# WSO Shell: The Hack Is Coming From Inside The House!

By Wordfence Author

Published: 2017-06-22 · Archived: 2026-04-06 15:37:49 UTC

Imagine that one day you discover that a burglar has broken into your home and attempted to make off with your big-screen TV. Fearing for your safety, you immediately contact local law enforcement, and they promptly apprehend the criminal. But to your horror, as they drag the burglar away in handcuffs, they have an additional shocking revelation: the burglar has not only been living in the basement of your home for months, entirely undetected by you, but he's also *converted your basement into an elaborate base for all of his criminal operations.*

You, of course, are both shocked and appalled! How could you not have noticed a nefarious criminal had hijacked your whole residence right under your nose? And how much damage have they already done, unbeknownst to you, all while secretly living under your own roof?

That's a lot like what it's like when an attacker compromises your website and quietly installs a malicious web shell, taking over and executing all kinds of malicious scripts and behavior: your website has been broken into, hackers have made themselves at home on your server, your bandwidth and storage space have been stolen, and you're none the wiser.

The Wordfence team has seen thousands of malicious scripts from hackers attempting to compromise the millions of sites that we protect. But there's one particularly invasive script that, once it makes its way onto your website, acts *exactly* like the burglar in the above scenario, living in your site's "basement" and allowing the attacker to wreak havoc almost completely undetected indefinitely: **the WSO web shell.**

## What Is a Web Shell?

A web shell is a script that runs on a web server, much like WordPress or any other PHP code. It allows the user to do things as if they were logged in to the server directly. It's like a server administration tool: it lets the user view or edit files, work with databases, and even run programs. Web shells created by hackers usually have additional malicious features, such as sending spam or automatically defacing a website.

Web shells are not inherently a type of attack or an exploit. Rather, they're a tool used to manipulate a site *after* it's already been broken into. We talk a lot about the different kinds of exploits and why they put your site at risk, but the truth is that security vulnerabilities and exploits are merely the first step in any successful hack. The goal is to break into your website, and then use a script to take over your site and wreak all sorts of havoc via your server.

That, in a nutshell, is exactly what the WSO web shell does. It takes over your site for the hacker's own purposes without you ever realizing it's there.

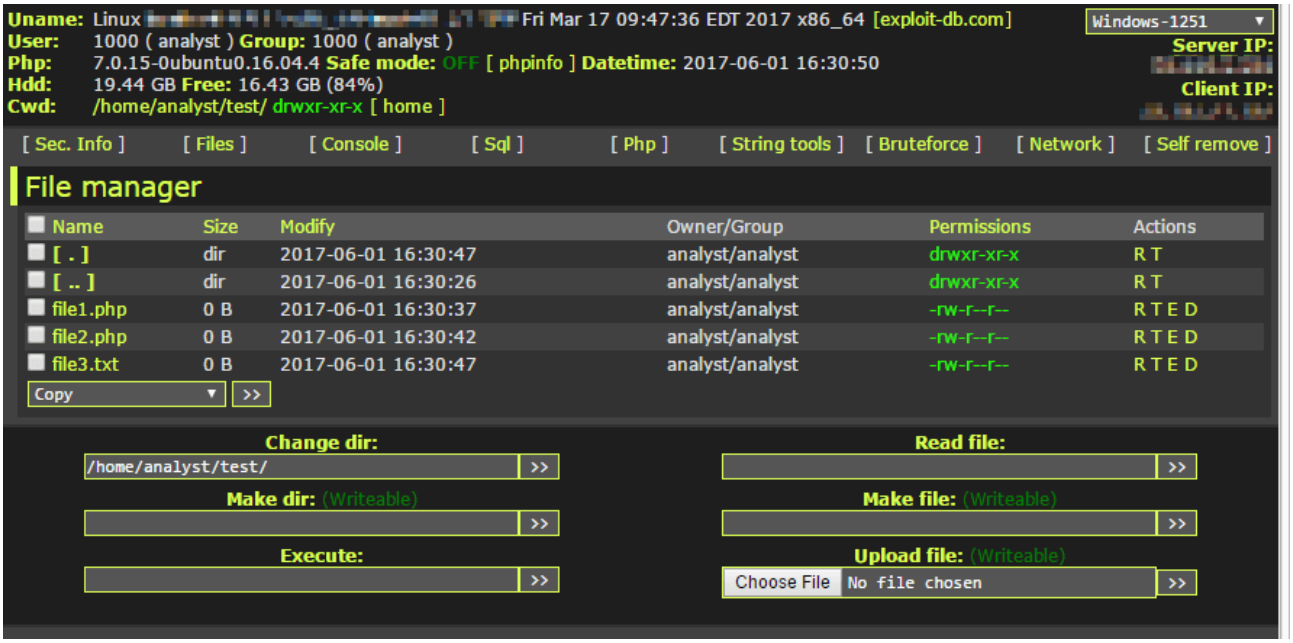
## What's "Special" About WSO?

WSO is a favorite web shell among hackers because of its particularly powerful set of features.

- Password protection
- Server information disclosure
- File management features like uploading, downloading, or editing files, creating directories, browsing through directories, and searching for text in files
- Command-line console
- Database administration
- PHP code execution
- Encoding and decoding text input
- Brute-force attacks against FTP or database servers
- Installation of a Perl script to act as a more direct backdoor on the server

Once they're installed on a website, web shells are notoriously difficult to remove, in large part because hackers often place multiple copies of a web shell all over a site to try to retain access even if some of their malware is removed.

WSO is designed to be used via a web browser, and it has a pretty simple user-friendly interface, making it very easy for any would-be hacker to learn and put to use.

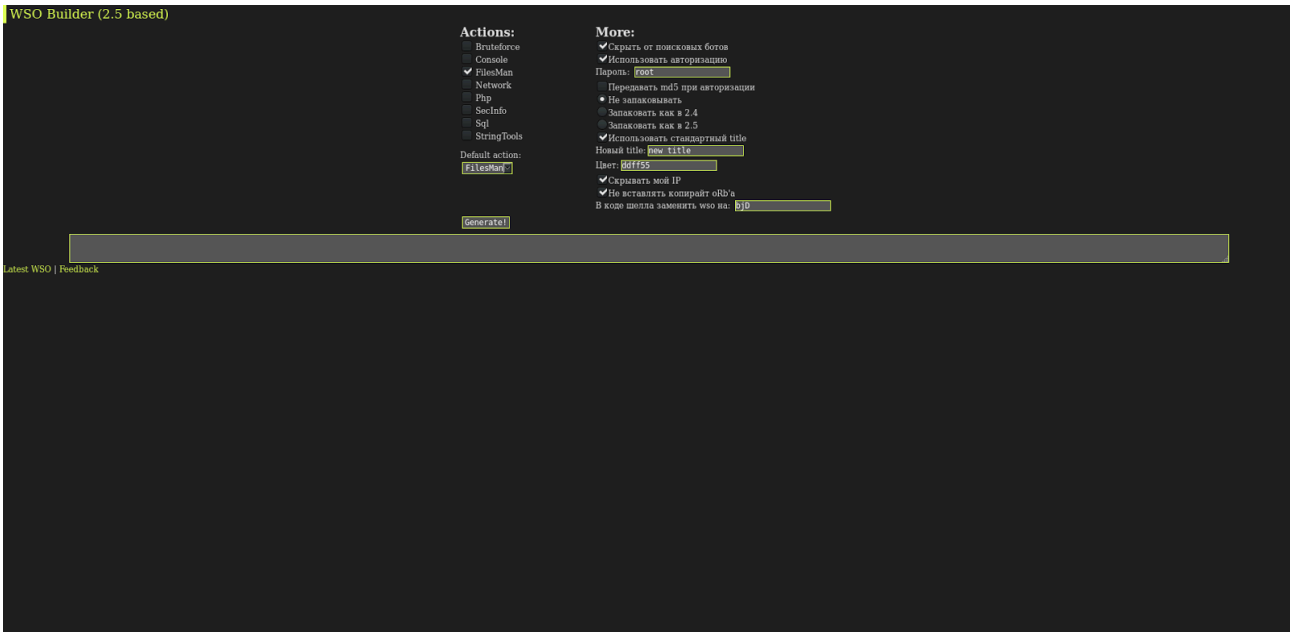



It seems to strike a good balance between simplicity and capability, since it's one of the most popular web shells out there. In fact, despite the simple browser interface, we see a lot of hackers using it simply to execute malicious PHP code on websites. In theory, that's something that a hacker could accomplish more easily with a very small amount of code:

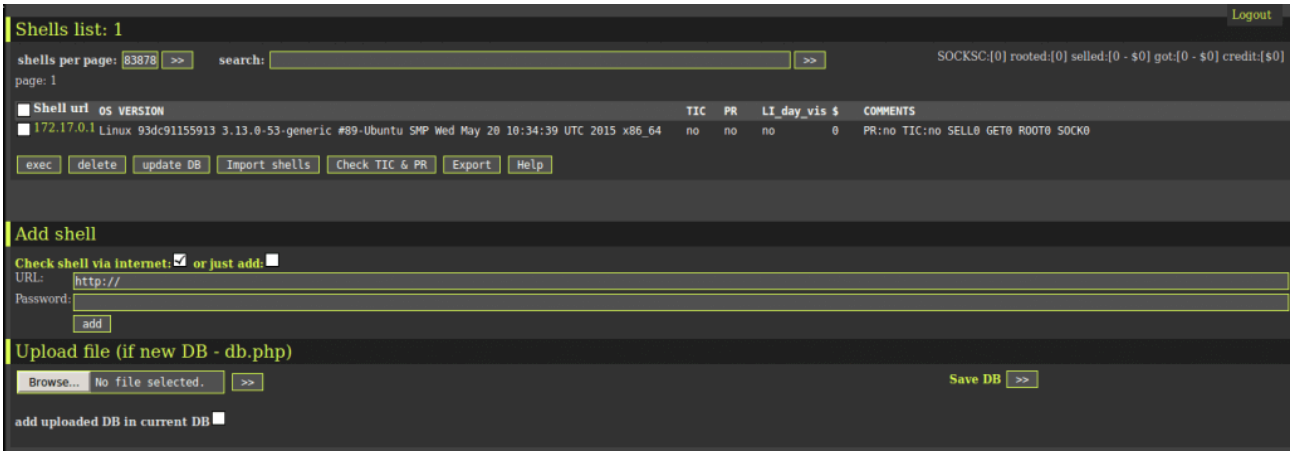
```
<?php eval($_POST['c']); ?>
```

But hackers seem to like and trust WSO so much that they want it on their compromised websites anyway.

A whole ecosystem has sprung up in the hacker community around WSO shell, with hackers developing secondary tools that support its execution and use. For example, there's a tool to build a customized version of the shell with only the features you want.




We've also seen a tool to manage multiple sites infected with it, making it that much easier for even entry-level hackers to take over a large number of websites relatively easily.




## History

For such a ubiquitous tool, WSO's origins remains something of an unsolved mystery.

WSO apparently stands for "web shell by oRb." It was first seen in hacker communities between 2008 and 2009. The earliest mention we could find was a thread in a Russian hacking forum in January of 2009 by a user named oRb, which the script has since been named after.

That thread was used to announce a major update to the script, though, so that probably wasn't the first release of WSO. But Google searches for "WSO Shell" started to pick up soon after.

oRb continued to post updates and new versions of the script until late 2010, when they released version 2.5. That remains the most popular version, though some hackers have released variations since then (and not always out of altruism toward other hackers – some releases include hidden code to notify the author where they're installed, thereby causing multiple levels of infiltration and damage).

The WSO shell is widely used by countless hackers all over the world, with the community of users who prefer it as a web shell growing every day.

In January of this year, for example, we published research about the ChickenKiev or 'CK' botnet which uses WSO as part of its operation.

Each new iteration is intended to make it easier and easier for hackers to take over websites and do whatever they want after that. The laziness of hackers in this regard can't be overstated. For example, one of the first lines in the WSO shell sets the password required to use it:

```
$auth_pass = "63a9f0ea7bb98050796b649e85481845";
```

Specifically, this sets the password to the word 'root.' Our WAF has blocked hundreds of attempts to upload WSO to websites we protect – all trying to execute with this simple no-brainer default password.

## How Wordfence Blocks WSO

We have been monitoring and blocking WSO shell hijacking attempts for some time, and as a direct result, we've developed a few powerful ways of making sure every website we protect is safe from this aggressive invasion.

Wordfence protects your site from exploitation using WSO shell in the following ways:

- Wordfence will detect and block *any* attempt to upload WSO shell. The Wordfence WAF scans all requests to your website to look for malicious code using our custom-designed malware signatures, which are continuously updated. The WAF, once installed on your site, will detect any attempt to upload WSO shell – and immediately block it.
- Wordfence's malware scanner will detect the presence of WSO shell on your filesystem if an attacker manages to find some other way to install it. You will be instantly alerted if WSO shell is found lurking anywhere on your server.
- Wordfence also blocks attempts to run WSO shell commands, so that even if a hacker manages to get past the first two defenses, it's a moot point: WSO shell commands simply won't work on your site.

## How to Tell If WSO Shell Is Lurking on Your Website

We have two incredibly easy ways that you can use to determine if WSO shell is secretly lying in wait on your website:

1. If you have Wordfence installed, simply run a scan. If the results come back clean, you almost certainly don't have WSO shell on your site.
2. If you *don't* have Wordfence installed, or if you use another content management system like Joomla or Drupal, simply use Gravityscan to scan your website. (**Important:** make sure you have the Gravityscan

Accelerator installed.) Gravityscan will scour your website's entire filesystem, and your scan results should let you know if you have WSO shell installed anywhere.

## Conclusion

Because of its low barrier of entry, WSO shell is one of the most popular and most malicious tools used by hackers to infect websites. Having WSO shell installed on your website can a dangerous liability for you and your business.

Of course, the best defense is a good offense, and using Wordfence or Gravityscan, you can not just block and easily detect its presence and keep your site safe from any would-be attackers – you can also make certain that they never break into your "home" on the web in the first place.

---