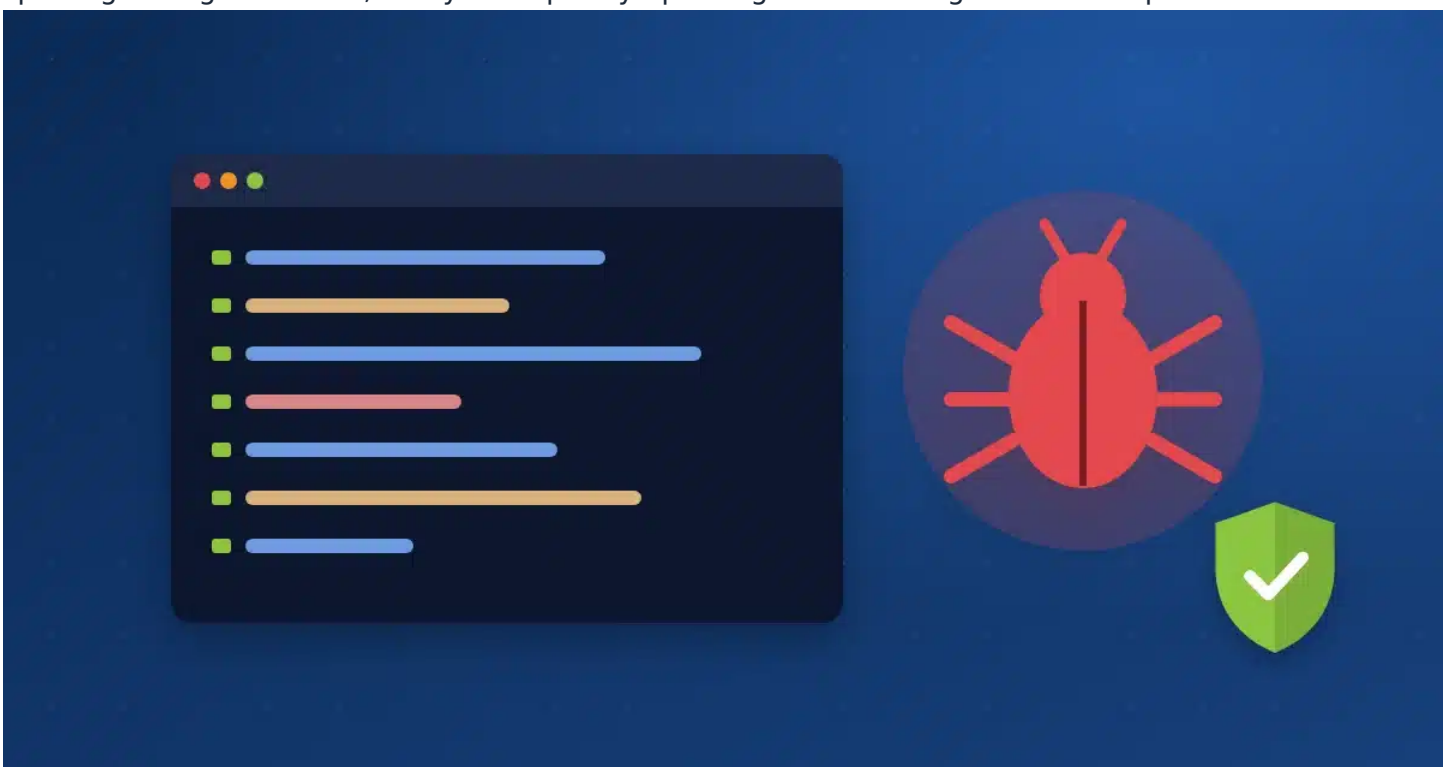
What Is a C99 Shell? How It Gets In and How to Find and Remove It

Website Security · https://www.hyyat.com/en/knowledgebase/hacking-tools-c99-shell/

In shortC99 is one of the best-known web shells: a malicious PHP file an attacker uploads to your site to control files and the database from a browser and send spam. It usually gets in through an outdated plugin, a nulled theme or an unprotected upload form. You find it by scanning files and spotting strange PHP files, and you stop it by updating and disabling PHP in the uploads folder.



What is a web shell?

A web shell is a script that gives whoever opens it in a browser a full control panel over your site: browse and edit files, read the database, upload new files and run commands on the server. C99 is one of the oldest and most famous, and many modified copies exist under other names.

How does it get into your site?

*1***Outdated plugin or theme**A known flaw that allows uploading a file without logging in.

*2***Nulled copies**“Free” themes and plugins from unofficial sites with the shell hidden inside.

*3***Unprotected upload form**A form that accepts any file type, so the attacker uploads PHP disguised as an image.

*4***Stolen password**Logging into WordPress or FTP and uploading the file directly.

Signs it is on your site

- PHP files inside `wp-content/uploads`, a folder that should hold only images and files.
- Files with odd names, or names that mimic WordPress core files in the wrong place.
- Long, obfuscated code using functions like `eval`, `base64_decode` and `gzinflate`.
- Spam leaving your account, or a hosting alert about high sending.
- A new admin user you do not recognize, or visitors being redirected to other sites.

How to remove it and clean your site

1. **Back up the current state:** Even infected, you need it to review what happened.
2. **Scan your files:** Run an ImunifyAV scan from cPanel; it lists infected files and cleans them.
3. **Delete malicious files and look for more:** Attackers usually leave more than one backdoor. Check theme, plugin and upload folders.
4. **Update everything and remove what you do not use:** WordPress, plugins and themes, and replace any nulled copy with the official one.
5. **Change every password:** WordPress, cPanel, FTP, database and email.
6. **Or restore a clean backup:** If you have a backup from before the infection, restoring it and then updating is faster and safer. Follow the steps to remove malware from WordPress.

Prevent it: disable PHP in the uploads folder

The uploads folder never needs to run PHP. Create a file named `.htaccess` inside `wp-content/uploads` with the cPanel File Manager and add:

```
<FilesMatch "\.(php|phtml|php5|php7|phar)$">
  Require all denied
</FilesMatch>
```

After that, even if a shell is uploaded to this folder, it will not run.

How Hyyat Host protects your site

- **ImunifyAV** scans website files daily, and **Imunify360** detects known web shells and blocks their upload.
- **ModSecurity** rules stop known upload and exploit requests before they reach your site.
- Account isolation with **CloudLinux**, so an infected site cannot spread to yours.

Frequently asked questions

Is deleting the shell file enough?
Usually not. Attackers leave more than one backdoor, and the original way in (an old plugin or a password) is still open. Clean the whole site and close the cause.

Will disabling PHP in uploads break my site?
No, because the uploads folder holds images and files only. A few plugins may store PHP files there, so test your site after the change.

Can you help me clean a hacked site?
Yes. Open a ticket and we will help you scan, read the logs and find the cause of the infection.

Want someone to look after your site for you?

Technical support and maintenance for WordPress sites and forums. **Technical support and maintenance →**

Related guides

- How to Keep Your Website Secure: Practical Tips to Prevent Hacking
- Brute Force Protection: What It Is and How Hyyat Host Protects Your Site

- The WordPress load-scripts.php Vulnerability (CVE-2018-6389) and How to Protect Your Site
- How to Protect Your Customers' Data on Your Website: A Practical Guide

All website security guides →

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.

Web HostingSaudi Hosting