

SAC057 / non-FQDN Certs

Fun with TLDs...

*Patrik Fältström & Warren Kumari
(RIPE DUBLIN, 2013-05)*

Internal Server Names

- *Designed for “internal only” type applications.*
 - *Often used by Microsoft Exchange, Active Directory.*
- *www.corp, www.accounting, mail.test*
- *Doesn't end in a TLD*
 - *can't be used on the Internet*
 - *nowhere to send the validation email*

Certificate request

Certificate Request:

Data:

Version: 0 (0x0)

Subject: C=US, ST=VA, L=Dulles,
O=**Dulles Steel and Forge Supplies**,

OU=IT - Internal WWW Site.,

CN=**www.site**/emailAddress=warren@kumari.net

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:da:ef:bd:d0:ee:db:...

....

Helpful...

[Manage Certificates](#) [Tools](#) [Help](#) [New Features](#) [Repository](#) [Report EV Abuse](#) [Feedback](#)

1-year Standard SSL

Select

Submit

What now?

Where is your certificate going to be hosted?

☐ Web Hosting, Grid Hosting, Website Builder, Quick Shopping cart, or Dream Design Team

☐ Dedicated Server or Virtual Dedicated Server, with Simple Control Panel

☒ Third Party, or Dedicated Server or Virtual Dedicated Server, without Simple Control Panel

Enter your Certificate Signing Request (CSR) below: [CSR Help](#)

```
ml/gjz9Ksoh0CZqV15wY9wfx64yH8s0Kk6zMwgMz96jAc0kqLhOA/kDLXrFbE1
01trKWe3LOzGzxngEh/fqFFt50s3YzMs/hGwn1AKdwFOTTYkR1Qj144Urv+jN6
k4lnDun13yyIw+MyDE8tLSeIMjcoImy+KxCcFZCIXed/Jg3eW72sZhbJnQIDAQAAB
oAAwDQYJKoZIhvcNAQEFBQADggEBALAwRDF+QFt6baX7MTARvCmsMOC2q/2TXczj
JnKeA5Hi1t3mAV4j9z+jVWiaRndgY1dOQ+VsKHrGqLAuOL5kZgWf+vKEOzsJk4fE
KISRELvyJLv4NsF1CKY9k7+kj/c0/1Pr162GcjraiBPRIAp3XjFLq8QsfOkvsW2w
rjPEtSHieDT6a1VpqaKQj/UziGKf9RwQA7/cQdmNyc5si6D+JZU7+pisDhvgZrQ
rIRJAzhQ6sMWa1Ag3EA0Qkh+Foc5W0PsITJLZbvDc8gCVu4JCvKN7C9A3bLpLJR
44klmLzumUCvKT84dsdwc3KaW1Aad/wO+anKzTwzLNzXyyI7zCg=
-----END CERTIFICATE REQUEST-----
```

Certificate issuing organization: [Learn more](#)

Go Daddy

The requested common name, **www.site**, is not a fully-qualified common name, and must be used on an internal server. Please confirm that this certificate is not meant to be World Wide Web-accessible, otherwise please use a fully-qualified common name.

☒ This certificate will be used on an internal server

Effective August 8, 2011, some certificates will require re-validation every three years. For more information, please [click here](#) to review the Subscriber Agreement.

[Next](#) [Cancel](#)

Copyright © 2003-2012. All rights reserved.
[Go Daddy Privacy Policy](#)
[Repository](#)

Thanks!

Issued Certificate

Data:

Version: 3 (0x2)

Serial Number:

27:e7:22:63:59:11:b0

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=Arizona, L=Scottsdale,

O=GoDaddy.com, Inc., OU=http://

certificates.godaddy.com/repository, CN=Go Daddy Secure
Certification Authority/serialNumber=07969287

Validity

Not Before: Oct 2 23:56:35 2012 GMT

Not After : Oct 2 23:56:35 2013 GMT

Subject: O=www.site, OU=Domain Control Validated,
CN=www.site

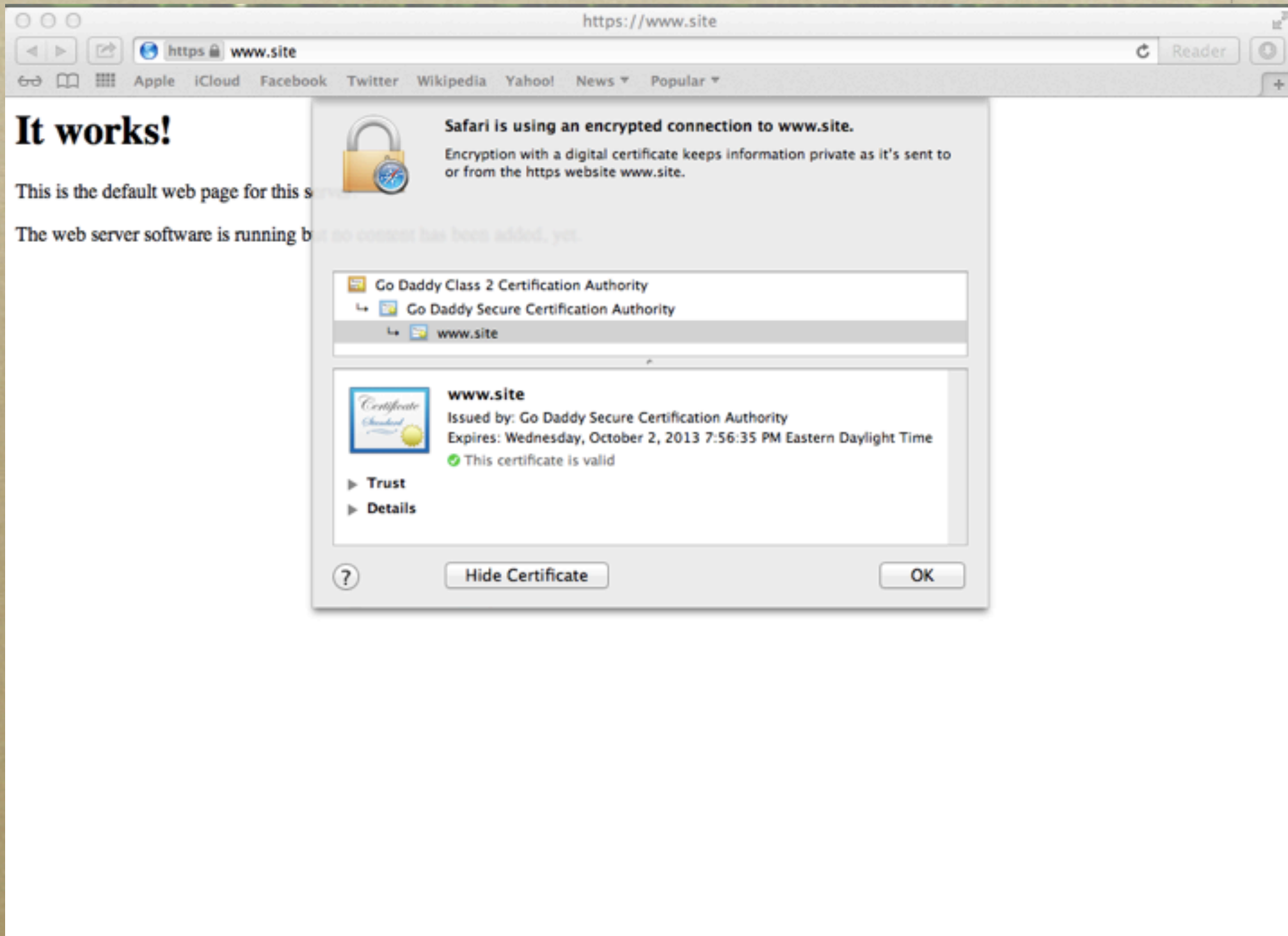
X509v3 Subject Alternative Name:

DNS:www.site, DNS:site

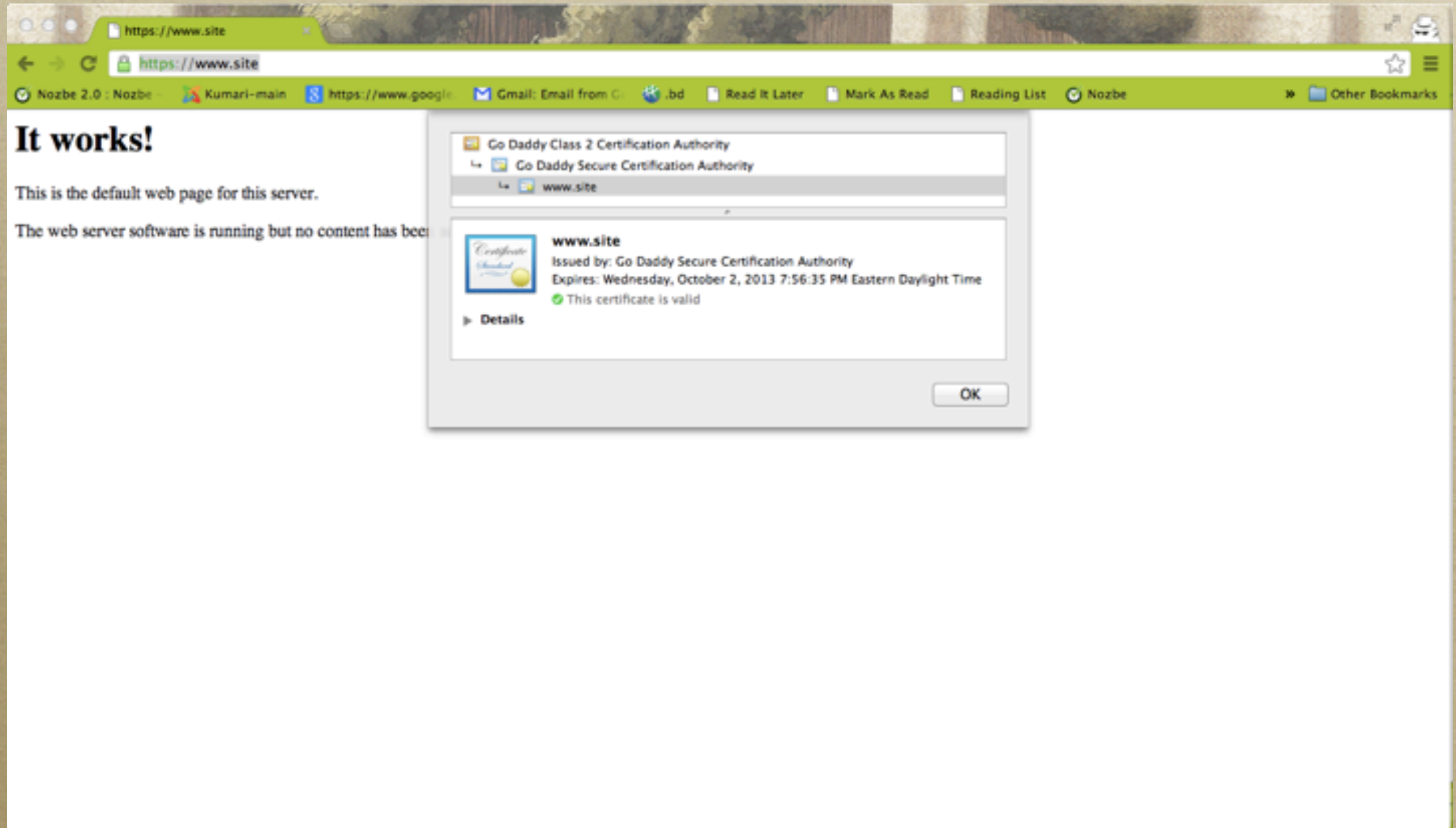
Testing

- *Setup a fake root*
- *Delegated .site to myself*
- *Setup a webserver, serving the cert*

Doh!



Doh!



Investigations by SSAC

- *SSAC formed a work party*
- *Researched prevalence of non-FQDN certs*
 - *Using the EFF SSL Observatory data*
 - *At least 157 CAs have issued such certs*
 - *Lower bounds estimate*
 - *CA/B Forum is aware of the issue*
 - *3 year from signing to revocation*
- *Conclusion:*
 - *ICANN must immediately do something*

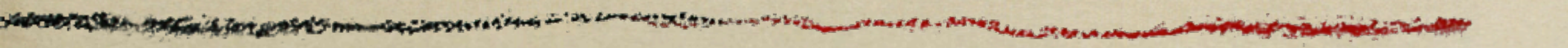
ICANN Actions

- *ICANN Security Team took the lead*
 - *“Coordinated Vulnerability Disclosure”*
 - *Contacted CA/B Forum Chair Jan 23*
 - *Briefed CA/B Forum Feb 5*
 - *Ballot 96 at CA/B Forum passed Feb 26*
 - *30 / 120 day period (instead of 3 years)*
- *SAC057 published Mar 15*
 - *Outreach, outreach and more outreach*

Solved? Nope...

- *Not all CAs are members of the CA/B Forum*
 - *So not bound by these agreements*
 - *But generally trustworthy / follow guidelines*
- *Revocation ineffective**
 - *Blocking CRL / OSCP / air-gapped networks*

* : <http://www.imperialviolet.org/2011/03/18/revocation.html>



Questions?