

A close-up photograph of a green, textured metal door. A large, circular, rusted metal handle is centered on the door. A heavy metal chain is wrapped around the handle, and a large, rectangular metal padlock is attached to the chain. The padlock has a small metal tag attached to it. The door shows signs of wear and rust. The text "Security Risks and Smart Configuration: Securing Your Drupal Site" is overlaid in white, bold, sans-serif font across the center of the image.

Security Risks and Smart Configuration: Securing Your Drupal Site

<http://www.flickr.com/photos/maistora/3237164755/>

Ben Jeavons

Drupaler for 4 years

Growing Venture Solutions

Provide Security Testing

Member of Drupal Security Team



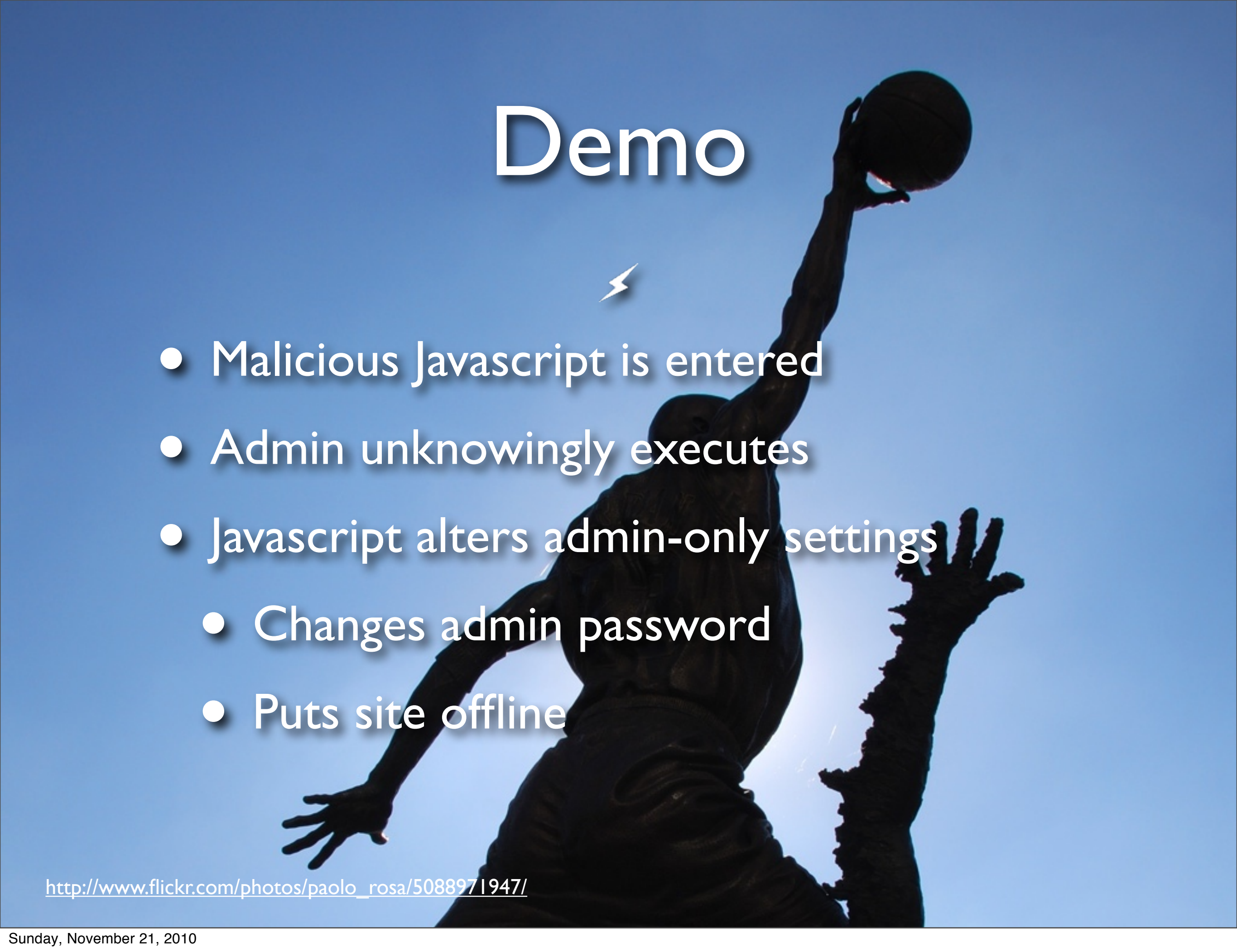
Lots of risks

- Mis-configuration
- Insecure code
- Unsafe practices

Mitigation

- Secure configuration
- Visitor access
- Secure processes
- Secure code

Demo

- 
- A silhouette of a basketball player in mid-air, shooting a ball. The player is positioned on the right side of the frame, with their right arm extended upwards holding the ball. Their left arm is also extended outwards. The background is a clear blue sky. A small white lightning bolt icon is positioned above the player's head, to the left of the word 'Demo'.
- Malicious Javascript is entered
 - Admin unknowingly executes
 - Javascript alters admin-only settings
 - Changes admin password
 - Puts site offline

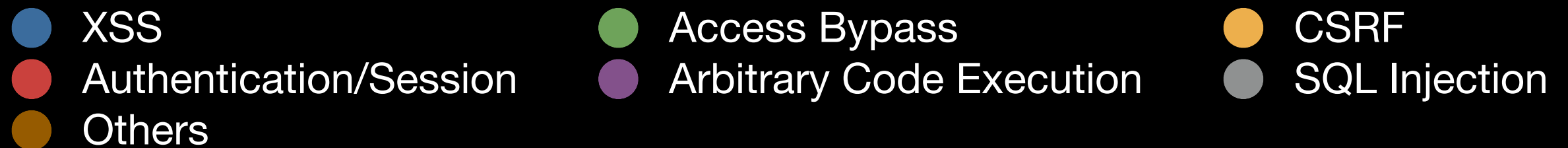
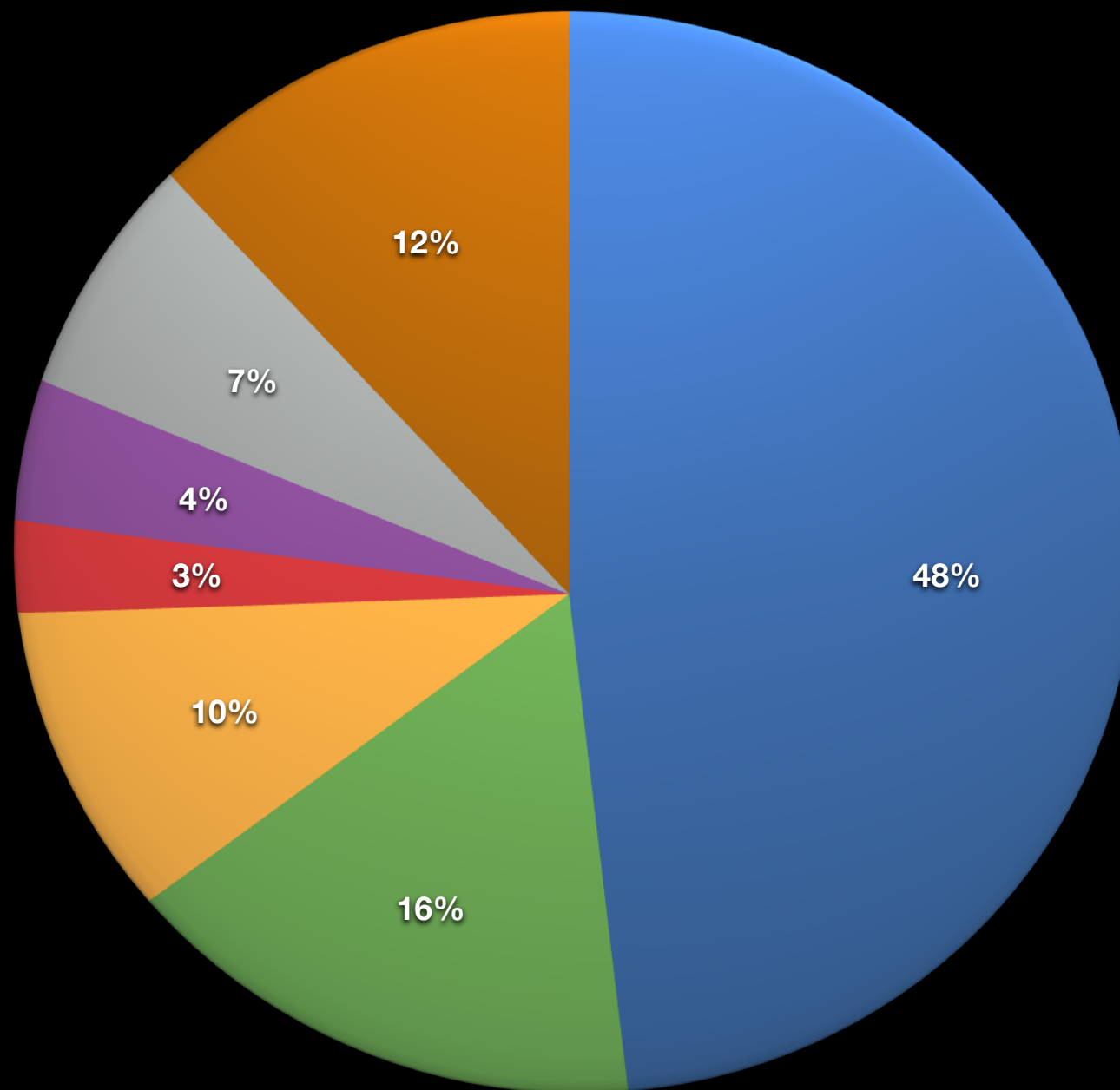
http://www.flickr.com/photos/paolo_rosa/5088971947/

Web security



- Protecting resources from abuse
- Protecting data
- Protecting available actions

Drupal vulnerabilities by popularity



reported in core and contrib SAs from 6/1/2005 through 3/24/2010

Examples

Examples

- Free shopping with Ubercart
- Own site with Webform
- Steal data with Views

Smart configuration

Smart configuration

- Control user input
 - Input formats
- Trust
 - Roles and permissions

Input formats

Default	Name	Roles	Operations	
<input checked="" type="radio"/>	Filtered HTML	All roles may use default format	configure	
<input type="radio"/>	Full HTML	group manager	configure	delete

Input formats

Default	Name	Roles	Operations	
<input checked="" type="radio"/>	Filtered HTML	All roles may use default format	configure	
<input type="radio"/>	Full HTML	group manager	configure	delete

- Formats run when displaying input
- Filtered HTML for *untrusted* roles
- Full HTML for completely *trusted* roles

Filtered HTML

- HTML filter
- Limits the allowed tags

Filters

Choose the filters that will be used in this filter format.

☒ **HTML corrector**
Corrects faulty and chopped off HTML in postings.

☒ **HTML filter**
Allows you to restrict whether users can post HTML and which tags to filter out. It will also remove harmful content such as JavaScript events, JavaScript URLs and CSS styles from those tags that are not removed.

☒ **Line break converter**
Converts line breaks into HTML (i.e.
 and <p> tags).

☒ **URL filter**
Turns web and e-mail addresses into clickable links.

Allowed HTML tags:

<a> <cite> <code> <dl> <dt> <dd>

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

Unsafe HTML tags



- Script tags or any that allow JS events
 - `<script>`
- Any that allow URL reference

Solution?



- Control access to full HTML tag usage
- Use HTML Purifier

Trust

Trust

- Know your roles
 - Which users have which roles
- How roles are granted

“Super-admin” permissions



- Permissions to give only, only to trusted people

“Super-admin” permissions



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

Trust

- Utilize principle of *Least Privilege*
 - Grant only the necessary permissions to carry out the required work

Search



Advance Search

updates

Apr 20, 2010
Maximizing your conference experience.

Apr 23, 2010
Blogging tips for the beginner.

**Psychological Trauma:
Neuroscience,
Attachment, and
Therapeutic Interventions**

May 19-22, 2010, Boston MA



TRAUMA CENTER
At Justice Resource Institute

**Improvisation & Cross-
Cultural Creativity:
Fostering Connections
Through Spontaneous
Musical Art**

De 2-5, 2010, Ann Arbor MI



Variable editor

This is a list of the variables and their values currently stored in variables table and the \$conf array of your settings.php file. These variables are usually accessed with `variable_get()` and `variable_set()`. Variables that are too long can slow down your pages.

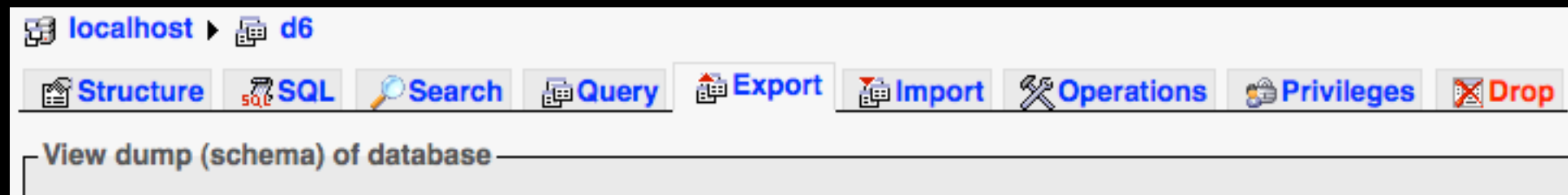
<input type="checkbox"/> Name ▲	Value	Length	Operations
<input type="checkbox"/> admin_menu_rebuild_links	b:1;	4	edit
<input type="checkbox"/> adserve	s:30:"sites/all/modules/ad/serve.php";	38	edit
<input type="checkbox"/> adserveinc	s:32:"sites/all/modules/ad/adserve.inc";	40	edit
<input type="checkbox"/> adserve_exit_text	s:6:"a:0:{}";	13	edit
<input type="checkbox"/> adserve_filter	s:6:"a:0:{}";	13	edit
<input type="checkbox"/> adserve_init_text	s:6:"a:0:{}";	13	edit
<input type="checkbox"/> adserve_select	s:6:"a:0:{}";	13	edit
<input type="checkbox"/> advuser_listno	i:50;	5	edit
<input type="checkbox"/> advuser_modify_mail	s:402:"==== User Information: ==== %user_name created on %us...	411	edit
<input type="checkbox"/> advuser_modify_notify	b:0;	4	edit
<input type="checkbox"/> advuser_modify_subject	s:49:"[%site] user (%user_name) modified their account.";	57	edit
<input type="checkbox"/> advuser_new_mail	s:402:"==== User Information: ==== %user_name created on %us...	411	edit
<input type="checkbox"/> advuser_new_notify	b:0;	4	edit
<input type="checkbox"/> advuser_new_subject	s:36:"[%site] has a new user (%user_name).";	44	edit
<input type="checkbox"/> advuser_profile_fields	N;	2	edit

Recovering from attack

Recovering from attack

- Restore from backup
- Upgrade to latest security releases
- Change your passwords
- Audit your configuration & custom code

Backups



- You do have backups, don't you?
- phpMyAdmin > Export
- mysqldump on the command line
- Be sure to check they worked!



Defense in Depth

<http://www.flickr.com/photos/zhzheka/522950864>

Sunday, November 21, 2010

Stay up-to-date



Stay up-to-date



- Know about security updates
 - Security Advisories
 - Update status module
 - Mailing list, RSS, Twitter
- Apply them!

Security updates

- Most security updates are small
 - But not always
- Apply updates to development instance
 - Test, then apply to production

FTP



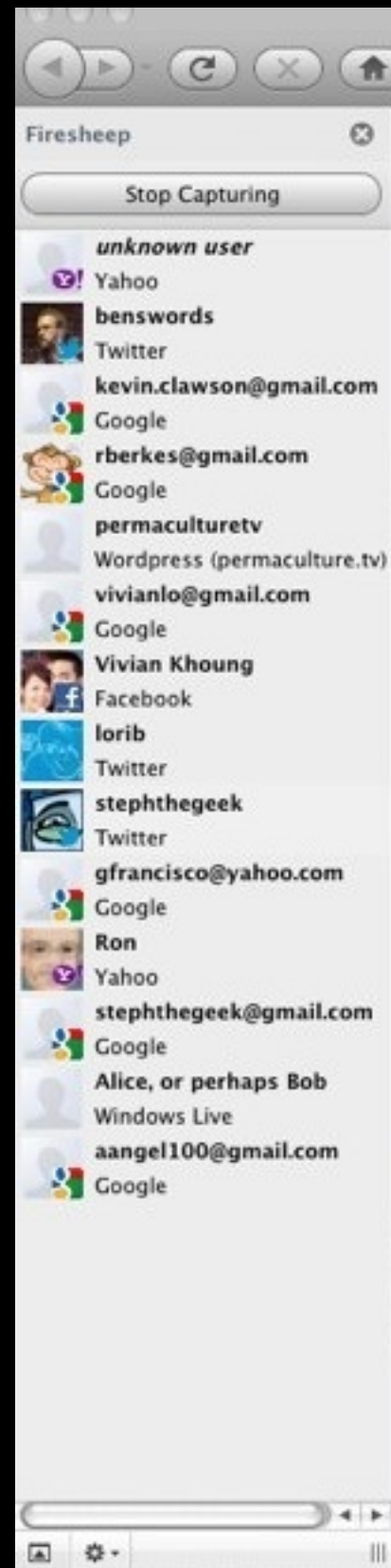
- Do not use it!
 - Common vector for attack
 - Really, we've moved past plain-text

SFTP



- “Secure” FTP
 - Your host should provide it
 - If not, consider a new one

SSL



Twitter / Home

http://twitter.com/

Session S... surveys a... Field Exa... Synch all ... Give war... Security r... Twitter Firesheep... tinyproxy... Twitte...

Stop Capturing

unknown user
Yahoo
benswords
Twitter
kevin.clawson@gmail.com
Google
rberkes@gmail.com
Google
permaculturetv
Wordpress (permaculture.tv)
vivianlo@gmail.com
Google
Vivian Khoung
Facebook
lorib
Twitter
stephthegeek
Twitter
gfrancisco@yahoo.com
Google
Ron
Yahoo
stephthegeek@gmail.com
Google
Alice, or perhaps Bob
Windows Live
aangel100@gmail.com
Google

twitter Search Home Profile Messages

stephthegeek

What's happening?

Timeline @Mentions Retweets Searches Lists

greg_harvey Greg Harvey
Unbelievable. Mid-November and I just killed a mosquito in our bedroom. One warm day and we have all the summer bugs again!
from Uzès, Gard
6 minutes ago

PavlovDawning Blake
The Inspiration Principle: Creativity can neither be created nor destroyed. It just changes form.
12 minutes ago

greg_harvey Greg Harvey
And like so many good movies, the original version was made in Asia (Hong Kong, to be precise - see Infernal Affairs).
from Uzès, Gard
14 minutes ago

jensimmons Jen Simmons
"Rockin' HTML5 + Drupal" revised slides are now up at
<http://jen.cm/h2> ! #drupal #html5 #badcamp
15 minutes ago

greg_harvey Greg Harvey
Just watched The Departed again. Great movie, all star cast:
<http://www.imdb.com/title/tt0407887/>
from Uzès, Gard
20 minutes ago

torgospizza torgospizza
Hello! Message me on Twitter!

Your Tweets **3,139**
5 hours ago: @melissamcewen thanks for the twitter updates btw. fascinating stuff!

Following **214**
Favorites **4**
★ **sotak** been playing with fusion core and skinr module yesterday. think its g...

Followers **996**
Listed **120**
Recently listed in: [Drupal](#), [drupal](#), [Drupal](#), [Web Development](#), [Drupal](#)

Trends
San Francisco · [change](#)
[#thingsthatgrindmygears](#)
[#badass](#)
[#kissmyass](#)
[Suu Kyi](#)
[Aung](#)
[Ocean Beach](#)
[Eddie Guerrero](#)
[WOD](#)
[Memorial Stadium](#)
[Jay Electronica](#)

Who to follow
Suggestions for you · [view all](#)
[katalene](#) · Follow
katherine smith
[EclipseGc](#) · Follow
EclipseGc
[joshuago78](#) · Follow
Joshua Gomez
[katherinebailey](#) · Follow
katherinebailey
[Refresh suggestions](#)
[Browse interests](#) · [Find friends](#)

Twitter for iPad
n. the official Twitter app for iPad.

About · Help · Blog · Status · Jobs · Terms · Privacy · Shortcuts
Businesses · Media · Developers · Resources · © 2010 Twitter

Find: csrf Next Previous Highlight all Match case

Done

SSL

- Run Drupal on full TLS/SSL
- Use `securepages` and `securepages_prevent_hijack` modules
- <http://crackingdrupal.com/blog/greggles/drupal-and-ssl-multiple-recipes-possible-solutions-https>
- Use a valid certificate

Security Review

- drupal.org/project/security_review
- File system permissions
- Granted “super-admin” permissions
- Input formats
- Allowed upload extensions
- PHP & Javascript in content

Custom code

- drupalsecurityreport.org
- Most vulnerabilities exist in custom code
 - Best practices and API is not followed despite documentation

Custom code

- Stay in this room to write secure code
- *Drupal Security for Coders*
 - with Greg Knaddison

Security Advisories

drupal.org/security

Handbooks

drupal.org/security/secure-configuration

drupal.org/writing-secure-code

Security Review module

drupal.org/project/security_review

Cracking Drupal Book

crackingdrupal.com

Thanks!

drupal.org & IRC: coltrane

ben@growingventuresolutions.com

@benswords

My thanks to Greg Knaddison

