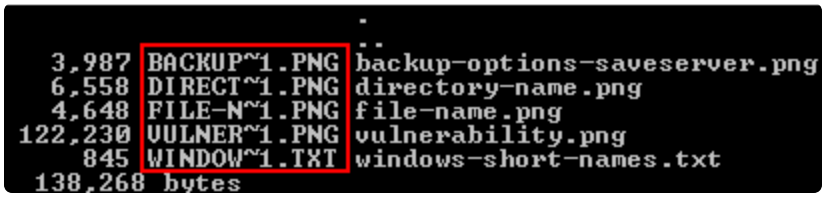
THE ACUNETIX BLOG › WEB SECURITY ZONE

Windows Short (8.3) Filenames – A Security Nightmare?

Bogdan Calin | July 3, 2012

Each time you create a new file on Windows, the operating system also generates an MS-DOS-compatible short file name in 8.3 format, to allow MS-DOS-based or 16-bit Windows-based programs to access files which have a long name. You can see these MS-DOS-compatible short file names by using the **/X** switch with the **dir** command. On my system I get something like this:



There have been a lot of security problems in the past related to short file names. Just yesterday, I found another paper that talks about this subject. The paper was written by Soroush Dalili and is called Microsoft IIS tilde character "~" Vulnerability/Feature – Short File/Folder Name Disclosure.

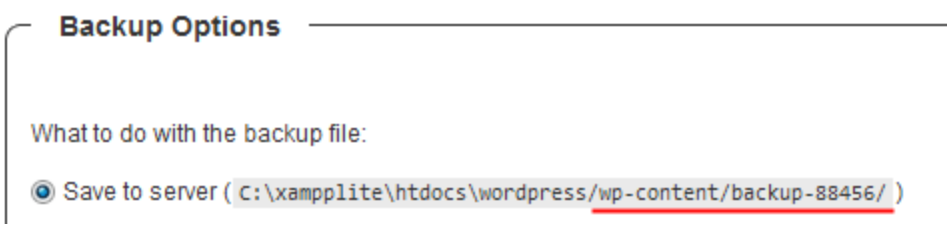
When using IIS, you can get a list of all the shortnames (both files and directories) from a certain directory. This can be a big problem if you can manage to guess, or bruteforce the full file or directory names from these short names. While working on a security script for Acunetix Web Vulnerability Scanner, I thought "Why you have to guess the full names once you have the short names? Why you cannot use the short names? It turns out that IIS doesn't accept short names for a variety of reasons,

Think of following scenario; a web application running on Apache on Windows, is creating a file with a long name that should not be guessed by an attacker. For example it creates a session file or an SQL backup file. In this case the security of this application relies on the fact that the name of this file cannot be guessed.

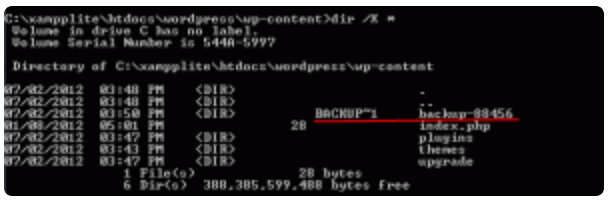
Let's assume that this file name is **backup-082119f75623eb7abd7bf357698ff66c.sql**. Windows will create a short name for this file, **BACKUP~1.SQL**. If I can access this file using the short file name then all the security is broken. I just request BACKUP~1.SQL and get the file, which includes a backup of an SQL database.

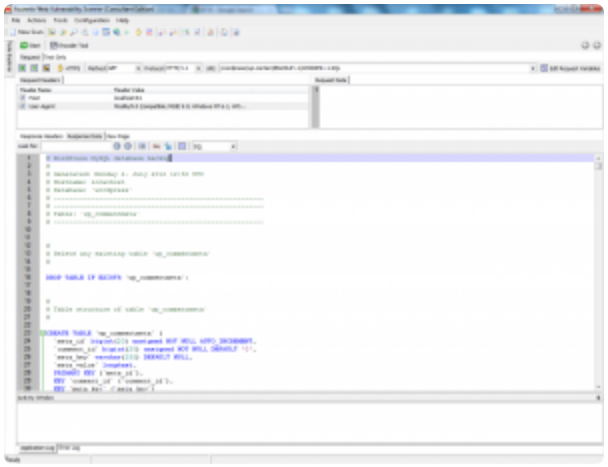
Being curious if this problem is a real life problem, I looked at two of the most popular backup plugins for WordPress. Both of them are affected by this problem, which is explained in detail below.

After installing one of the plugins, I have requested a backup of my WordPress blog:



The plugin creates a custom directory for this backup (**backup-88456**). Once the backup is completed, the directory contained a file named **wordpress_wp_20120702_576.sql**, which is the WordPress database backup. This should be pretty hard to guess. We have 5 numbers in the directory name (100 000 combinations) plus the date and plus **3** more numbers. In total it should be at least **100,000,000** combinations if we ignore the date. What do you think are the short names for this directory and file? Using short names this is pretty easy to guess.





What can you do to protect yourself against this problem, and who's fault is it?

Is Microsoft's fault that they still support the short names in 2012? Maybe. I'm not sure but legacy and security do not go well together. Or is it Apache's fault that they support the short names? Maybe. I don't think it is the fault of the person who wrote the WordPress plugin.

The solution

There is a way to disable Windows 8.3 short name creation.You can create a registry key named **NtfsDisable8dot3NameCreation** in HKLMSYSTEMCurrentControlSetControlFileSystem and set it to 1. That should disable short names creation. Refer to this Microsoft TechNet article to read more about the solution.

THE AUTHOR

Bogdan Calin

Acunetix developers and tech agents regularly contribute to the blog. All the Acunetix developers come with years of experience in the web security sphere.

Related Posts:

Four ways to combat the cybersecurity skills gap

Read more →

Common password vulnerabilities and how to avoid them

Read more →

How Acunetix addresses HTTP/2 vulnerabilities

Read more →

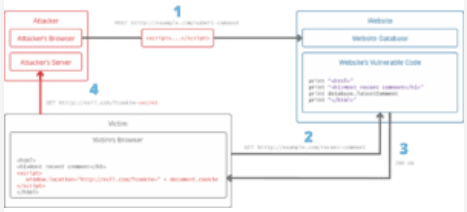
Acunetix by Invicti

Get a demo

Acunetix by Invicti

What is SQL Injection (SQLi) and How to Prevent It

Read more →



Cross-site Scripting (XSS)

Read more →

Acunetix by Invicti

Google Hacking: What is a Google Hack?

Read more →

← Older **Newer →**

Subscribe by Email

Get the latest content on web security in your inbox each week.

Enter E-Mail | Subscribe

We respect your privacy

Learn More

IIS Security

Apache Troubleshooting

Security Scanner

DAST vs SAST

Threats, Vulnerabilities, & Risks

Vulnerability Assessment vs Pen Testing

Acunetix by Invicti

Get a demo

Blog Categories

Articles

Web Security Zone

News

Events

Product Releases

Product Articles

PRODUCT INFORMATION

AcuSensor Technology

AcuMonitor Technology

Acunetix Integrations

Vulnerability Scanner

Support Plans

USE CASES

Penetration Testing Software

Website Security Scanner

External Vulnerability Scanner

Web Application Security

Vulnerability Management Software

WEBSITE SECURITY

Cross-site Scripting

SQL Injection

Reflected XSS

CSRF Attacks

Directory Traversal

LEARN MORE

White Papers

TLS Security

WordPress Security

Web Service Security

Prevent SQL Injection

COMPANY

About Us

Customers

Become a Partner

Careers

Contact

DOCUMENTATION

Case Studies

Support

Videos

Vulnerability Index

Webinars

Acunetix
by Invicti

Get a demo