

# Penanganan Serangan Slot Gacor

Oleh : Candra Adi Putra

UPT Pusat Teknologi Informasi dan Pangkalan Data

UIN SYAHADA padangsidempuan

<https://www.uinsyahada.ac.id>



# TOPIK

Penanganan ini hanya untuk website

Berbasis Wordpress

- Best Practise Wordpress
- Plugin Security
- Plugin Backup Data
- Google Search Console



# Best Practice Security Wordpress

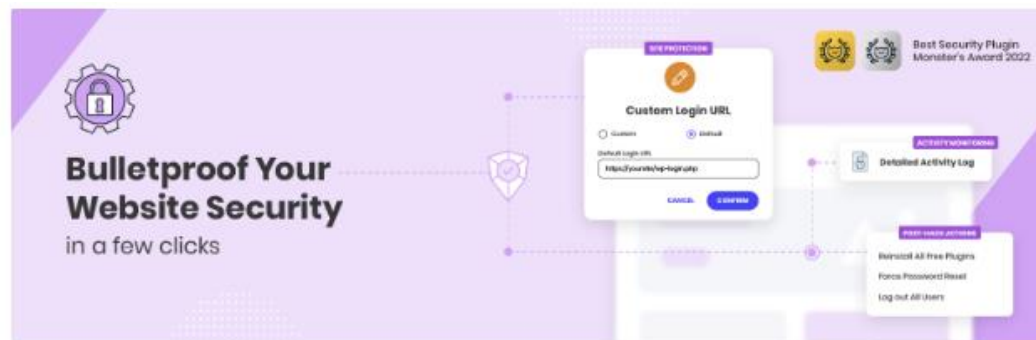
- Selalu Update Wordpress core, Tema dan Plugin ke Versi terbaru
- Gunakan SSL untuk website serta redirect halaman http ke HTTPS
- Custom Lokasi instalasi wordpress dan Halaman Login
- Gunakan 2FA login
- Batasi Limit Login ( missal 3 kali login ip di blokir)
- Hapus semua sisa instalasi di webserver
- Disable directory Indexing

# Best Practice Security Wordpress -Lanjutan



- Disable Eksekusi File PHP di folder upload
- Aktifkan WAF missal mod\_security2
- Disable XML- RPC
- Buat Backup Terjadwal

# Plugin Security Security Optimizer



Security Optimizer – The All-In-One Protection Plugin

By [SiteGround](#)

Download


<https://wordpress.org/plugins/sg-security/>

# Fitur



- **2FA (Two-Factor Authentication)** 2FA untuk login dengan Menggunakan Google Authenticator
- **Limit Login Attempts** Deteksi login pihak lain dan usaha brute force
- **Custom Login URL** -> *website.ac.id/sukasukalogin*
- **Advanced XSS Protection** -> **Proteksi XSS**
- **Lock and Protect System Folders** Mengamankan System Folder
- **Disable Themes & Plugins Editor**
- **Hide WordPress Version** Menyembunyikan fitur wordpress Lebih Lanjut
- Use **Activity Log** cek activity Log dan Memblokir IP
- **Post-Hack Actions** Reinstall semua Plugin dan Thema

# Plugin Backup UpdraftPlus



The image shows the UpdraftPlus logo on an orange background, with a yellow arrow pointing to a grid of icons representing various backup destinations. The icons include Google Drive, FTP, OneDrive, Amazon S3, a download icon, an email icon, a shield icon, a folder icon, a monitor with a refresh icon, and a cloud icon.

UpdraftPlus: WP Backup & Migration Plugin  
By [UpdraftPlus.Com](https://updraftplus.com), DavidAnderson

Download

<https://wordpress.org/plugins/updraftplus/>



## Fitur Backup

- Full backup dan Parsial backup
- Remote Backup to Dropbox, Google Drive, Amazon S3 (or compatible), Rackspace Cloud, FTP, DreamObjects, Openstack Swift or email.
- Restore Full atau hanya DB, Plugin, Tema atau Wp-Contents
- Mendukung WP-CLI





## Mencegah Deface & Proteksi File

- Untuk Pengguna Server Linux / VPS Linux  
`chattr +i index.php`

Selain file diatas, File penting di Wordpress agar tidak bisa di hapus atau di modifikasi diantaranya `.htaccess`, `wp-config.php`, `wp-settings.php`

Untuk mengembalikan file seperti semua ( bisa diedit) gunakan perintah

```
chattr -i index.php
```

# Offensive Security

- Jika sejak awal kita membahas Defensive dan pecegahan, kita bisa juga melakukan testing keamanan Wordpress dengan wpscan.
- Referensi penggunaan tool ini bisa dibaca di webnya <https://wpscan.com>

```
(dachman@dachman)-[~]
$ wpscan -h

WordPress Security Scanner by the WPScan Team
Version 3.8.20

 @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Usage: wpscan [options]
--url URL
The URL of the blog to scan
Allowed Protocols: http, https
Default Protocol if none provided: http
This option is mandatory unless update or help or hh or ver
-h, --help
--hh
--version
Display the simple help and exit
Display the full help and exit
Display the version and exit
-v, --verbose
Verbose mode
--[no-]banner
Whether or not to display the banner
```



# Google Search Console

- Sitemap
- Removal Content
- Security
- Monitoring

# Tambah Domain Property

## Select property type



Domain new

- All URLs across all subdomains (m., www. ...)
- All URLs across https or http
- Requires DNS verification

example.com

Enter domain or subdomain

CONTINUE

or



URL prefix

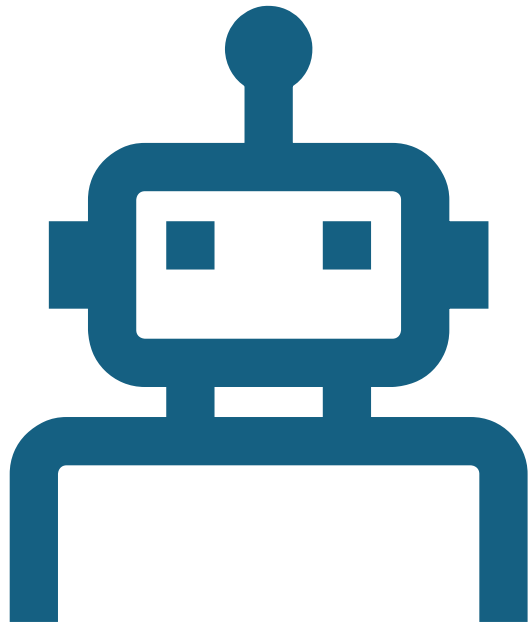
- Only URLs under entered address
- Only URLs under specified protocol
- Allows multiple verification methods

https://www.example.com

Enter URL

CONTINUE

[LEARN MORE](#) [CANCEL](#)



# Google Search Console Sitemap

- Digunakan Untuk Menambahkan `sitemap.xml` agar Mesin pencari lebih cepat mengindeks
- Halaman ini juga bisa digunakan untuk mendeteksi sitemap yang diletakan oleh hacker sehingga kita bisa menghapusnya.
- Kadang website yang terserang Cuma satu URL namun karena sitemapnya banyak sehingga tampak ada sekian puluh bahkan ratusan halaman yang terserang
- Untuk membuat sitemap di Wordpress tool yang bisa di pakai adalah <https://wordpress.org/plugins/google-sitemap-generator/>

# Tampilan Search console - Sitemap

Enter sitemap URL

### Submitted sitemaps

Sitemap	Type	Submitted ↓	Last read	Status	Discovered pages	Discovered videos
<a href="https://perpustakaan.uinsyahada.ac.id/sitemap.xml">https://perpustakaan.uinsyahada.ac.id/sitemap.xml</a>	Sitemap index	Jul 12, 2024	Jul 12, 2024	Success	207	0
<a href="https://spi.uinsyahada.ac.id/sitemap.xml">https://spi.uinsyahada.ac.id/sitemap.xml</a>	Sitemap index	Jul 11, 2024	Jul 11, 2024	Success	23	0
<a href="https://karier.uinsyahada.ac.id/sitemap.xml">https://karier.uinsyahada.ac.id/sitemap.xml</a>	Sitemap index	Jul 11, 2024	Jul 11, 2024	Success	58	0
<a href="https://mahad.uinsyahada.ac.id/sitemap.xml">https://mahad.uinsyahada.ac.id/sitemap.xml</a>	Sitemap index	Jul 11, 2024	Jul 11, 2024	Success	69	0

# Tampilan Search console - Removals

## New Request

TEMPORARILY REMOVE URL

CLEAR SNIPPET

Block URL(s) from Google Search results for about six months and clear the snippet the next time Google reindexes the page. For permanent removal, either block pages from indexing or remove them from the site. [Learn more](#)

https://fi.uinsyahada.ac.id

All URL variations (www/non-www and http/https) will be affected

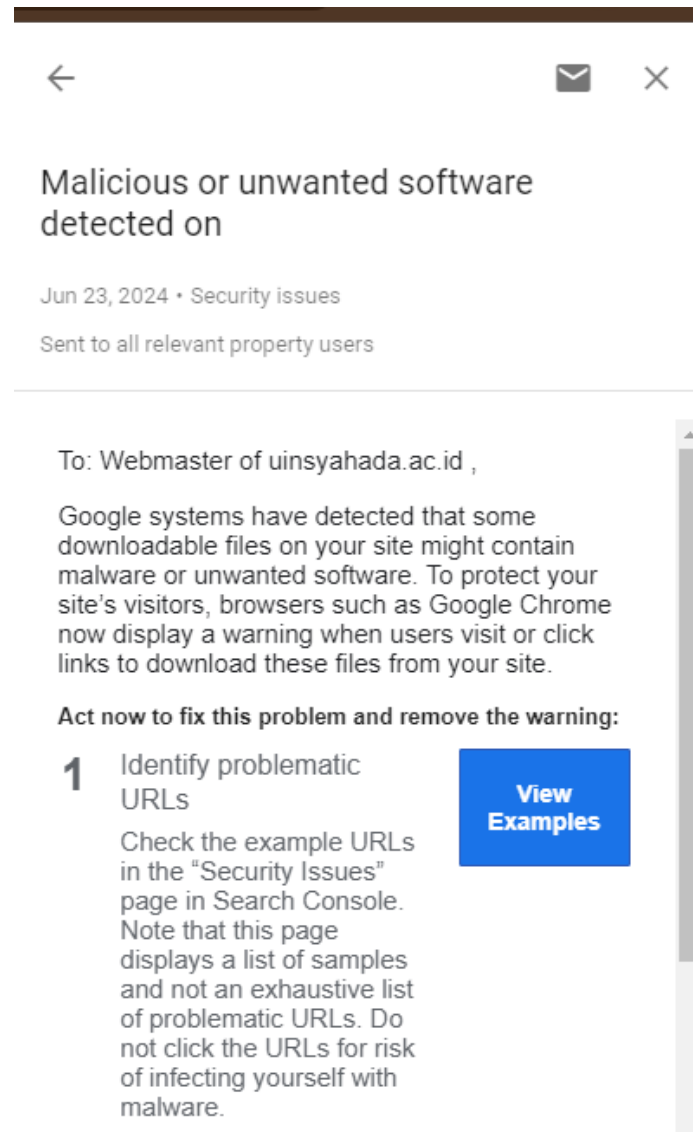
- Remove this URL only
- Remove all URLs with this prefix

Removals of other URLs leading to this content must be requested separately

CANCEL

NEXT

# Tampilan Search console - Security Issues



## Malicious or unwanted software detected on

Jun 23, 2024 • Security issues

Sent to all relevant property users

To: Webmaster of uinsyahada.ac.id ,

Google systems have detected that some downloadable files on your site might contain malware or unwanted software. To protect your site's visitors, browsers such as Google Chrome now display a warning when users visit or click links to download these files from your site.

**Act now to fix this problem and remove the warning:**

### 1 Identify problematic URLs

Check the example URLs in the "Security Issues" page in Search Console. Note that this page displays a list of samples and not an exhaustive list of problematic URLs. Do not click the URLs for risk of infecting yourself with malware.

[View Examples](#)



# Search Console Insight

## How people find you



### Google Search

How visitors find your site on Google



#### Most searched queries

16	berapa persen bunga yang diperbolehkan dalam islam	Avg. position: 1.1  Top 5 results	142 clicks
17	logo uin syahada	Avg. position: 1  Top 5 results	139 clicks
18	https //pmb.uinsyahada.ac.id	Avg. position: 1  Top 5 results	138 clicks
19	login siacad	Avg. position: 3.2  Top 5 results	134 clicks
20	beli chip domino	Avg. position: 19.1	121 clicks



## Referensi

- <https://jetpack.com/blog/guide-to-wordpress-security/>
- <https://www.wpbeginner.com/wordpress-security>
- <https://www.hostinger.com/tutorials/how-to-secure-wordpress>
- <https://www.hostinger.com/tutorials/wp-content/uploads/sites/2/2022/01/WordPress-Security-Checklist.pdf>
- <https://sucuri.net/guides/wordpress-security/>