Abstract

The government of Tanzania has been adopting various web-based systems to improve public services to its citizens. With these systems being online, security and privacy have started to play a key role. Many systems use HTTP over Transport Layer Security (HTTPS) to secure their web front ends. However, many HTTPS implementations still suffer from several security and privacy problems. This study investigated the security of HTTPS implementations government web-based systems in Tanzania. Using a sample of 74 government web-based systems, an automated tool testssl was used to check for well-known HTTPS/SSL vulnerabilities, configuration mistakes, support for outdated and vulnerable protocols, and adherence to HTTPS best practices. Results show that 43% of web systems have serious HTTPS security issues due to vulnerabilities, and configuration mistakes. These issues can lead to system compromise, disclosure of sensitive information, and loss of privacy to citizens. The study highlights these security issues that may have been overlooked and offers suggestions that may prevent them in the future.
References

11. Thai Duong. BEAST, 2011.
23. Qualys. SSL Server Test (Powered by Qualys SSL Labs), 2017.
26. Ivan Ristic. SSL 3 is dead, killed by the POODLE attack — Qualys Blog, 2014.

Index Terms

Computer Science    Security
Keywords

Web Security, HTTPS, TLS/SSL, e-Government