US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Technical Information Paper TIP-12-298-01

Website Security

Huyen Vu, Quentin Caboga, Chris Hallenbeck

October 24, 2012

Introduction

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.

Mitigation Strategies

The purpose of this document is to provide 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. It is recommended that organizations routinely conduct a risk assessment on their environment to identify weaknesses or vulnerabilities. For assistance in conducting a risk assessment see the National Institute of Standards and Technology (NIST) Special Publication 800-30 "Guide for Conducting Risk Assessments".

- **Web Server Security:**
  - Recommended web server security.
    - Ensure that web server host systems are built with only essential applications and components required to perform their intended functions. All other applications should be removed or disabled. For example, a web server does not require web browsing capability and if a web server is not performing FTP functionality there is no need to have that service running. Removing or disabling any unused components will reduce the attack surface area.
    - Web servers should be designed with very strict access to any back end data.
    - Web SQL services:
      - Prevent applications from connecting to databases with privileged access.
      - Validate input for length, range, format, and type.
      - Restrict input to lists of acceptable characters and deny any other characters not on the list.
      - Limit the use of dynamic SQL code. Use prepared statements, queries with parameters, or stored procedures whenever possible.
  - Recommended Operating System Security:
    - Accounts that enable access to the underlying operating system of the web server should follow the concept of least-privileges and should not be unique for each individual. A single admin account will prevent non-repudiation of activity and limit forensic capabilities if a compromise occurs. Also, a web server should be considered a critical service and thus should require two-factor authentication.
    - Enforce a strong password creation policy for administrators such as:
      - Minimum password length of 15 characters for privileged accounts.
      - Use of strong passwords requiring alphanumeric, uppercase, lowercase, and special characters.
      - Require recurring password changes at least every 90-180 days.

        - Enable password history limits to prevent the reuse of previous passwords.
        - Prevent the use of personal information in usernames and passwords, such as phone numbers, date of birth, and first name [dot] last name.
        - Require the use of passphrases instead of passwords.
    - Change all default usernames and passwords.
    - Disable or delete all unused accounts such as Guest accounts.
    - Disable credential caching for critical systems if possible.
  - Keep web servers patched and up to date.
  - Monitor mailing lists and/or websites for security related announcements.
  - Web servers should be built on isolated hardware or on secure multi-tenant virtualized technology with direct communication to potential other virtualized guests disabled. This can potentially help limit the damage or compromise of multiple services if a single service is attacked as well as reduce the attack surface area of a single service.
  - Employ web authentication and encryption technologies such as SSL/TLS based upon the nature of web server data (e.g. sensitive, private, confidential, etc.).

Employ revision control processes to document all changes being made to the system, application, or web content.
Further guidance is available in NIST Special Publication 800-44 Version 2 "Guidelines on Securing Public Web Servers".

- **Secure Web Services:**
  Below is a list of possible mitigations an organization can consider to further secure web services and applications. Not all items will be applicable to all organizations, a balance must be struck between the cost benefits provided by each mitigation and the potential risk an organization is willing to accept for their web services. See NIST Special Publication 800-95 "Guide to Secure Web Services" for more information.
  - **Enable extensive logging** and collect the IP address of the system accessing the service, the username, the resource accessed, account privilege changes, whether the attempt was successful or not, and other potential suspect activities. Unusual/questionable access must be reported immediately and will require investigation.
  - **Data service replication** – DoS and DDoS attacks are not new, but they are still occurring and have become a favorite attack method of some groups, so it is in the best interest of any organization to have applications and data replicated or backed up on a recurring basis, preferably to an offline storage location. Offline backup storage will help prevent tampering of the data and applications as well as provide redundancy in the event that the data and applications need to be moved to other platforms.
  - **Logging services** are critical to provide non-repudiation and accountability for any transaction preformed on a server. Logging is also critical in identifying malicious activity after a compromise has occurred as well as potentially identifying malicious activity that is occurring. How much logging to enable and how often to archive the logs will be determined by how much storage space is available in your environment

as well as how active your network is. Additional services or software may be required to support the level of security and accountability and non-repudiation that your environment requires.

- **Secure software development and design –** Secure software development is one of the most critical aspects in application security, simply because the less built-in vulnerabilities that any application has the less likely it is to be compromised. NIST suggests the use of threat modeling and risk analysis to identify weaknesses in software. Open Web Application Security Project (OWASP) has a number of documents on secure coding techniques and methodologies freely available, as well as a best practices guide on the top 10 attacks attackers are most likely to use. Another aspect of secure software is maintaining the security of the software. This can be accomplished through recurring patching and monitoring the National Vulnerability Database for any new vulnerabilities, or signing up for the US-CERT weekly vulnerability bulletins.
- **Securing web server infrastructure –** Web servers should be located inside a secure Demilitarized Zone (DMZ) structure with one-way trust relationships configured to have the DMZ trust the internal network, but the internal network not trusting communications from the DMZ. Also consider restricting any communications or requests from web servers to internal resources.

In conclusion, web servers and services are responsible for providing web content and are a necessary component for many business and organizations. The extended loss of these services can have catastrophic results. Because of this it is essential to treat these services as essential and protect them as such.

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov
Voice: 1-888-282-0870
Incident Reporting Form: https://forms.us-cert.gov/report/

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/