Asset Enumeration: Expanding a Target's Attack Surface

backcover7 / 2019-09-10 08:52:45 / 浏览数 2329 渗透测试 渗透测试 顶(0) 踩(0)

本文是一篇翻译文章，原链接为：https://captmeelo.com/bugbounty/2019/09/02/asset-enumeration.html

介绍

当我对一个很大范围的资产做漏洞赏金活动时（例如，CIDR，子域名，一个公司的所有资产等）。我一直对搜集信息以扩大我的供给面这件事很有压力。就像是一个更大的

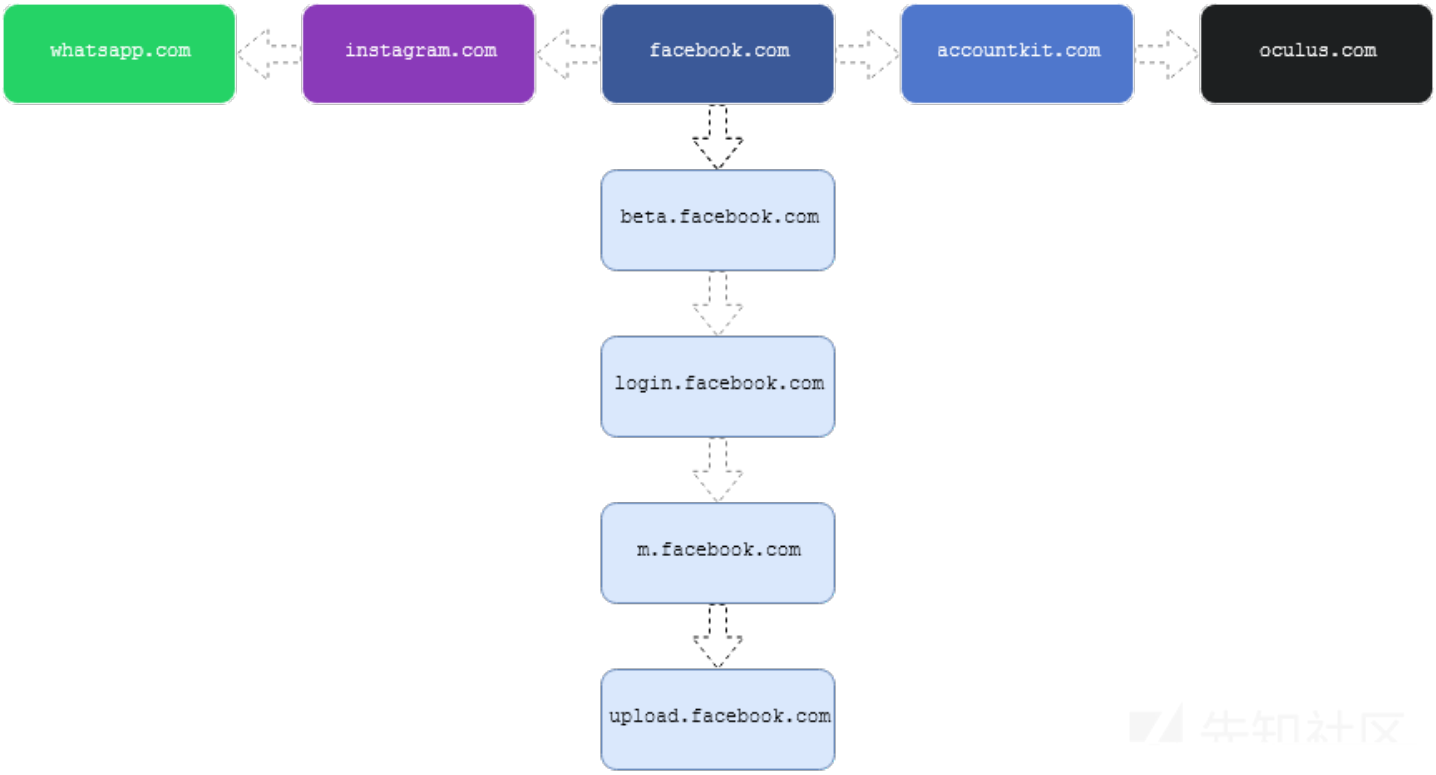
在这篇文章中，我将会描述我在测试时如何扩大目标站点或公司的攻击面。需要注意的是，这个技术仅限于罗列关于木站点的子域名和找到新域名。

资产发现

针对一个目标域，有两种方法扩展它的攻击面：

1. 找到更多和目标站点享有同个一级域名的站点，这个叫做子域名罗列。
2. 确认所有和目标站点有关系的域名。

下图可以帮助区分这两个方法：



现在我们来看一下我用来进行子域名罗列和找到有关系域名的方法。

子域名罗列

这步的关键就是找到尽可能多的目标域的子域名站点。理想的情况下，我们希望越挖越深。我的意思是指我并不想单单只罗列目标域的子域名，还要挖掘这些子域名的子域名

有很多工具可以进行子域名罗列，但是他们并不能给出一个不错的结果。个人来说，我更加喜欢使用可以综合所有罗列工具的结果的工具，并且拥有很多我需要的选项和功能

针对子域名罗列，我一直是用Amass这个工具作为起步，使用它的passive选项。

```
amass enum -passive -d <DOMAIN> -o <OUT_FILE>
```

然后是针对目标域的子域名使用暴力猜解，猜解字典为all.txt（https://github.com/OWASP/Amass/blob/master/wordlists/all.txt）和commonspeak2（https://github.com/assetnote/commonspeak2-wordlists/blob/master/subdomains/subdomains.txt）。

```
amass enum -brute -w <WORDLIST> -d <DOMAIN> -o <OUT_FILE>
```

如果你想加快工具的扫描速度，你就要使用noalts选项和norecursive选项，以及max-dns-quries选项。但是不要惊讶结果的输出，因为这样会得到很少的信息。

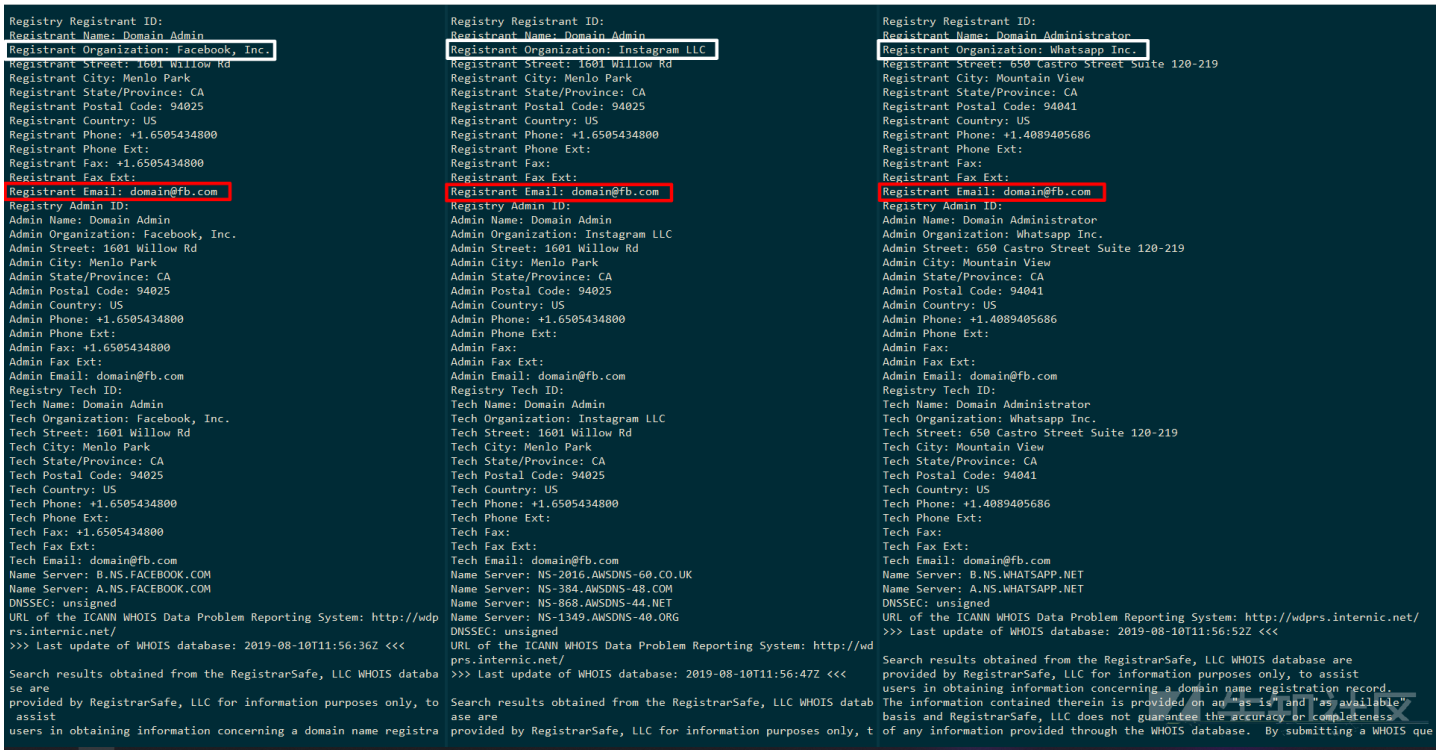
通过上面方法得到的子域名中，不是所有都可以正常解析IP地址。筛选出可以正常解析IP地址的域名，我推荐使用Massdns。

```
./bin/massdns -r lists/resolvers.txt -o S <LIST_OF_SUBDOMAINS> | grep -e ' A ' |  cut -d 'A' -f 1 | rev | cut -d "." -f1 --com
```

相关域名罗列

通过获取和融合，有时候可能不是同一家公司的域名但是他们之间有联系。例如，Facebook同时拥有Instagram和Whatsapp，也就是说instagram.com和whatsapp.com和

我们从下面的whois输出信息可以发现，facebook.com,instagram.com和whatsapp.com都由邮箱地址domain@fb.com 注册。



```
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Facebook, Inc.
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax: +1.6505434800
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Facebook, Inc.
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax: +1.6505434800
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: B.NS.FACEBOOK.COM
Name Server: A.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdp
rs.internic.net/
>>> Last update of WHOIS database: 2019-08-10T11:56:36Z <<<

Search results obtained from the RegistrarSafe, LLC WHOIS databa
se are
provided by RegistrarSafe, LLC for information purposes only, to
 assist
users in obtaining information concerning a domain name registra
```

```
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Instagram LLC
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Instagram LLC
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Instagram LLC
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: NS-2016.AWSDNS-60.CO.UK
Name Server: NS-384.AWSDNS-48.COM
Name Server: NS-868.AWSDNS-44.NET
Name Server: NS-1349.AWSDNS-40.ORG
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wd
prs.internic.net/
>>> Last update of WHOIS database: 2019-08-10T11:56:47Z <<<

Search results obtained from the RegistrarSafe, LLC WHOIS datab
ase are
provided by RegistrarSafe, LLC for information purposes only, t
```

```
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Whatsapp Inc.
Registrant Street: 650 Castro Street Suite 120-219
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94041
Registrant Country: US
Registrant Phone: +1.4089405686
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Whatsapp Inc.
Admin Street: 650 Castro Street Suite 120-219
Admin City: Mountain View
Admin State/Province: CA
Admin Postal Code: 94041
Admin Country: US
Admin Phone: +1.4089405686
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Whatsapp Inc.
Tech Street: 650 Castro Street Suite 120-219
Tech City: Mountain View
Tech State/Province: CA
Tech Postal Code: 94041
Tech Country: US
Tech Phone: +1.4089405686
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: B.NS.WHATSAPP.NET
Name Server: A.NS.WHATSAPP.NET
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-08-10T11:56:52Z <<<

Search results obtained from the RegistrarSafe, LLC WHOIS database are
provided by RegistrarSafe, LLC for information purposes only, to assist
users in obtaining information concerning a domain name registration record.
The information contained therein is provided on an "as is" and "as available"
basis and RegistrarSafe, LLC does not guarantee the accuracy or completeness
of any information provided through the WHOIS database.  By submitting a WHOIS que
```

为了搜集有关联的域名，我们可以获取whois信息中的Registrant
Email这个字段，然后做一个反向whois查询。这个操作可以在viewdns.info和whoisxmlapi.com这个两个站点上完成。

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **Reverse Whois Lookup**

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. FAQ.

Registrant Name or Email Address:

GO

Reverse Whois results for domain@fb.com
==========

There are 3,739 domains that matched this search query.
The first 500 of these are listed below:

Download The Full Report for $49

Domain Name	Creation Date	Registrar
0facebook.me	2010-04-09	REGISTRARSAFE, LLC
0fb.me	2010-04-09	REGISTRARSAFE, LLC
123riff.com	2015-03-05	MARKMONITOR INC.
123riff.net	2015-03-05	MARKMONITOR INC.
123riff.org	2015-03-05	MARKMONITOR INC.
1ccountkit.com	2016-03-18	MARKMONITOR INC.
2ccountkit.com	2016-03-18	MARKMONITOR INC.
2cthefacebook.com	2008-05-06	MARKMONITOR INC.
2minadayworkouts.com	2016-02-23	MARKMONITOR INC.
321riff.com	2015-03-05	REGISTRARSEC LLC
321riff.net	2015-03-05	MARKMONITOR INC.
321riff.org	2015-03-05	MARKMONITOR INC.
32665.mobi	2006-09-26	1API GMBH
360videofb.com	2016-02-29	REGISTRARSAFE, LLC
360videofb.net	2016-02-29	REGISTRARSAFE, LLC
360videofb.org	2016-02-29	REGISTRARSAFE, LLC
aboutfacebook.com	2009-06-26	MARKMONITOR INC.

通过Registrant Email和Registrant Organization记录进行反向查询很容易出现重复结果，所以需要多加操作进行结果去重。

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **Reverse Whois Lookup**

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. FAQ.

Registrant Name or Email Address:

GO

Reverse Whois results for Facebook, Inc.
==========

There are 2,912 domains that matched this search query.
The first 500 of these are listed below:

Download The Full Report for $49

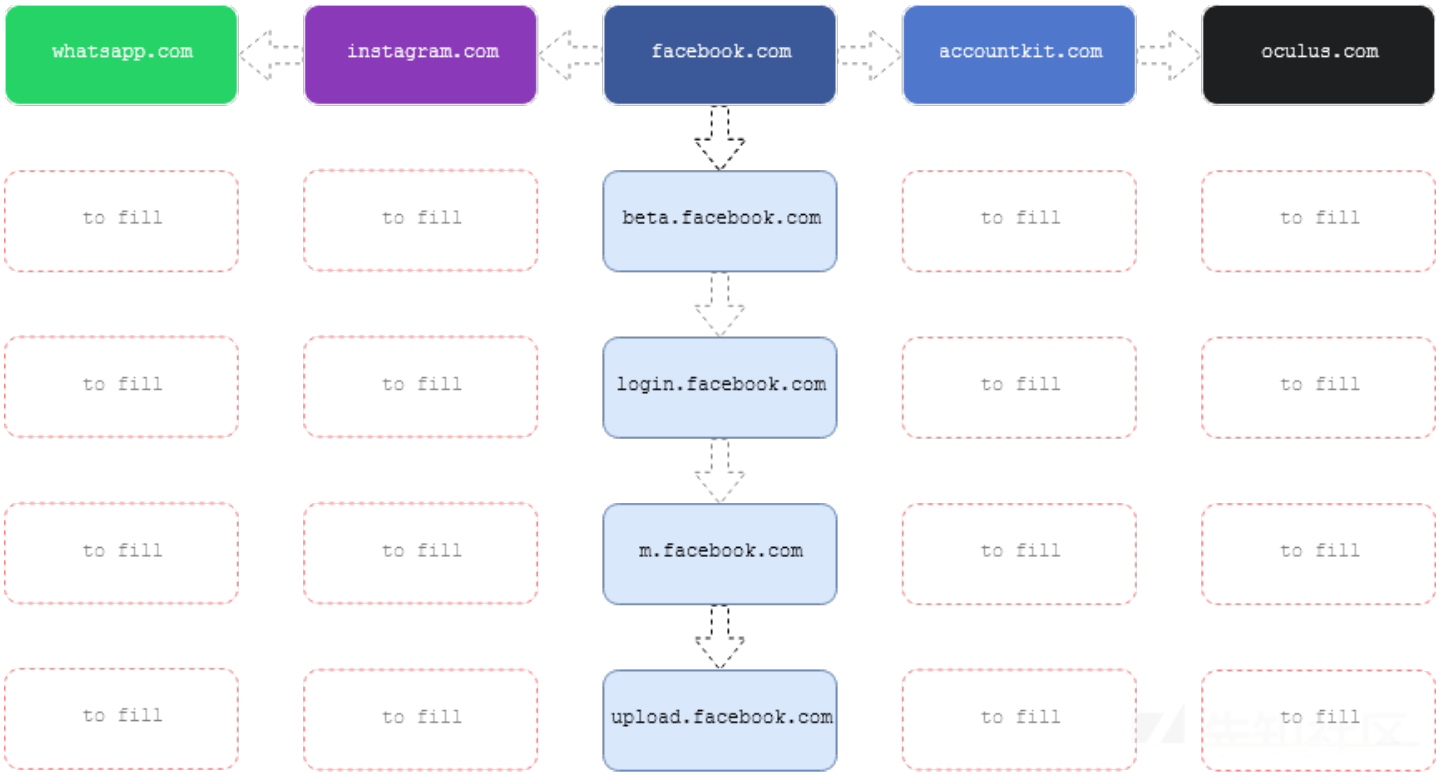
Domain Name	Creation Date	Registrar
123riff.com	2015-03-05	MARKMONITOR INC.
123riff.net	2015-03-05	MARKMONITOR INC.
123riff.org	2015-03-05	MARKMONITOR INC.
1ccountkit.com	2016-03-18	MARKMONITOR INC.
2ccountkit.com	2016-03-18	MARKMONITOR INC.
2cthefacebook.com	2008-05-06	MARKMONITOR INC.
2minadayworkouts.com	2016-02-23	MARKMONITOR INC.
321riff.net	2015-03-05	MARKMONITOR INC.
321riff.org	2015-03-05	MARKMONITOR INC.
32665.mobi	2006-09-26	1API GMBH
aboutfacebook.com	2009-06-26	MARKMONITOR INC.
abouttimetobuyfacebooklikes.top	2016-06-24	1API GMBH
abuseregistrarsafe.com	2018-05-09	REGISTRARSEC LLC
abuseregistrarsafe.org	2018-05-09	REGISTRARSEC LLC
abuseregistrarsec.com	2018-05-09	REGISTRARSEC LLC
abuseregistrarsec.org	2018-05-09	REGISTRARSEC LLC
accessfacebook.net	2007-06-12	MARKMONITOR INC.
accluntkit.com	2016-03-18	MARKMONITOR INC.
acco7ntkit.com	2016-03-18	MARKMONITOR INC.
accohntkit.com	2016-03-18	MARKMONITOR INC.
accointkit.com	2016-03-18	MARKMONITOR INC.
accojntkit.com	2016-03-18	MARKMONITOR INC.

需要留神的是大多数使用反向whois查询是免费的，但是你如果想要得到更多的结果或者完整的结果往往是需要你付费的。

填充空白区域

现在我们已经通过纵横交错的方法完成了域名收集，现在是否可以开始进行攻击测试了？答案是不。

如果我们可以填充下图中的空白区域，那么是不是能更加扩展我们的攻击面呢？



我们可以针对我们子域名罗列发现的域名都进行关联域名发现。但是这意味着我们需要花更长的时间进行子域名罗列，但是谁关心时间更长呢？记住，一个更大攻击面=更多

但是在这之前，先把可以解析的关联域名筛选出来：

```
./bin/massdns -r lists/resolvers.txt -o S <LIST_OF_ASSOCIATED_DOMAINS> | grep -e ' A ' |  cut -d 'A' -f 1 | rev | cut -d "." -
```

然后通过如下命令进行子域名罗列：

```
amass enum -passive -df <LIST_OF_RESOLVED_ASSOCIATED_DOMAINS> -o <OUT_FILE>
```

或者进行暴力猜解：

```
amass enum -brute -w <WORDLIST> -df <LIST_OF_RESOLVED_ASSOCIATED_DOMAINS> -o <OUT_FILE>
```

如果你有个给劲的机器，你可以使用GNU Parallel（https://www.gnu.org/software/parallel/
）或Xargs（http://man7.org/linux/man-pages/man1/xargs.1.html ）进行多进程工作来加快速度。例如：

```
cat <LIST_OF_RESOLVED_ASSOCIATED_DOMAINS> | parallel -j <NO_OF_CONCURRENT_JOBS> "amass enum -passive -d {} -o {}.out"
```

我更倾向于使用GNU Parallel，所以这里不会有Xargs的命令。

一旦你罗列出所有关联域名的子域名，接下来使用Massdns进行dns解析来筛选可解析的域名。

接下来？

做完如上的操作后，最后一步就是去重。

- 使用这些得到的域名和主机，你可以做如下的操作：
- 检查子域名是否可以被接管
- 端口扫描并确认运行的服务
- 记录运行web服务的主机
- 进行目录暴力猜解
- 等等

结论

如上的方法就是我在进行漏洞赏金活动时做的操作，我不能保证它也同样适用于你，也不能保证你遵循如上操作就会找到漏洞。这篇文章的目的在于共享我的方法给那些苦于

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板