



VISION

To build the most effective and affordable cloud-based technology and services for website security and performance, while producing the most concise educational website security resources.

BRANDMARK

Primary Logo



Secondary Logo



The Lock Box Monogram



Small sizes approved for use in 3 different colors.



THE LOCK BOX LOGO

The Sucuri logo is composed of the Lock Box and a logotype based off Avenir Next LT Pro Bold.

The Lock Box is our promise to our customers that their website is safe in our hands. Blocking malicious actors from the outside but still being open to allow the flow of good traffic to their website.

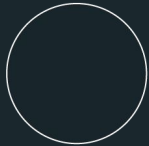


BRAND COLORS

Primary Color



Sucuri Main Green
Hex #008775



Sucuri Midnight
Hex #18262c

Secondary Color



Secondary Green
Hex #2bb79c



Dark Gray
Hex #686969



Light Gray
Hex #e9e8e8

Tertiary Color



Sucuri Red
Hex #ce2f31



Sucuri Blue
Hex #506cb2



Sucuri Yellow
Hex #f5be19

TYPOGRAPHY

TITILLIUM WEB - BOLD

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk
Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu
Vv Ww Xx Yy Zz
0123456789

OPEN SANS - BOLD

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk
Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu
Vv Ww Xx Yy Zz
0123456789

OPEN SANS - REGULAR

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk
Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu
Vv Ww Xx Yy Zz
0123456789

ICONS

**Sucuri icons are used across different brand touchpoints.
They provide symbolism, conceptual clarity and visual interest in simplistic shapes and forms.**



PHOTOGRAPHY

Featured Image Content

According to content image should show:

- A laptop or a desktop computer (with or without people);
- People using computers or mobile devices;
- Office atmosphere.
- Busy and dynamic but relaxed atmosphere



SOCIAL ADS

 **Automate your
WordPress
Workflow**



[Signup Now](#)

 **Magento Security**
A FREE EMAIL COURSE FOR MAGENTO USERS



[Sign Up Today](#)

 **FREE EMAIL COURSE:
How To Add Security
To Your Customers'
Website**

[Sign Up Today](#)



GUIDES

**What is a Web Application
Firewall (WAF)?**

See how WAFs work &
find the best solution.

[Learn more](#)

 **FREE EMAIL COURSE:
How To Add Security
To Your Customers' Website**



[Sign Up Today](#)

 **WordPress Security**
A FREE EMAIL COURSE FOR WORDPRESS USERS



[Sign Up Today](#)

REPORT

 **SUCURI**

**267,614 infected
websites** were
detected by our
**free SiteCheck
scanner**

Download our FREE
Q2 SiteCheck Report

[Download Now!](#)





**PCI Compliance
& Security for
Ecommerce Websites**

A FREE EMAIL COURSE
FOR ONLINE STORE

[Sign Up Today](#)

INFOGRAPHIC

An Introduction to WordPress Security

This guide is intended to educate those who have not previously been exposed to the various security issues that can affect a WordPress site. It is not intended to be a security manual or a list of security best practices.

over 28% of websites are hacked each year

Step 1: Software Vulnerabilities

- 1.1 **Active Plugins & Themes**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 1.2 **WordPress Core**
Check for updates and vulnerabilities. If WordPress is outdated, it may be vulnerable to attacks.
- 1.3 **PHP Version**
Check for updates and vulnerabilities. If PHP is outdated, it may be vulnerable to attacks.
- 1.4 **Database**
Check for updates and vulnerabilities. If the database is outdated, it may be vulnerable to attacks.
- 1.5 **Server**
Check for updates and vulnerabilities. If the server is outdated, it may be vulnerable to attacks.
- 1.6 **SSL Certificate**
Check for updates and vulnerabilities. If the SSL certificate is outdated, it may be vulnerable to attacks.

Step 2: Access Control

- 2.1 **User Management**
Check for updates and vulnerabilities. If user management is outdated, it may be vulnerable to attacks.
- 2.2 **Permissions**
Check for updates and vulnerabilities. If permissions are outdated, it may be vulnerable to attacks.
- 2.3 **Roles**
Check for updates and vulnerabilities. If roles are outdated, it may be vulnerable to attacks.
- 2.4 **Capabilities**
Check for updates and vulnerabilities. If capabilities are outdated, it may be vulnerable to attacks.
- 2.5 **Capabilities**
Check for updates and vulnerabilities. If capabilities are outdated, it may be vulnerable to attacks.
- 2.6 **Capabilities**
Check for updates and vulnerabilities. If capabilities are outdated, it may be vulnerable to attacks.

Step 3: Proactive WordPress Security

There is no 100% complete solution to protect your WordPress site from attacks. However, there are several steps you can take to reduce the risk of a successful attack.

- 3.1 **Regular Backups**
Create regular backups of your site. This will allow you to restore your site to a previous state if it is hacked.
- 3.2 **Limit Login Attempts**
Limit the number of login attempts for each user. This will help prevent brute force attacks.
- 3.3 **Two-Factor Authentication**
Enable two-factor authentication for all users. This will add an extra layer of security to your site.
- 3.4 **Security Plugins**
Install a security plugin. This will help protect your site from various types of attacks.
- 3.5 **Security Services**
Consider using a security service. This will provide you with additional protection for your site.

Step 4: Hardening Recommendations

- 4.1 **Change Default WordPress Installation Files**
Change the default WordPress installation files to something unique. This will help prevent attackers from using known vulnerabilities.
- 4.2 **Change Default WordPress Installation Files**
Change the default WordPress installation files to something unique. This will help prevent attackers from using known vulnerabilities.
- 4.3 **Change Default WordPress Installation Files**
Change the default WordPress installation files to something unique. This will help prevent attackers from using known vulnerabilities.
- 4.4 **Change Default WordPress Installation Files**
Change the default WordPress installation files to something unique. This will help prevent attackers from using known vulnerabilities.
- 4.5 **Change Default WordPress Installation Files**
Change the default WordPress installation files to something unique. This will help prevent attackers from using known vulnerabilities.
- 4.6 **Change Default WordPress Installation Files**
Change the default WordPress installation files to something unique. This will help prevent attackers from using known vulnerabilities.

Step 5: Security Services

Consider using a security service. This will provide you with additional protection for your site.

Do you need help cleaning your WordPress site?

View the full guide at [sucuri.net/guides](#)

HACKED DRUPAL

Steps to CLEANING a hacked Drupal site

COMMON INDICATORS OF A HACKED DRUPAL SITE

- 1.1 **Scan Your Site**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 1.2 **Check Modified Files**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 1.3 **Audit User Logs**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 1.4 **Check Diagnostic Pages**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.

STEP 1 - IDENTIFY HACK

- 1.1 **Scan Your Site**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 1.2 **Check Modified Files**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 1.3 **Audit User Logs**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 1.4 **Check Diagnostic Pages**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.

STEP 2 - FIX HACK

- 2.1 **Clean Hacked Server Files**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 2.2 **Clean Hacked Database Tables**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 2.3 **Remove Hidden Backdoors**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.

Remove Malware Warnings

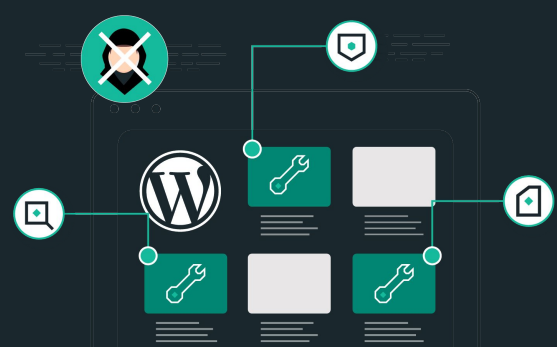
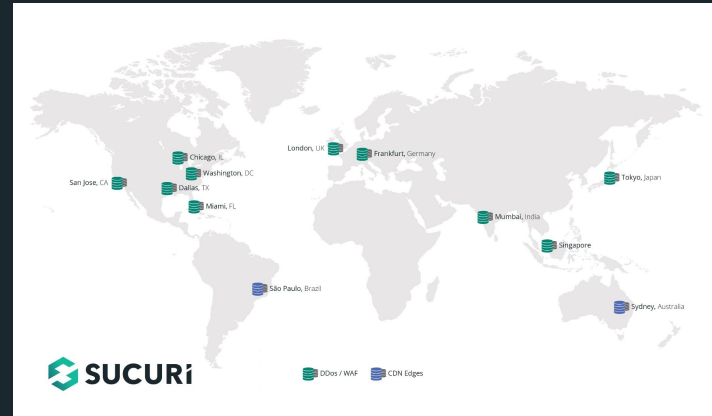
Steps to CLEANING a hacked Drupal site

STEP 3 - POST - HACK

- 3.1 **Update and Reinstall**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 3.2 **Set Backups**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 3.3 **Scan Your Computer**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.
- 3.4 **Protect Your Site**
Check for updates and vulnerabilities. If a plugin or theme is outdated, it may be vulnerable to attacks.

Do you need help cleaning a Drupal site?

View the full guide at [sucuri.net/guides](#)



OPEN GRAPH IMAGE

 **SUCURI** KNOWLEDGE BASE

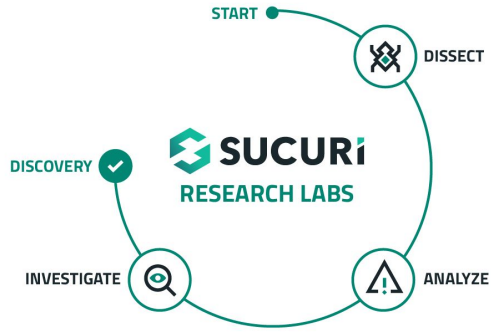


f t @ in SucuriSecurity | Sucuri.net

 **SUCURI** Multi-Site



f t @ in SucuriSecurity | Sucuri.net



 **SUCURI** INFOGRAPHIC

..... An Introduction to

..... **WordPress Security**



f t @ in SucuriSecurity | Sucuri.net

MOCKUP

