Security Tips for OA Websites

While it is relatively easy to create a website, security and maintenance can push the limits of a service body's capability. First, using a reputable *website builder* can help because the builder will release regular security updates. Second, it is critical that everyone with access to your website use a complex (strong) password and two-factor or multi-factor authentication to log in.

User accounts

- Change all passwords to complex (strong) passwords.
- Delete accounts for all past users.
- Require two-factor or multi-factor authentication for all users.

WordPress *(tips may apply to other website builders)*

- Change and hide the login URL (Uniform Resource Locator) from the default **/wp-login.php** or **/wp-admin/** to a custom, hidden URL. Example: Use the "WPS Hide Login" plugin.
- At your discretion, disable editing of the website theme and plugins through the theme editor and plugin editor.

Web applications

- Implement a secure password feature in the web application.
- Users must use complex (strong) passwords.
- Make sure appropriate file permissions are set up in the web application installation process.

MySQL

- User accounts used to access the database via the web application should have limited privileges to execute SQL (Structured Query Language) commands and should not be a root-level user.
- Only allow trusted administrators access to a MySQL root user account.

Web server

- Revisit all users and passwords for the web server account.
- Only give web server (e.g. Apache) users on the server "write access" (e.g. file uploads) to any public directory.
- Limit administrative server access, which gives direct access to the server. This generally takes one of two forms: a user account on the server accessed either over SSH (Secure Shell) or via SFTP (Secure File Transfer Protocol). SSH access is strongly preferred, where only users with valid SSH keys can access the server and password access is disabled. SFTP is vulnerable and can be gained with access to the host account.

Repository (e.g., Github)

- Use a private repository to limit access to the codebase.

OA Responsibility Pledge

Always to extend the hand and heart of OA to all who share my compulsion; for this I am responsible.

OA Board-approved. Overeaters Anonymous®, Inc.
6075 Zenith Court NE
Rio Rancho, New Mexico 87144-6424 USA
Mail Address: PO Box 44727, Rio Rancho, NM 87174-4727 USA
Tel: 1-505-891-2664 • info@oa.org • oa.org
© 2023 Overeaters Anonymous, Inc. All rights reserved.