Open Standards Everywhere

Technical User Implementation of Secure Open Internet Standards Across a Web Server

@Andrew Muturi, Internet Society Kenya Chapter

Introduction

This document has not been entirely created from scratch. There will be reference to other existing excellent tutorials on this topic and their links have been attached. The documentation has been developed and tested on web servers running Debian OS and either Apache or NGINX. For TLS security Let's Encrypt certificates have been used.
NB:
For shared hosting packages, the user will have to reach out to the provider to implement some of these changes.

1. Install Apache on web server
Use this link for a step by step process:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-lamp-stack.md

2. Install NGINX on web server
Use this link for a step by step process:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-lemp-stack.md

3. IPv6 Support on web server
Use this link for a step by step process to enable support over Apache Web Server:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-ipv6-apache.md

Use this link for a step by step process to enable support over NGINX Web Server:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-ipv6-nginx.md

Use this link for a step by step process to enable support over a CDN Web Server:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-ipv6-cdns.md

4. DNSSEC Support
This implementation might require the domain registry client to enable this as it does not come set by default. To enable use this link:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-dnssec-apache-nginx.md

5. TLS / SSL enablement

i. Apache
   a) Use this link to enable and upgrade to the most recent secure version: https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-1-3-apache.md
   b) Use this link to disable the lower phased out versions: https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-versions-apache.md

ii. NGINX
   a) Use this link to enable and upgrade to the most recent secure version: https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-1-3-nginx.md
   b) Use this link to disable the lower phased out versions: https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-versions-nginx.md

6. TLS / HSTS

For Apache, use this link:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-hsts-apache.md

For NGINX, use this link:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-hsts-nginx.md

In instances where the above does not work use the below:
TLS (SSL) uses multiple cryptographic ciphers for encryption and digital signatures – Implement version 1.2 and 1.3

For Apache, edit options-ssl-apache.conf
i. Find SSLProtocol line and set it to:
   a) SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
   b) Save file and restart apache

For NGINX, edit options-ssl-nginx.conf
i. Find SSL_protocols line and set it to:
   a) SSL_protocols TLSv1.2 TLSv1.3
   b) Save file and restart NGINX

7. Cipher order

On Apache, use the below link:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-cipher-order-apache.md

On NGINX, use the link:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-cipher-order-nginx.md

8. Security Headers

On Apache, use the link below:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-cipher-order-nginx.md

On NGINX, use the link below:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-http-security-headers-nginx.md

9. HTTPS/2

On Apache, follow the link:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-http2-apache.md

On NGINX, follow the link:
https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-http2-nginx.md

About the author

Andrew Muturi is an ICT Consultant at Inscap Associates, where he advices on best Information Security Practices for the diverse clients as well as engaging in audit services from start to finish. Andrew had worked with reputable global investment firms, Fin-Tech startups as well as SME's among others.

Andrew helps companies to formulate better technical roadmaps that fit best within their business scope, budget and goals. He is a member of professional member bodies like ISOC and ISACA. He is quite focused on lean startups, innovation and technology for change.

The Internet Society

Internet Society Kenya Chapter is an Internet technical community chartered by the Internet Society and registered in the Republic of Kenya. It seeks to provide leadership on Internet policy, technology standards and future development of the Internet in Kenya. The Chapter establishes and promotes principles that are intended to persuade governments and other stakeholder to make decisions that are right for the citizens and the nation's future.

Internet Society is the world's trusted independent source of leadership for Internet policy, technology standards, and future development. The Society has for many years been the champion for Internet advancement and open resource usage. More than simply advancing technology, we work to ensure the Internet continues to grow and evolve as a platform for innovation, economic development, and social progress for people around the world.

Preparing a new generation to succeed as Internet technology, policy, and business leaders is a key objective for the Internet Society. To be successful, the next generation of Internet leaders will require a wide range of skills in a variety of disciplines as well as the ability and experience to work with people at all levels of society.

For more information, please visit the Internet Society Kenya Chapter website at:
www.internetsociety.ke
Follow us: @ISOC_Kenya