do_action('hack_me')
Who are we and why are we talking about this?

ABOUT US
Joshua Hansen
• This is my first WordCamp
• Security and Open Source enthusiast
• Prefers British television
• Finding vulnerabilities is fun

Kurt Payne
• WordPress core contributor
• Makes inside jokes about Futurama
• Television Snob
• Can’t sleep when unit tests are failing
Reasons your site gets hacked

WHY ME?
Money

• Phishing Site
• Malware Downloads
• Warez/Piracy
• SEO
• Spam
• DDOS
What are they exploiting?

COMMON VULNERABILITIES
OWASP Top Ten

- Injection
- Cross-Site Scripting
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-Site Request Forgery
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards
Explanation and Example

REMOTE FILE INCLUSION
Prevention

REMOTE FILE INCLUSION
• Never trust user supplied input!
• Sanitize your data -
  http://codex.wordpress.org/Data_Validation
• Verify length
• Verify type
• Test against regex
• Compare against whitelist
• Validate inputs
EXPLANATION AND EXAMPLE

CROSS-SITE SCRIPTING (XSS)
Prevention

CROSS-SITE SCRIPTING (XSS)
• Never trust user supplied input!
• Sanitize your data - 
  http://codex.wordpress.org/Data_Validation
• Escape based on context
• Use the methods provided by WordPress
Explanation and Example

SQL INJECTION
Prevention

SQL INJECTION
• Never trust user supplied input!
• Sanitize your data -
  http://codex.wordpress.org/Data_Validation
• Use Prepared Statements – wpdb::prepare()
• Escape user supplied input
• Least Privilege
• Whitelist input validation
Tools and Resources

WHAT CAN I DO?
RIPS
Vulnerability Databases
Links

- W3AF - [http://w3af.sourceforge.net/](http://w3af.sourceforge.net/)
- OWASP - [https://www.owasp.org](https://www.owasp.org)
- WordPress SQLi - [http://codex.wordpress.org/Class_Reference/wpdb#Protect_Queries_Against_SQL_Injection_Attacks](http://codex.wordpress.org/Class_Reference/wpdb#Protect_Queries_Against_SQL_Injection_Attacks)
- WordPress Data Validation – [http://codex.wordpress.org/Data_Validation](http://codex.wordpress.org/Data_Validation)