HOW TO HACK AND DEFEND A WORDPRESS WEBSITE
AGENDA

WHY SECURITY IS IMPORTANT

HOW TO HACK
- VULNERABLE PLUGINS (SCAN)
- PASSWORD GUESSING
- SQL INJECTION

HOW TO DEFEND
- THE ROLE OF WEB HOSTING
- THE ROLE OF CORE, THEMES, AND PLUGINS
- WORDPRESS SECURITY IN EASY STEPS
- ADVANCED WORDPRESS SECURITY
- FIXING A HACKED SITE
ABOUT ME

Internet marketing since 2003.

I’ve only ever worked online. Built hundreds of sites, code (mostly PHP) and I work with WordPress and Laravel.

I have two security certifications: Security+ and Certified Ethical Hacker.

I built the Cybersecurity Community’s largest and most indexed Conference Directory called infosec-conferences.com

I manage a Growth Marketing Agency called: Growth Hackers!

www.growthhackers.hk
These slides and videos will be placed on the following URL:

www.growthhackers.hk/wordcamp
WHY WORDPRESS SECURITY IS IMPORTANT
WHY WORDPRESS SECURITY IS IMPORTANT

- Loss of time/energy
- Loss of Revenue
- Loss of Sensitive Data/PII
- Downtime
- Moral and “Bad For Reputation”
AVERAGE HACK GOES UNNOTICED FOR 1,345 DAYS...
HOW TO HACK

HACK #1 BRUTE FORCE
HOW TO HACK

HACK #2 PASSWORD GUESSING
root@kali:~Desktop/cupp

```python
# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgen@remote-exploit.org ]

[ Options ]

-h  You are looking at it baby! :)  
    For more help take a look in docs/README
    Global configuration file is cupp.cfg

-i  Interactive questions for user password profiling

-w  Use this option to improve existing dictionary,  
    or W00p output to make some pwnsausage

-l  Download huge wordlists from repository

-d  Parse default usernames and passwords directly from Alecto DB.  
    Project Alecto uses purified databases of Phrack31 and CIIT  
    which where merged and enhanced.

-v  Version of the program
```

root@kali:~Desktop/cupp#
HOW TO DEFEND
2.1 The Role of Web Hosting | It Makes a Big Difference

- Basic Server Security
- Shared vs Dedicated
- VPS
- Managed
- SSL
HOW TO DEFEND

2.2 THE ROLE OF CORE, THEMES, AND PLUGINS | UPDATE THEM, OR PAY THE PRICE!

- Avoid Known Vulnerabilities
- Core, Theme, and Plugin Updates
- Automatic Core Updates Automated Updates (with backups)
- Use Supported Themes
- Avoid Free Versions of Paid Plugins
HOW TO DEFEND | PRACTICAL WAYS
CHANGE THE DEFAULT “ADMIN” USERNAME ANYTHING BUT ADMIN.

Three Methods:

1. Create a new admin username and delete the old one.
2. Use the Username Changer plugin
3. Update username from phpMyAdmin
INSTALL A WORDPRESS BACKUP SOLUTION
BACK THAT SITE UP!

Choose a plugin

- VaultPress (with Jetpack), BackupBuddy or UpdraftPlus
- Full Backups vs. Snapshots
- Automated Backups, How Often?
- Backups before Updates
INSTALL A WORDPRESS SECURITY PLUGIN

CHOOSE WISELY...

- Sucuri Security
- Wordfence
- iThemes Security

Follow the Instructions / Read the Directions
Backups before Updates
HOW TO DEFEND

ENABLE WEB APPLICATION FIREWALL (WAF)
STOP PROBLEMS BEFORE THEY GET TO YOUR SITE

- Sucuri
- CloudFlare

Paid Services
“Set and Forget”
Backups before Updates
Off-site Storage
HOW TO DEFEND

USE 2-FACTOR AUTHENTICATION FOR LOGIN
ALL THE COOL KIDS ARE DOING IT.

Two types of algorithms
  - Time-based One-time Password (TOTP)
  - HMAC-based One-time Password (HOTP)

Two Factor Authentication Plugin
  - Supports Google Authenticator and more
  - Don’t use SMS or Email
HOW TO DEFEND

DISABLE TRACKBACKS

WHY BOTHER WITH IT?

Spammy, Fake, and Annoying

Settings > Discussion

Uncheck “Allow link notifications from other blogs (pingbacks and trackbacks)”
HOW TO DEFEND

DISCOURAGE SPAMMERS
ADD A HUMAN TOUCH.

Human Interface Form
- Akismet Anti-Spam
- Captcha Plugins (there are many)
- Some Contact Form Plugins already include as an option

Disable Comments
- Or outsource comments to Disqus
DON'T ADD SECURITY QUESTIONS TO LOGIN

Decreases security because the answers are almost always public data!

Don't use them. Period.
HOW TO DEFEND | ADVANCED WAYS
DISABLE FILE EDITING, LOCK IT DOWN.

You can easily do this by adding the following code in your wp-config.php file.

```
1 // Disallow file edit
2 define( 'DISALLOW_FILE_EDIT', true );
```
DISABLE PHP FILE EXECUTION
NO PHP, NO CRY.

Disable PHP file execution where it’s not needed e.g. /wp-content/uploads/

Open a text editor, save as “.htaccess” in /wp-content/uploads/
Can also be done with specific directories using `php.ini` if host allows
HOW TO DEFEND

LIMIT LOGIN ATTEMPTS
THREE STRIKES AND YOU’RE (LOCKED) OUT.

- Easily done with Plugins
- Login LockDown Plugin
- Wordfence Security Plugin
- Limit number of login attempts
- Block invalid Usernames
HOW TO DEFEND

CHANGE WORDPRESS DATABASE PREFIX

Change Table Prefix in wp-config.php from “wp_” to something else like this “z7s8_”

Change all Database Tables Name

Search the options table for any other fields that is using “wp_”

Search the usermeta for all fields that is using “wp_”

Backup and Done
HOW TO DEFEND

PW PROTECT WP-ADMIN AND LOGIN

Only if SSL is enforced

Can be done in Cpanel OR:

Create a .htpasswd file and upload this file outside your /public_html/ directory

```
AuthName "Admins Only"
AuthUserFile /home/yourdirectory/.htpasswd/public_html/wp-admin/passwd
AuthGroupFile /dev/null
AuthType basic
require user putyourusernamehere
```
HOW TO DEFEND

DISABLE DIRECTORY INDEX/BROWSE
REVEAL NOTHING

Open the .htaccess file in your root directory

Add the following line at the end of the .htaccess file

Save and upload .htaccess file back to your site

Options -Indexes
HOW TO DEFEND

DISABLE LOGIN HINTS

Open functions.php file

Add this code:

Change the “What the heck are you doing?! Back off!” message to better fit your mood.

```php
function no_wordpress_errors(){
    return 'What the heck are you doing?! Back off!';
}
add_filter( 'login_errors', 'no_wordpress_errors' );
```
FIX A HACKED SITE
HOW TO DEFEND

YOU’VE BEEN HACKED
NOW WHAT? FUTURE CORE UPDATES.

Archive current site directory and database for forensic analysis

Restore from backups (hopefully?)

Malware Scan and removal
HOW TO DEFEND

YOU’VE BEEN HACKED

CLEANING UP

- Update Plugins and Core
- Verify permissions are minimal (most malware makes things 777)
- Force PW change at next login
- Change admin PW
- Change DB PW and secret keys