Glossary for hacked sites

The glossary covers a collection of technical terms that are referenced throughout our security documentation. The list is ordered alphabetically with each term in bold text followed by a definition of the term.

Administrator privileges

Administrator privileges are the highest level of permission account setting on a system. These type of privileges allow actions like deleting the entire site, resetting passwords, or uploading files.

Back door

A back door is a program installed on a system to bypass authentication controls and maintain access.

Cloaking

Cloaking is the practice of presenting different content or URLs to human users and search engines.

For example, dynamic scripts and .htaccess rules can return status codes based on the requests processed. Using this tactic, hackers hide their tracks by returning a 404 or 500 error code to certain IP addresses or browsers, while serving spam to other IP addresses or browsers.

Configuration files

Configuration files are used to store information like database location and credentials for dynamic sites.

Content Management System (CMS)

Content management systems are software packages that help users easily create and edit websites. Examples include WordPress, Drupal, and Joomla!, though there are many others, including some that are custom-built.

Digital forensic specialists

Digital forensic specialists are people or teams that can help you clean your site and identify how your site was compromised.

Static web page

A static web page has a single, constant file that displays content for a website.

Dynamic web page

A dynamic web page uses scripts to generate content on the site. A dynamic web page uses software to generate pages each time they are requested, using a combination of scripts and templates to place content.

`eval()`

In PHP and JavaScript, `eval()` is a function that evaluates a string and returns the result. Eval functions are discouraged when a site deals with user input because it opens a vulnerability that allows attackers to sneak in malicious code (i.e. the injection of harmful PHP commands).

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a protocol used to transfer files from one machine to another.

Hidden files

Hidden files are files that don’t show up in a directory by default. Typically, files like .htaccess are hidden to protect important information from being accidentally modified. You need to configure your filesystem to allow you to see and edit hidden files.

HTTP Status Codes

HTTP Status codes are standardized responses that web servers return along with content when users try to interact with a page, e.g. loading a page or submitting a comment. These codes help users understand how the website is responding or identify errors. Refer to the

World Wide Web Consortium’s Status Code page for a full list of status codes and what they mean.

iFrame

An iFrame allows a web page to display content from one page within another. Hidden iframes are a common tactic used by hackers to redirect users to their sites.

Log file

Log files are files where web servers record user requests to keep track of all activities performed on the server. You can identify hacking attempts or suspicious traffic to your site by looking through log files.

Malware

Malware is any software specifically designed to harm a computer, the software it is running, or its users. Learn more about malware.

Obfuscation

Obfuscation is a tactic used to confuse people interpreting code by making the code harder to read. Common obfuscation methods by hackers include character substitution, intentionally confusing variable names, using encodings like `base64`, `rot13`, `gzip`, url encoding, hex encoding, or a combination of them. Sometimes these methods, such as `base64` and `gzip`, are also used to compress and hide large amounts of code, like entire web shells.

Phishing

Phishing is a form of social engineering that tricks users into giving away sensitive information (for instance, user names or passwords) by masquerading as a trusted source. For example, a phisher will email a potential victim pretending to be their bank and ask for their bank account credentials. Learn more about phishing.

Search Console

Google Search Console is a free service offered by Google that helps you monitor and maintain your site's presence in Google Search results. Google also uses Search Console to communicate with webmasters about website issues. Learn more about Search Console.

Sitemap

A sitemap is a file containing a list of web pages on a site that informs search engines about the organization of the site’s content. Learn more about sitemaps.

Social engineering

Social engineering is a technique for gaining access to or control of sensitive information by trying to trick people into providing access rather than attacking the code directly. One of the most common forms of social engineering is phishing. Learn more about social engineering.

Traffic spike

Traffic spikes are a sudden or unexpected surge in website traffic.

Two-factor authentication (2FA)

Two-factor authentication is a security mechanism for protecting account login by requiring at least two tokens of proof. For example, a user using two-factor authentication would need both a password and security code received via SMS in order to access their account.

Web hosting service

A web hosting service provides users with space to host their site on a web server, for example Google Sites. Extra features or tools may be available depending on the service.

Web scripting languages

Web scripting languages are usually used in combination with HTML to add extra features to a site. For example, scripting languages are used for processing forms, moderating comments, or special visual effects. In context, the hacked recovery guides use the term scripting language to refer to either PHP or JavaScript.

PHP is a server-side scripting language, which means the web server interprets and executes its commands.

Javascript is primarily a client-side language, which means the user's browser interprets and executes its commands.

Web server

A web server is the machine and software that hosts and controls web pages and other files related to a website.

Web shell

A web shell is a back door script that allows attackers to maintain access over a server.

Webspam

Webspam is blackhat search engine optimization (SEO) tactics or spam content that attempts to boost the ranking or popularity of a site by deceiving and manipulating search engines.

Last updated December 22, 2017.