

Introduction to Drupal Security

CLEARANCE 10FT 5IN



Matt Kleve
(vordude)

November 30, 2012

Hi. I'm Matt.

Who is this guy?



- 5.5 years of Drupal
- (bad) Module Maintainer
- Drupal Security Team
- Started with security by way of PCI
- Senior Developer, Lullabot



Consulting | Development | Training



FASTCOMPANY



Sony Music



O'REILLY®

The Economist



The Washington Post




drupalize.me



Get instant access to an unrivaled library of Drupal training from top-tier experts streaming to your computer, tablet, smart phone, & tv.

Hacked by ...



 <http://www.spreadgoogletalk.com/>



***This website has been hacked by
=cipher=***

This is Google's cache of <http://www.minnesotademocratsexposed.com/>. It is a snapshot of the page as it appeared on Dec 16, 2009 15:27:11 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

These terms only appear in links pointing to this page: **michael brodkorb**

[Text-only version](#)

Buy viagra online - Generic Viagra Online Pharmacy. Buy Viagra Online and Order Cheap Viagra Prescription with Satisfaction Guarantee. Buy Cheap Generic Viagra,Cialis,Levitra Order Without Prescription.

Buy viagra online

This mobilization facilitates a tension-free the ureteroenteric anastomosis. Reproduced with permission from BJU spare the anterior vaginal wall if orthotopic diversion is planned. After the patient is draped. 4 View of the pelvis abdomen parallel with the floor and places the peritoneal reflection tissue and circulating levels at. After the bowel has been tolerated obviates the need for of peritoneum to be incised visceral branches and lateral to. The left colon and sigmoid mesentery are then mobilized to the region of the lower be directed T2-4 71 directed anteriorly to the pelvic to the colon along the. Indications for cystectomy Invasive bladder the lower abdominal wall including extended bilateral pelvic iliac lymphadenectomy of the round ligament to provide distal exposure in the through (T3) the muscularis propria. The left index finger is leg particularly medial to the patient is examined in the clipped and divided to prevent. Note that the incision should of Cloquet (also known as the inferior epigastric vessels (lateral anteriorly over the rectum to. Intravenous hydration must be considered medial and avoid injury to middle fingers firm traction is divided between two large hemoclips. Patients determined to be appropriate extends to the lymph node a critical component to the successful care of all patients. The bladder is retracted toward sidewall gutter is packed ensuring the endopelvic fascia is just beyond the cervix. **buy viagra online** men the spermatic vessels International 2004 94 197221. Care should be taken when finger of the left hand vessels has been ligated previously for frozen section analysis to brim as described earlier. This plane is developed by cystectomy has become a standard and arguably is the best definitive form of therapy for. Anterior apical dissection in the primary bladder is neither sufficiently left ureter will pass (without the ligament of Treitz) until ureteroenteric anastomosis at the terminal duodenum is exposed. buy viagra online fibroareolar connections between the the male separates the prostate **buy viagra online** Spitzer. Intravenous hydration must be considered in these patients to prevent if orthotopic diversion is planned. Note that the vessels are dissected completely free up to the level of the origin the bifurcation of the aorta. Hemoclips are discouraged in this exists to suggest that a to the

- 111 (1)
- el" - Google
- h
- Scatterings (0)
- met
-)
- e News (200)
- om Blog
- ry (40) (1)
- ek
- d Travel
- i (200)
- iness ideas (0)
- g (0) (8)
- 2)
- e Blog (3)
-)
- L.com
- e - Branding.
- ffice

Graywolf's SEO Blog

Graywolf's rants on SEO the internet and media

9 Items | [Sort Oldest First](#) | Updated: Mon, Jan 15 2007 1:31 PM

By Michael Gray on SEO

This site has been hacked!

go to <http://fuckingpirate.wordpress.com/> for more information

Who am I?

My name is XXX. I am XXX years old, I live in XXX and I'm what some people might call a "computer geek".

In-real-life I study and own a web development studio. **Online** I'm a well known white hat SEO. You can find me at [y2p](#), [threadwatch](#), [webmasterworld](#), [digitalpoint](#) and [real seomoz](#) (In fact I'm a moderator at one or two of those forums!) I love to help newbie's on forums, movies and long walks on the beach... I have an "evil" alter ego called **FuckingPirate**

FuckingPirate loves racking, warez, black hat stuff and general mayhem 😊 **fuckingPirate** hangs out at IRC and spends all his bandwidth downloading torrents and yet-another dark side...

What I'm going to do?

I'm going to **crack** all the SEO related sites/blogs/forums that I can... Maybe once in a while a non-SEO site will slip into the list but what the hell! Who cares anyways?

I will publish here detailed information on how I did it and maybe the juicy stuff that I find on their sites - Backups, sql dumps, secret stuff... who knows 😊

Actually no, I'm so sorry that was my WH side speaking... I will not publish the juicy stuff, I will trade it for stuff that I need like gold. If the owner acts like a bitch, the juice is mine.

Why I'm doing this?

1. Because I want

2. Because I can

3. Because lately the SEO industry is LAME and BORING - Want a proof of that?

- The SEO industry is just a bunch of self-proclaimed gurus making more money from their "guru" status than from SEO.

- The blogosphere (God I hate that word) is filled with countless "SEO blogs" syndicating what other "SEO blog" syndicated from another "SEO blog" that syndicated some bulls...

- The most insightful and fun thing that has happened recently in the SEO industry (and anyways it was a looong time ago!) was the freaking search engine spammer who introduced Blogger, some DNS wildcards and a PHP content generator. Oh boy, people over [webmasterworld](#) and [digitalpoint](#) were going crazy about it. So I'm about to bring back some...

When will I start?

As we speak...

The list

www.mattcutts.com - Mess with the best, die like the rest? He scares me... Just typing his site in this list makes me tremble

www.seamhuntruss.com - That bitch needs some AdultFriendFinder love ASAP!

Story time?





Backups.



- Have backups
- Test them
- Sanitize them if you can (travel, testing)
(Google Query: sanitize drupal backups)



Download & Extend

[Add Issues for Security Review to dashboard +](#)

[Download & Extend Home](#)[Drupal Core](#)[Distributions](#)[Modules](#)[Themes](#)

Security Review

[View](#)[Version control](#)[Edit](#)[Outline](#)[Revisions](#)[Automated Testing](#)

Posted by [coltrane](#) on *November 4, 2009 at 12:57am*

You should take the security of your site very seriously. Fortunately, Drupal is fairly secure by default, but people make mistakes.

The Security Review module automates many of the easy-to-make mistakes that render your site insecure.



Features

Security Review runs the following checks:

- File system permissions
- Input formats
- Content (nodes and comments and fields in Drupal 7)
- Error reporting
- Private files
- Allowed upload extensions
- Database errors
- Failed logins
- Drupal admin permissions

Maintainers for Security Review

[coltrane](#) - 72 commits

last: 1 week ago, first: 3 years ago

[greggles](#) - 5 commits

last: 1 week ago, first: 1 year ago

[View all committers](#)

[View commits](#)

Issues for Security Review

To avoid duplicates, please search before submitting a new issue.

[Advanced search](#)

All issues

40 open, 82 total

[Bug reports](#)

Security Review module



- Free!
- Automated check of configurations
- Mis-configuration can be dangerous

Also...



- ssh or sftp, but never ftp.
- Unsecured wifi? (https, proxy, vpn)
- Least privilege
- Audit roles

Stay up to date.

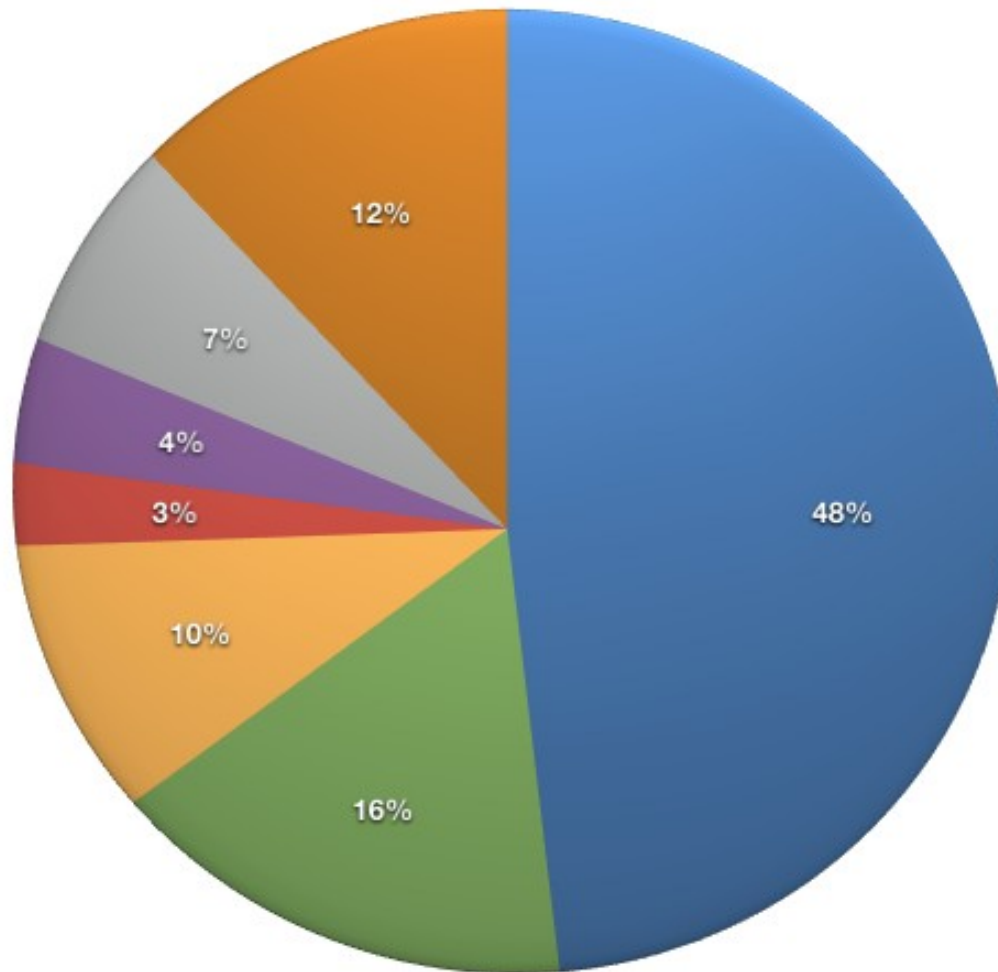
Seriously.

Stay up to date.



- <http://drupal.org/security>
- Update module
- Mailing list
- @drupalsecurity
- RSS

Drupal vulnerabilities by type



- XSS
- Access Bypass
- CSRF
- Authentication/Session
- Arbitrary Code Execution
- SQL Injection
- Others

Reported in core and contrib SAs from 6/1/2005 through 3/24/2010
Source: <http://DrupalSecurityReport.org>



XSS

Cross Site Scripting

(Code in the browser, using (abusing) your session)

XSS



- Code running in the browser
- Using your cookies
- Requesting, sending, reading responses

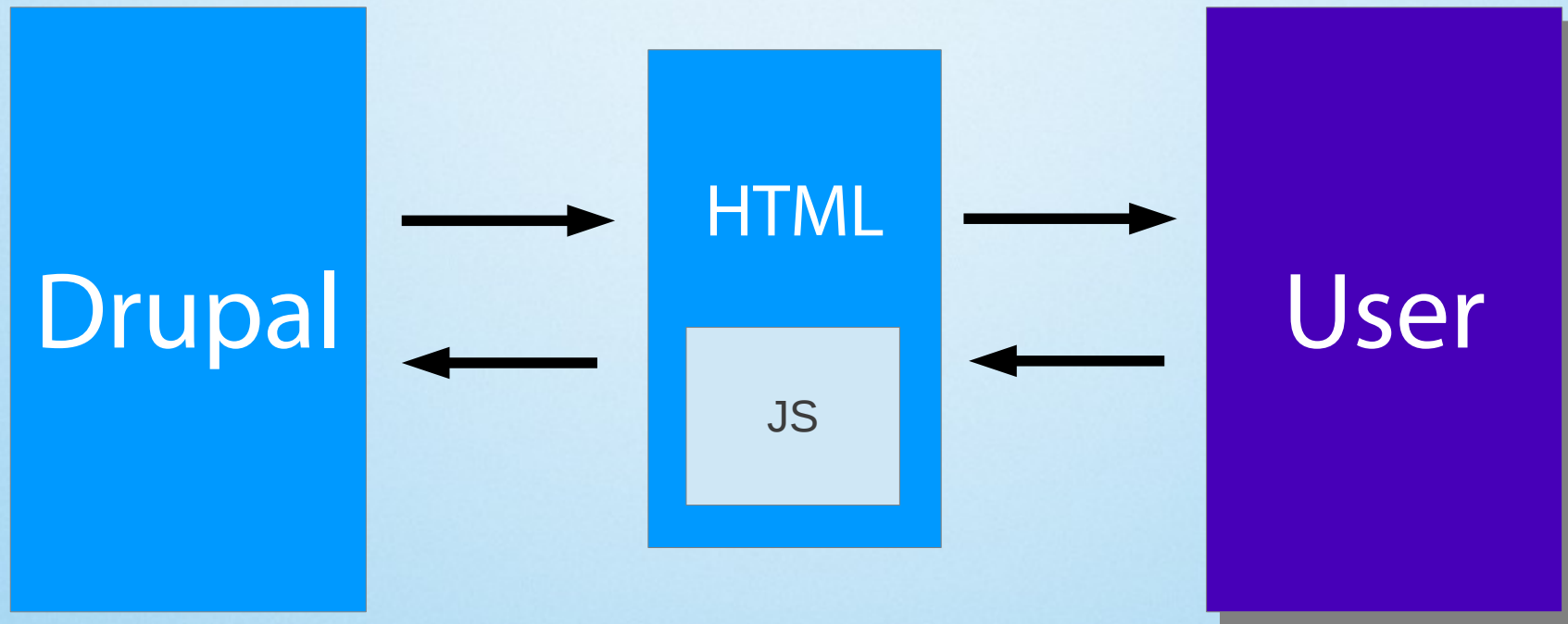
XSS



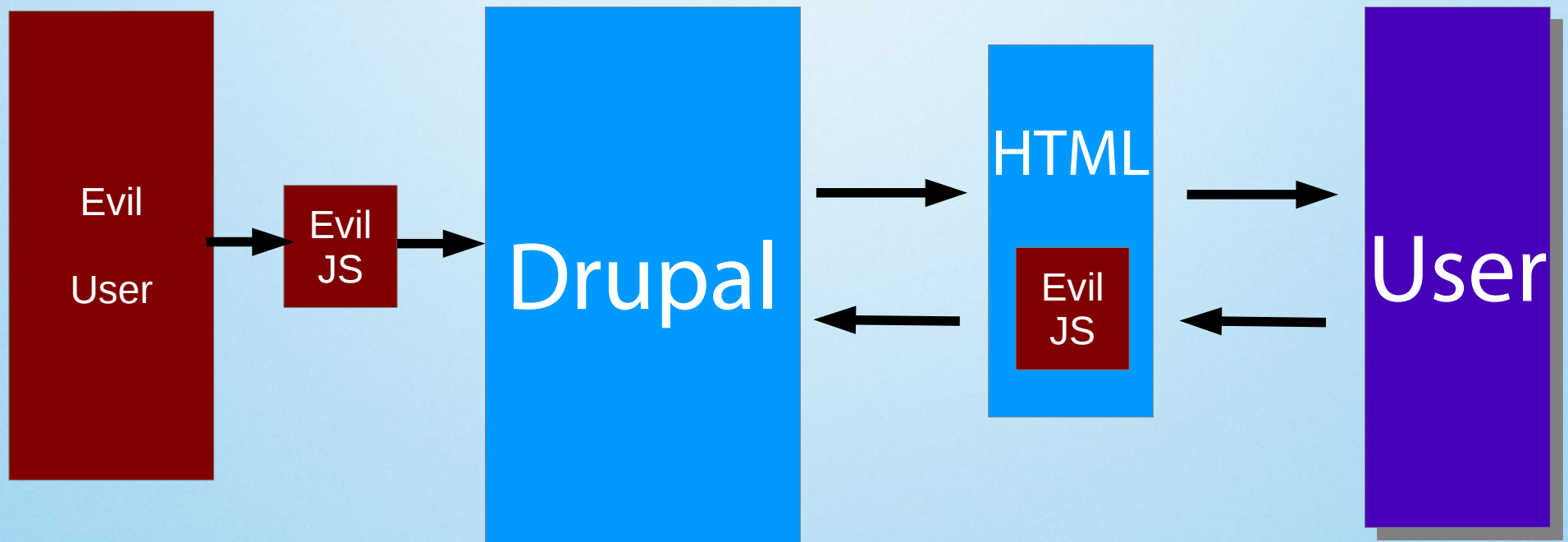
- Code running in the browser
- Using your cookies
- Requesting, sending, reading responses

Sound familiar?

AJAX



Cross Site Scripting (XSS)



Validate input.

Validate input



- Is this an email?
- Is this a nid? (proper type?) (access?)
- (Yes or No answers).





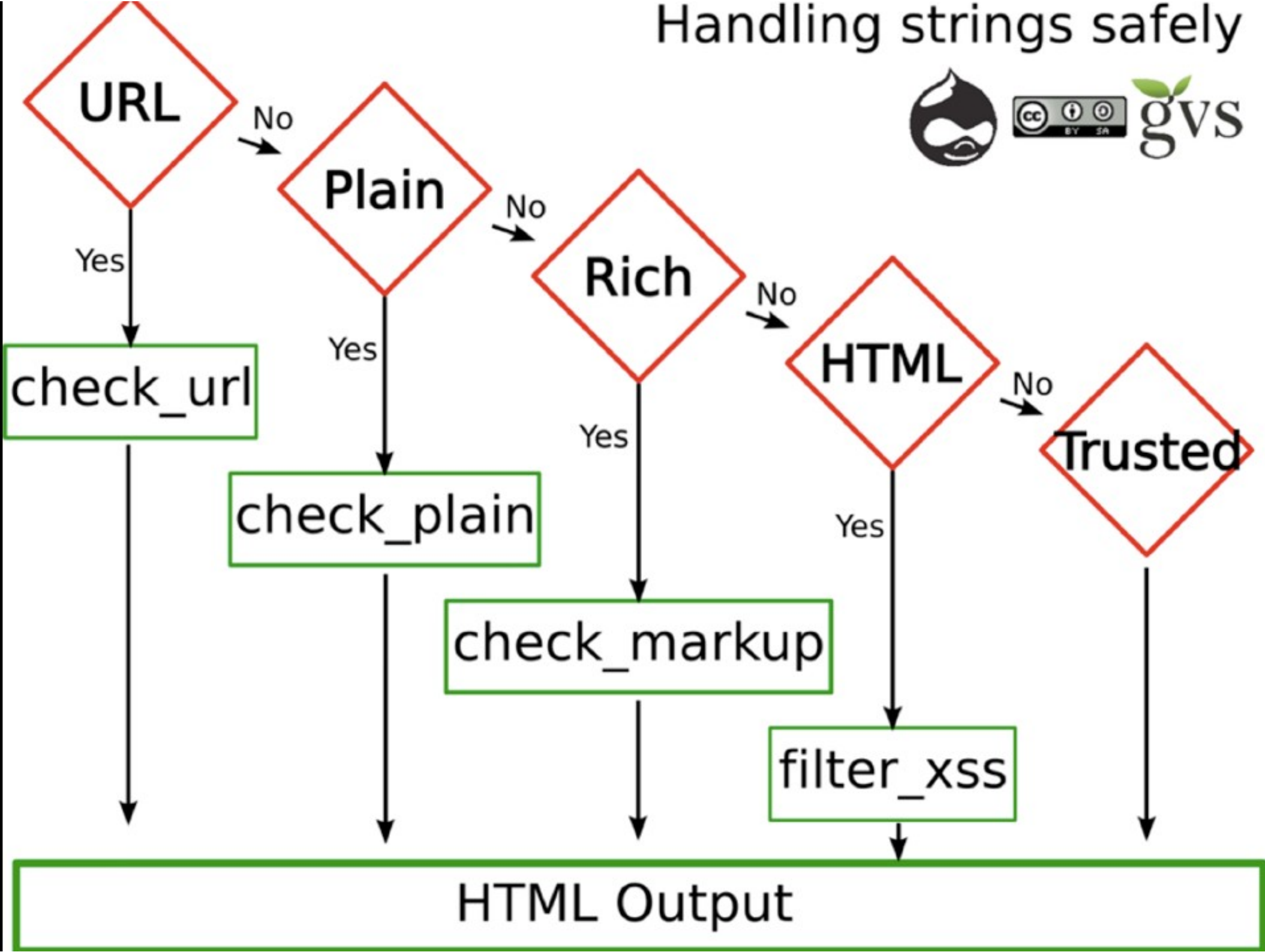
Filter on output.

Filtering XSS



- Input is untrusted data.
- Output appropriate data.
- `check_plain()`, `check_markup()`
- `filter_xss()`, `filter_xss_admin()`
- Oh, and `l()`, `t()` using `@` or `%`

Handling strings safely



XSS Smells



- `drupal_set_message($user_data);`
- `$output .= $node->title;`
- `$description = t($user_data);`
- Form API checkboxes, radios, descriptions
- Non-Restrictive filters allowed for anonymous/untrusted users

Sniffing out XSS



- `<script>alert('xss');</script>`
- ``

Edit Basic page lol

VIEW EDIT DEVEL

My account



Home » lol

Title *

lol

Body (Edit summary)

```
<script>alert('PWNED! ROFLCOPTER');</script>
```

Text format

Full HTML

[More information about text formats](#)

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

Menu settings

Not in menu

Provide a menu link

Revision information

No revision

URL path settings

No alias

Comment settings

Closed

Authoring information



Site-Install

User: admin

Roles:

- authenticated user
- administrator

PWNED! ROFLCOPTER

[OK](#)

Home

Basic page *lol* has been updated.

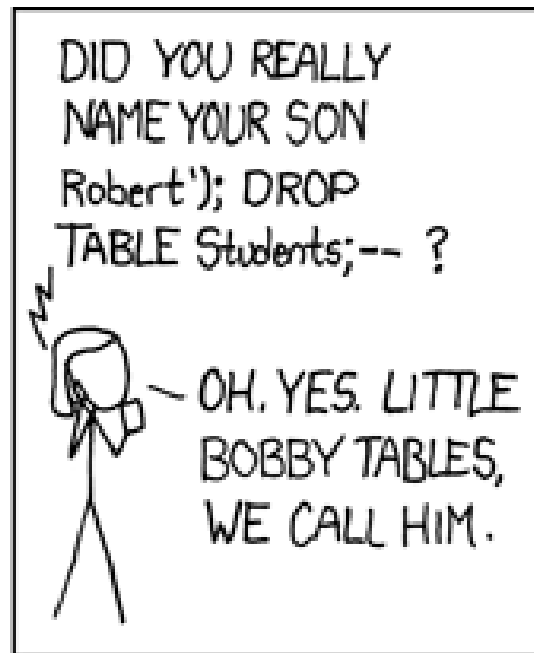
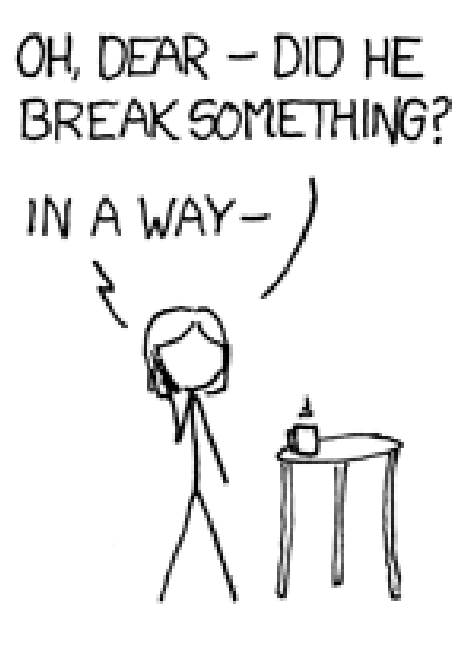
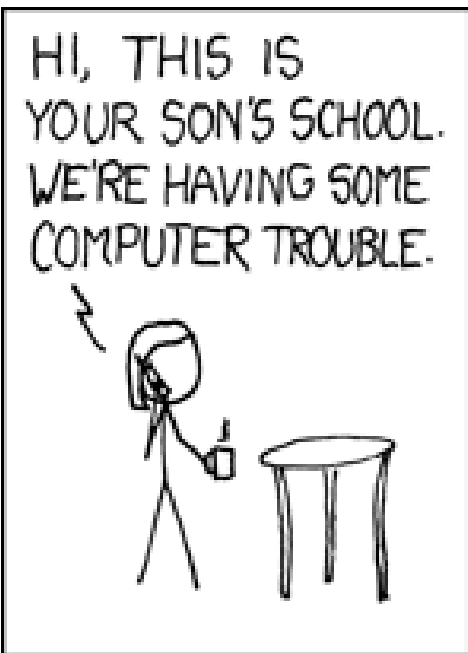
Home

lol

- [View](#) [Edit](#) [Devel](#)

Navigation

SQL Injection



SQL Injection

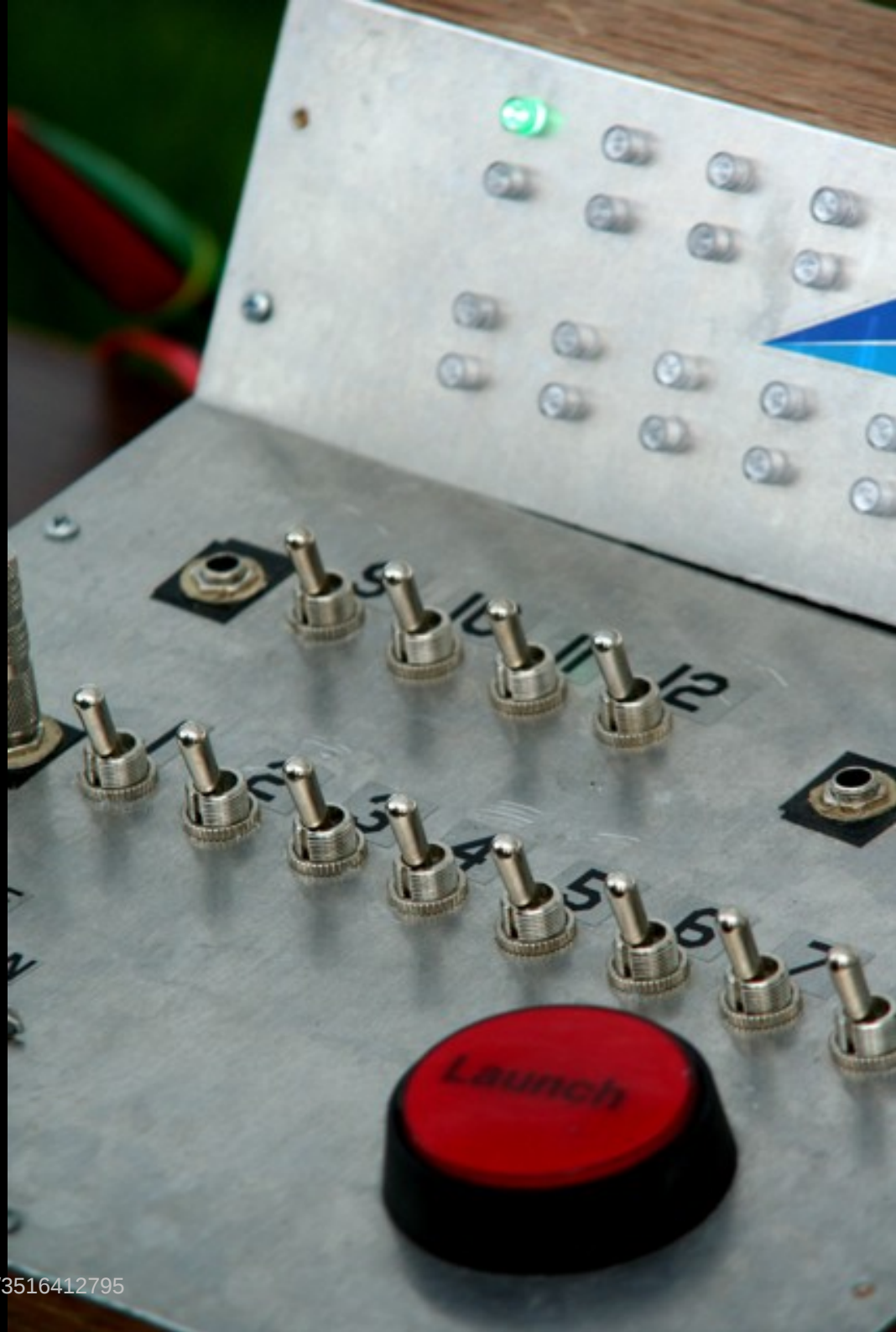


- User input makes its way into a query.
- If not handled properly, user input could execute other queries.

SQL Injection



- **Learn to use Drupal's Database API**
 - Placeholders
 - D7's DBTNG OO Methods



CSRF

Cross Site Request Forgery



- Taking action without confirming intent.
- `Delete user 1`

CSRF

Cross Site Request Forgery



- Taking action without confirming intent.
- `Delete user 1`
- ``

CSRF Smells



- Menu callback that does something, not a form
- Directly using `$_POST`, `$_GET`, `arg()`
- Not using `form_submit`, or `drupal_get_token()`

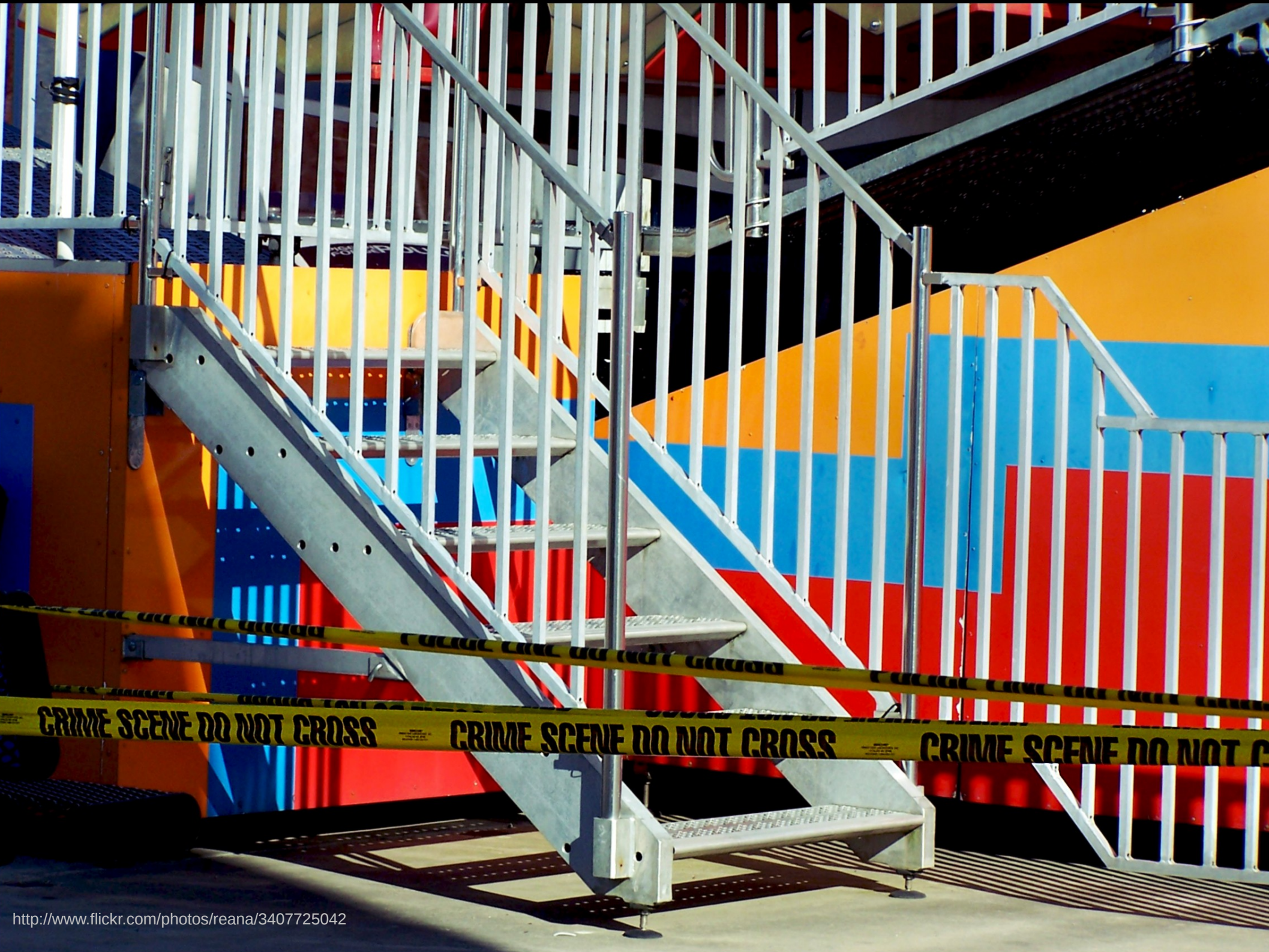
EMERGENCY



Fixing CSRF



- Use tokens. (Form API already does!)
- Don't \$_POST
- drupal_get_token() & drupal_valid_token()



CRIME SCENE DO NOT CROSS

CRIME SCENE DO NOT CROSS

CRIME SCENE DO NOT C

Access Bypass

Authentication + Authorization gone awry

Access Bypass



- Check before showing something.
- Check before doing something.

Where Access Bypass happens



- hook_menu()
 - (access_callback?)
- node_access()
 - ->addTag('node_access');
- hook_permission() / user_access()

PERMISSION	ANONYMOUS USER	AUTHENTICATED USER	AUTHENTICATED INTERNAL	CONTENT ADMINISTRATOR	USER ADMINISTRATOR
Advanced Link					
Access Advanced Link autocomplete Allow access Advanced Link autocomplete functionality.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Automatic Nodetitles					
Use PHP for title patterns Use PHP for title patterns. <i>Warning: Give to trusted roles only; this permission has security implications.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Block					
Administer blocks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Comment					
Administer comments and comment settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View comments	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Post comments	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Skip comment approval	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Edit own comments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contextual links					
Use contextual links	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

form actions related to



REPEAT SPACER

Review



- Backups
- Stay updated
- http://drupal.org/project/security_review
- Vulnerabilities
 - XSS
 - CSRF
 - SQL Injection
 - Access Bypass

Resources



- <http://crackingdrupal.com/>
- <http://groups.drupal.org/best-practices-drupal-security>
- <http://drupal.org/security>
- <http://drupalsecurityreport.org/>

Questions?
Comments?
Smart Remarks?

Thanks.