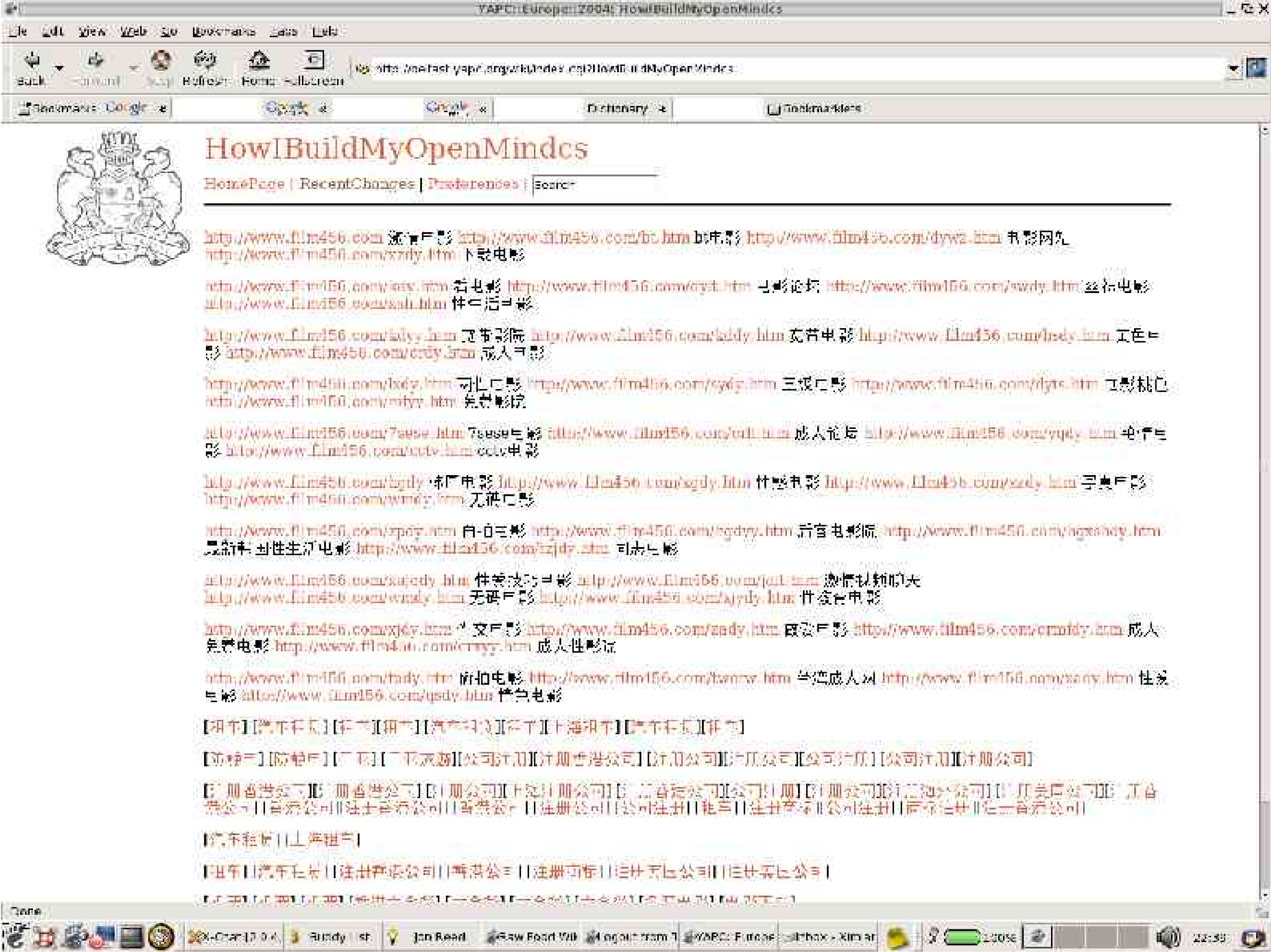
Protecting your web applications with the DNS

Jonathan Stowe


YAPC::Europe::2004: HowIBuildMyOpenMindcs
File Edit View Web Go Bookmarks Tabs Help
Back Forward Stop Refresh Home Fullscreen
http://belfast.yapc.org/wiki/index.cgi?HowIBuildMyOpenMindcs
Bookmarks Google Google Google Dictionary Bookmarklets
Done
X-Chat Buddy List Jon Reed Raw Food Wiki Logout from YAPC::Europe Inbox - Ximian
22:35

HowIBuildMyOpenMindcs

HomePage | RecentChanges | Preferences | Search

http://www.film456.com 激情电影 http://www.film456.com/bt.htm bt电影 http://www.film456.com/dywz.htm 电影网站 http://www.film456.com/xzdy.htm 下载电影

http://www.film456.com/ssy.htm 看电影 http://www.film456.com/dylt.htm 电影论坛 http://www.film456.com/swdy.htm 丝袜电影 http://www.film456.com/sxh.htm 性生活电影

http://www.film456.com/zdyy.htm 在线影院 http://www.film456.com/kbdy.htm 恐怖电影 http://www.film456.com/hsdy.htm 黄色电影 http://www.film456.com/crdy.htm 成人电影

http://www.film456.com/tzdy.htm 同志电影 http://www.film456.com/sjdy.htm 三级电影 http://www.film456.com/dyts.htm 电影桃色 http://www.film456.com/mfyy.htm 免费影院

http://www.film456.com/7sese.htm 7sese电影 http://www.film456.com/crlt.htm 成人论坛 http://www.film456.com/sqdy.htm 色情电影 http://www.film456.com/cctv.htm cctv电影

http://www.film456.com/hgdy 韩国电影 http://www.film456.com/xgdy.htm 性感电影 http://www.film456.com/xzdy.htm 写真电影 http://www.film456.com/wmdy.htm 无码电影

http://www.film456.com/zpdy.htm 自拍电影 http://www.film456.com/hgdyy.htm 后宫电影院 http://www.film456.com/zxhgxshdy.htm 最新韩国性生活电影 http://www.film456.com/rbdy.htm 日本电影

http://www.film456.com/xajqdy.htm 性爱技巧电影 http://www.film456.com/jqlt.htm 激情视频聊天 http://www.film456.com/wmdy.htm 无码电影 http://www.film456.com/xjydy.htm 性教育电影

http://www.film456.com/xjdy.htm 性交电影 http://www.film456.com/zady.htm 限制电影 http://www.film456.com/crmfdy.htm 成人免费电影 http://www.film456.com/crxyy.htm 成人性影院

http://www.film456.com/tpdy.htm 偷拍电影 http://www.film456.com/twcrw.htm 台湾成人网 http://www.film456.com/xady.htm 性爱电影 http://www.film456.com/qsdy.htm 情色电影

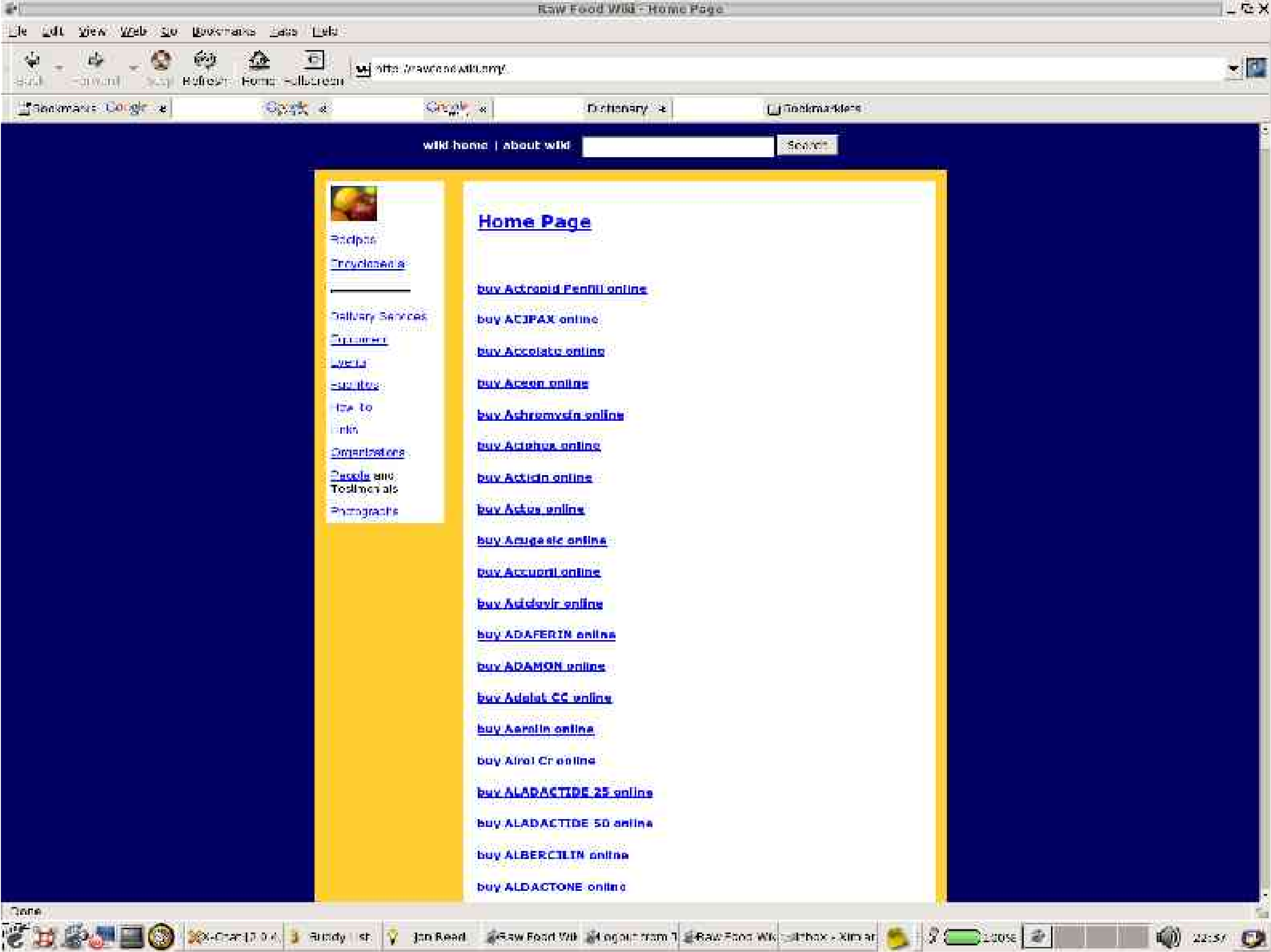
[租车][汽车租赁][租车][租车][汽车租赁][租车][上海租车][汽车租赁][租车]

[防静电][防静电][广告][广告策划][公司注册][注册香港公司][注册公司][注册公司][公司注册][公司注册][注册公司]

[注册香港公司][注册香港公司][注册公司][上海注册公司][注册香港公司][公司注册][注册公司][注册离岸公司][注册美国公司][注册香港公司][香港公司][注册香港公司][香港公司][注册公司][公司注册][租车][注册商标][公司注册][商标注册][注册香港公司]

[汽车租赁][上海租车]

[租车][汽车租赁][注册香港公司][香港公司][注册商标][注册美国公司][注册美国公司]


Raw Food Wiki - Home Page
File Edit View Web Go Bookmarks Tabs Help
Back Forward Stop Refresh Home Fullscreen
Bookmarks Google Google Google Dictionary Bookmarklets
wiki home | about wiki
Search
Done
X-Chat Buddy List Jon Reed Raw Food Wiki Logout from Raw Food Wiki

Recipes

Encyclopedia

Delivery Services

Suppliers

Events

Retreats

How To

Links

Organizations

People and Testimonials

Photographs

Home Page

buy Actrapid Penfill online

buy ACJPAX online

buy Accolate online

buy Aceon online

buy Achromycin online

buy Actiphos online

buy Acticin online

buy Actos online

buy Acugesic online

buy Accupril online

buy Aciclovir online

buy ADAFERIN online

buy ADAMON online

buy Adalat CC online

buy Aerolin online

buy Airol Cr online

buy ALADACTIDE 25 online

buy ALADACTIDE 50 online

buy ALBERCILIN online

buy ALDACTONE online

What is the DNSBL?

- Perform DNS lookup of a host in a particular format
- Returns a result if the queried host is of interest to the creator of the 'block list'
- Some lists return different values to indicate the nature of the entry.
- May also have TXT records containing further information about the entry.

Why use a block list

- Automated comment spam
- Open proxies, 'zombies' and other known abusive hosts are listed in various DNSBL
- Logs submitted by NMS guestbook users suggest that 50% of abusive hosts listed.
- Dynamic and more flexible than application or server configuration based on static lists.

How to use the DNSBL

- DNSBL query is for a DNS 'A' record in the form

  ```
  4.3.2.1.dnsbl-zone
  ```

  Where the host IP is 1.2.3.4 and dnsbl-zone is the zone being queried.

- Corresponding BIND zone file record will look like:

  ```
  4.3.2.1  IN    A  127.0.0.1
  ```

How to use the DNSBL

The simplest of Perl code:

```
sub rbl_check
 {
    my ( $ip, $zone ) = @_;


    my $rc = 1;


    if ( $ip =~ /(\d+)\.(\d+).(\d+)\.(\d+)/ ) {
       my $query = "$4.$3.$2.$1.$zone.";
       my $res   = gethostbyname($query);
       if ( defined $res ) {
             $rc = 0;
       }
    }




    return $rc;
 }
```

How to use the DNSBL

Using it in a CGI program:

```
if (!rbl_check($ENV{REMOTE_ADDR},'xbl.spamhaus.org')
{
    print "Status: 403 Forbidden\n\n";
    exit;

}
```

Testing

- Get yourself in a block list
- Alternatively create your own block list
  - Local DNS server (such as BIND)
  - Add zone to DNS Server configuration
  - Create zone file containing your host
  - Point resolver at your DNS server
  - Query against your new zone

Testing

BIND configuration to add zone:

```
zone "test.relay" {
   type master;
   file "test.relay";
};
```

Testing

Create zone file “test.relay” :

```
$TTL 1d
@       IN      SOA     localhost. root.localhost.   (
                                              1997022700
                                              28800
                                              14400
                                              3600000
                                              86400 )
            IN   NS       localhost.

1.0.0.127   IN   A  127.0.0.2
```

Which DNSBL to use?

- Select a DNSBL zone that lists the appropriate hosts
  - e.g xbl.spamhaus.org lists open proxies and other exploited machines
- Check that the policy of the DNSBL permits this kind of usage. Some may want to be notified before you use them.
- Investigate the reliability of the service.

Taking it further

- Use Net::DNS to retrieve TXT record from lists that provide this, in order, for example, to give a message indicating the reason for refusing access.
- Create a mod_perl access handler that can protect a whole site or part of a site.
- Maintain your own private DNSBL.

The Abusive hosts blocking list.

- Lists and categorizes hosts that are known to have been used in abusive actions on the internet.
- Returns a different value dependent on the kind of “abuse” the host was engaged in.
- Not all entries are appropriate for protecting applications
- Has a “comment spam” category.

The Abusive hosts blocking list.

```
127.0.0.2 - Open Relay
127.0.0.3 - Open Proxy
127.0.0.4 - Spam Source
127.0.0.5 - Provisional Spam Source Listing block (will be removed if spam stops)
127.0.0.6 - Formmail Spam
127.0.0.7 - Spam Supporter
127.0.0.8 - Spam Supporter (indirect)
127.0.0.9 - End User (non mail system)
127.0.0.10 - Shoot On Sight
127.0.0.11 - Non-RFC Compliant (missing postmaster or abuse)
127.0.0.12 - Does not properly handle 5xx errors
127.0.0.13 - Other Non-RFC Compliant
127.0.0.14 - Compromised System - DDoS
127.0.0.15 - Compromised System - Relay
127.0.0.16 - Compromised System - Autorooter/Scanner
127.0.0.17 - Compromised System - Worm or mass mailing virus
127.0.0.18 - Compromised System - Other virus
127.0.0.19 - Open Proxy
127.0.0.20 - Blog/Wiki/Comment Spammer
127.0.0.127 - Other
```

http://www.ahbl.org/docs/dnsbl.php