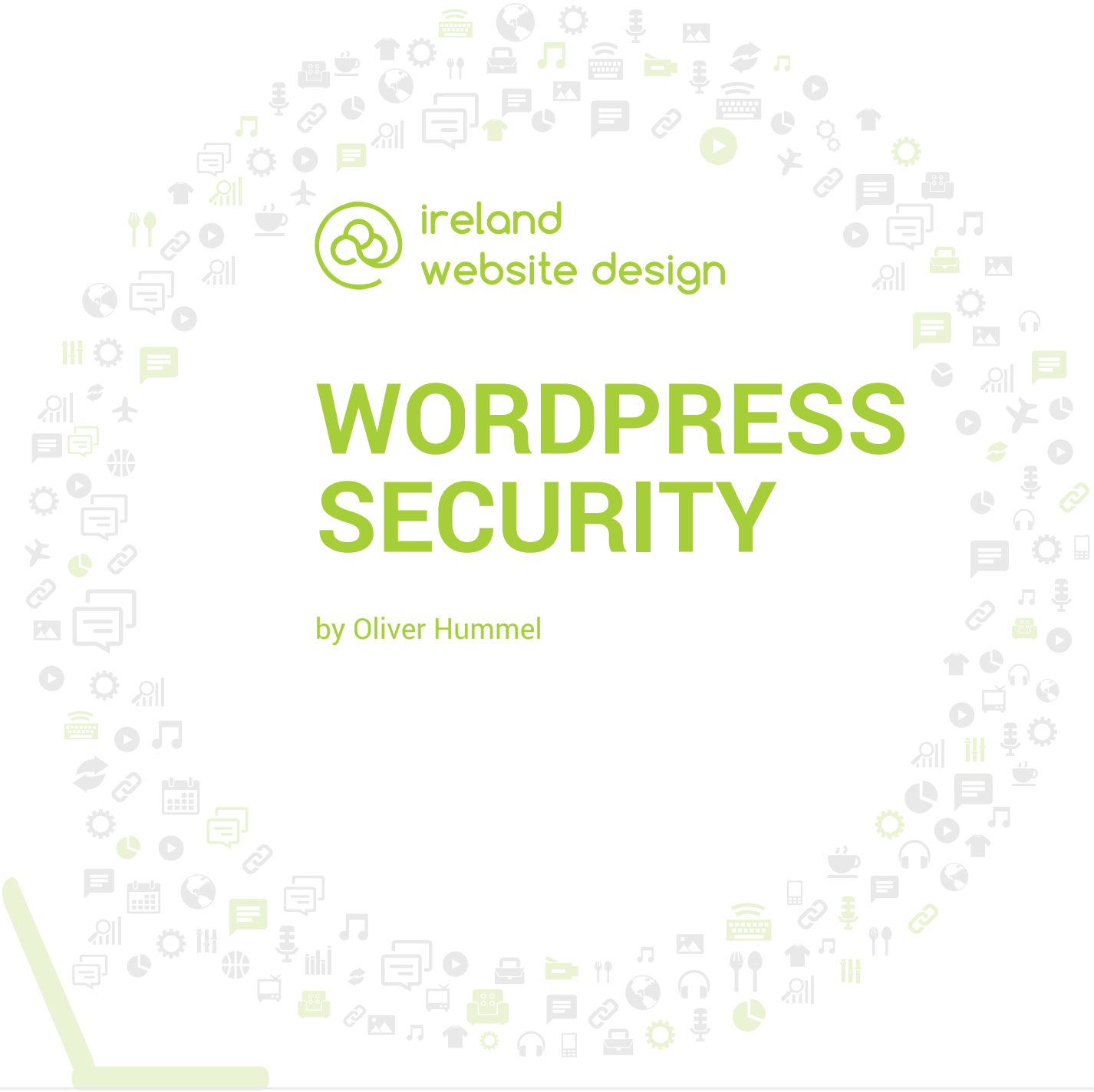

ireland
website design

WORDPRESS SECURITY

by Oliver Hummel

ADDRESS
Unit 12D, Six Cross Roads Business Park, Waterford City

CONTACT
Nicholas Butler
051-393524 | 089-4278112
info@irelandwebsitedesign.com

Contents

Introduction

This document gives you a detailed look into securing your Wordpress website. Worpress ist the most common Content Management System for websites. This makes it an attractive target for hackers. By following the steps in this whitepaper you can greatly improve the security of your website.

Plugin

The plugin we use is called iThemes Security.
More information and download link can be found here:
https://wordpress.org/plugins/better-wp-security/

Security Service

Sucuri offers software and services to detect viruses on your website.
More information and download link can be found here:
https://sucuri.net/

General Security Measures

Update Wordpress and Plugins

This is the most important step to protect your website. Old versions of wordpress and plugins can contain security vulnerabilities. Updating everything protects you from the latest exploits like SQL Injection and Cross Site Scripting. Wordpress will notify you about new software versions on the dashboard. Updates can be done through Wordpress itself with the click of a button. We recommend doing a backup before.

Regular Backups

Backup your site on a regular basis, but at least before and after doing major changes to content or the backend. This way you can roll back to the latest functioning version without losing much content in the case of an attack or some form of data loss. Because Wordpress uses files and a database to store content, you need to back up both. To back the site up, you can either download all files in the directory where wordpress is installed and download an sql dump from the database or you can use a plugin:

We use WP Clone by WP Academy (https://wordpress.org/plugins/wp-clone-by-wp-academy/) to make a full backup of a site. You can also use this plugin to easily move a Wordpress installation to another server. In general when backing up data, keep the 3-2-1 rule in mind. Always have 3 copies on 2 different physical drives with 1 at another physical location.

Use different usernames

The standard administrator username used to be *admin* in Wordpress. Now it can be changed but many new installations sticked with it. Because of this, hackers try this username first. But other usernames like webmaster and root are next on their list. If a hacker has especially targeted your business and it's not just a bot, he might also try your actual name. Try to come up with something that other people will not relate to your business! This gives you an additional layer of security against Brute Force Attacks.

Strong Passwords

The next step is of course having strong passwords. Unfortunately lots of people still use password or 123456 as password. Dictionary attacks which try out as many words as possible try those first. Safe passwords should contain upper and lowercase letters, numbers and special characters. Some plugins can also require the users to change their password on a regular basis, but sometimes this is counterproductive because then they tend to write their passwords down if they can't memorize it.

Unsecure Hosting and Clients

Unfortunately you only have limited control over this. But it is crucial since many sites get compromised because hackers just took over the entire server with all files on it. If your hosting company gives you trouble, you might consider switching. Choose a company that is well established in their business and look for independent reviews. The cheapest option might not offer the service and support you require. Use an antivirus software for your personal computer.

File Permissions

Some plugins change the file permissions on the server upon installation or updating. Wordpress works fine with the directory permissions set to 755 and file permission set to 644. You can either change those permissions via FTP or with those commands if you have shell access to the server:

```
find /path/to/your/wordpress/install/ -type d -exec chmod 755 {} \;
find /path/to/your/wordpress/install/ -type f -exec chmod 644 {} \;
```

Disable File Editing

PHP files can be editied from the Wordpress backend by default. This can be disabled if you have FTP access anyway and other users don't have to change anything in those files. Place this line in wp-config.php:

```
define('DISALLOW_FILE_EDIT', true);
```

iThemes Security Plugin

Following all steps in the last chapter makes your site safer than the majority of the Wordpress installations out there. This plugin helps you to increase the security even more. The basic version provides all these functionalities. The professional version also includes two factor authentication, extended logging and extended support.

Brute Force Protection

As mentioned above, brute forcing passwords by trying out lots of passwords is a common way to hack a website. You should still set a strong password but this plugin helps by locking out users after too many failed login attempts. This is done by banning the attacker's IP for a set amount of time.

Hide the Login

By default, the Wordpress backend can be found at *domain.com/wp-admin* This can be changed with this plugin which makes it harder for attackers to find the actual login page. Also it will instantly turn away most of the bots that try to hack sites, because they only look in the default place.

File Change Detection

The iThemes plugin can detect if files on the server are changed and will send you an email. This notifies you about a potential security breach on your website.

Bot Detection

When a bot is scanning your website for potential vulnerabilities, it usually generates quite a lot of 404 Page not Found errors. The plugin can detect this and temporarily block the IP address after a set amount of errors.

Other Tools

The plugin can rename the admin account, enforce strong passwords, lock out blacklisted users and does database backups. The official website of the plugin lists all tools and offers a detailed comparison between the basic and the professional version.

Visit www.ithemes.com/security for more information.

Sucuri Security

Sucuri offers a variety of solutions and software to protect your website against hackers. Pre-emptive and after an attack.

Visit www.sucuri.net for more information.

Website Firewall

By using Sucuri's network as a proxy in front of your website, they are able to filter out traffic, used for Denial of Service attacks. They block requests which are not necessary for a webserver and try to limit the traffic during an attack by using heuristic algorithms. The website firewall also protects against common hacking attempts like SQL Injection, Cross Site Scripting and brute forcing passwords.

Website Antivirus

The antivirus package includes all features of the firewall. Additionally security experts will monitor your site for malware and spam and perform a cleanup if anything is found.

Blacklist Removal

If your website gets hacked and sends out malware or spam to users, Google or other authorities might flag it as infected. This is very bad for you because it will turn many visitors away. After cleaning up your site, Sucuri can use their connections to web authorities to get your website removed from blacklists quickly.

Unit 12D, Six Cross
Roads Business Park,
Waterford 051-393524 | 089-4278112
www.irelandwebsitedesign.com
info@irelandwebsitedesign.com