QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

Website Security - TIP-12-298-01

Every community organization, corporation, business, or government agency relies on an outward-facing website to provide information about themselves, announce an event, or sell a product or service. Consequently, public facing websites are often the most targeted attack vectors for malicious activity. Web server attacks include:

- Exploitation of software bugs in the Web server
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks
- Compromising "backend" data through command injection attacks, such as Structured Query Language (SQL) injection; Lightweight Directory Access Protocol (LDAP) injection; and cross-site scripting (XSS)
- Website defacement for malicious purposes
- Using compromised Web server capabilities to attack external entities
- Using a compromised Web server to distribute malware.

There are a number of challenges associated with securing a Web server because not only does the operating system need to be secured but so do the associated Web applications and services running on the device. One of the most difficult aspects is often keeping abreast of new and emerging vulnerabilities to both the Operating system and the Web applications as well as keeping those systems patched and up to date.

This TIP provides basic guidelines and security safeguard concepts that can be applied to public facing websites to reduce the attack surface area or mitigate the effects of a compromise.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- WebsiteSecurity.pdf