commonplaces
www.commonplaces.com

Hack-proof Your Drupal App

Key Habits of Secure
Drupal Coding

Introductions

- CommonPlaces
  - Erich Beyrent, V.P. of Engineering
  - Amanda Giovanni, Director of Enterprise Risk Management

Introductions

- WhiteHat Security
  - Arian Evans, Operations Director

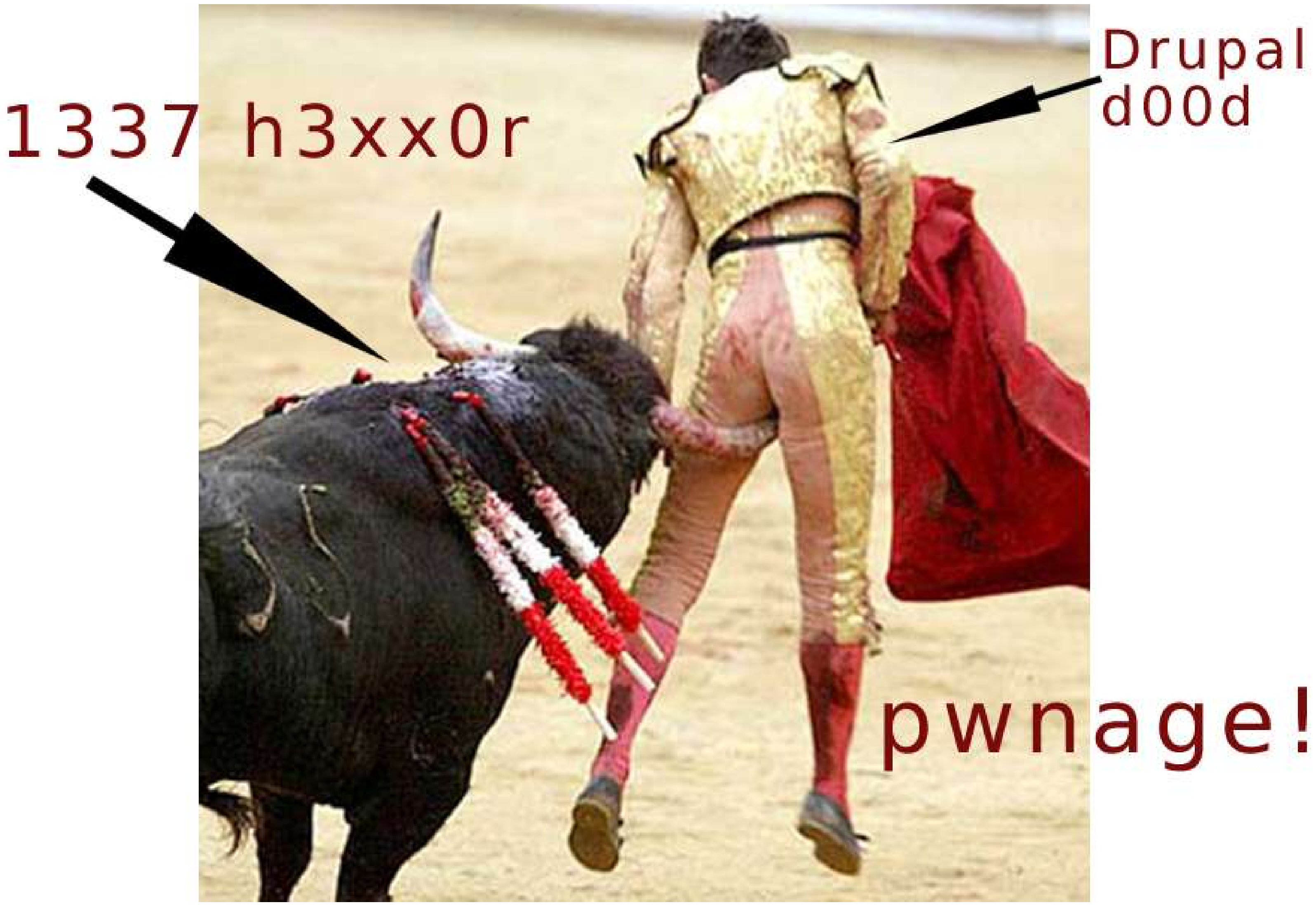
Introductions

KATALYST STRATEGIES, LLC
Comprehensive Cyber Security Solutions

- Katalyst Strategies
  – Matthew J. Nash, Director of Cyber Risk Management

Security? Who cares?

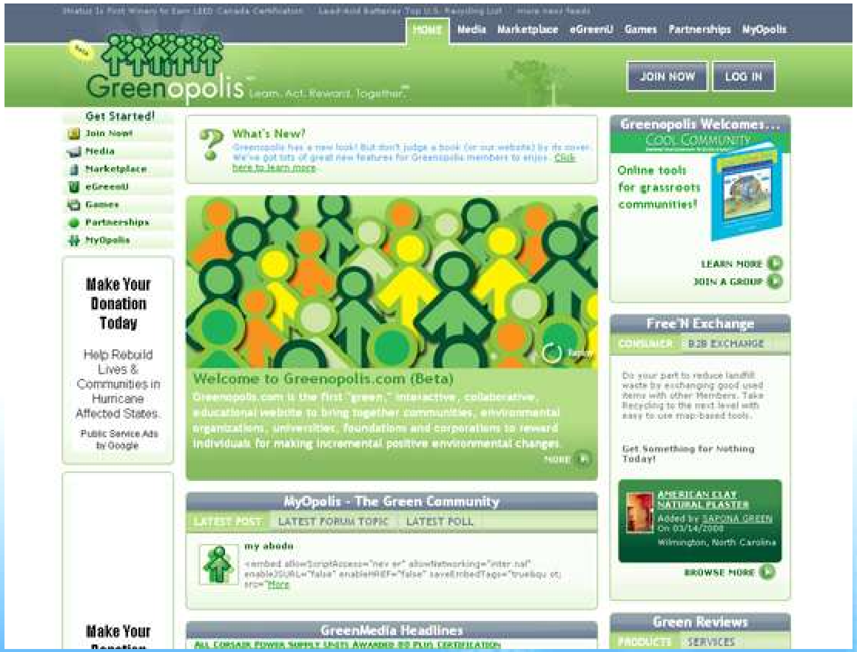
Have you ever been hacked?



Web Application Security

- Analysts estimate that 75% of attacks against web servers enter at the application, not the network level
- As many as 15% of these attacks are due to poor coding practices

Case Study: Greenopolis.com


Stratus Is First Winery to Earn LEED Canada Certification · Lead-Acid Batteries Top U.S. Recycling List · more news feeds

HOME · Media · Marketplace · eGreenU · Games · Partnerships · MyOpolis

Greenopolis™ Learn. Act. Reward. Together.™

JOIN NOW · LOG IN

Get Started!
- Join Now!
- Media
- Marketplace
- eGreenU
- Games
- Partnerships
- MyOpolis

Make Your Donation Today

Help Rebuild Lives & Communities in Hurricane Affected States.

Public Service Ads by Google

What's New?

Greenopolis has a new look! But don't judge a book (or our website) by its cover. We've got lots of great new features for Greenopolis members to enjoy. Click here to learn more.

Welcome to Greenopolis.com (Beta)

Greenopolis.com is the first "green," interactive, collaborative, educational website to bring together communities, environmental organizations, universities, foundations and corporations to reward individuals for making incremental positive environmental changes.

MORE

MyOpolis - The Green Community

LATEST POST · LATEST FORUM TOPIC · LATEST POLL

my abodo

<embed allowScriptAccess="never" allowNetworking="internal" enableJSURL="false" enableHREF="false" saveEmbedTags="true&qu ot; src="More

GreenMedia Headlines

ALL CORSAIR POWER SUPPLY UNITS AWARDED 80 PLUS CERTIFICATION

Greenopolis Welcomes...

COOL COMMUNITY

Online tools for grassroots communities!

LEARN MORE
JOIN A GROUP

Free'N Exchange

CONSUMER · B2B EXCHANGE

Do your part to reduce landfill waste by exchanging good used items with other Members. Take Recycling to the next level with easy to use map-based tools.

Get Something for Nothing Today!

AMERICAN CLAY NATURAL PLASTER
Added by SAPONA GREEN
On 03/14/2008
Wilmington, North Carolina

BROWSE MORE

Green Reviews

PRODUCTS · SERVICES

Make Your Donation

commonplaces
www.commonplaces.com

Case Study: Greenopolis.com

- Modules
- Theme
- Flash and Flex
- Security Audit Results

Greenopolis Modules

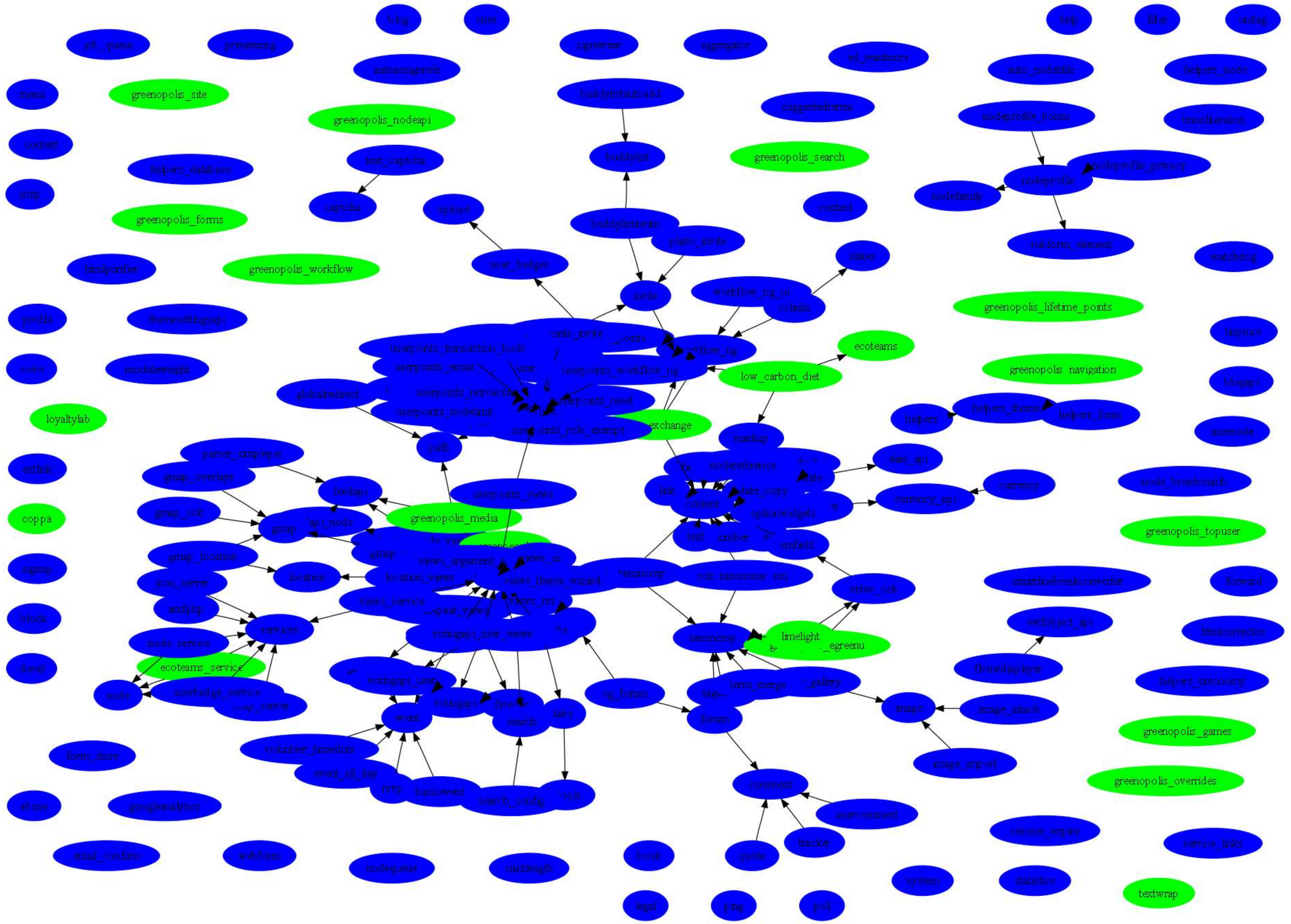
- Greenopolis currently uses 92 modules

Greenopolis Modules

- Greenopolis currently uses 92 modules
- 20% of those modules are custom

commonplaces

www.commonplaces.com



Greenopolis Theme

- Greenopolis uses a custom theme
- template.php, lots of individual templates

Flash and Flex

- Greenopolis has Flex widgets that can be embedded on any site, which get data via Services

Flash and Flex

- Greenopolis has Flex widgets that can be embedded on any site, which get data via Services
- Greenopolis has an interactive Flash map of the US that gets data from Services

commonplaces
www.commonplaces.com

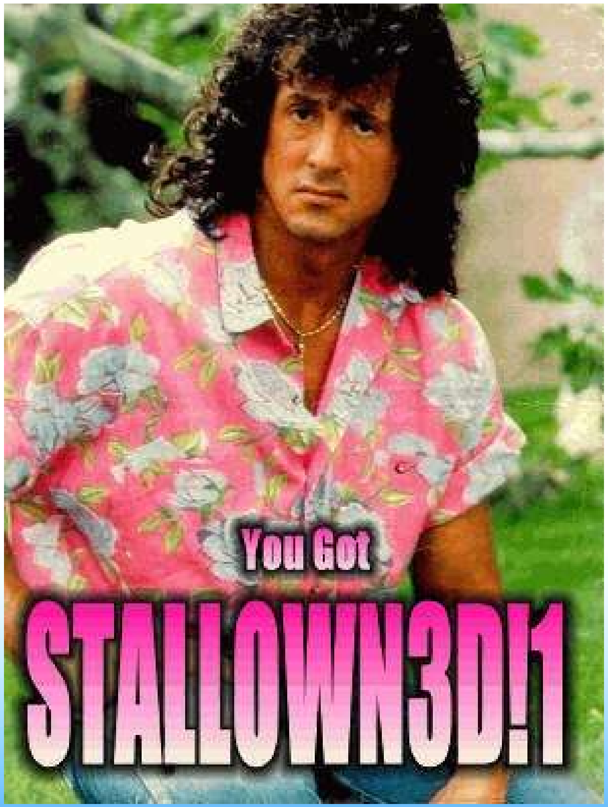
Flash and Flex

- Greenopolis has Flex widgets that can be embedded on any site, which get data via Services
- Greenopolis has an interactive Flash map of the US that gets data from Services
- Greenopolis has a Flex TiltingPane widget that displays partner logos, populated via Services

Security Audit Results

- WhiteHat Security performed an audit of the application layer

Security Audit Results



- 120 vulnerabilities were discovered in the following categories:
  - XSS
  - CSRF
  - SQL Injection
  - Session fixation
  - Insufficient Authorization

What We Learned:

- 90% of the vulnerabilities existed in the theme

Fixing The Problems:

- Completely reviewed the theme, implementing Drupal output filters

Fixing The Problems:

- Completely reviewed the theme, implementing Drupal output filters
- Code was audited to ensure sanitization of all user generated data

Fixing The Problems:

- Completely reviewed the theme, implementing Drupal output filters
- Code was audited to ensure sanitization of all user data
- Rewrote the search forms to sanitize user generated data

Fixing The Problems:

- Completely reviewed the theme, implementing Drupal output filters
- Code was audited to ensure sanitization of all user data
- Rewrote the search forms to sanitize user data
- Implemented web services proxy

Key Habits of Secure Drupal Coding

www.commonplaces.com

We are going to discuss:

- Sanitize Your Output

We are going to discuss:

- Sanitize Your Output
- Protect Your Database

We are going to discuss:

- Sanitize Your Output
- Protect Your Database
- User Input

commonplaces
www.commonplaces.com

We are going to discuss:

- Sanitize Your Output
- Protect Your Database
- User Input
- AJAX Risks

Sanitize Your Output:

- check_plain()
- check_markup()
- filter_xss()
- filter_xss_admin()

Sanitize Your Output:

Correct Usage:

```
echo check_plain($node->field_fname[0][‘value’]);
echo content_format(‘field_fname’, $node->field_fname[0][‘value’]);
echo t(‘%fname’, array(‘%fname’ => $node->field_fname[0][‘value’]));
echo t(‘@fname’, array(‘@fname’ => $node->field_fname[0][‘value’]));
```

Incorrect Usage:

```
echo $node->field_fname[0][‘value’];
```

Protect Your Database:

- db_query()
- db_rewrite_sql()

Protect Your Database:

Correct usage:

$result = db_query(“SELECT foo FROM {bar} WHERE foo = ‘%s’, $unsafe_var);

Incorrect usage:

$result = db_query(“SELECT foo FROM {bar} WHERE foo = $unsafe_var”);

User Input:

- Use the Form API

User Input:

- Use the Form API
  - Sanitize $_POST (and $_GET) data

Javascript and AJAX:

- Rule #1 – Javascript can be disabled
- Don’t assume data to AJAX postback functions are coming from your javascript
- Don’t assume AJAX transactions are private and cannot be observed by users
- Re-encode and escape all output

Don’t Trust User Input!

Things That Will Bite You:

- Outputting raw values
- Modifying data with $_GET
- Parameterized queries? WTF?
- Hacking core and killing kittens

Drupal Security Resources

- Drupal.org
  - http://drupal.org/writing-secure-code
  - http://drupal.org/node/28984
- Drupal Security Team
  - http://drupal.org/node/32750
- Pro Drupal Development book
  - http://drupalbook.com

Drupal Tools

- Update module http://drupal.org/project/update_status
- Coder module http://drupal.org /project/coder
- Interactive debuggers (Zend, XDebug)

Participate!

- Subscribe to the Drupal Security RSS feed
- Send vulnerabilities and patches to the Drupal Security Team

commonplaces
www.commonplaces.com

Q & A

Erich Beyrent, erich@commonplaces.com

Arian Evans, arian.evans@whitehatsec.com