元/一个月 季付155元	稳如泰山	购买
大三元	PR4+PR5+PR6	各5个共15个	100元/一个月 季付240元	稳如泰山	购买
大四喜	PR3+PR4+PR5+PR6	各5个共20个	110元/一个月 季付260元	稳如泰山	购买
大吊车	PR7	1个	25元/一个月 季付60元	稳如泰山	购买
包月套餐 每天为您的站点增加外链，PR3-PR6 持续一个月 意向者请联系客服 QQ:694907742					

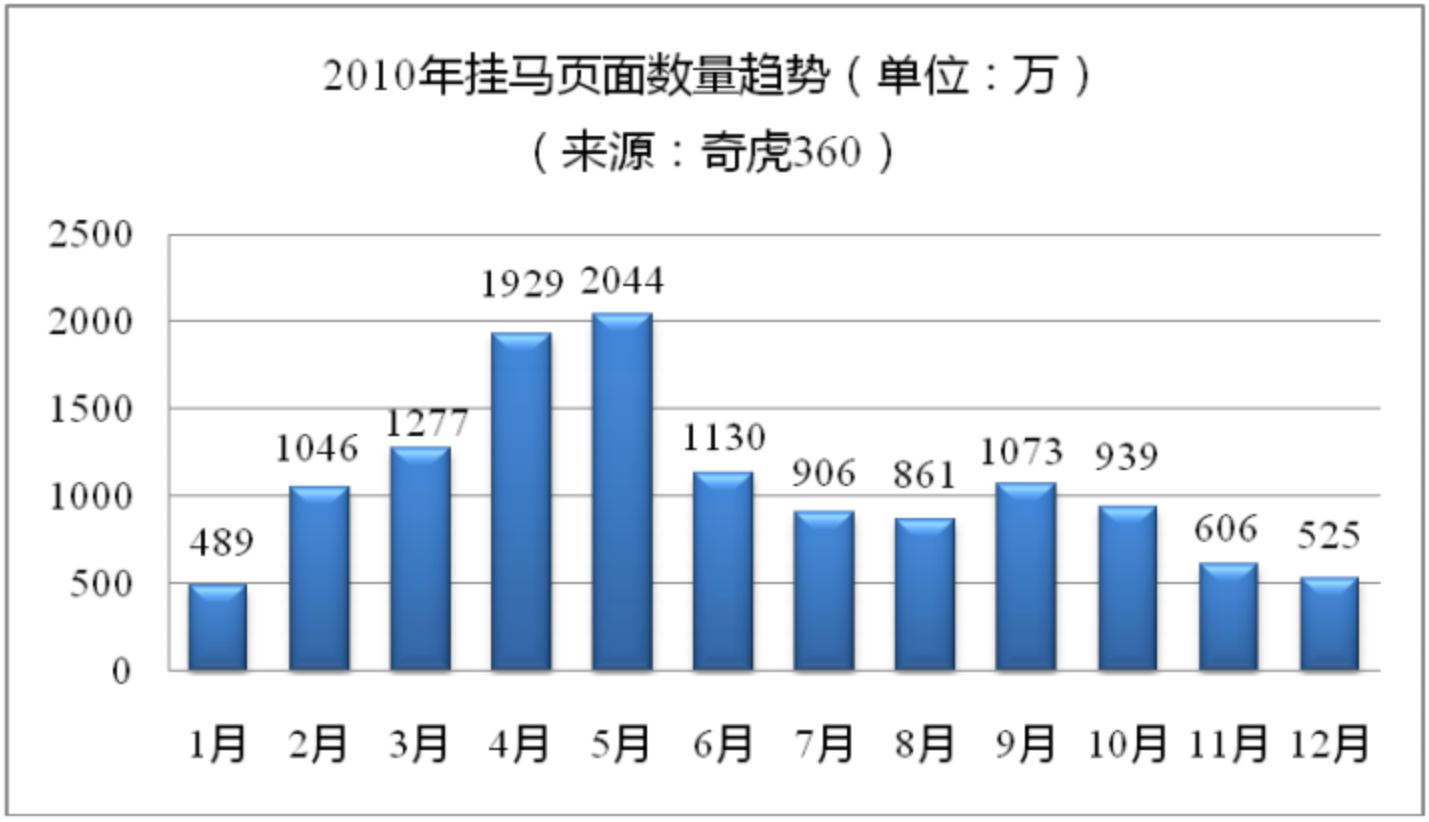
我们支持淘宝交易，并加入消费者保障服务计划，让您无忧购买，让我们过硬的高质量黑链赢得您的信任

淘宝旺旺: 和我联系 淘宝店铺: 淘宝网 卖家信用： 服务承诺：

想SEO?就 我爱黑链网
www.52taok.com
诚信交易·一诺千金 丢一
倾力打造专业黑链平台 销售 供链 售后 三部门各

首页 | 黑链SEO | 黑链 黑链出售交易中心,黑链购买首选--我爱黑链

基础套餐					
方案组	PR值	网站数量	服务价格/时间	质量	购买
招牌A套餐	PR5-PR6	PR6=5个 PR5=6个 11个站	70元/月 200元/季度	稳定	购买
实惠B套餐	PR5-PR7	PR7=1个 PR6=5个 PR5=9个 15个站	100元/月 280元/季度	稳定	购买
超值C套餐	PR5-PR7	PR7=2个 PR6=4个 PR5=11个 17个站	120元/月 330元/季度	稳定	购买
D套餐	PR6-PR7	PR6=7个 PR7=3个 10个站	120元/月 330元/季度	稳定	购买
E套餐	PR7	PR7 4个站	100元/月 280元/季度	稳定	购买
F套餐	PR3-PR6	每天固定新的10个链	800元/月 2200元/季度	稳定	购买
组合1	PR3-PR5	PR5=5个PR4=5个PR3=5个 15个站	50元/月 130元/季度	稳定	购买
组合2	PR4-PR6	PR6=3个PR5=5个PR4=7个 15个站	70元/月 200元/季度	稳定	购买
英文链	PR0-PR6	10个站	70元/月 200元/季度	稳定	购买
购买联系QQ：34574508					


2010年挂马页面数量趋势（单位：万）
（来源：奇虎360）
2500
2000
1500
1000
500
0
489
1046
1277
1929
2044
1130
906
861
1073
939
606
525
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月

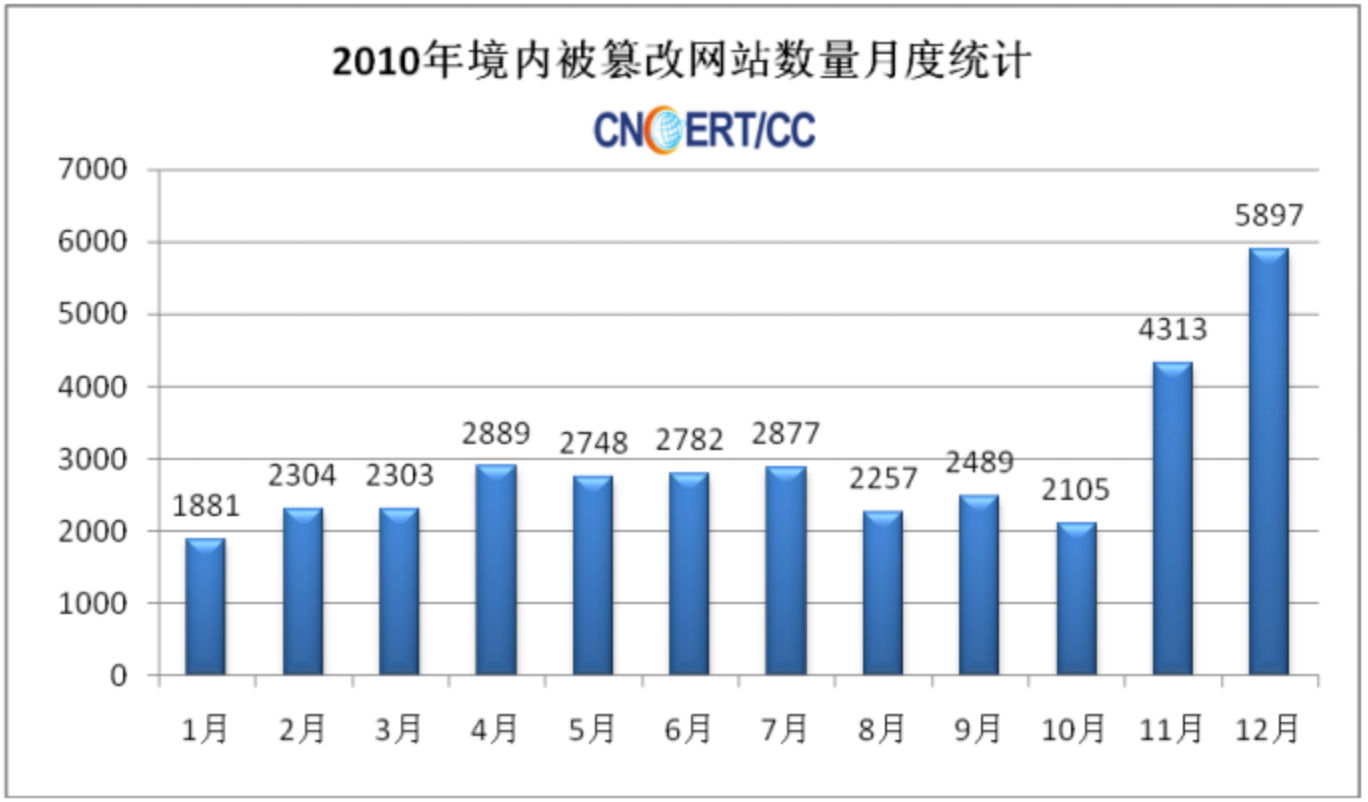


图 4-1　2010 年境内被篡改网站数量月度统计

- Pangolin Details
- Web security situation in China
- Web security testing
- Demo

- Crawler
  - Javascript
  - Flash
  - Web2.0 (AJAX, RSS…)
- Testing
  - OWASP
  - WebAppSec
- Pentesting
  - Sql Injection

- Demo


360网站安全检测
360 Web security platform
首页 特色功能 常见问题 谁在使用 企业安全 360首页>>
zwell@nosec.org| 退出
解决：漏洞 + 挂马 + 篡改
轻松解决网站安全问题 免费 专业
免 费
输入网址，快速检测(网站漏洞、挂马、篡改)：
demo.nosec.org
立即扫描
体验效果：demo.nosec.org
360网站安全检测 三大产品 五大服务
漏洞检测:
最全面深入
83%的网站存在SQL注入，跨站脚本等40余类漏洞。及时检测修复可有效防止挂马、数据泄露和破坏等严重问题。
挂马检查：
第一时间通知
有1.4亿网页被挂马，且被各类搜索引擎、安全软件拦截。利用360网站安全检测，3亿用户时刻为您监控，第一时间通知网页挂马。
篡改检测：
最高效及时
2010年起有5.6万中国网站被篡改，加入反动、黄色、黑客信息或植入后门、黑链。360网页安全检测7x24帮您监控网页篡改情况。
我们为您提供：
实时监控
解决方案
专业报告
7x24服务支持
免费
联系我们
关注我们：新浪微博
276288123
2567356988
websecurity360@hotmail.com
talk 360websecurity@gmail.com
相关报道
DedeCMS高危漏洞威胁40万家网站 360率先提供专业检测服务
360网站安全平台正式上线


360可信认证
360 Site Certification
首页
申请认证
认证查询
常见问题
联系我们
360首页>>
360可信认证
确保身份可信、网站可信、安全运营
360可信认证查询:
立即查询
加入360可信认证
"360可信认证"中心通过对企业进行全方位资质审核认证，解决用户对网站的信任问题，提高企业的互联网品牌形象。通过"360可信认证"的企业网站，可以在页面展示"360可信认证"安全标示，即展现了企业实力，又解决用户信任问题，并且可以获得360网站安全检测服务，让您的网站安全得到保障。
1. 申请认证
2. 身份审核
3. 安全检测
4. 收录到认证中心
选择"360可信认证"的四大理由
解决网站难辨真伪问题：
辨别钓鱼假冒网站，保护企业网站权益。
解决用户的信任问题：
360可信认证，让用户放心访问。
增加360网站安全检测服务：
360权威安全检测，解决网站安全问题。
360全方位资质认证：
展现企业综合情况，提高企业品牌效益。
常见问题解答：
"360可信认证"是做什么的?
申请"360可信认证"需要哪些材料?
什么是"360可信认证"标识?
用户如何查询网站的可信认证?
最近认证通过的网站：
www.99bill.com
www.suning.cn
www.ccb.com
查看加入"360可信认证"流程
飞信：124149843
QQ：2319981748
Copyright©2005-2011 360.CN All Rights Reserved 360安全中心

- Pangolin Details
- Web security situation in China
- Web security testing
- Demo

- Dedecms 0day
- Zuitu 0day

Q&A

Thanks!

北京市朝阳区建国路71号惠通时代广场D座1号楼 100025
Block 1, Area D, Huitong Times Plaza No.71 JianGuo Road, ChaoYang District Beijing 100025, P.R.C.
Tel: +86 10 5878 1000 **Fax:** +86 10 5878 1001