WordPress Security Essentials

The Whirlwind Tour

April 5th-6th, 2012

David Wilemski

@davidwilemski

davidwilemski.com

The Goal: Staying Afloat

photo by Flickr user davidesimonetti

WordPress Security

- Security Basics
- Plugins and services
- Disaster recovery

SUPER MEGA AWESOME:

http://codex.wordpress.org/Hardening_WordPress

Vulnerabilities

photo by Flickr user misterbisson

Common Attacks

- Most attacks aren't targeted
- Little time per site (blackhat seo)
- Known exploits (implies known solutions)

Change Database Table Prefix

- Defaults to "wp_"
- Use anything else
- Makes SQL injection a little more difficult

Delete 'admin' user

- In WP Dashboard create a new administrative user
- Log in as the new user, delete the original user
- Some scripts are programmed to target 'admin'
- You don't need to use an admin user for day to day posting and editing

Password Brute-forcing

- Automated attack on a user's account
- [usually] Takes time, will show up in logs
- Some evidence of scripts that are distributed across multiple nodes

> "On all the requests we logged, they only tried to guess the password for the user “admin”."

http://blog.sucuri.net/2012/03/brute-force-attacks-against-wordpress-sites.html

CHOOSE A SECURE PASSWORD!

- You know the deal: no dictionary words, use numbers and symbols
- or just use a strong password generator (and manager)
  - LastPass
  - 1Password
  - KeePassX

Passwords attempted

On all the requests we logged, they only tried to guess the password for the user “admin”. Of the attacks we analyzed, these were the top ranking passwords in each attack:

```
administrator
admin123
admin
soccer
root
qwerty
q1w2e3
password1
password
pass
admin12
admin1
987654321
123456
12345
111111
000000
passwd
```

http://blog.sucuri.net/2012/03/brute-force-attacks-against-wordpress-sites.html

Limit Login Attempts

- Rate limits failed login attempts
- Can hinder brute force attacks
- Notifies in case of too many failures

http://wordpress.org/extend/plugins/limit-login-attempts/

Check your site for known malware
and other undesirable things:

http://sitecheck.sucuri.
net/scanner/

Sucuri SiteCheck

Sitecheck Results | Website details | Blacklisting status

web site: davidwilemski.com
status: Verified Clean
web trust: Not Blacklisted

**This site was just scanned a few minutes ago.*

Security report (*No threats found*):

Blacklisted:	No
Malware:	No
Malicious javascript:	No
Malicious iFrames:	No
Drive-By Downloads:	No
Anomaly detection:	No
IE-only attacks:	No
Suspicious redirections:	No
Spam:	No

Raising The Bar

photo by Flickr user Mike_tn

Change wp-config.php secrets

- Security keys used for setting various cookies and internal crypto properties
- Changing them will just cause any logged in user to need to re-authenticate
- Use the generator:

https://api.wordpress.org/secret-key/1.1/salt/

- Bonus: IP restrict wp-admin

  - Use .htaccess to restrict access to the dashboard
  - If your public IP address changes you will get locked out of WP and need to edit the .htaccess via FTP or shell access

http://httpd.apache.org/docs/2.2/mod/mod_authz_host.html

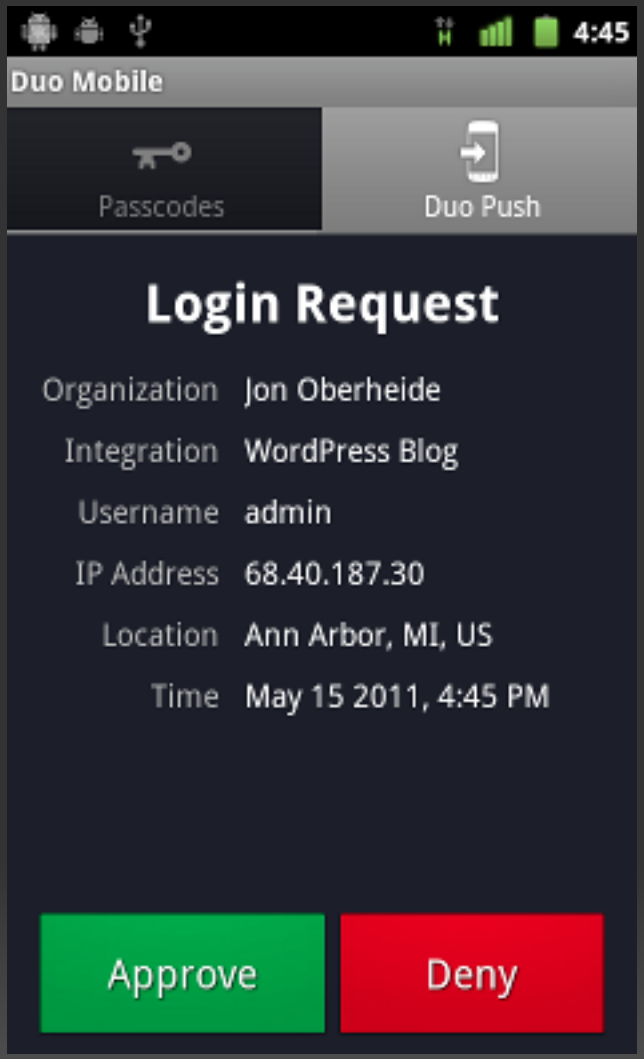
Unlimited Power

photo by Flickr user Frank.Li

Duo WordPress

- Two-factor authentication for your WordPress site
- Protects from account take over

Duo Push Notification



http://wordpress.org/extend/plugins/duo-wordpress/

Emergency Preparedness

photo by Flickr user doisespressos

Backups!

- Backup your WP database regularly (and the site files)!
- Do them, test them!
- Plugins: WP-DB-Backup or PressBackup

http://wordpress.org/extend/plugins/pressbackup/

http://wordpress.org/extend/plugins/wp-db-backup/

Disaster Recovery

photo by Flickr user born1945

Restore your site

- Do NOT just try to 'clean' the site
- You could miss hidden backdoors
- Backup the infected site for later analysis
- Restore from a known good backup

Protect your online identity

- Change your passwords to your database and WP user accounts
- Check your computer for malware
- Update your site and plugins
- Unsure of yourself? Hire an expert.

Investigate the attack

- Consider checking up the backed up copy of your site
- If the attack is made via a flaw in WP, file a bug or inform the mailing list

http://ottopress.com/2011/how-to-cope-with-a-hacked-site/

http://codex.wordpress.org/FAQ_My_site_was_hacked

Overwhelmed yet?

photo by Flickr user andresthor

VaultPress

- Paid service offered by Automattic to backup, scan, and protect your WordPress website
- Makes it easy to restore site backups
- Worth it if you don't have the time or want to manage things yourself

Once more

- Your site can be better protected with just a little effort
- It's all about raising the bar!
- Backups, backups, backups!

Thank You!
Questions?

David Wilemski
@davidwilemski