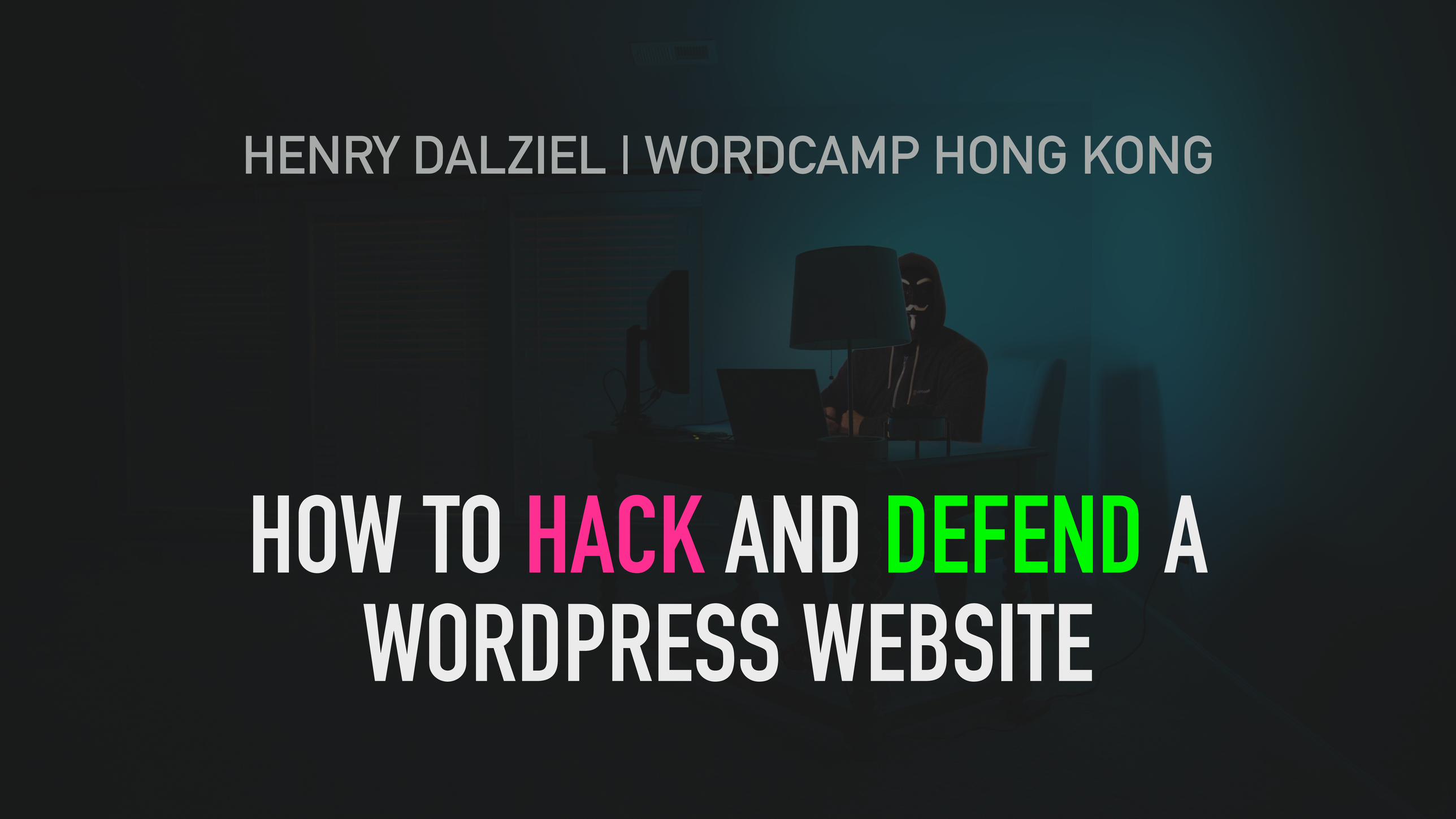
HENRY DALZIEL | WORDCAMP HONG KONG



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

ACCESS THIS CONTENT

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...

SOME CLEVER PERSON

HOW TO HACK

HACK #1 BRUTE FORCE

```
top - 13:17:14 up 8 min,  1 user,  load average: 0.03, 0.12, 0.08
Tasks: 156 total,   1 running, 155 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.6 us,  0.7 sy,  0.0 ni, 98.8 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3952668 total,  2647052 free,   616124 used,   689492 buff/cache
KiB Swap:  4092924 total,  4092924 free,        0 used.  3077808 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 1467 root      20   0 1753600 253436  63352 S   2.3  6.4   0:18.08 gnome-shell
 1056 Debian-+  20   0 1811356 145452  54108 S   0.7  3.7   0:05.49 gnome-shell
 1301 root      20   0  436532  77052  37068 S   0.7  1.9   0:04.55 Xorg
 1020 Debian-+  20   0  357140  39812  29856 S   0.3  1.0   0:02.26 Xorg
 2313 root      20   0  590512  52812  31932 S   0.3  1.3   0:00.37 terminator
 2330 root      20   0   44892   3808   3148 R   0.3  0.1   0:00.04 top
    1 root      20   0  139408   7260   5268 S   0.0  0.2   0:01.13 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:00.01 ksoftirqd/0
    4 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    7 root      20   0       0      0      0 S   0.0  0.0   0:00.10 rcu_sched
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
    9 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 migration/0
   10 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 lru-add-drain
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/0
   12 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/0
   13 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/1
   14 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/1
   15 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 migration/1
   16 root      20   0       0      0      0 S   0.0  0.0   0:00.00 ksoftirqd/1
   18 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/1:0H
   19 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/2
   20 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/2
   21 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 migration/2
   22 root      20   0       0      0      0 S   0.0  0.0   0:00.00 ksoftirqd/2
   24 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/2:0H
   25 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
   26 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 netns
   27 root      20   0       0      0      0 S   0.0  0.0   0:00.00 khungtaskd
   28 root      20   0       0      0      0 S   0.0  0.0   0:00.00 oom_reaper
   29 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 writeback
   30 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kcompactd0
   32 root      25   5       0      0      0 S   0.0  0.0   0:00.00 ksmd
   33 root      39  19       0      0      0 S   0.0  0.0   0:00.00 khugepaged
   34 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 crypto
   35 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kintegrityd
   36 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 bioset
   37 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kblockd
   38 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 devfreq_wq
   39 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 watchdogd
   40 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kswapd0
   41 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 vmstat
   51 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kthrotld
   52 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 ipv6_addrconf
   60 root      20   0       0      0      0 S   0.0  0.0   0:00.02 kworker/1:1
   93 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 ata_sff
  109 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/u6:1
  138 root      20   0       0      0      0 S   0.0  0.0   0:00.00 scsi_eh_0
```

HOW TO HACK

HACK #2 PASSWORD GUESSING

```
root@kali: ~/Desktop/cupp 210x58
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
cupp  katana  sn1per  sqli-scanner  Trity
root@kali:~/Desktop# cd cupp
root@kali:~/Desktop/cupp# ls
CHANGELOG.md  cupp3.py  cupp.cfg  cupp.py  dictionaries  LICENSE  README.md  test_cupp.py
root@kali:~/Desktop/cupp# python cupp.py

  cupp.py!                  # Common
     \                      # User
      \   ,__,              # Passwords
       \  (oo)____          # Profiler
          (__)    )\
             ||--|| *       [ Muris Kurgas | j0rgan@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 WyD.pl output to make some pwnsauce

       -l      Download huge wordlists from repository

       -a      Parse default usernames and passwords directly from Alecto DB.
                Project Alecto uses purified databases of Phenoelit and CIRT
                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

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

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

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

DISABLE TRACKBACKS
WHY BOTHER WITH IT?

Spammy, Fake, and Annoying

Settings > Discussion

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

DISCOURAGE SPAMMERS
ADD A HUMAN TOUCH.

Human Interface Form

- Akismet Anit-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.

```php
// Disallow file edit
define( 'DISALLOW_FILE_EDIT', true );
```

DISABLE PHP FILE EXECUTION
NO PHP, NO CRY.

```
1 <Files *.php>
2 deny from all
3 </Files>
```

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

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

CHANGE WORDPRESS DATABASE PREFIX

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

Change all Database Tables Name

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

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

```
1  AuthName "Admins Only"
2  AuthUserFile
   /home/yourdirectory/.htpasswds/public_html/wp-
   admin/passwd
3  AuthGroupFile /dev/null
4  AuthType basic
5  require user putyourusernamehere
```

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
```

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.

```
function no_wordpress_errors(){
  return 'What the heck are you doing?! Back off!';
}
add_filter( 'login_errors', 'no_wordpress_errors' );
```

FIX A HACKED SITE

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

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