Abusing Certificate Transparency

Or how to hack Web Applications before Installation

Hanno Böck
https://hboeck.de/

HTTPS

Certificate Authorities

Can we trust Certificate Authorities?

No

CAs are bad, we need to get rid of them

Popular Infosec opinion

Reality

Nobody has a feasible plan how to replace CAs

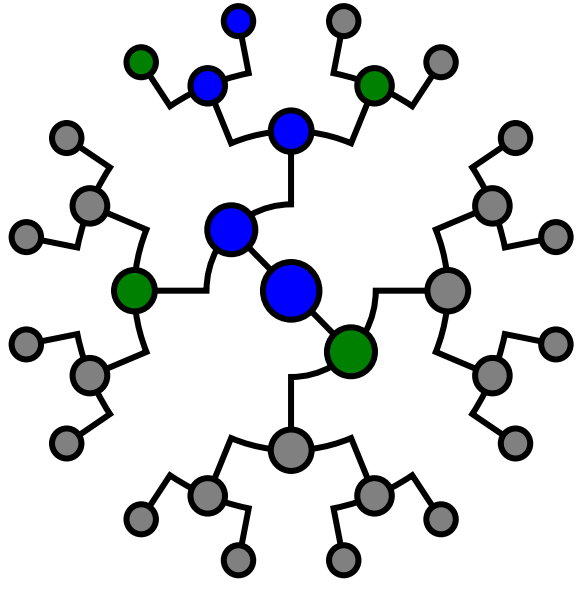
Improving the CA system

Baseline Requirements

HTTP Public Key Pinning (HPKP)

Certificate Authority Authorization (CAA)

Certificate Transparency



Public logs

CT Details

Merkle Hash Trees, Signed Certificate Timestamps (SCT), Signed Tree Head (STH), Precertificates, Monitors, Gossip, ...

Certificate logging

Next year (April) logging will be required for all certificates

Today

The CA watchdog

Everyone can check logs for suspicious activity

```
Issuer:
    commonName                = thawte EV SSL CA - G3
    organizationName          = thawte, Inc.
    countryName               = US
Validity
    Not Before: Sep 14 00:00:00 2015 GMT
    Not After : Sep 15 23:59:59 2015 GMT
Subject:
    commonName                = www.google.com
    localityName              = Mountain view
    stateOrProvinceName       = California
    countryName               = US
    serialNumber              = 2158113
    businessCategory          = Private Organization
    organizationName          = Symantec Corp
    jurisdictionStateOrProvinceName = Delaware
    jurisdictionCountryName   = US
```

```
Issuer:
    commonName                = DigiCert SHA2 High Assurance Server CA
    organizationalUnitName    = www.digicert.com
    organizationName          = DigiCert Inc
    countryName               = US
Validity
    Not Before: Oct  6 00:00:00 2014 GMT
    Not After : Dec 13 12:00:00 2017 GMT
Subject:
    commonName                = *.adoftheyear.com
    organizationalUnitName    = IT
    organizationName          = Metrixlab B.V.
    localityName              = Rotterdam
    stateOrProvinceName       = California
    countryName               = NL
```

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS:www.intesavita.org
        DNS:www.intesavita.net
        DNS:www.intesavita.info
        DNS:www.intesavita.eu
        DNS:www.intesavita.cn
        DNS:www.intesavita.biz
        DNS:www.intesavita.com
        DNS:www.intesavita.it
        DNS:www.intesasanpaolovita.org
        DNS:www.intesasanpaolovita.info
        DNS:www.intesasanpaolovita.eu
        DNS:www.intesasanpaolovita..biz
        DNS:www.intesasanpaolovita.com
        DNS:www.intesasanpaolovita.it
        DNS:intesasanpaolovita.it
        DNS:intesasanpaolovita.com
```

https://crt.sh

Certificate Transparency is also a data source

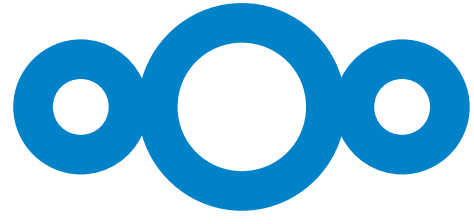
Feed of new host names

Let's talk about something else

Web applications

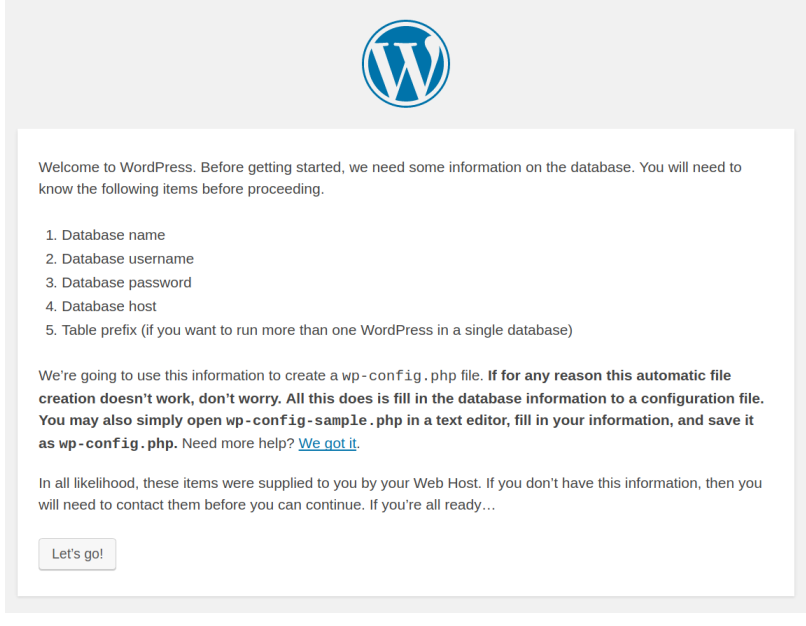
WordPress

Joomla!®



Nextcloud

Installers



Welcome to WordPress. Before getting started, we need some information on the database. You will need to know the following items before proceeding.

1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

We're going to use this information to create a `wp-config.php` file. **If for any reason this automatic file creation doesn't work, don't worry. All this does is fill in the database information to a configuration file. You may also simply open `wp-config-sample.php` in a text editor, fill in your information, and save it as `wp-config.php`.** Need more help? We got it.

In all likelihood, these items were supplied to you by your Web Host. If you don't have this information, then you will need to contact them before you can continue. If you're all ready…

Let's go!

No authentication!

Old: Google dorking web installers

New idea

There is a time window between uploading files and completing the installer

Remember: We have a feed of newly created host names

Attack

Monitor CT logs, extract host names

Check hosts for common installers

If installer found: Install the application

Upload a plugin with code execution backdoor

Revert installation

Database credentials

Use external database host

Demo

Challenges

Logged certificates aren't immediately public (around 30 minutes)

Optimizations

Instead of checking sites once one could check them multiple times

Numbers

5000 Wordpress installations within three months.

500 x Joomla, 120 x Nextcloud, 70 x Owncloud.

Protection

Installers need authentication

Challenge

Application programmers want easy installations

Security tokens

Webapp creates token file, user has to read token

Vendors

Drupal, Typo3, Owncloud

... no reaction

Vendors

Wordpress, Nextcloud, Serendipity participated in cross-vendor discussion, but no action

MediaWiki 1.28.2 installation

MediaWiki home
User's Guide
Administrator's Guide
FAQ

Read me
Release notes
Copying
Upgrading

Complete!

Congratulations! You have installed MediaWiki.

The installer has generated a `LocalSettings.php` file. It contains all your configuration.

You will need to download it and put it in the base of your wiki installation (the same directory as index.php). The download should have started automatically.

If the download was not offered, or if you cancelled it, you can restart the download by clicking the link below:

Download `LocalSettings.php`

Note: If you do not do this now, this generated configuration file will not be available to you later if you exit the installation without downloading it.

When that has been done, you can **enter your wiki**.

- Language
- Existing wiki
- Welcome to MediaWiki!
- Connect to database
- Upgrade existing installation
- Database settings
- Name
- Options
- Install
- **Complete!**

- Restart installation

Did you know that your wiki supports extensions?

You can browse extensions by category or the Extension Matrix to see the full list of extensions.

It still allows to create an SQLite database

Can this be exploited?

Joomla! is free software released under the GNU General Public License.

Warning
You want to use a database host which is not localhost. For security reason, you need to verify the ownership of the used webhosting account. Please see here [docspagelink] for more information.

Error
In order to confirm that you are the the owner of this webhost please delete the file _JoomlaA1YDCdBBa3gocxAzcW8CK.txt we have just created in the "installation" folder of your Joomla.

1 Configuration | 2 Database | 3 Overview

Database Configuration

Previous | Next

Database Type * MySQLi

This is probably "MySQLi".

Host Name * example.org

This is usually "localhost" or a name provided by your host.

Whitelisting localhost

This was my idea, but I don't like it

What can users do?

Be fast?

Certificate redaction?

.htaccess

Defending as a user is hard

We need fixes from vendors

Do attackers already use this?

```
x.x.x.x - - [09/Jul/2017:12:03:03
+0200] "GET / HTTP/1.0" 403 1664 "-"
"Mozilla/5.0 (compatible;
NetcraftSurveyAgent/1.0;
+info@netcraft.com)"
```

Takeaway

Unauthenticated installers are a security risk

Takeaway

No more secret hostnames

Takeaway

Certificate Transparency is a valuable data source for attackers and defenders

Thanks for listening!

Questions?

https://hboeck.de/

https://github.com/hannob/ctgrab