Simple WordPress Security

Barry Gould, BlogSec.net
Barry@blogsec.net

Why should we worry?

Hacked site = Loss of business / reputation from loss of customer trust. Cleanup costs.

Even ‘small’ sites are at risk; bots don’t discriminate!

Threats:

- BotNets - password guessing or exploitation
- Spammers / Spambots
- Black Hat Hackers & Script Kiddies

Why should we worry?

Ars Technica reports a BotNet with 90,000 IP addresses is trying to brute-force WordPress installs via password guessing.

Why should we worry?

What are they after:

- admin accounts & user accounts
    - admin access
    - email addresses & passwords
- hack your site to direct traffic to another site
    - fake Viagra, etc.
- grow their botnets - use your servers to:
    - send spam / malware
    - hack other sites
- defacement of popular sites

How can I protect myself?
Password Security

Passwords should be UNIQUE, esp. for your own sites and your email.

If you re-use passwords, when LinkedIn or Adobe gets hacked, now someone can login to your:

- email
- Facebook
- WP
- Bank Accounts

Password Complexity

Use Strong passwords on Important sites:

- at least 8 characters (letters + numbers/sym)
- mix upper & lower case
- best not to use words or names
- but make it easy to remember

PassPhrases: long but easy to remember

- AllRoadsLeadtoRom3. (19ch)
- movie quotes, song lyrics, jingles, etc.
- random words: CorrectHorseBatteryStaple

Passwords cont.

Or, take a phrase & make a shorter password:

- All Roads Lead to Rome -> ArltR2013 (9ch)
- CorrectHorseBatteryStaple -> CoHoBaSt.

WordPress Accounts

Separate Admin account; restrict use.

Delete the default ‘admin’ account!

Use Editor / Author / contributor account(s) instead of using Admin all the time. Only use Admin when needed. Each account should have a different password.

(at least) 1 acct. for each human; don’t share!

Password guesser protection

Plugin: “**Limit Login Attempts**”

- blocks attempts after 5 failed logins
- configurable # and timeout

Plugins & Themes

Choose your plugins carefully.

"7 out of top 10 most popular e-commerce plugins are vulnerable to common Web attacks

"20% of the 50 most popular WordPress plugins are vulnerable to common Web attacks"
- CheckMarx, June 2013

Many WP Themes have vulnerabilities as well.

Plugins & Themes

Make sure all plugins & themes are safe & maintained / actively developed:

- get plugins/themes from well-known sites
- skip ones that haven’t been updated in years
- skip ones that don’t seem to have any community (forums, bug trackers, etc.)

Make sure to keep everything updated!

Delete themes & plugins you’re no longer using

Application Security

Make sure to keep everything updated!

- WP + Themes & Plugins
- OS + Apache, PHP, etc.

If using managed / shared hosting, make sure host keeps things updated, or reminds you to.

Check regularly.

Operational Security

Don’t login from shared computers, ever. (unless you’re using 2-factor auth)

- If you had to, change your password when you get to the office or home.

Don’t login to anything from public networks / WiFi without SSL, SSH, SFTP

- sniffers can easily steal your password

Operational Security, cont.

Run Anti-Virus software on your PCs & Macs.

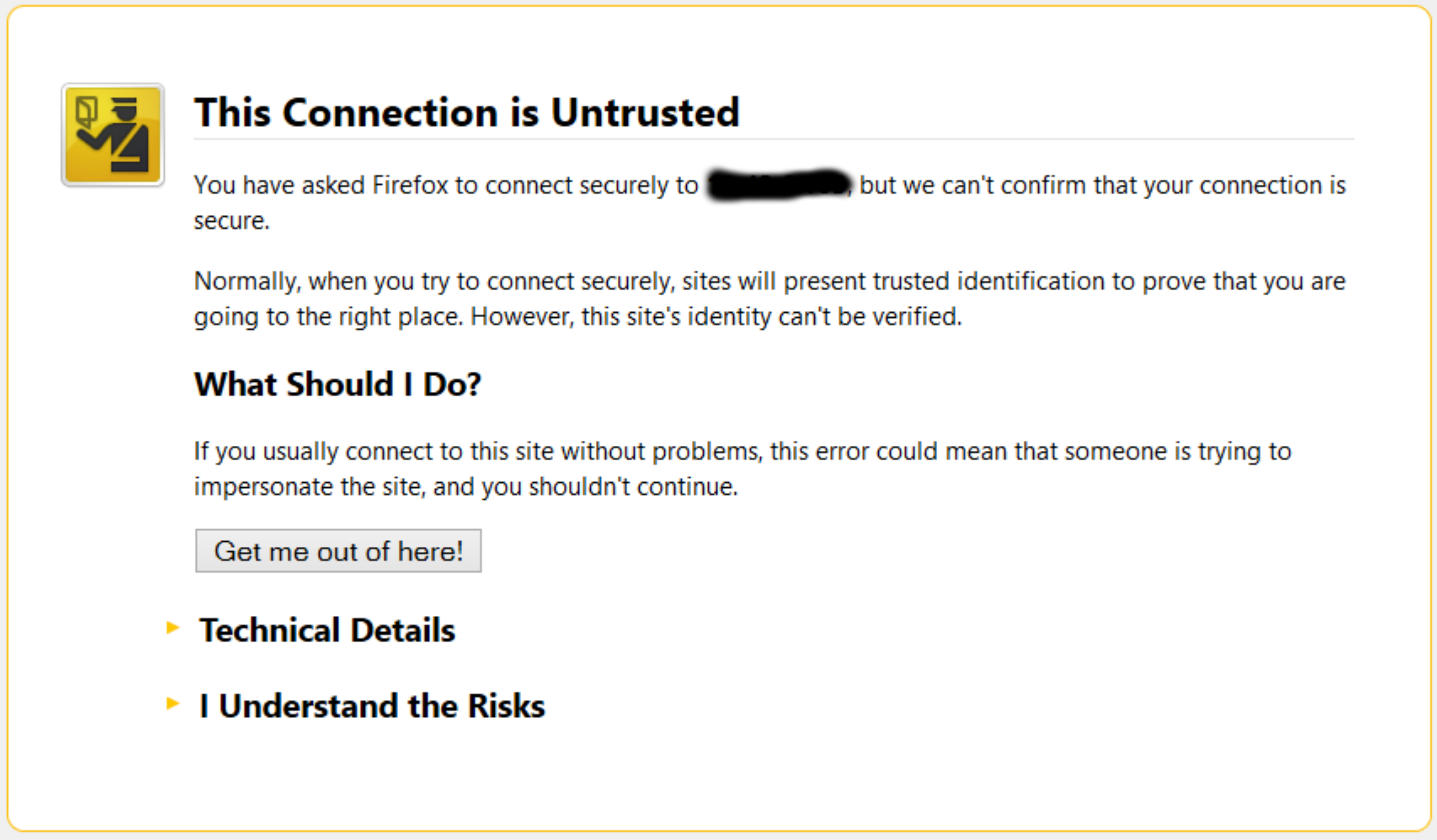
Use secure protocols, esp. on public networks:

- HTTPS / SSL instead of HTTP for admin
- SFTP / SCP instead of FTP
- SSH instead of Telnet

Applies to Phones / Tablets too.

Pay attention to browser/app certificate warnings.

Example Certificate Warning



This Connection is Untrusted

You have asked Firefox to connect securely to [redacted], but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

▸ Technical Details

▸ I Understand the Risks

Operational Security, cont.

Backup regularly - Data + code

- Don’t leave backup files on the server
- code backups allow reference / diff in case of hack

Don’t leave sensitive info on the server or in WP:

- inactive email lists
- billing info

Advanced Security Topics

- Don’t expose the database to internet
- change permissions on .htaccess!
- use a separate Dev/Staging site
  - or your PC - Desktop Server, XAMPP, Local WP...
- 2-Factor authentication
  - Google Authenticator on phone + WP plugin
- use Version Control software
- Firewalls
- WAFs (ModSecurity, etc.)
- IPS (Intrusion Protection System)
- VPNs

Advanced Security Topics

Network / Vulnerability Scanning:

Scan yourself, using Web Application Vulnerability Scanner(s):

- Nessus
- Nikto
- Acunetix
- OpenVAS

Get familiar, then watch for changes

Further learning

Books:

WordPress 3 Ultimate Security (2011)

Google is your Friend.

Meetups - participate / ask questions!

Questions?

Questions?

Future Presentations?:

- eCommerce security / PCI DSS
- Advanced WP security / lockdown

Contact me:

Barry@BlogSec.net

http://BlogSec.net