Drupal Security

Configuration and Process

Ben Jeavons

- Drupaler for 3+ years
- Member of Drupal Security Team
- Growing Venture Solutions
  - Provides Security Testing

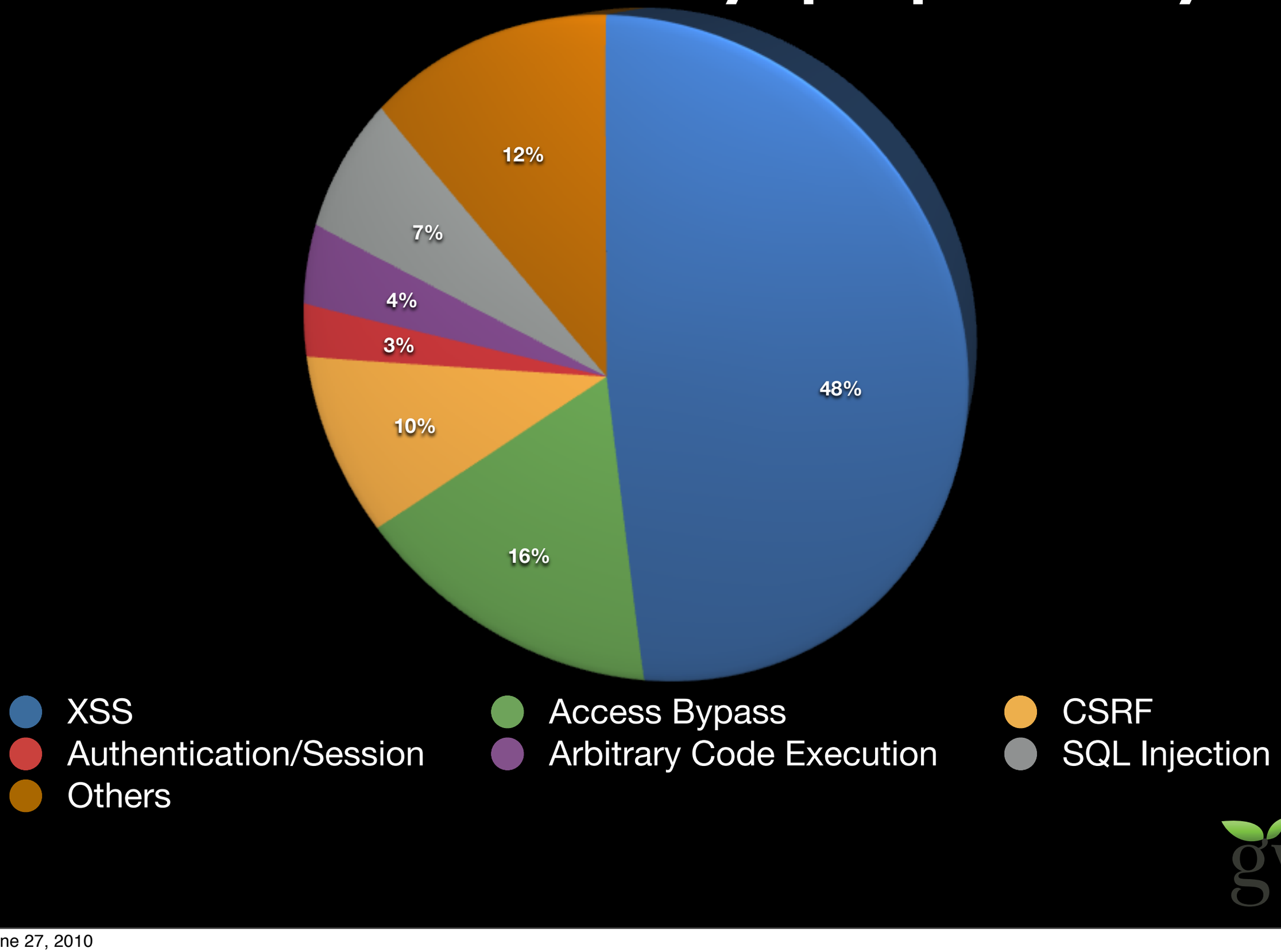
Web security

- Protecting resources from abuse
- Protecting data
- Protecting available actions
- Attackers exploit a weakness to do harm

Demo

- Malicious Javascript is entered
- Admin unknowingly executes
- Javascript alters admin-only settings
  - Changes admin password
  - Puts site offline

Vulnerabilities by popularity



Cross Site Scripting

- Attacker injects malicious code into weak website
- Site visitor unknowingly runs code

Access Bypass

- Inadequate or weak access control over a resource

Cross Site Request Forgery

- Attacker makes action occur on site
- On your behalf
- Without you knowing or approving

SQL Injection

- Attacker "tricks" SQL into interpreting some incoming data as a command
- Command gets or deletes private data

Common vulnerabilities

- Cross Site Scripting (XSS)
- Access Bypass
- Cross Site Request Forgery (CSRF)
- SQL Injection
- (lots more)

Lots of risks

- Prioritize your actions
  - Secure configuration
  - Careful processes
    - Keep code up-to-date
  - Audit custom code

Smart configuration

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

Input formats

Default	Name	Roles	Operations	
◉	Filtered HTML	All roles may use default format	configure	
○	Full HTML	group manager	configure	delete

- Input formats control what happens when user-supplied data is displayed

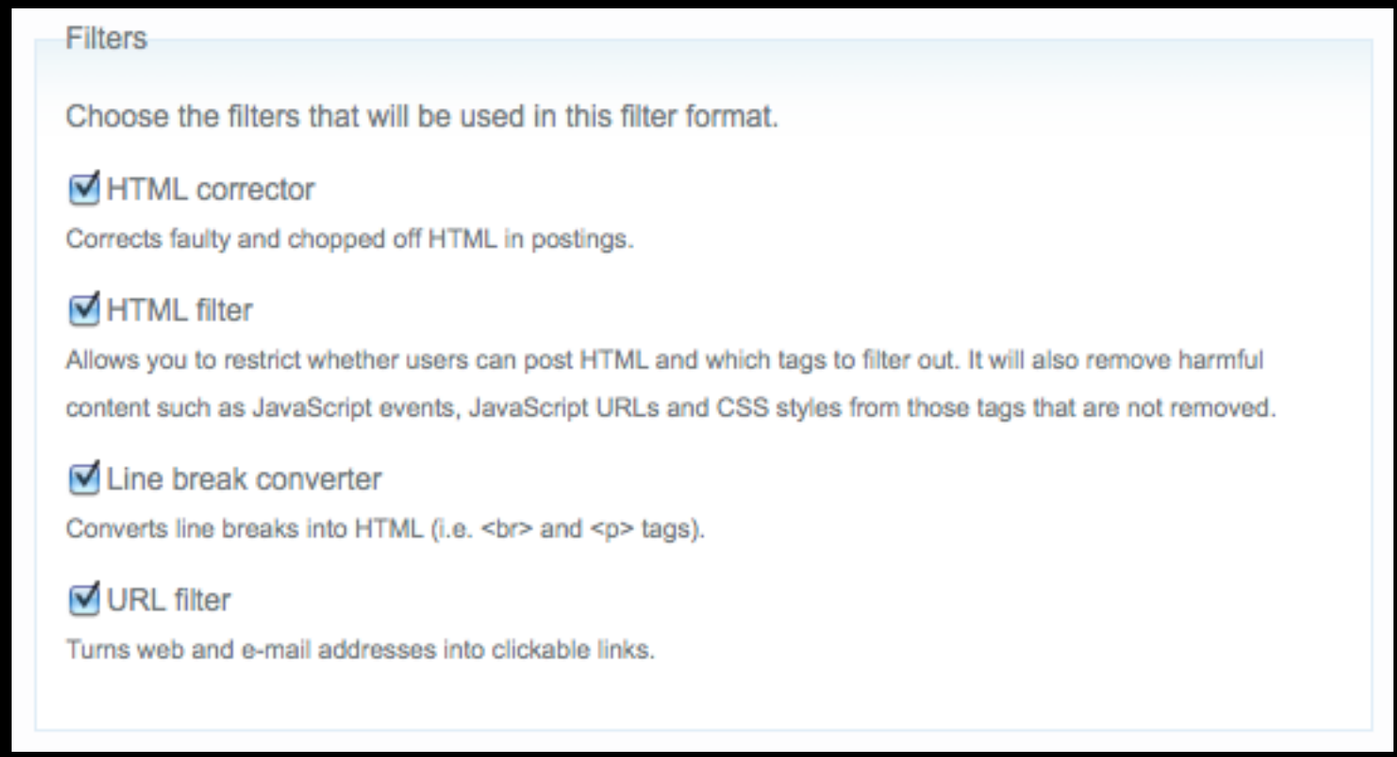
Input formats

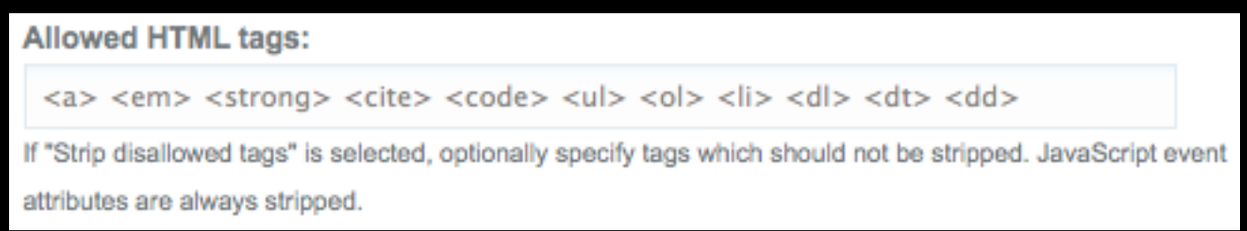
Default	Name	Roles	Operations	
◉	Filtered HTML	All roles may use default format	configure	
○	Full HTML	group manager	configure	delete

- Filtered HTML for *untrusted* roles
- Full HTML for completely *trusted* roles

Filtered HTML

- HTML filter
  - Limits the allowed tags





Unsafe HTML tags

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

No image tags?!

- Image tags allow for CSRF attacks
- It's a matter of trust
- Use CCK & imagefield

Solution?

- Control access to full HTML tag usage

Trust

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

“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

[redacted]updates

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

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

De 2-5, 2010, Ann Arbor MI

Variable editor

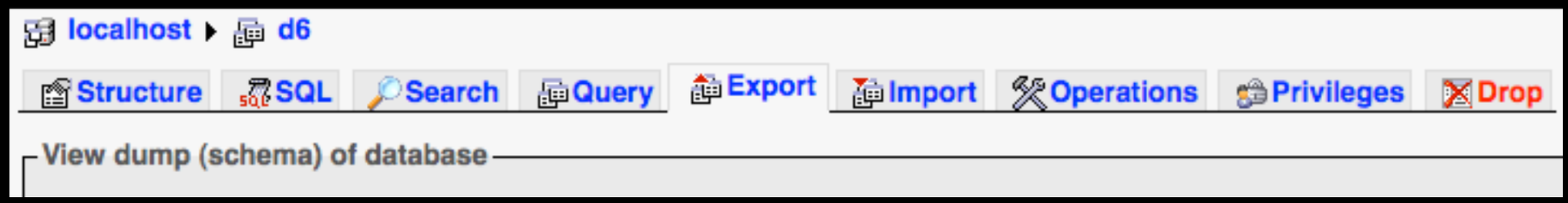
This is a list of the variables and their values currently stored in variables table and the `$conf` array of your settings.php file. These variables are usually accessed with variable_get() and variable_set(). Variables that are too long can slow down your pages.

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

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!

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

Security Review

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

Custom code

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

- Security Advisories
  - http://drupal.org/security
- Handbooks
  - http://drupal.org/security/secure-configuration
  - http://drupal.org/writing-secure-code
- *Cracking Drupal* Book
  - http://crackingdrupal.com
- #dcco10 *Breaking into a Drupal site*
  - Tomorrow at 9am by Greg Knaddison

Thanks!

- drupal.org & IRC: coltrane
- ben@growingventuresolutions.com
- @benswords