Top ways websites get hacked by spammers

Understanding how your site was compromised is an important part of protecting your site from attacks. In this article, we will cover some security vulnerabilities that can result in your site being compromised.

Compromised passwords

Attackers can use password guessing techniques by trying different passwords until they guess the right one. Password guessing attacks can be conducted through various methods such as trying common passwords or scanning through random combinations of letters and numbers until the password is discovered. To prevent this, create a strong password that is difficult to guess. You can find tips for creating a strong password in Google's help center article.

There are two important points to remember. First, it's important to avoid reusing passwords across services. Once attackers are able to identify a working username and password combination, they will try to use the username and password combination on as many services as possible. Therefore, using different passwords on different services can prevent other accounts on other services from being compromised.

Second, take advantage of two-factor authentication (2FA) like Google 2-Step Verification if the option is available. 2FA allows a second layer of login credentials, usually via a text message code or other dynamically generated pin, that diminishes an attacker's ability to access your account with just a stolen password. Some CMS providers have guidance on configuring 2FA: see documentation for Joomla!, WordPress, or Drupal.

Missing security updates

Older versions of software can be affected by high-risk security vulnerabilities that enable attackers to compromise an entire site. Attackers actively seek out old software with vulnerabilities. Ignoring a vulnerability on your site increases the chance of your site being attacked.

Note: It's essential to periodically check for software updates for your site in order to patch vulnerabilities. Better yet, set up automatic updates for your software where possible and sign up for security announcement lists for any of your active running software.

Some examples of software to you'll want to keep updated include:

- Web server software, if you run your own servers
- Content Management System. Example: security releases from Wordpress, Drupal, and Joomla!.
- All plugins and add-ons you use on your site

Insecure Themes and Plugins

Plugins and themes on a CMS add valuable, enhanced functionality. However, outdated or unpatched themes and plugins are a major source of vulnerabilities on websites. If you use themes or plugins on your site, make sure to keep them up to date. Remove themes or plugins that are no longer maintained by their developers.

Be extremely cautious of free plugins or themes from untrusted sites. It's a common tactic for attackers to add malicious code to free versions of paid plugins or themes. When removing a plugin, make sure to remove all its files from your server rather than simply disabling it.

Social engineering

Social engineering is about exploiting human nature to bypass sophisticated security infrastructure. These types of attacks trick authorized users into providing confidential information such as passwords. For example, a common form of social engineering is phishing. During a phishing attempt, an attacker will send an email pretending to be a legitimate organization and request confidential information.

Caution: According to a study from Google about social engineering, some of the most effective phishing campaigns have a 45% success rate!

Remember never to give out any sensitive information (e.g. passwords, credit card numbers, banking information, or even your date of birth) unless you're sure about the requestor's identity. If your site is managed by several people, consider providing training to raise security awareness against social engineering attacks. You can refer to the Gmail Help Center for basic phishing protection tips.

Security policy holes

If you are a system administrator or run your own site, remember that poor security policies can allow attackers to compromise your site. Some examples include:

- Allowing users to create weak passwords
- Giving administrative access to users who don't require it
- Not enabling HTTPS on your site and allowing users to sign in using HTTP
- Allowing file uploads from unauthenticated users, or with no type checking

A few basic tips to protect your site:

- Ensure your website is configured with high security controls by disabling unnecessary services
- Test access controls and user privileges
- Use encryption for pages that handle sensitive information, like login pages
- Regularly checking your logs for any suspicious activities.

Data leaks

Data leaks can happen when confidential data is uploaded and a misconfiguration makes that confidential information publicly available. For example, error handling and messaging in a web application can potentially leak configuration information in an unhandled error message. Using a method known as "dorking", malicious actors can exploit search engine functionality to find this data.

Ensure that your site doesn't reveal sensitive information to unauthorized users by conducting periodic checks and restricting confidential data to trusted entities through security policies. If you do happen to discover any sensitive information displayed on your site that urgently needs to be removed from Google Search results, you can use the URL removal tool to remove individual URLs from Google Search.

Last updated December 22, 2017.