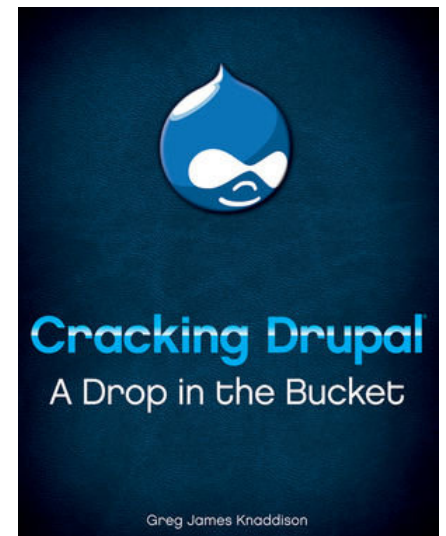


# Drupal Security

## Who

- Ben Jeavons
  - Drupaler for 3 years
  - Joined security team in Spring
  - Growing a mustache for charity (I know you were curious)
- Growing Venture Solutions
  - Full service design and development
  - Training service and usability reviews
  - Security reviews



Your site is vulnerable

You can make it safer

## What attackers do

- Steal resources
- Steal data
- Alter data



## Demo of a defacement attack

# Vulnerabilities by Type



- XSS
- Access Bypass
- CSRF
- SQL Injection
- Code Execution
- Clarification, PSA, etc.
- Session Fixation
- Others

## Common attacks

- Cross-site scripting (XSS)
- Access bypass
- Cross-site request forgery
- SQL injection

## Stay safe with smart configuration

- Sensible input formats
  - Avoid XSS
- Least privilege permissions
  - Avoid access bypass











## Input Formats

Default	Name	Roles	Operations
<input checked="" type="radio"/>	Filtered HTML	All roles may use default format	<a href="#">configure</a>
<input type="radio"/>	Full HTML	No roles may use this format	<a href="#">configure</a> <a href="#">delete</a>

[Set default format](#)

Also, don't enable the PHP Filter unless really needed

## Input Formats

Name	Weight
 URL filter	0 
 HTML filter	1 
 Line break converter	2 
 HTML corrector	10 

Save configuration

Drupal.org <http://drupal.org/node/224921>  
Cracking Drupal: Chapter 3

## Input Formats

### Allowed HTML tags:

```
<a> <em> <strong> <cite> <code> <ul> <ol> <li> <dl> <dt> <dd>
```

If "Strip disallowed tags" is selected, optionally specify tags which should not be stripped. JavaScript event attributes are always stripped.

### Tags you should not grant to untrusted users:

script, img, iframe, embed, object, input, link, style, meta, frameset, div, base, table, tr, td

XSS demo

## “Super” permissions

- Administer permissions
- Administer users
- Administer filters
- Administer content types
- Administer site configuration

Give these to trusted users only

## Contrib Permissions

- XSS common in contrib modules
- Utilize principle of *Least Privilege*
  - Provide only the necessary permissions

## Recovering

- Backups
  - You do have backups, don't you?
- Update your code
- Change your passwords



## Prioritize your actions

Stay ahead of the pack?

Protect valuable assets?



## Keep your site up to date

- Know about updates
  - Update status module
  - Security updates via email or RSS
  - Mailing list and Twitter accounts
- Choose an update method

## Keep your site up to date

- Know about updates
- Choose an update method
  - drupal.org tgz files
  - CVS from drupal.org or 3rd-party hosts
  - Drush
  - Aegir
  - Acquia's remote administration

## Resources

- Drupal.org - <http://drupal.org/security-team>
- <http://drupal.org/security>
- <http://drupal.org/writing-secure-code>
- <http://drupal.org/security/secure-configuration>
- <http://groups.drupal.org/node/15254> - discussion group
- Security Team leader's blog - <http://heine.familiedeelstra.com/>
- Cracking Drupal - <http://crackingdrupal.com>