Moving Toward SSL:

What it is, How to do it, & Why you should care

Mukalele Rogers, #WordCampKampala

Saturday, 16 December 2017

Hello!

A bit about me…

@mrogers4christ

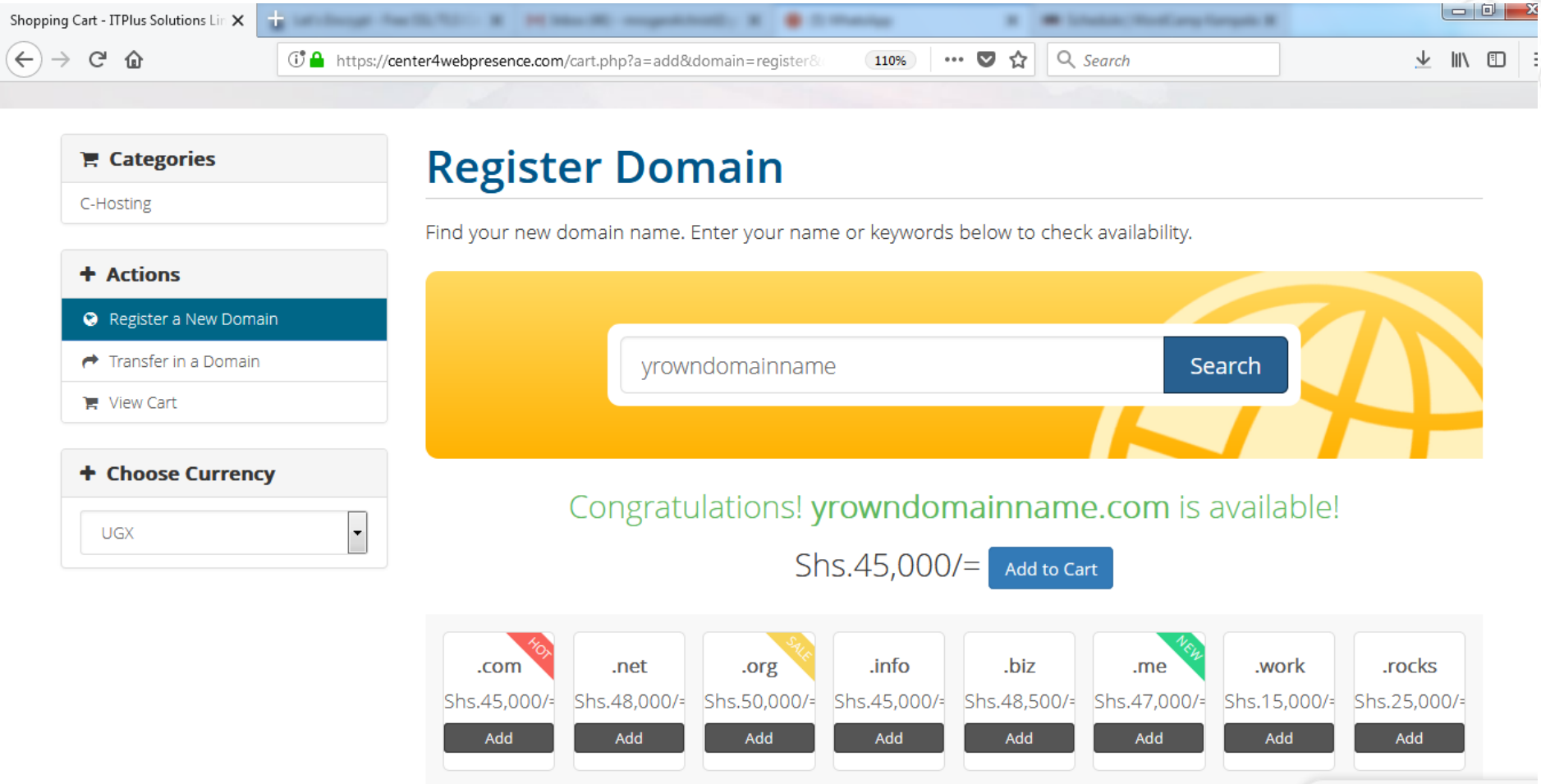
www.mukalele.net

What I Do

center4webpresence.com

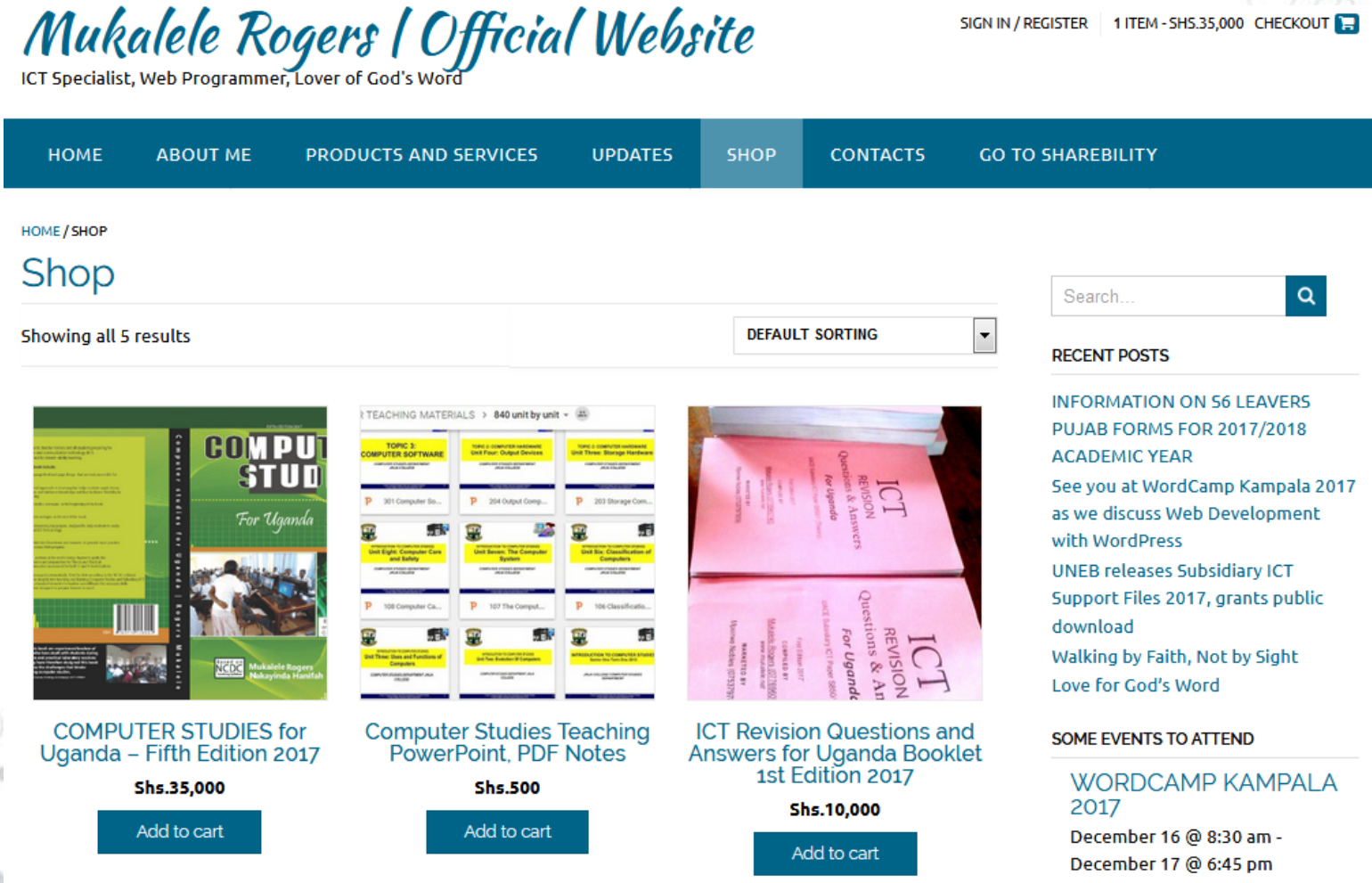
Offering domain name registration and Web Hosting For Less!

+Free SSL



What I Do

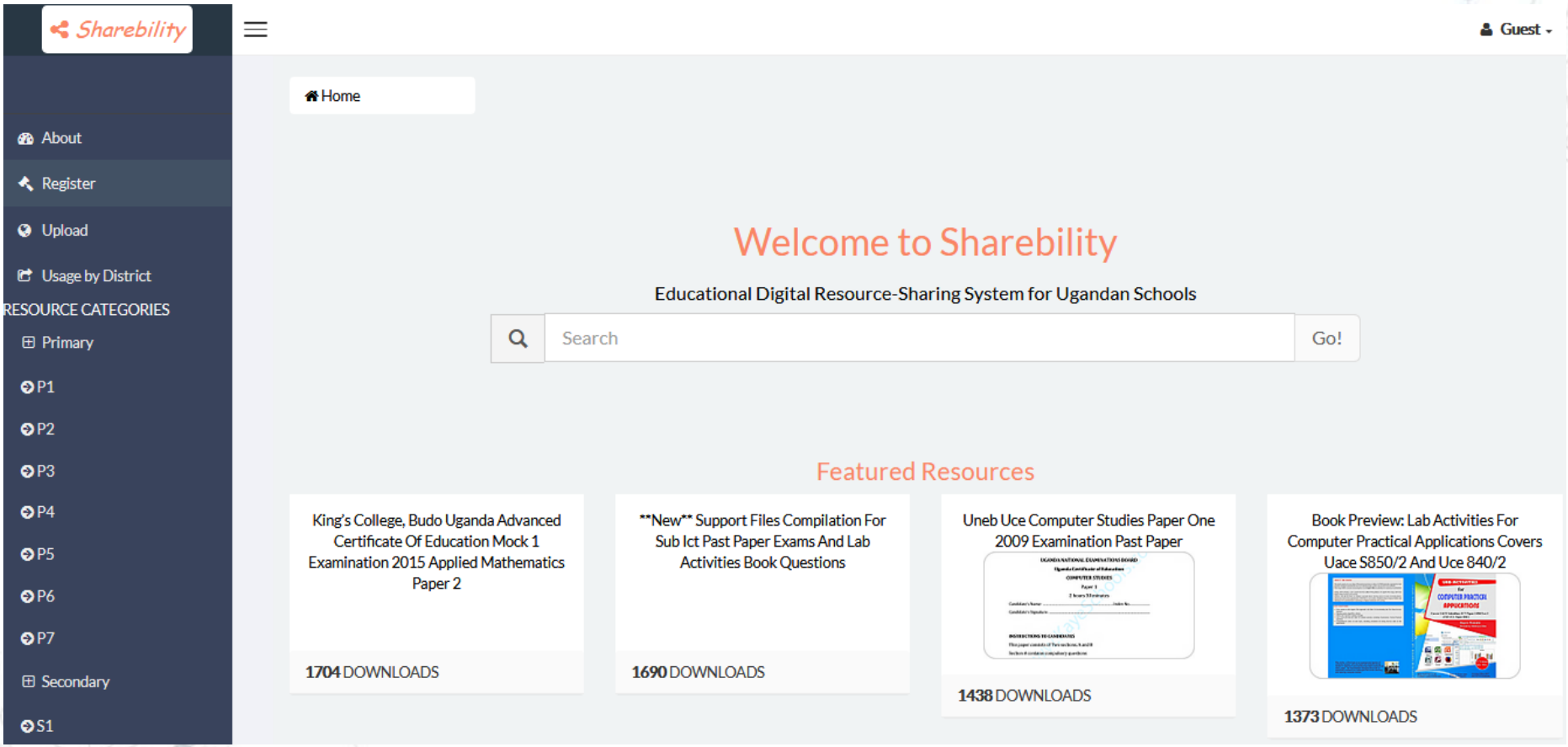
As an ICT Teacher / Trainer, I maintain an online shop powered by + WOO COMMERCE at mukalele.net



What I Do

Sharebility Uganda - sharebility.mukalele.net

An educational digital resource sharing system for Ugandan Schools



Moving Toward SSL

Posted December 1, 2016 by Matt Mullenweg. Filed under Development.

We're at a turning point: 2017 is going to be the year that we're going to see features in WordPress which require hosts to have HTTPS available. Just as JavaScript is a near necessity for smoother user experiences and more modern PHP versions are critical for performance, SSL just makes sense as the next hurdle our users are going to face.

SSL basically means the link between your browser and the server is encrypted. SSL used to be difficult to implement, and often expensive or slow. Modern browsers, and the incredible success of projects like Let's Encrypt have made getting a certificate to secure your site fast, free, and something we think every host should support by default, especially in a post-Snowden era. Google also weighs SSL as a search engine ranking factor and will begin flagging unencrypted sites in Chrome.

First, early in 2017, we will only promote hosting partners that provide a SSL certificate by default in their accounts. Later we will begin to assess which features, such as API authentication, would benefit the most from SSL and make them only enabled when SSL is there.

Separately, I also think the performance improvements in PHP7 are particularly impressive, and major kudos to everyone who worked on that. We will consider whether hosts use PHP7 by default for new accounts next year as well.

See Also:

For more WordPress news, check out the WordPress Planet.

There's also a development P2 blog.

To see how active the project is check out our Trac timeline, it often has 20–30 updates per day.

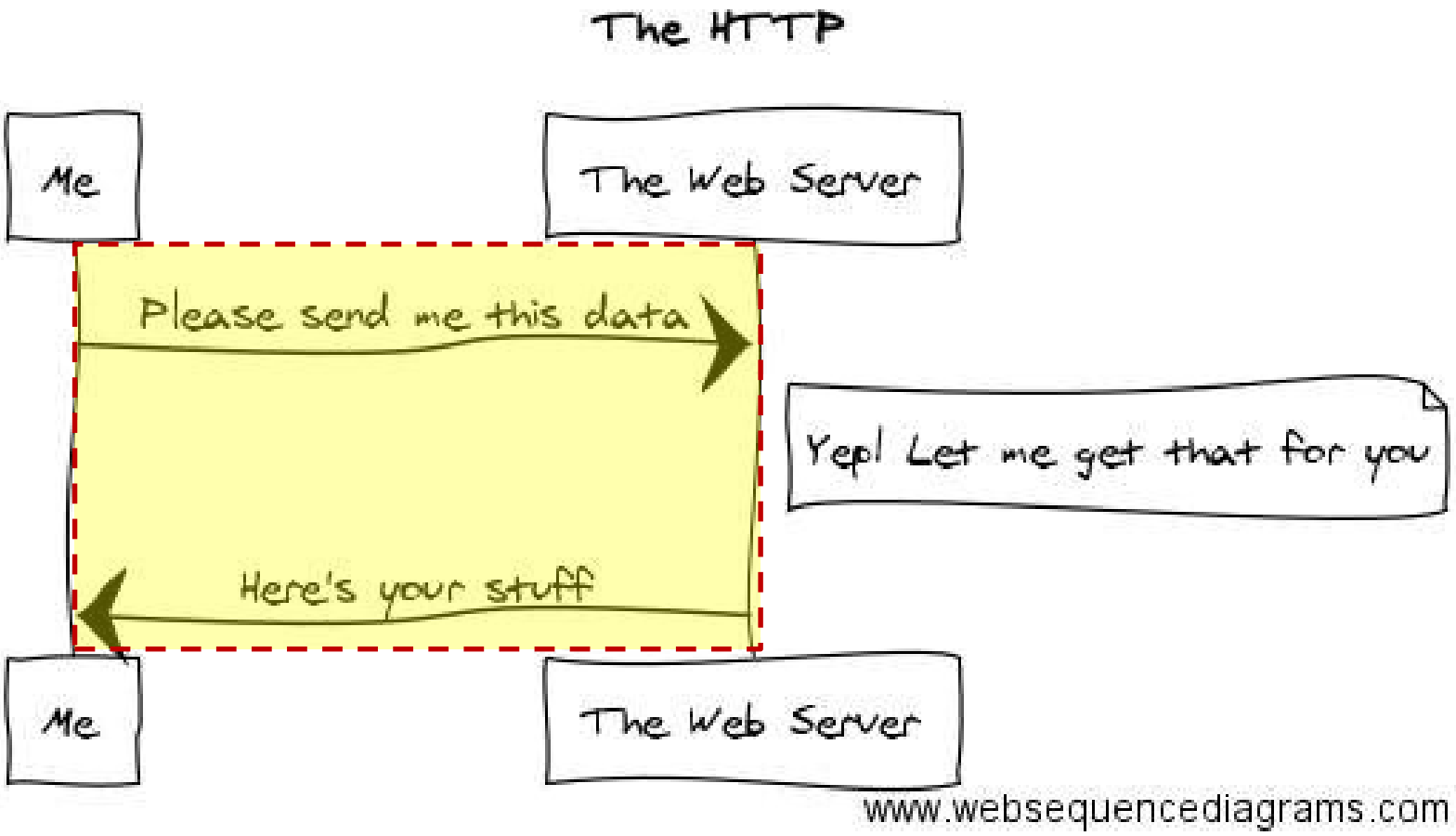
Categories

- Releases (206)
- Development (191)
- Security (47)
- Community (43)
- Meta (43)
- Events (33)
- Testing (23)
- WordCamp (20)
- General (18)
- Documentation (15)

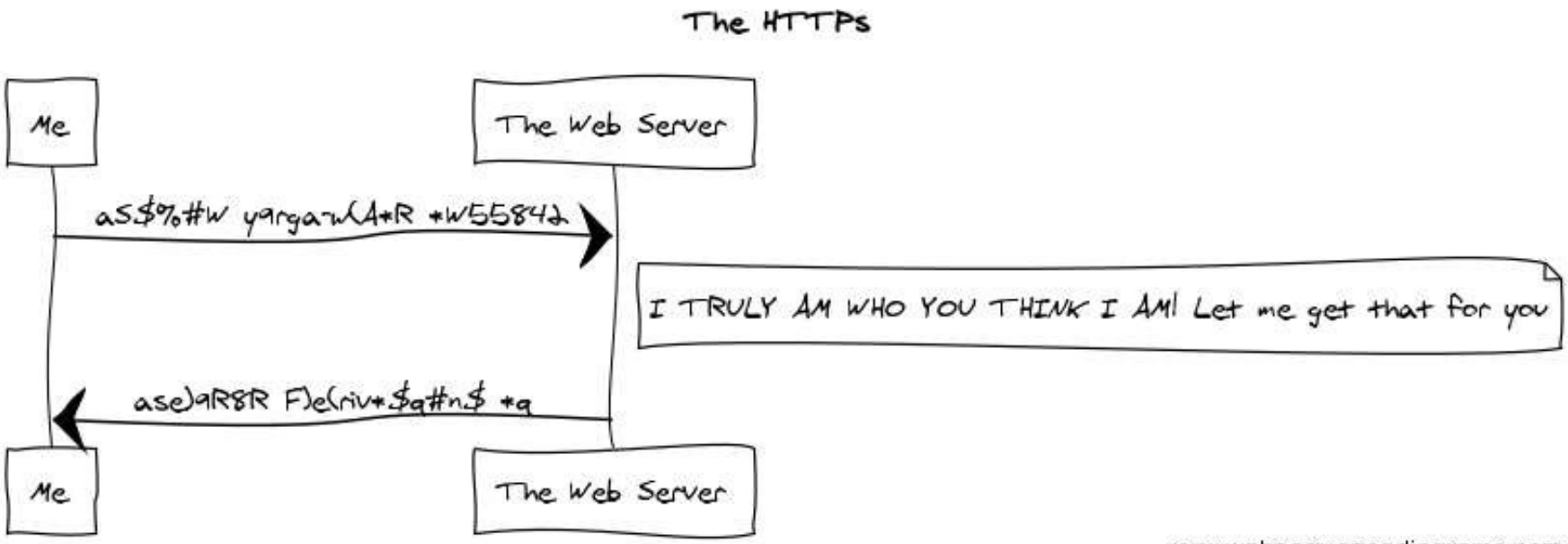
1.

SSL: What it is

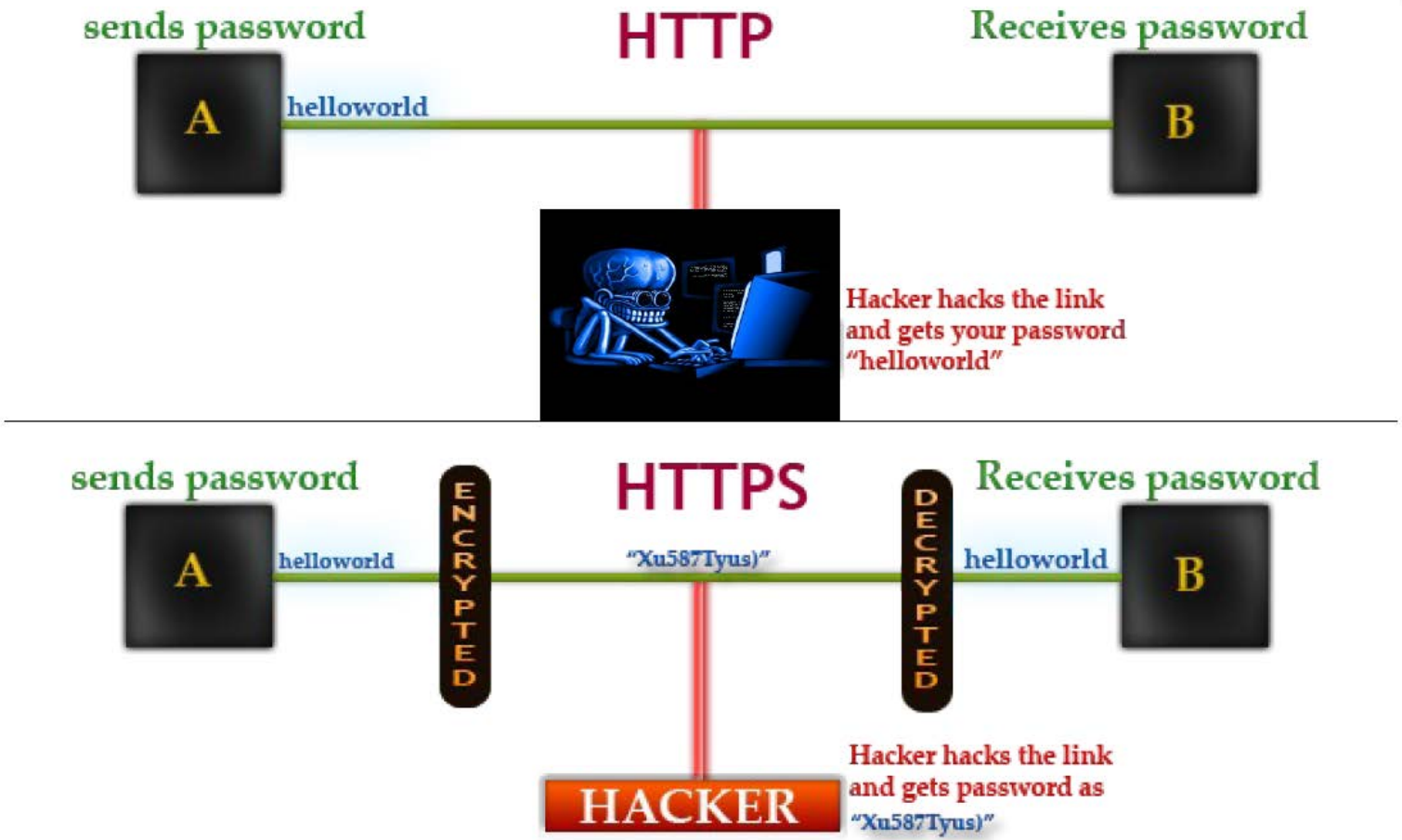
HTTP Review


The HTTP
Me
The Web Server
Please send me this data
Yep! Let me get that for you
Here's your stuff
Me
The Web Server
www.websequencediagrams.com

HTTPS


The HTTPs
Me
The Web Server
a5$%#w yargarA*R *W55842
I TRULY AM WHO YOU THINK I AM! Let me get that for you
ase)aR8R F)e(riv*$q#n$ *q
Me
The Web Server
www.websequencediagrams.com

HTTP vs HTTPS



How does HTTPS work: SSL explained

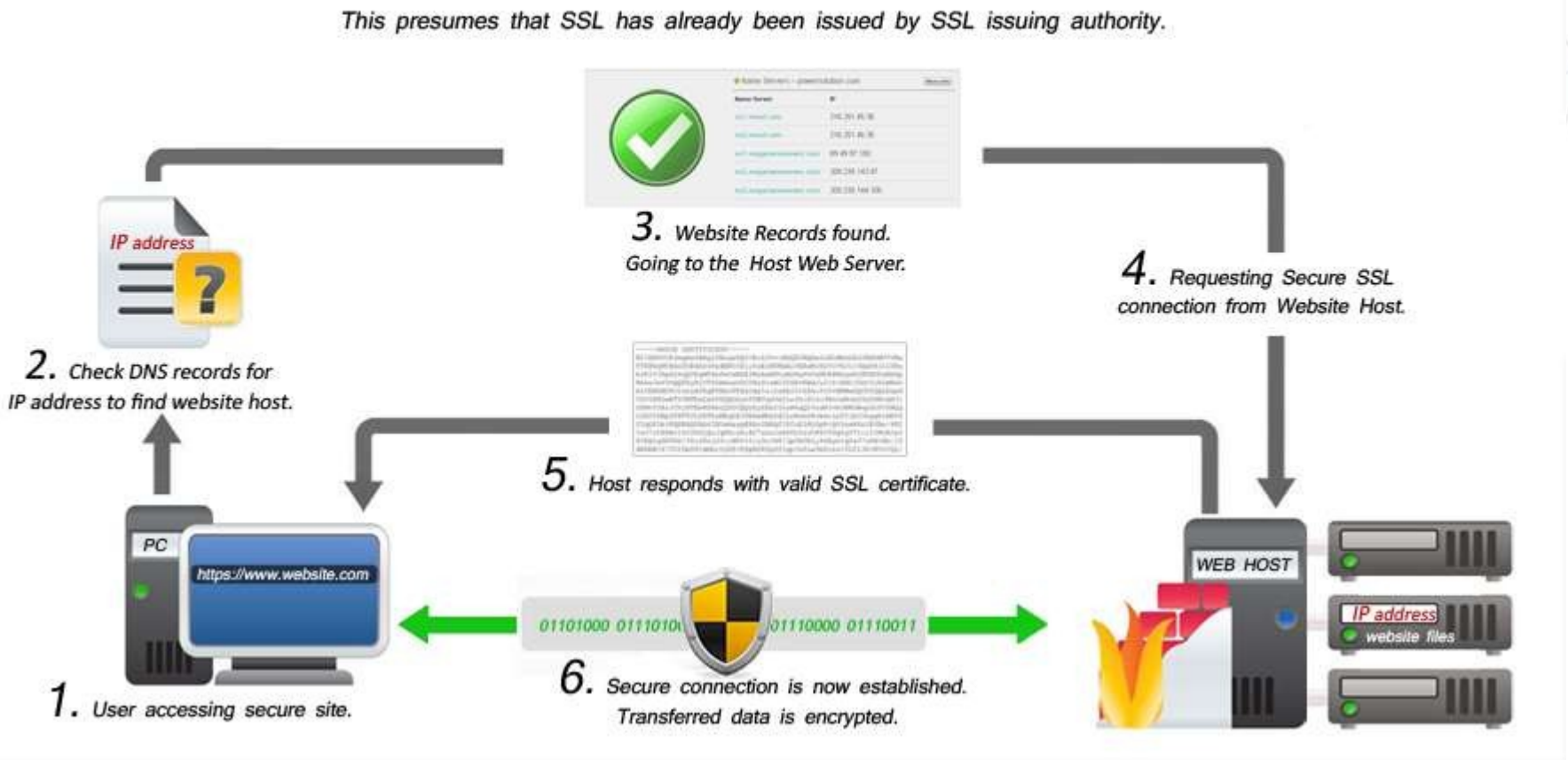


Image: https://thenocman.com/ssl-certificates/

2.
Why you should care

Who Needs It?

- E-Commerce
- Social Media
- Form Data e.g wp-login form
- Mandatory for many functionalities **See goo.gl/LoY7u5**

  e.g. Geolocation, Device motion, EME, getUserMedia, AppCache, Notifications
- SEO for websites
- Everyone!

Username or Email Address

Password

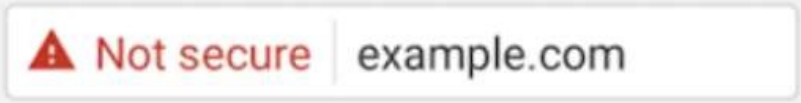
Remember Me

Log In

Lost your password?

← Back to bitworx

Eventual treatment of all
HTTP pages in Chrome:



3.

How to do it

You'll Need…

```
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIQKAIzIuRmTHxcwwABHyda7zANBgkqhkiG9w0BAQUFADBz
MQswCQYDVQQGEwJHQjEbMBkGA1UECBMSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYD
VQQHEwdTYWxmb3JkMRowGAYDVQQKExFDT01PRE8gQ0EgTGltaXRlZDEzMBcGA1UE
AxMQUG9zaXRpdmVTU0wgQ0EgMjAeFw0xNDAzMDUwMDAwMDBaFw0xNTAzMDUyMzU5
NTlaMFoxITAfBgNVBAsTGERvbWFpbiBDb250cm9sIFZhbGlkYXRlZDEUMBIGA1UE
CxMLUG9zaXRpdmVTU0wxHzAdBgNVBAMTFnd3dy5qb2hudG90aGV3b3JsZC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzs7SFnemzta92OHfvIPql
+5kBfzuDOWWGyEFdSfhBY9Y4LM0POj2+tKPiUzY1qgKE9g43jef+6PXMqLCXUJ6S
HNWzOTDdgUuEmjTGGzdjD+vuu0io3DkuqRn3a6VUmrmquKlY1ZQK1Bzec+fGXbI7
BTFWs3wlTLPenGRAUZGjxj4CWnF6XaNuXsr7bEHGltaefOv1qZ4JPzdd78QxRiWQ
O8lNDdreiJHPQaabWIELFOfm/a4+kwm4GwFAd6SDMCAG5CHpsWWqLMzrujfcMDRV
vNTaU8UNAOrUYfOsShbeyf5F/EER/9NKh2Y1rKJF7TsY9GjZD/MSOX5H1TxOZdN1
AgMBAAGjggG1MIIBsTAfBgNVHSMEGDAWgBSZ5EBfaxRePgXZ3dNjVPxiuPcArDAd
BgNVHQ4EFgQUl9iRosAURI7hur0c8abfWwUbr5MwDgYDVR0PAQH/BAQDAgWgMAwG
A1UdEwEB/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMFAGA1Ud
IARJMEcwOwYLKwYBBAGyMQECAgcwLDAqBggrBgEFBQcCARYeaHR0cDovL3d3dy5w
b3NpdGl2ZXNzbC5jb20vQ1BTMAgGBmeBDAECATA7BgNVHR8ENDAyMDCgLqAshipo
dHRwOi8vY3JsLmNvbW9kb2NhLmNvbS9Qb3NpdGl2ZVNTTENBMi5jcmwwbAYIKwYB
BQUHAQEEYDBeMDYGCCsGAQUFBzAChipodHRwOi8vY3JOLmNvbW9kb2NhLmNvbS9Q
b3NpdGl2ZVNTTENBMi5jcnQwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmNvbW9k
b2NhLmNvbTA1BgNVHREELjAsghZ3d3cuam9obnRvdGhld29ybGQuY29tghJqb2hu
dG90aGV3b3JsZC5jb20wDQYJKoZIhvcNAQEFBQADggEBAJgjwJvrIcOEYF110EkO
qwvqb5ZB7f61ZKOdhcUvE4JO7uSE5K2i38D9bjSntmt6jZVrNJwrlNRE4YPZvWHe
b9T8XKSYk8iU4Qfk+BdVe/DZVZYgluo4l9i487vti2/7Gp/kIPpUFg+xQxh/OQM7
B90xvhbnx/neiUht4tFKB89t1vEX7cq22291/vVS/BXWJfcUc5RZ1LB9qMkdZMpY
oo+aO56tk0gjJa/2XhLANzBTEmOf8p1OjJXm3aWplx0ZHv+lfpCaXCBKWB35M9mc
np7EZMq1gdaTutqRIvGXxAe8MvvOESbmZZ5mgA5AYrUHl2APDz6GxQM9FHPS17WX
8QA=
-----END CERTIFICATE-----
```

Certificate contents

- Domain name (common name)
- Public key
- Owner of certificate (subject)
- Issuer of certificate (CA)
- Expiration data
- Serial number

Types of Certificates

- Domain Validation – CA checks right of applicant to use domain name
- Organization Validation – CA does above + vets organization
- Extended Validation – CA does above + thorough vetting of organization

Basic Steps for Adding SSL

1. Generate a CSR (certificate signing request) at your web host
2. Buy a certificate from a vendor
3. Validate your domain/certificate
4. Send the CSR, certificate, and bundle files to your web host
5. Configure your site to use SSL
6. Upon renewal, repeat steps #1-41

RAPIDSSL CERTIFICATE

Starting at

$49.95

USD annually

- Dynamic VPS, Cloud & Flex Servers

- **Secure** Site Seal
- **256** Bit Encryption

GET RAPIDSSL

GLOBALSIGN ONECLICK ALPHA

MOST POPULAR!

Starting at

$49.95

USD annually

- Web Hosting, Managed VPS & Managed Dedicated

- **Secure** Site Seal
- **256** Bit Encryption
- **1-Click** Setup
- **Requires** cPanel

GET ALPHA

GLOBALSIGN ONECLICK DOMAIN VERIFIED

Starting at

$129.95

USD annually

- For our cPanel managed accounts

- **Verified** Domain
- **256** Bit Encryption
- **1-Click** Setup
- **Requires** cPanel

GET GLOBALSIGN

SSL Certificate Solutions

GLOBALSIGN ALPHA WILDCARD

Starting at

$149.95

USD annually

- **Secure** Site Seal
- **Unlimited** Subdomains
- **256** Bit Encryption
- **2048** Bit Key

GET ALPHA

GLOBALSIGN DOMAIN VERIFIED WILDCARD

MOST POPULAR!

Starting at

$449.95

USD annually

- **Secure** Site Seal
- **Unlimited** Subdomains
- **256** Bit Encryption
- **2048** Bit Key
- **Domain** Authentication

GET GLOBALSIGN

GLOBALSIGN ORGANIZATION VERIFIED WILDCARD

Starting at

$499.95

USD annually

- **Secure** Site Seal
- **Unlimited** Subdomains
- **256** Bit Encryption
- **2048** Bit Key
- **Organization** Authentication

GET GLOBALSIGN

Let's Encrypt

- Free, automated, open Certificate Authority
- Domain validation
- 3-month expiry

MAJOR SPONSORS

letsencrypt.org

Lets Encrypt Support

Providers that Enable Let's Encrypt and Redirect HTTP->HTTPS by Default

This is the best support of Let's Encrypt's mission ***"to create a more secure and privacy-respecting Web."***

- EasyStore.co 4.2k (Source 324)
- Inspedium Corp. 270 (Source 20)
- manitu 1.8k (Source 81)
- Neocities 2.5k (Source 137)
- Netsite 369 (Source 13) (*both in Danish*)
- Pride Tech Design 174 (Source)
- Shopify 397 (Source 97)
- Squarespace 2.5k (Source 254)
- Tumblr 130 (Source 32)
- WordPress.com 7.8k (Source 2.7k)
- XS4ALL 2.2k (Source)

Web Hosting Providers with Let's Encrypt Support

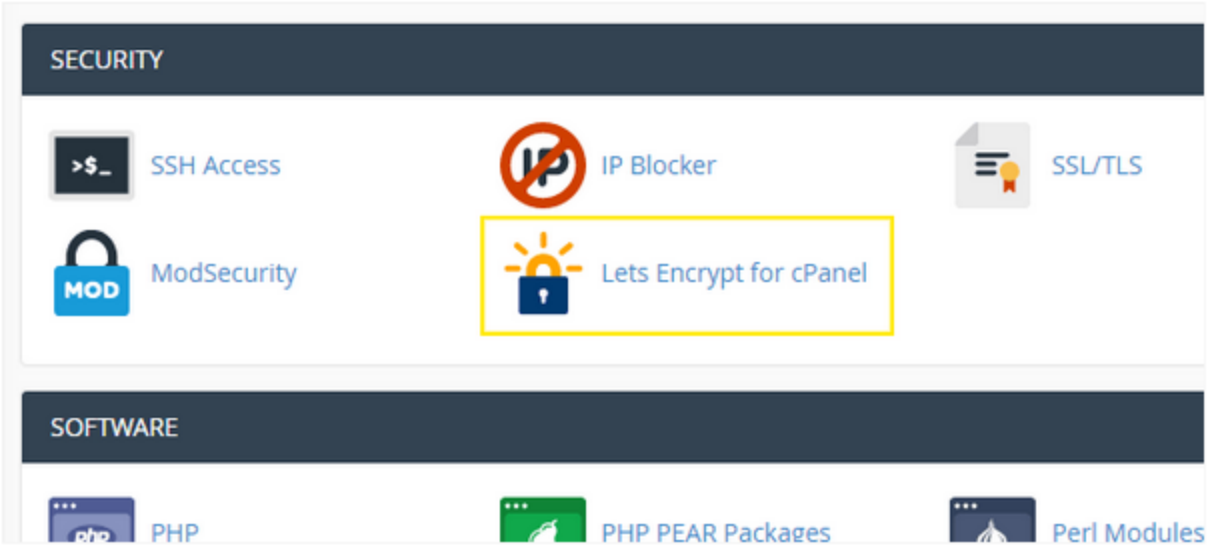
- 1and1.co.uk 691 (Source)
- 34SP.com 2.0k (Source 311)
- a2hosting.com 4.4k (Source 1.7k)
- Active24.co.uk 1.1k (Source 84)
- Active24.cz 624 (Source 144)
- all-inkl.com 1.8k (Source 629, more detailed instructions 1.7k) (*both in German*)
- Antagonist 446 (Source 67)
- Antilope Hosting 144 (Source 4)
- Apis Networks 628 (Source 57)
- blueboard.cz 552 (Source 39)

Full List goo.gl/1BsdZF

Lets Encrypt plugin for cPanel

Installing a Certificate

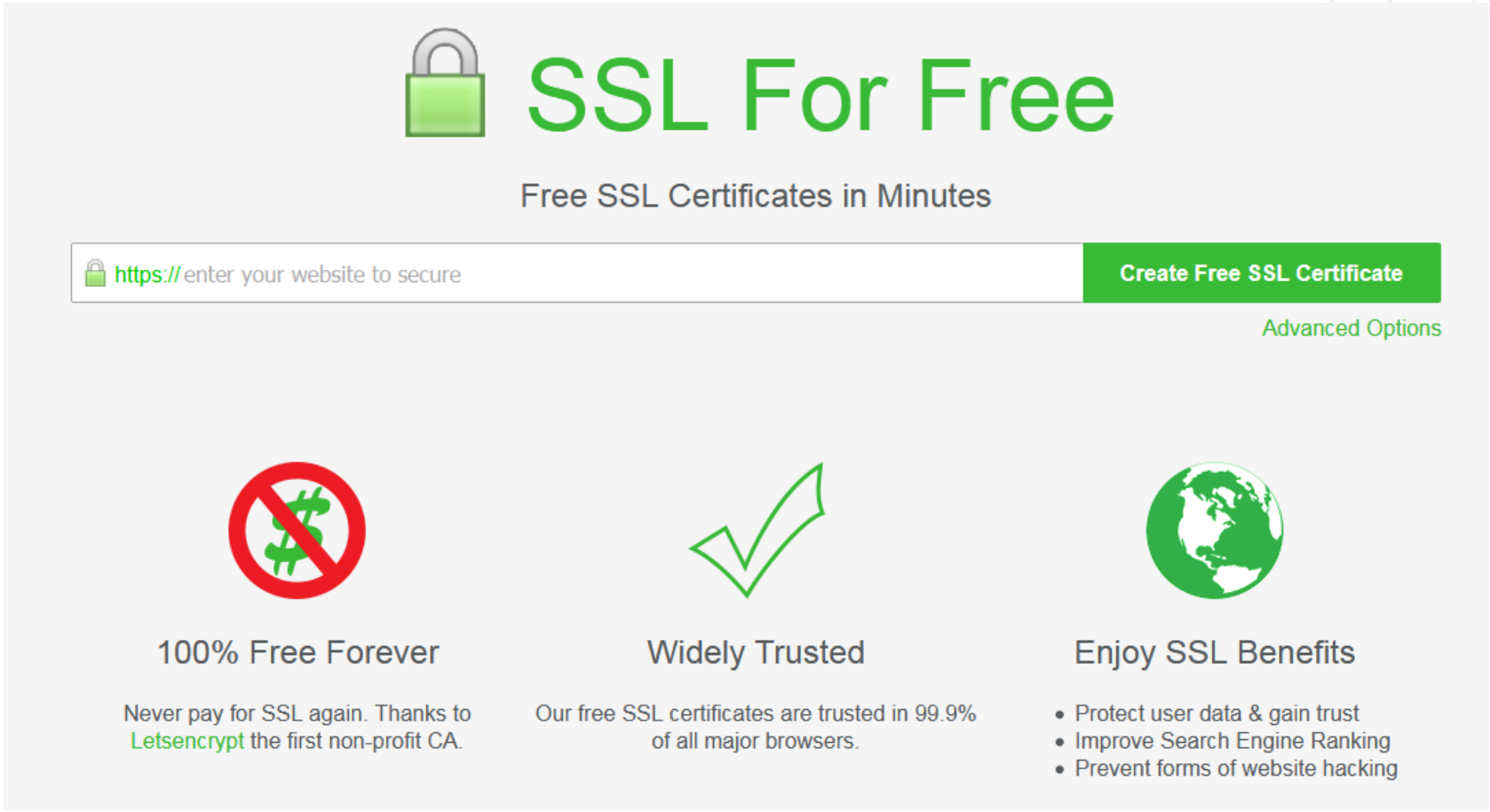
Once you're logged into cPanel, you should see a **Let's Encrypt for cPanel** button under **Security**. Click on it to access your active domains list to install a certificate.



All the issued certificates are *Cross-signed* by **IdenTrust**. In this way, all the L.E. certificates are trusted by major browsers.

Details: goo.gl/uHF8rS

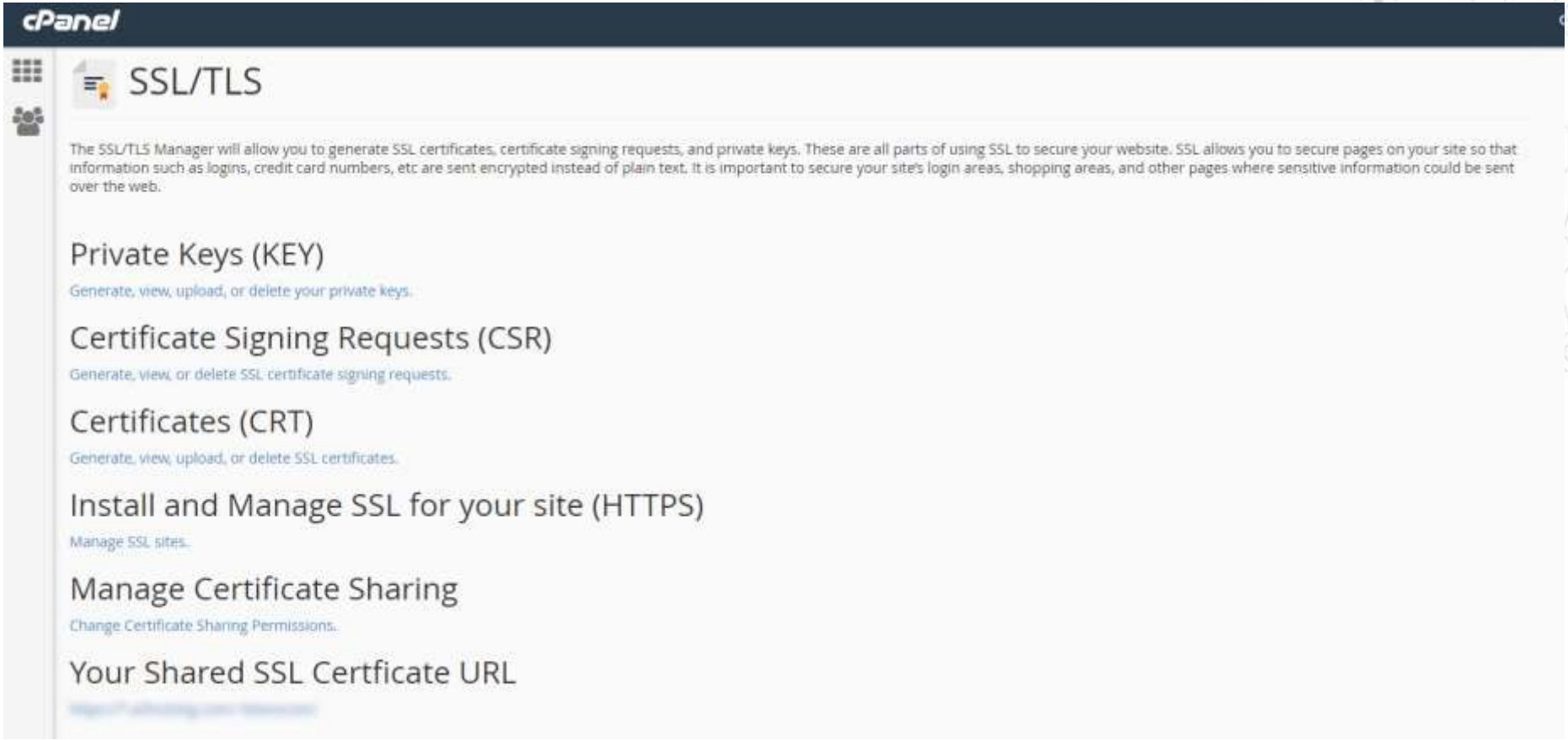
Tool for Generating Certificates in Minutes



Wildcard Certificates Supported? They are not supported but you can add up to 100 domains and or subdomains per certificate.

Details: sslforfree.com

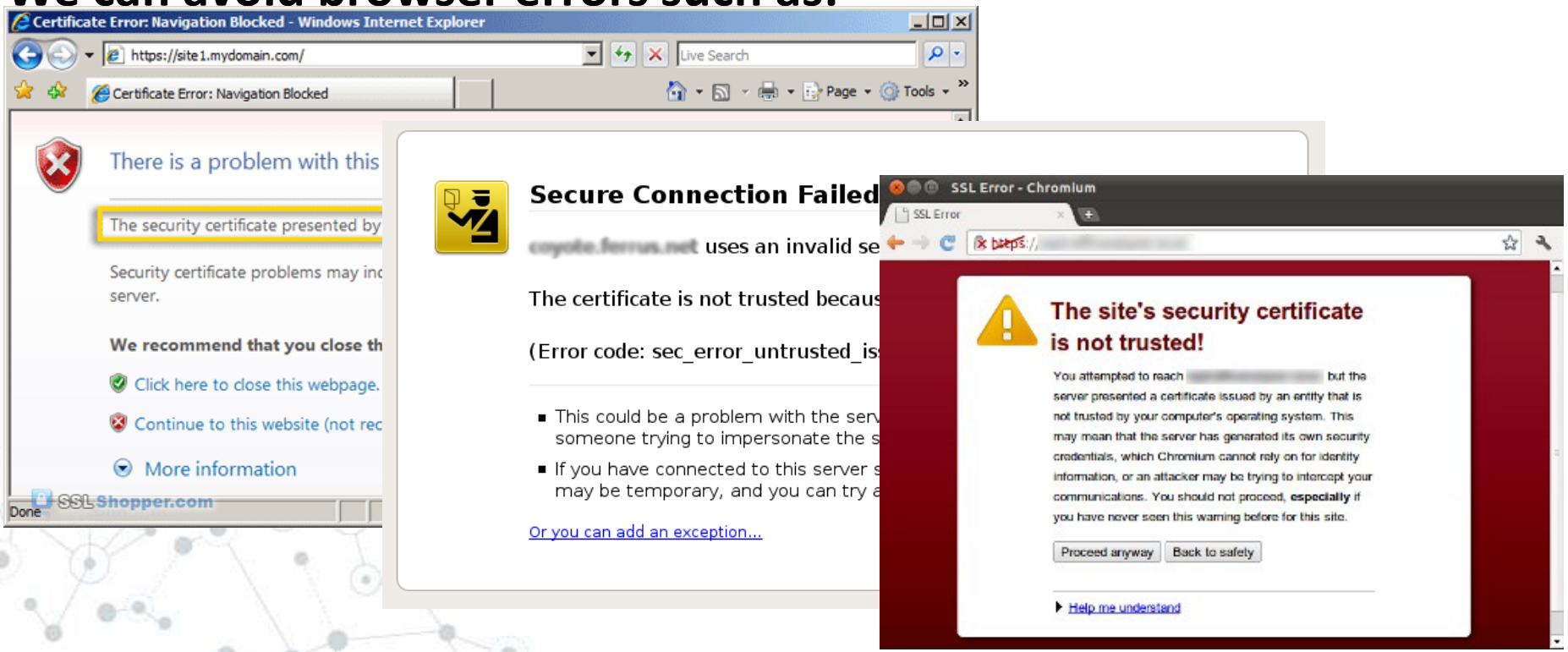
cPanel SSL/TLS Manager



Validity

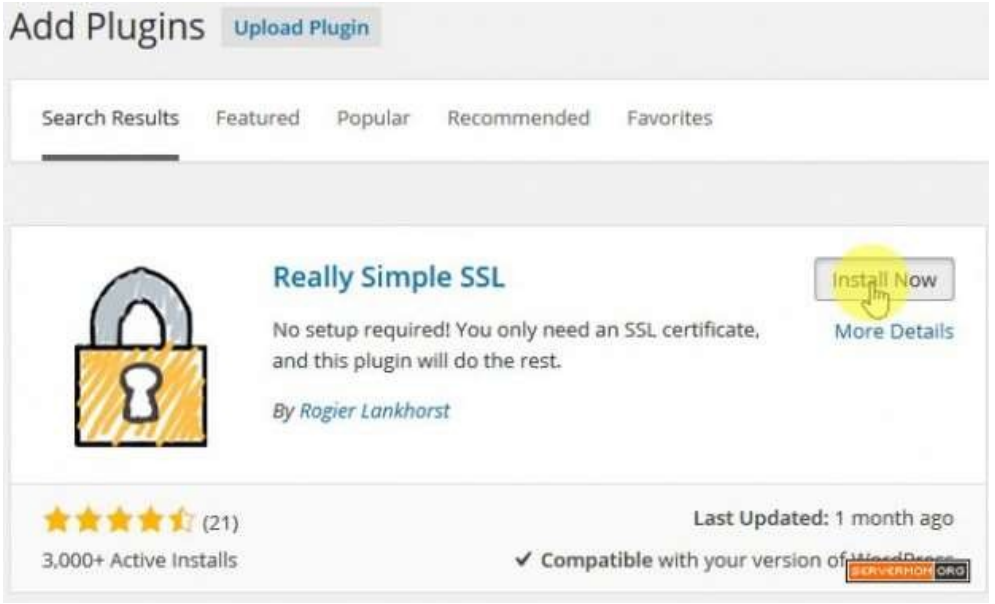
- Lets Encrypt certificates have a **90 days** validity. After the expiry, the certificates are not valid anymore and the browsers will raise security errors.
- You will receive *remind emails* whenever a certificate is near to expire. Certificate renewal can be automated with a **cron** task.

We can avoid browser errors such as:



WordPress SSL / HTTPS Tools

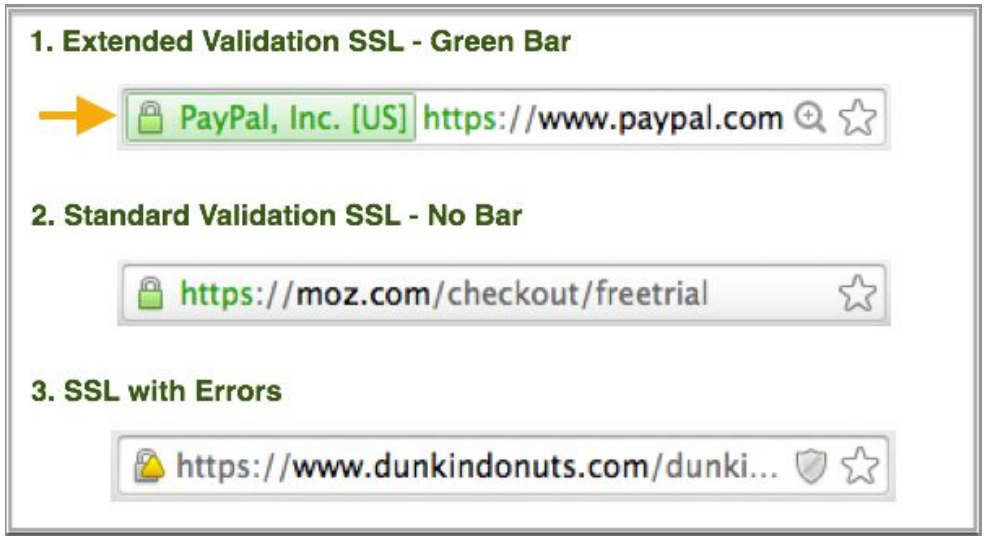
- Update Site URL from http:// to https://
- Force http requests to https



Why No Padlock?

Here's a simple tool that will tell you about any insecure items on your SSL page!

Why No Padlock?



whynopadlock.com

Removing SSL

- wp-config.php
- .htaccess
- Updating site URL (functions.php)

ssl-certificate-codes.txt | wp-config.php

```
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'economicblogs_db' );

/** MySQL database username */
define( 'DB_USER', 'economicblogs_db' );

/** MySQL database password */
define( 'DB_PASSWORD', '2dCZ9qArwq' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

define('FORCE_SSL_ADMIN', true);

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
```

Currently editing: /home2/bonzrco/public_html/.htaccess

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Thanks!

Demo Time and questions.