BKM: Security for the ReUse Project

By Jeffrey Schachtsick

March 9, 2017

Reticulum Team – Winter 2017

Introduction

This is a Best-Known-Method (BKM) for enabling Security for the ReUse Project with GoDaddy. This document is intended to give a very brief introduction on website security, as well as a how-to on how to setup security for a site on GoDaddy. This document is NOT intended to be an all-inclusive research on website security. Because security is quickly becoming a prominent and vast topic in the technology space, this document will probably just cover the tip of the tip of the iceberg of security.

Technology is constantly evolving and it is very difficult to achieve full-proof security. Staying current and making/maintaining a website with security in mind, can help prevent malicious activity to your site.

Why Security

The internet has data traffic that moves freely around the world. People from around the world use the internet to do such things as playing games with others, research on topics, and making bank transactions. To be able to do many of the things now, we need to give some information in order to get information. It is important a web service is communicating information through a secured and encrypted connection, so that it is not picked up by an intruder.

One of the reasons for having security is to protect the integrity of the web service. Persons who can be both malignant and benign can go to your site and attempt to exploit unprotected gaps in the site.

Another reason to consider security is to protect the users. A secure connection helps to prevent intruders from listening on communications between the user and the website. It is very important to have a secure website, especially when you are holding personal data such as name and credit card information.

What Makes a Secure Connection

Users of the internet, use a cooperative public data network of carriers who transmit data to different places. Back in the day, the original un-secure schema was to use hypertext transfer protocol (HTTP) to do all the transmissions in data. Now, we are doing so much more, that we need to have secure connection to ensure we have true connection to the intended destination.

To enhance security and privacy, more and more sites are making the switch to HTTP Secure (HTTPS). You can sometimes notice the difference between the two when you visit a site and you see 'https', a green lock, or something in the URL prior to the address. Such is the example below on Google Chrome with going to www.godaddy.com there is a green lock, 'GoDaddy INC. [US]' can be clicked to view the certificate, and 'https' is at the front of the URL.

When you have something like above, this means you have a security certificate and a key from the website, ensuring you have reached your intended destination. This ensures privacy and data integrity between the two communication end points. To be able to make communication with the certificate, a secured connection known as Secure Sockets Layer/Transport Layer Security (SSL/TLS) are used to securely communicate between the user and the web service.

How to secure with GoDaddy

The following below, is a short tutorial to setting up generating an SSL site. As of the writing of this tutorial, the writer of this document is unaware of the GoDaddy subscription used for the ReUse Project. No attempt was made on testing this tutorial with the ReUse Project. Also, it is possible GoDaddy or cPanel can make changes to the interface making directions obsolete.

It is best to contact GoDaddy assistance to ensure setting up SSL for the ReUse Project will not incur extra charges to the organization without first approval.

1. Login to the godaddy account.
2. Click on 'Manage' button for the 'WEB HOSTING'

3. Click on the 'Manage' button for the ReUse Project (app.sustainablecorvallis.org).
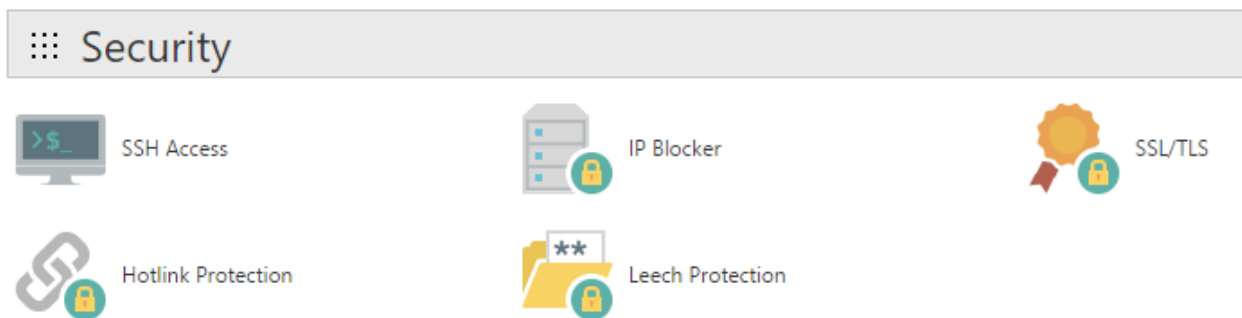

app.sustainablecorvallis.org

Up and running with no issues.

Manage   **Settings**

cPanel North America

4. Scroll down to the 'Security' section and click on the 'SSL/TLS' button.

5. This should take you to the 'SSL Manager'. GoDaddy may not label this page as such, but as you navigate around to do the next tasks the links will direct you back to this page. You will need to generate a Private Key and a CRT.

   a. Under the heading 'Private Keys (KEY)', click the link 'Generate, view, upload, or delete your private keys.'

   b. A new page will load and under the heading, 'Generate a New Private Key', fill in the form and then click the 'Generate' button.

   c. Another page will display with your private key. NOTE: the private key could be saved to be used later or you will need to copy the private key data to be used later.

   d. Get back to SSL Manager.

   e. You will need to generate a certificate for your SSL. Under the 'Certificates (CRT)' heading, click on 'Generate, view, upload, or delete SSL certificates'.

f. Under the 'Generate a New Certificate' heading, fill out the form. Then when finished, click the 'Generate' button.

g. Upon completion, should take you to a new page where it will display your CRT data. NOTE: the CRT could be saved to be used later or you will need to copy the CRT data to be used later.

6. An SSL/TLS page will appear. Under the Install and Manage SSL for your site (HTTPS), click on 'Manage SSL sites'.

7. Fill out the form under the heading 'Install an SSL Website' ensuring your CRT and Private Key are in the form fields. Click 'Install Certificate' when completed.

8. You should then get confirmation of installation. Next is to ensure the site now has a security certificate when the site is loaded and also has 'https'.

References

1. Urlscan.io, March 8, 2017, https://urlscan.io/about/
2. GRC "Fingerprints", March 8, 2017, https://www.grc.com/fingerprints.htm
3. Transport Layer Security, March 8, 2017, https://en.wikipedia.org/wiki/Transport_Layer_Security
4. 'Why HTTPS Matters', Kayce Basques, Google, March 8, 2017, https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https
5. 'Installing a Godaddy SSL Certificate in WHM cPanel', CreatingaWebstore, March 8, 2017, https://www.youtube.com/watch?v=7nChK01UKks.