CANADIAN CENTRE FOR CYBER SECURITY

UNCLASSIFIED

Security Considerations When Developing and Managing Your Website

NOVEMBER 2021 | ITSAP.60.005

Your website is a critical component of your business; it provides access to your services and visibility of your products. However, cyber threats can compromise your website, harming your business functions, revenue, and reputation. To reduce the likelihood and impact of threats, you should develop and maintain your website with security in mind. Below, we've included a few security and privacy protection measures to get you started, but you can find more information in *ITSM.60.005 Security Considerations for Your Website*. For more cyber security tips and best practices, visit our website at cyber.gc.ca.

THREAT EXAMPLES

The list below includes some common threats to be aware of when developing and maintaining your website.

- **Injection attacks**: A general term for any exploitation in which a threat actor provides an untrusted input (e.g. injects malicious code) into a system to modify operations or data.
- **Cross-site scripting (XSS) attacks:** A threat actor uses XSS to compromise a web server and inject malicious code into trusted websites. When users visit the website, their browsers execute the script, putting cookies, session tokens, or sensitive information at risk. XSS attacks exploit the trust that a user has in a website.
- **Cross-site request forgery (CSRF) attacks:** An attack that tricks users into executing unwanted actions in their browsers, such as logging out, downloading account information, or uploading a site cookie. CSRF attacks exploit the trust that a website has in a user's browser.

If your website is compromised, your organization is not the only one at risk; threat actors can also target your supply chain, affiliated organizations, and customers.

Your website is the gateway between the Internet and your organization. Threat actors can exploit vulnerabilities and misconfigurations to steal, alter, or delete sensitive data (e.g. vendor portals, customer data, sales leads, operational and financial information). Stay one step ahead by reviewing the following aspects of your website. If using a hosting service, you should discussion each of the topics below with your service provider.

SECURE ARCHITECTURE

Your website's architecture (e.g. its elements, relationships, selected components, and design principles) should be secure. You should apply principles like segregation and redundancy.

Segregate your web service components. If one component is compromised, the other components are protected because they have been segregated. You should also segregate your application server and database to protect sensitive data.

You should design your website to add redundancies in your web service components (i.e. replicate them). With redundancies, you can ensure that your operations continue if one component fails.

Require the use of HTTPS by default on your website to ensure sensitive data, like authentication data and propriety information, is encrypted in transit. HTTPS uses the Transport Layer Security (TLS) protocol to encrypt and authenticate web page visits.

AUTHENTICATION

Authentication refers to the mechanisms used to validate a user's identity.

Implement a strong password policy that includes multi-factor authentication (MFA) for additional security. Never send passwords in plaintext over the Internet. Instead, use hashes and encryption.

After a threshold of unsuccessful login attempts, lock accounts and delay logins. Ensure you have a secure account recovery process.

ACCESS CONTROL

Access controls define who can access what resources on your website and restrict what information they can see and use. Define specific access controls and implement the principle of least privilege to ensure that users only have the access needed to carry out their authorized functions.

Consider all web application access control layers (e.g. application presentation layer, data layer) and the following types of permissions: URL-based, file system and server, application business logic (i.e. what the user can do). Identify access control layers in your coding standards and rigorously test them before deploying your web services.

SERVICE PROVIDERS

If using a service provider, you may not have access to the infrastructure or control over the associated security functions. However, even when using a service provider, your organization is still legally responsible for protecting the confidentiality and integrity of your data.

Before contracting a service provider, review their data security and privacy protection capabilities and policies. Clearly define your organization's and your service provider's roles and responsibilities with regards to security. You can use the sections in this document to guide your discussion with a service provider on their security capabilities.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Cat. No. D97-1/60-005-2021E-PDF | ISBN 978-0-660-40248-2

INPUT VALIDATION

Input validation is the process of verifying that users and applications can only input properly formed data, such as in fields, forms, or queries.

All inputs on your website should be considered untrusted. Validate inputs within your web services, including those in the following areas: client browsers, web application firewalls, web servers, databases, and application business logic. You should validate inputs as early as possible in the processing process to reduce strain on your servers. Test input validation during your development process.

Inputs should also be controlled. Enforce expected input lengths to weed out invalid values and limit free-form inputs to minimize the risk of script injection. Hide structured query language (SQL) error messages from end users, as these messages contain valuable information about your database.

SECURE CONFIGURATION

Although vendor-recommended security configurations generally provide a good baseline, these defaults may not provide the level of security needed to protect your systems and data from cyber threats. Be sure to review configurations to identify any vulnerabilities (e.g. unused ports or services, unprotected files or directories).

You should turn off directory browsing, as it provides insight on your website's structure. Remove any unnecessary web operation files (e.g. source code or back-up files that could contain passwords). Disable browser credential caching. Although credential caching is convenient for users, it can put sensitive information at risk.

You should implement configuration management to promote secure coding and maintain baselines across your organization.

SESSION MANAGEMENT

A session is an exchange of information between two or more entities, such as two devices or a user and a web server. Session management is the process of initiating, controlling, maintaining, and ending these exchanges. If sessions aren't handled securely, threat actors can interrupt or hijack sessions to intercept data or impersonate authenticated users.

Randomize your session identifiers to prevent threat actors from inferring session identifier sequences. Session identifiers should have an acceptable minimum length to protect against brute force attacks.

Store sensitive session tracking data on web service servers with an appropriate retention period and destroy it at the expiry date. Expire session data when a user logs out or is inactive for a specified time.

Session cookies, also known as in-memory cookies, allow users to be recognized while they navigate the website (e.g. items stay in their carts). Use the secure cookie attribute to prevent cookies from being sent over an unencrypted channel.

SECURE OPERATIONS

Once your website is running, you need to prevent, identify, and respond to cyber threats and incidents. You should continuously monitor website activity for anomalous behaviours, such as repeated log-in or injection attempts. For example, in credential stuffing attacks, threat actors use leaked or stolen credentials and "stuff" them into log-in pages of other websites until matches are found.

To promote the ongoing security and functionality of your web services, implement a patch management process to acquire, test, and install patches and updates on your systems and devices. Be sure to patch underlying systems, content management systems, web applications, and plug-ins.

You should also promote security awareness within your organization and with your customers. With greater transparency of the steps that you are taking to protect data, you can foster trust with your partner organizations, supply chain, and customers.

REPORT AN INCIDENT

If your organization is a victim of fraud, contact your local police and file a report online through the Canadian Anti-Fraud Centre's online reporting system.

LEARN MORE

The Open Source Web Application Security Project (OWASP) has a list of the Top 10 Web Application Security Risks.

For our complete catalogue of guidance publications, visit cyber.gc.ca. Some related publications include:

- *Website Defacement (ITSAP.00.060)*
- *Managing and Controlling Administrative Privileges (ITSAP.10.094)*
- *Secure Your Accounts with Multi-Factor Authentication (ITSAP.30.030)*
- *Protecting Your Organization Against Denial of Service Attacks (ITSAP.80.100)*

Communications Security Establishment   Centre de la sécurité des télécommunications

Cat. No. D97-1/60-005-2021E-PDF | ISBN 978-0-660-40248-2

Canada