21 August 2012

Think like a hacker: Secure Drupal code

Greg Knaddison

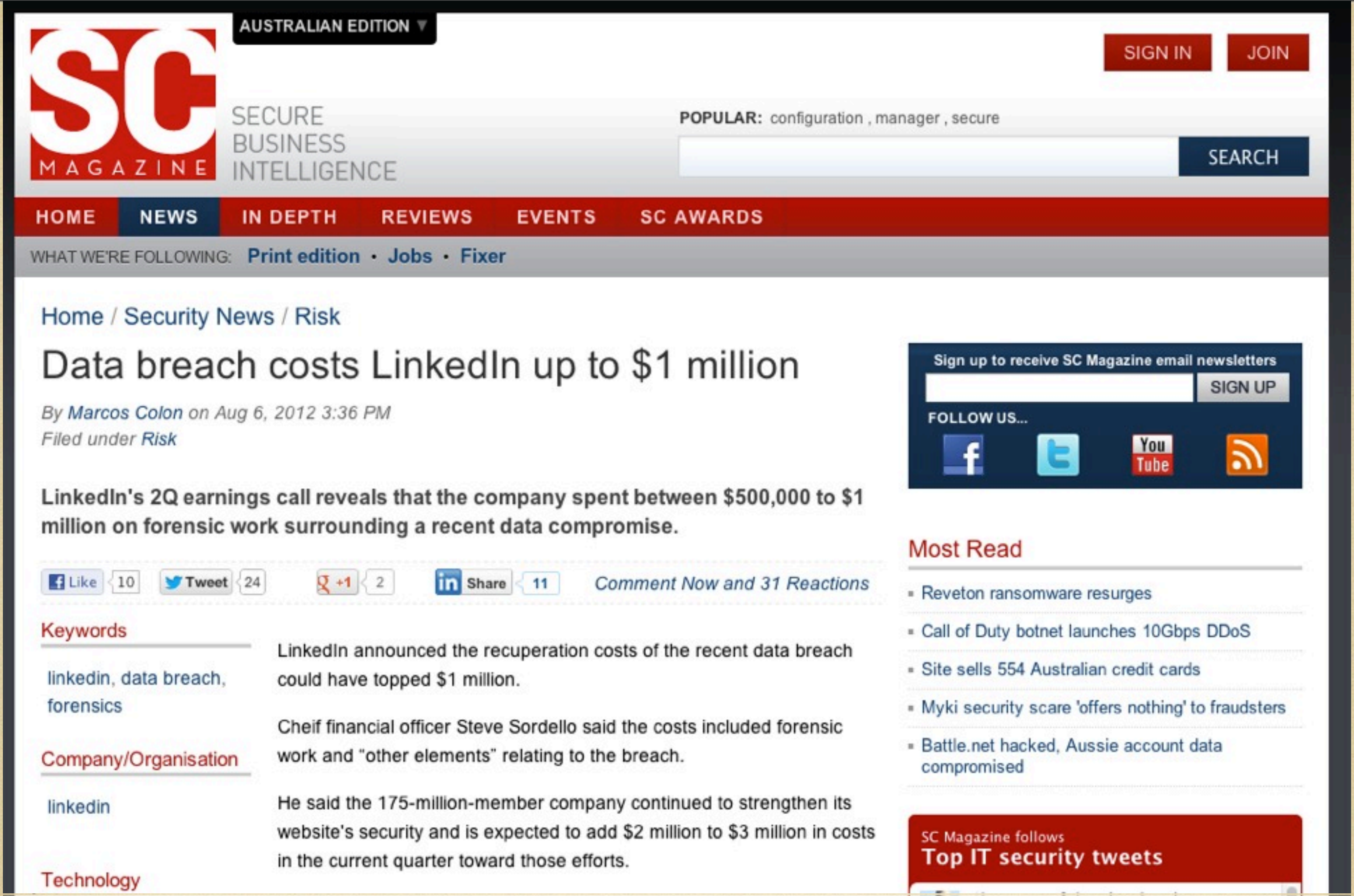
Ben Jeavons

Security is boring*

Doesn't affect me

Doesn't **have** good ROI

* May not apply to you.


AUSTRALIAN EDITION
SC MAGAZINE
SECURE BUSINESS INTELLIGENCE
SIGN IN
JOIN
POPULAR: configuration , manager , secure
SEARCH
HOME
NEWS
IN DEPTH
REVIEWS
EVENTS
SC AWARDS
WHAT WE'RE FOLLOWING: Print edition • Jobs • Fixer

Home / Security News / Risk

Data breach costs LinkedIn up to $1 million

By Marcos Colon on Aug 6, 2012 3:36 PM
Filed under Risk

LinkedIn's 2Q earnings call reveals that the company spent between $500,000 to $1 million on forensic work surrounding a recent data compromise.

Like 10
Tweet 24
+1 2
Share 11
Comment Now and 31 Reactions

Keywords

linkedin, data breach, forensics

Company/Organisation

linkedin

Technology

LinkedIn announced the recuperation costs of the recent data breach could have topped $1 million.

Cheif financial officer Steve Sordello said the costs included forensic work and "other elements" relating to the breach.

He said the 175-million-member company continued to strengthen its website's security and is expected to add $2 million to $3 million in costs in the current quarter toward those efforts.

Most Read

- Reveton ransomware resurges
- Call of Duty botnet launches 10Gbps DDoS
- Site sells 554 Australian credit cards
- Myki security scare 'offers nothing' to fraudsters
- Battle.net hacked, Aussie account data compromised

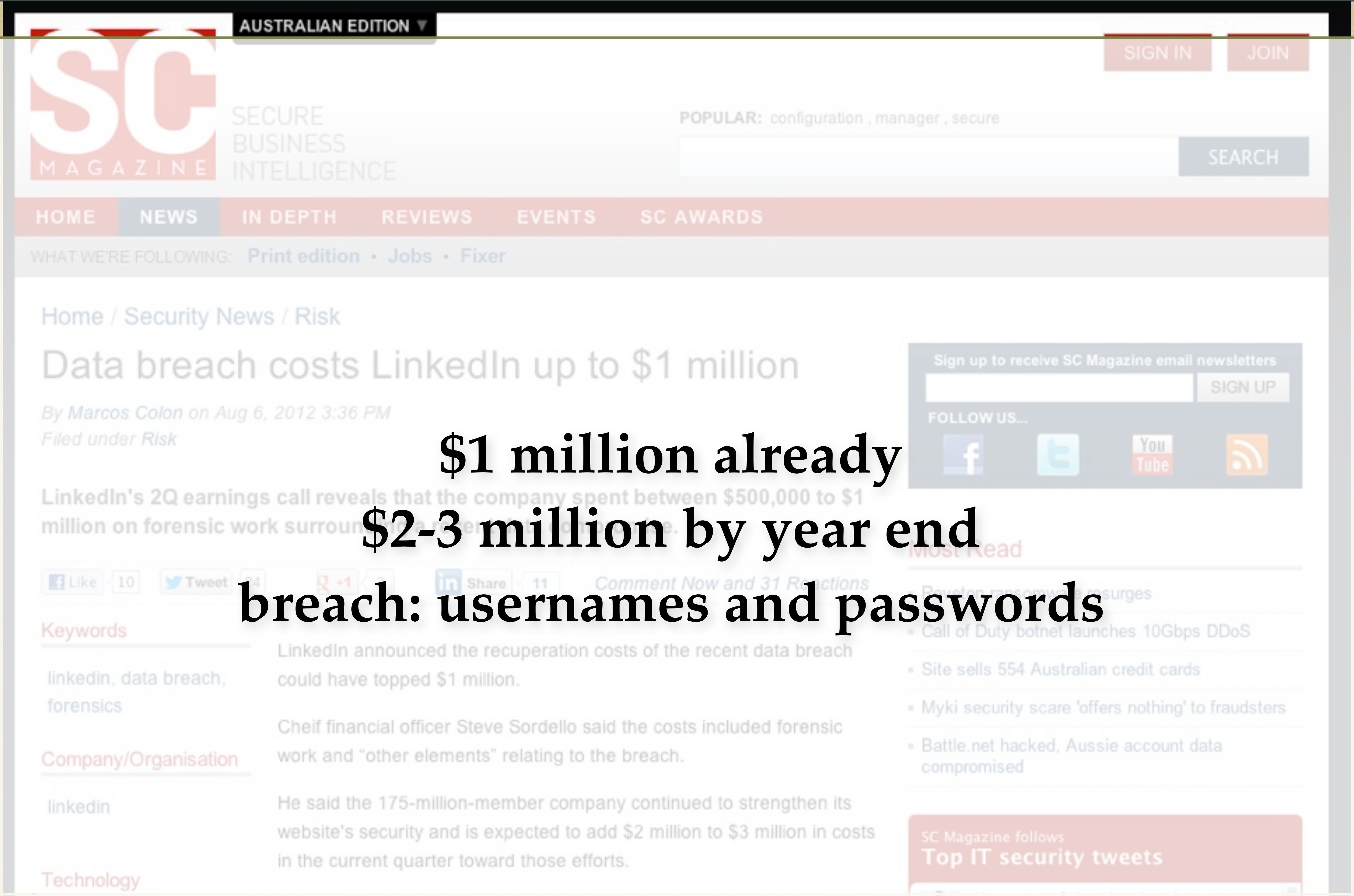
SC Magazine follows
Top IT security tweets

http://www.scmagazine.com.au/News/310976,data-breach-costs-linkedin-up-to-1-million.aspx

$1 million already

$2-3 million by year end

breach: usernames and passwords



AUSTRALIAN EDITION

SC MAGAZINE

SECURE BUSINESS INTELLIGENCE

SIGN IN JOIN

POPULAR: configuration , manager , secure

SEARCH

HOME NEWS IN DEPTH REVIEWS EVENTS SC AWARDS

WHAT WE'RE FOLLOWING: Print edition · Jobs · Fixer

Home / Security News / Risk

Data breach costs LinkedIn up to $1 million

By Marcos Colon on Aug 6, 2012 3:36 PM
Filed under Risk

LinkedIn's 2Q earnings call reveals that the company spent between $500,000 to $1 million on forensic work surroun

Like 10 Tweet Share 11 Comment Now and 31 Reactions

Keywords

linkedin, data breach, forensics

Company/Organisation

linkedin

Technology

LinkedIn announced the recuperation costs of the recent data breach could have topped $1 million.

Cheif financial officer Steve Sordello said the costs included forensic work and "other elements" relating to the breach.

He said the 175-million-member company continued to strengthen its website's security and is expected to add $2 million to $3 million in costs in the current quarter toward those efforts.

Sign up to receive SC Magazine email newsletters

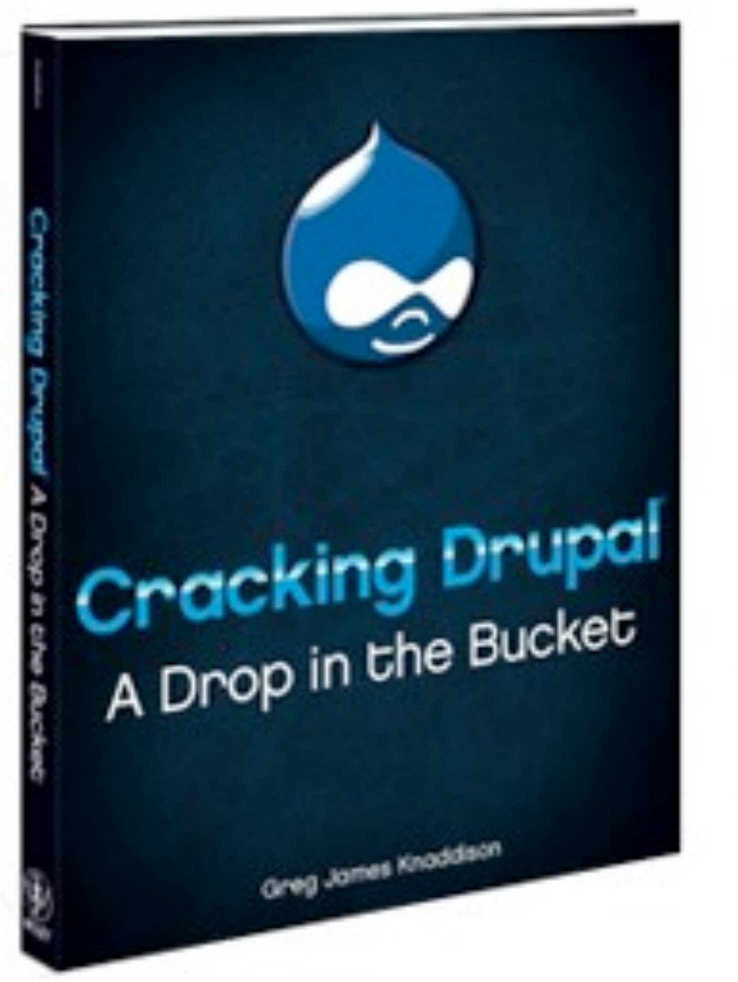
SIGN UP

FOLLOW US...

Most Read

- Reveton ransomware resurges
- Call of Duty botnet launches 10Gbps DDoS
- Site sells 554 Australian credit cards
- Myki security scare 'offers nothing' to fraudsters
- Battle.net hacked, Aussie account data compromised

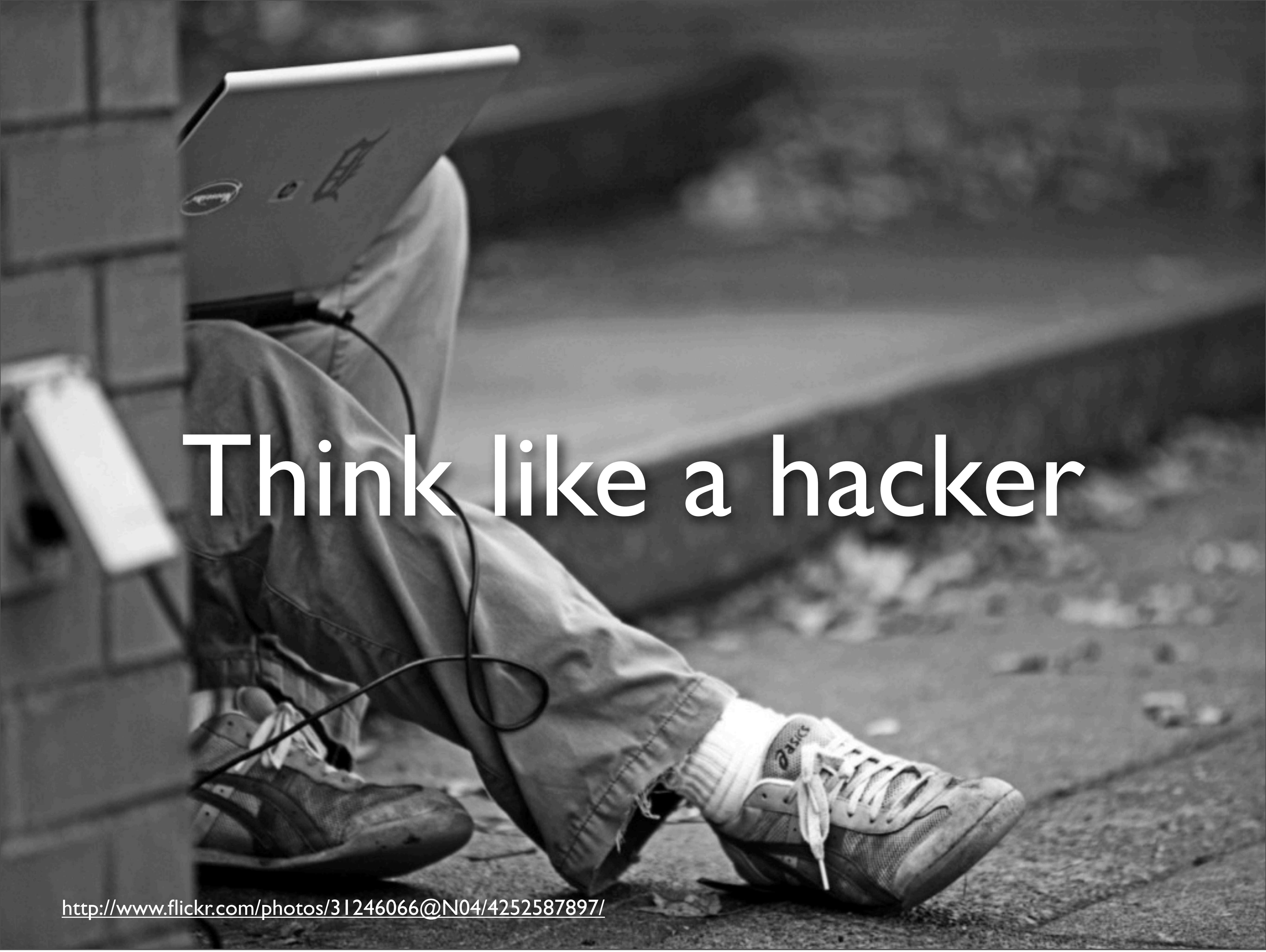
SC Magazine follows
Top IT security tweets



Cracking
Drupal
€25

SIGNED
by the author

http://www.flickr.com/photos/ezrabg/6860635970/



Think like a hacker

http://www.flickr.com/photos/31246066@N04/4252587897/

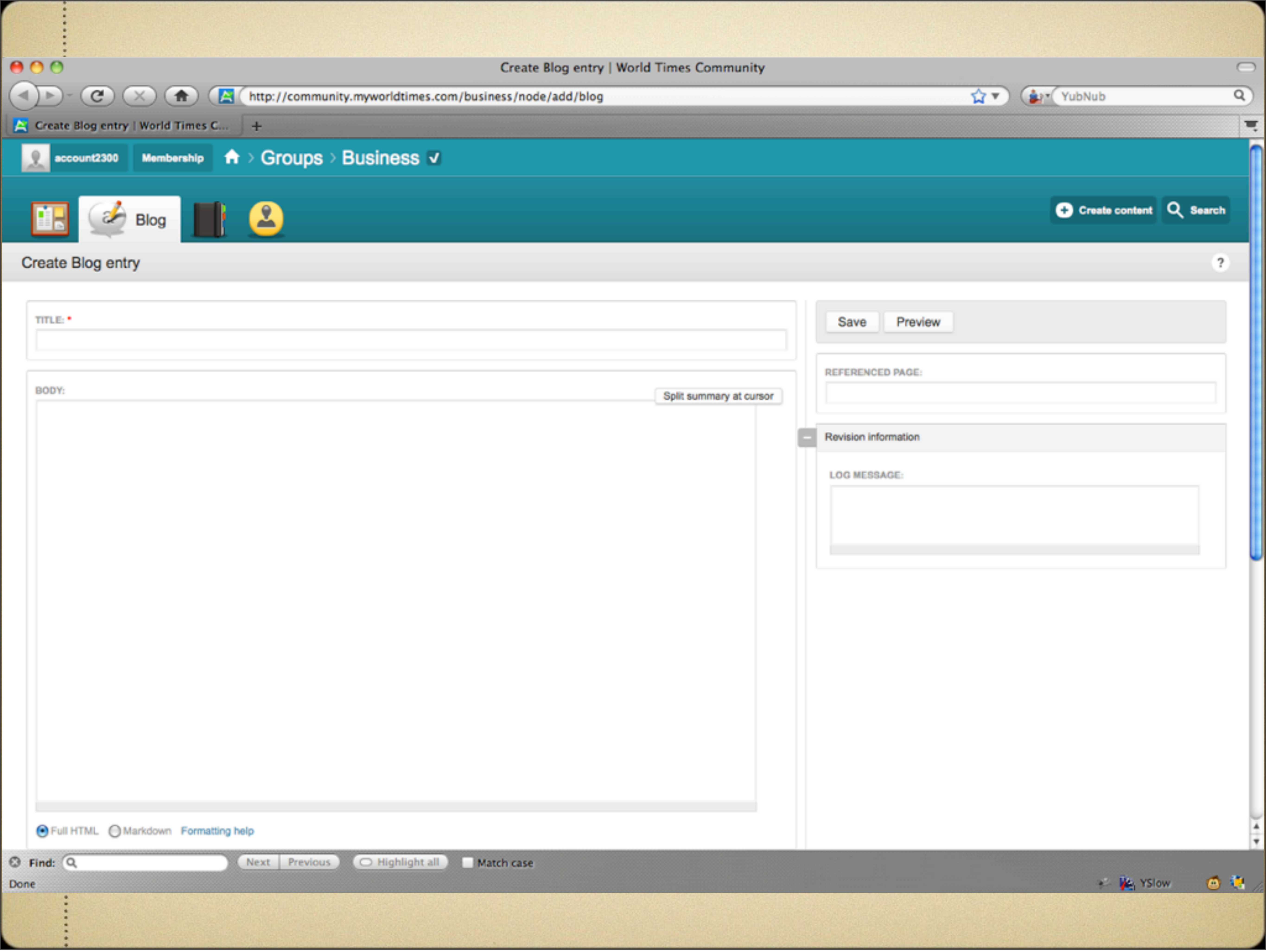
Greg Knaddison	@greggles
Ben Jeavons	@benswords

Acquia™

Members of Drupal Security Team

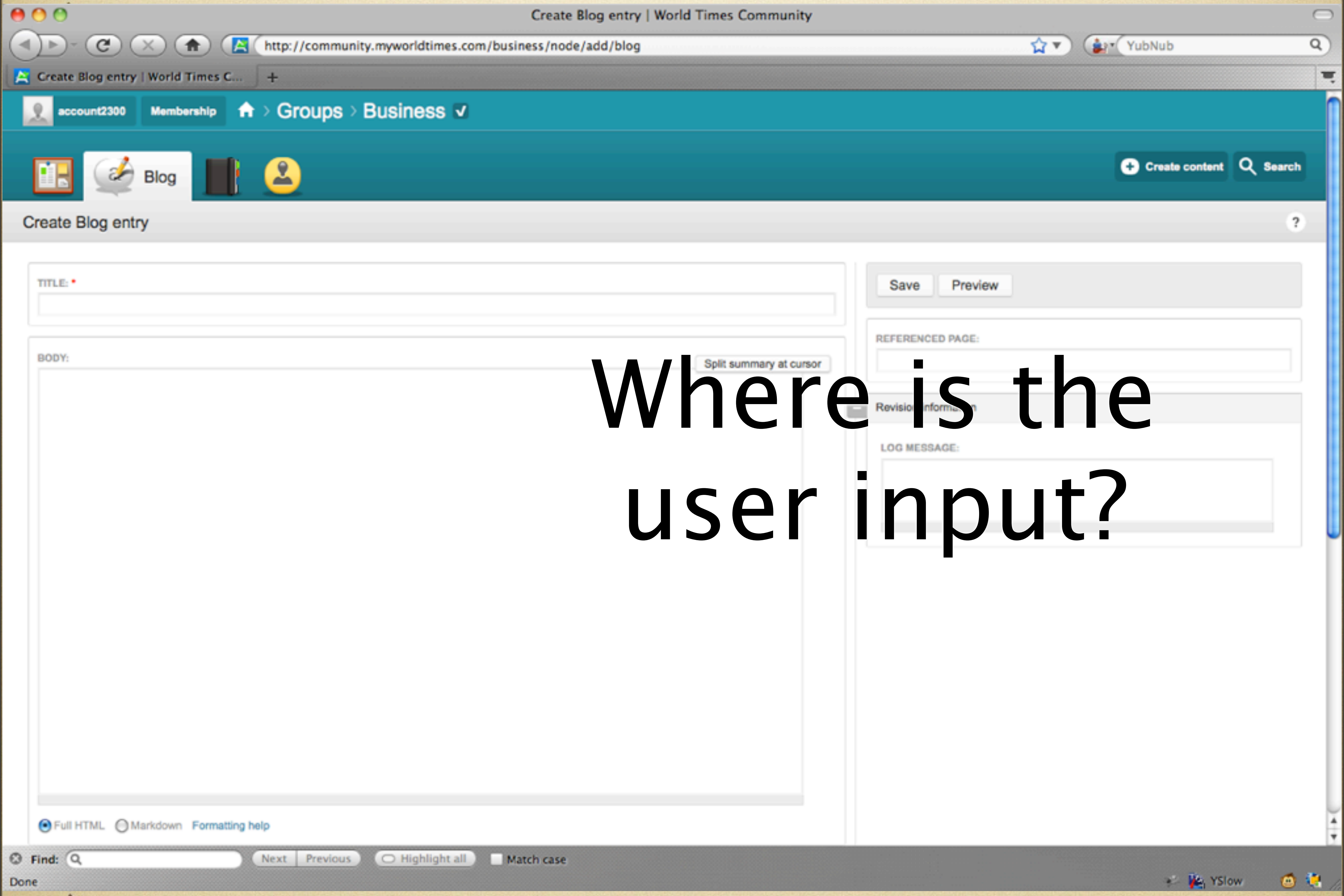
be the attacker

Say hello to $user_data



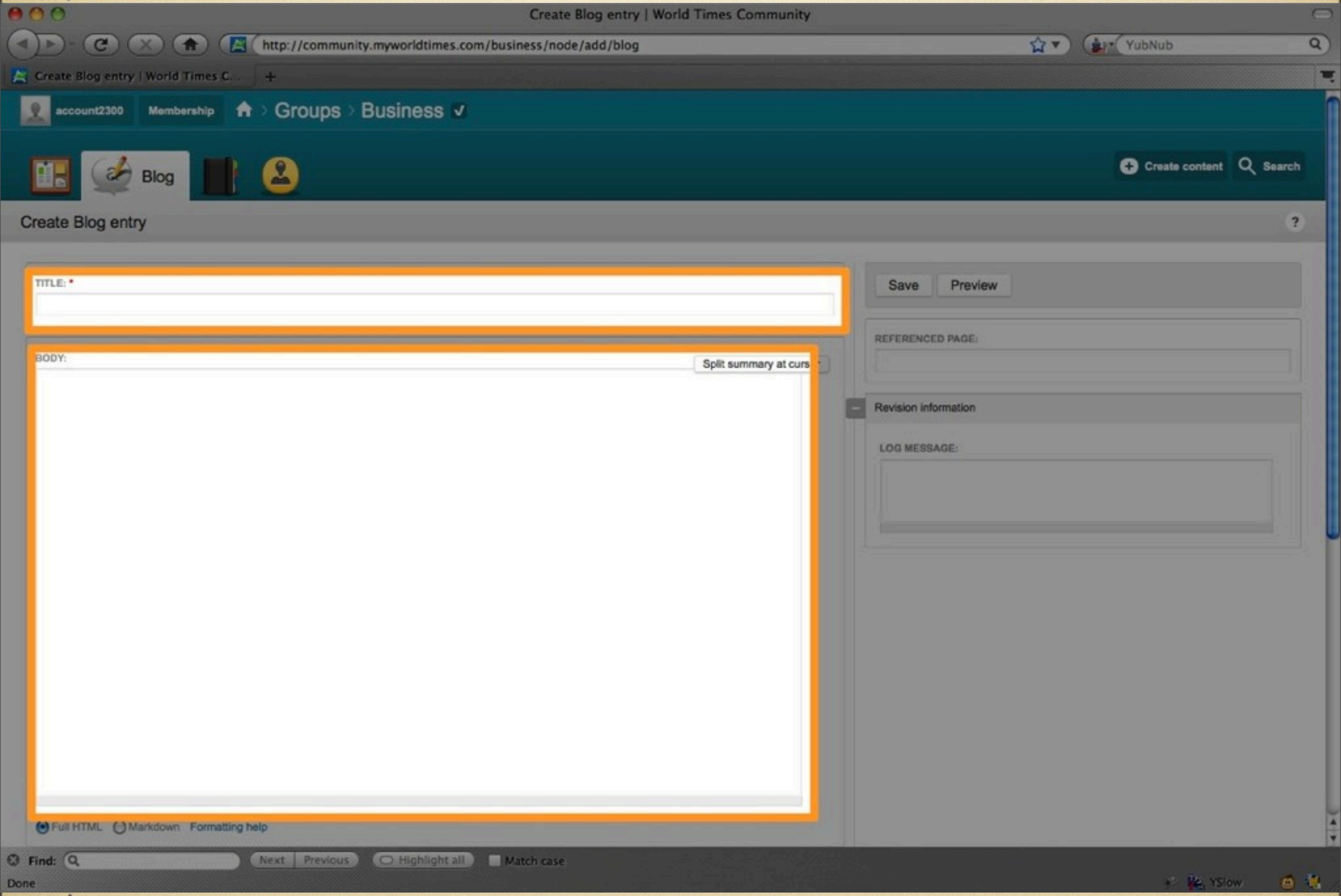
Create Blog entry | World Times Community

http://community.myworldtimes.com/business/node/add/blog



● Full HTML ○ Markdown

Where is the user input?



Create Blog entry

TITLE: *

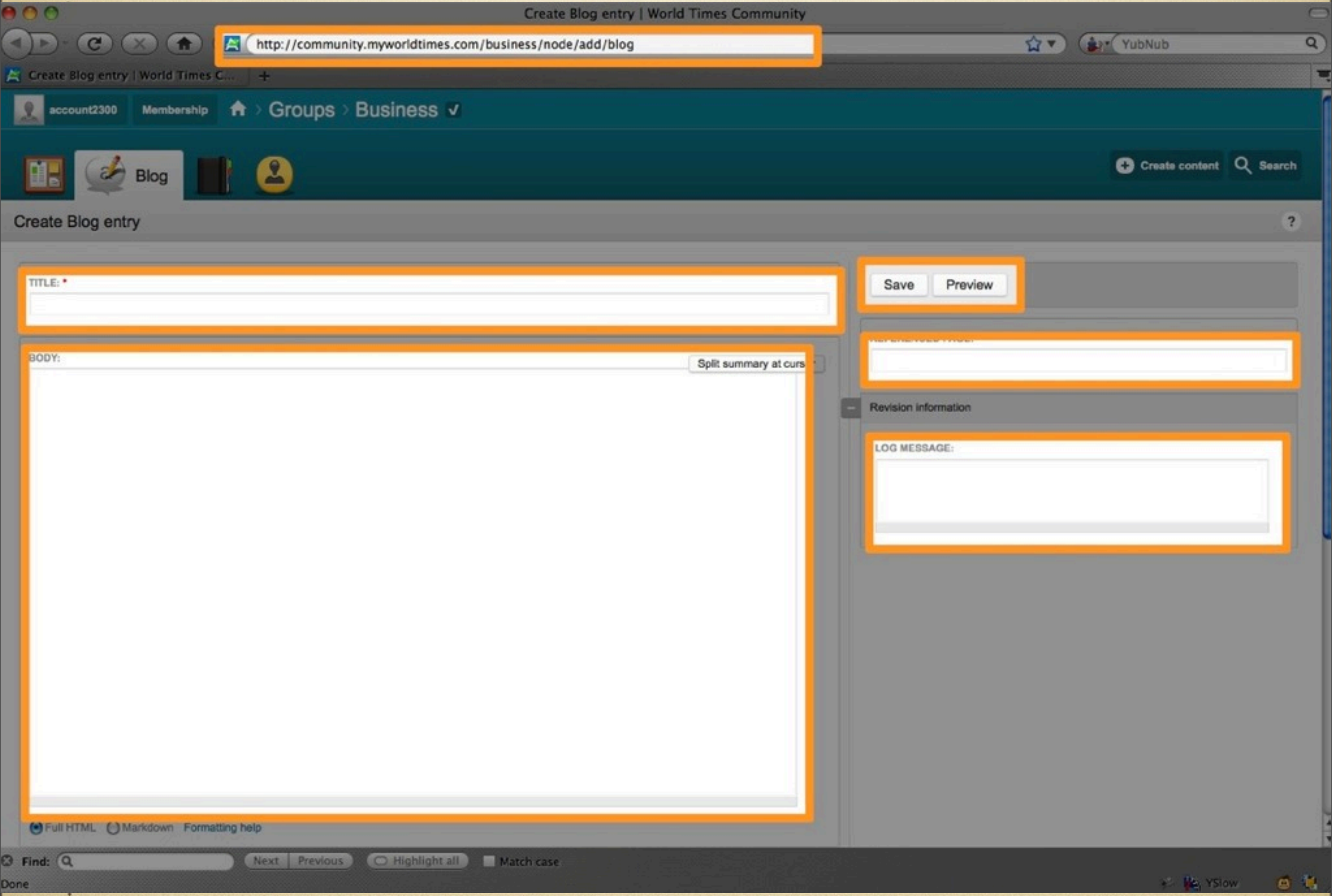
BODY:

Save

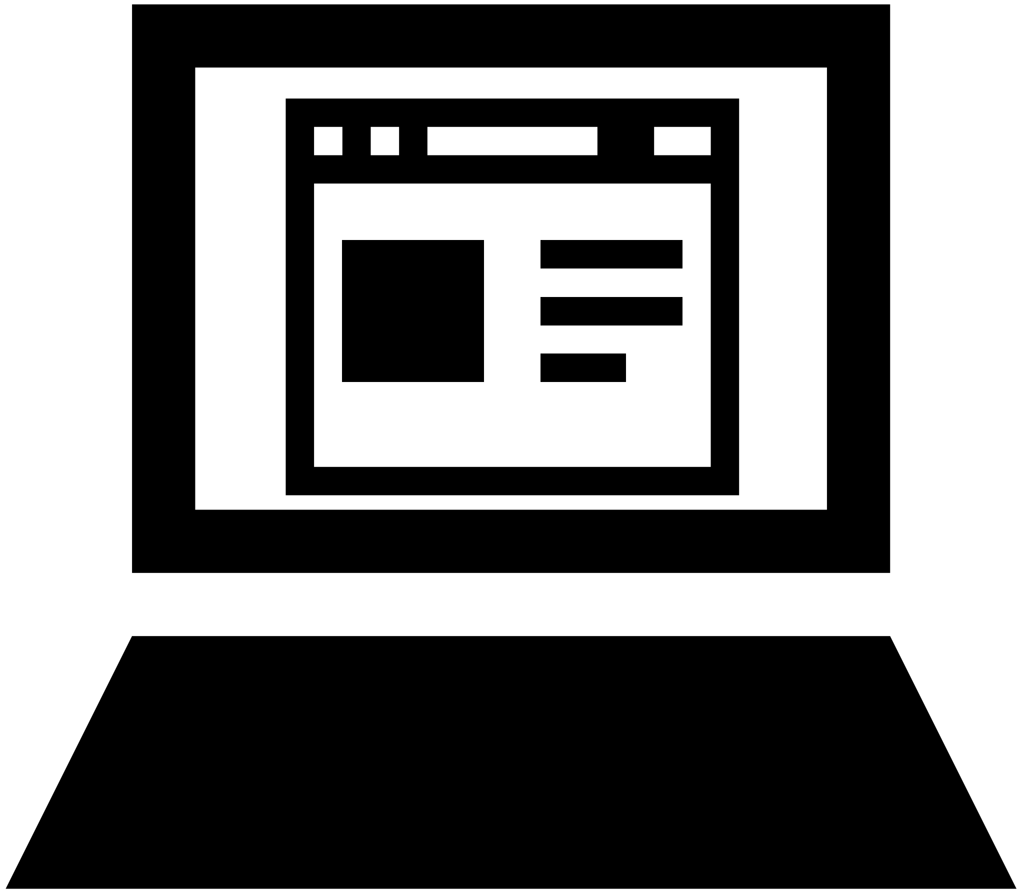
Preview

REFERENCED PAGE:

LOG MESSAGE:



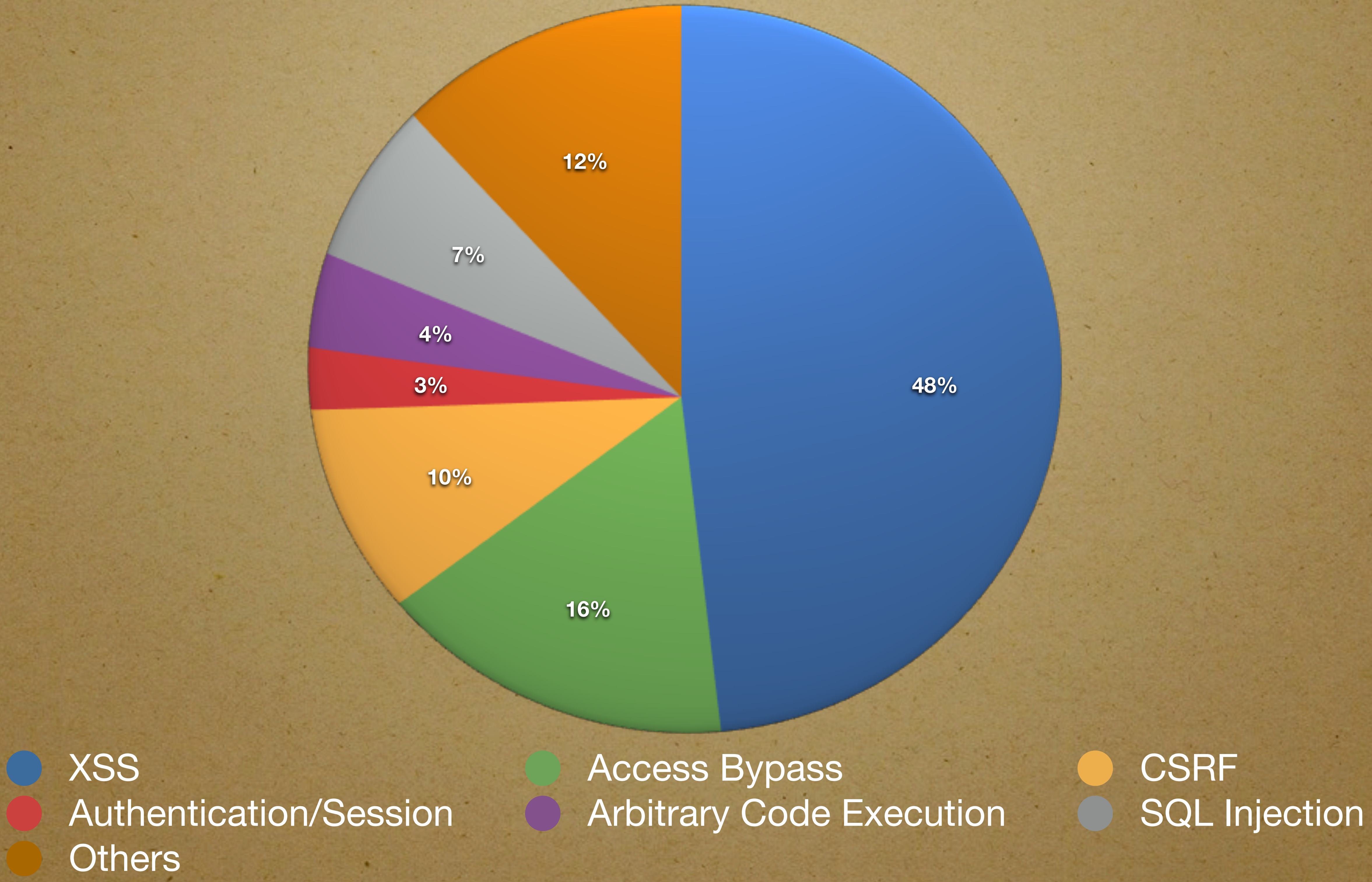
http://community.myworldtimes.com/business/node/add/blog



user agent
language
time zone
referrer
& more HTTP request headers

Lots of tools/ways to modify these for requests

Drupal vulnerabilities by type



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

CSRF

Cross Site Request Forgery

Taking action without confirming intent.

Taking action without confirming intent.

How do we confirm intent?

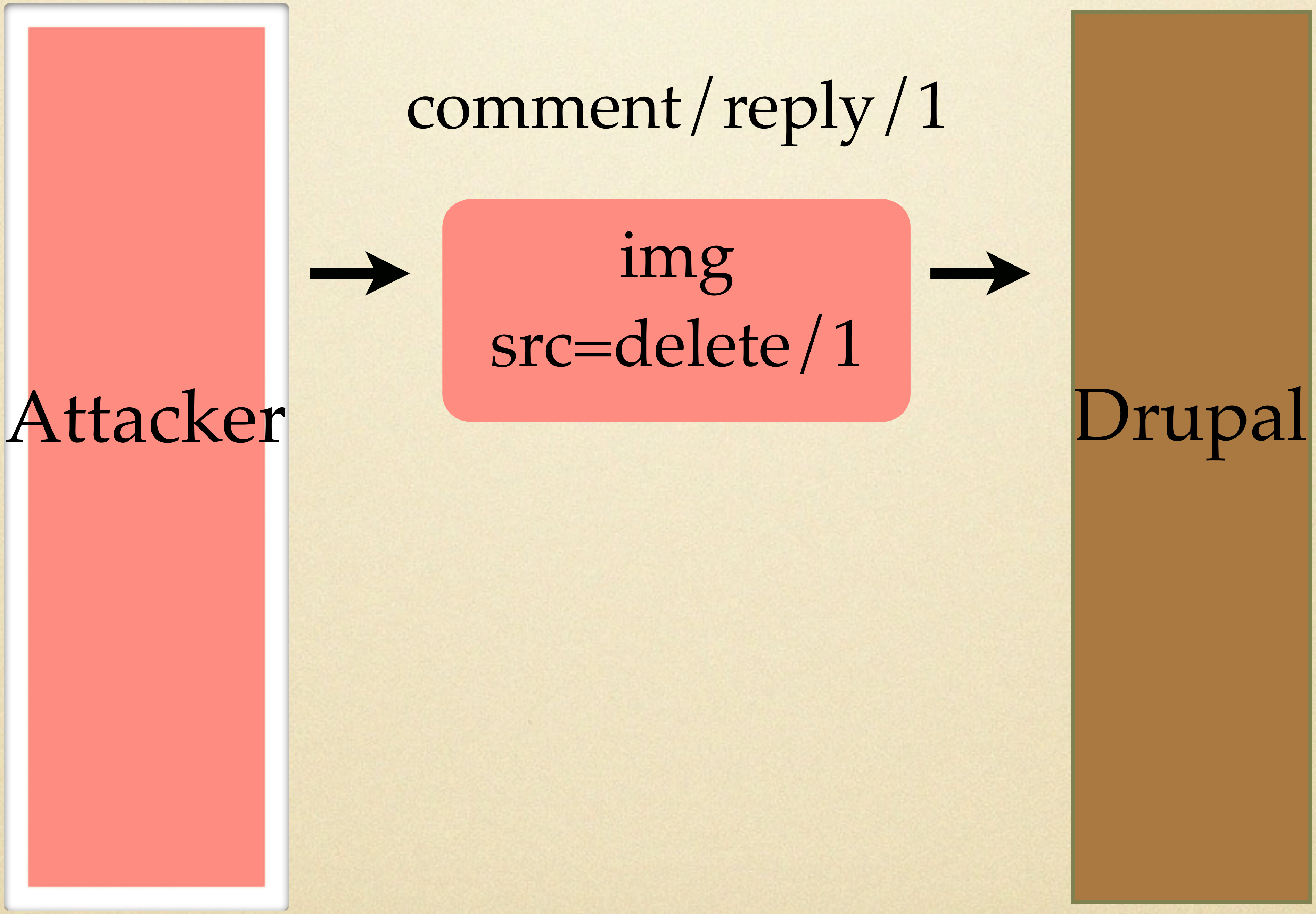
WTF is intent?

```
<a href=”/delete/user/1”>Delete user 1</a>
```

```
<a href=”/delete/1”>Delete user 1</a>

<img src=”/delete/1”>
```

CSRF Flow



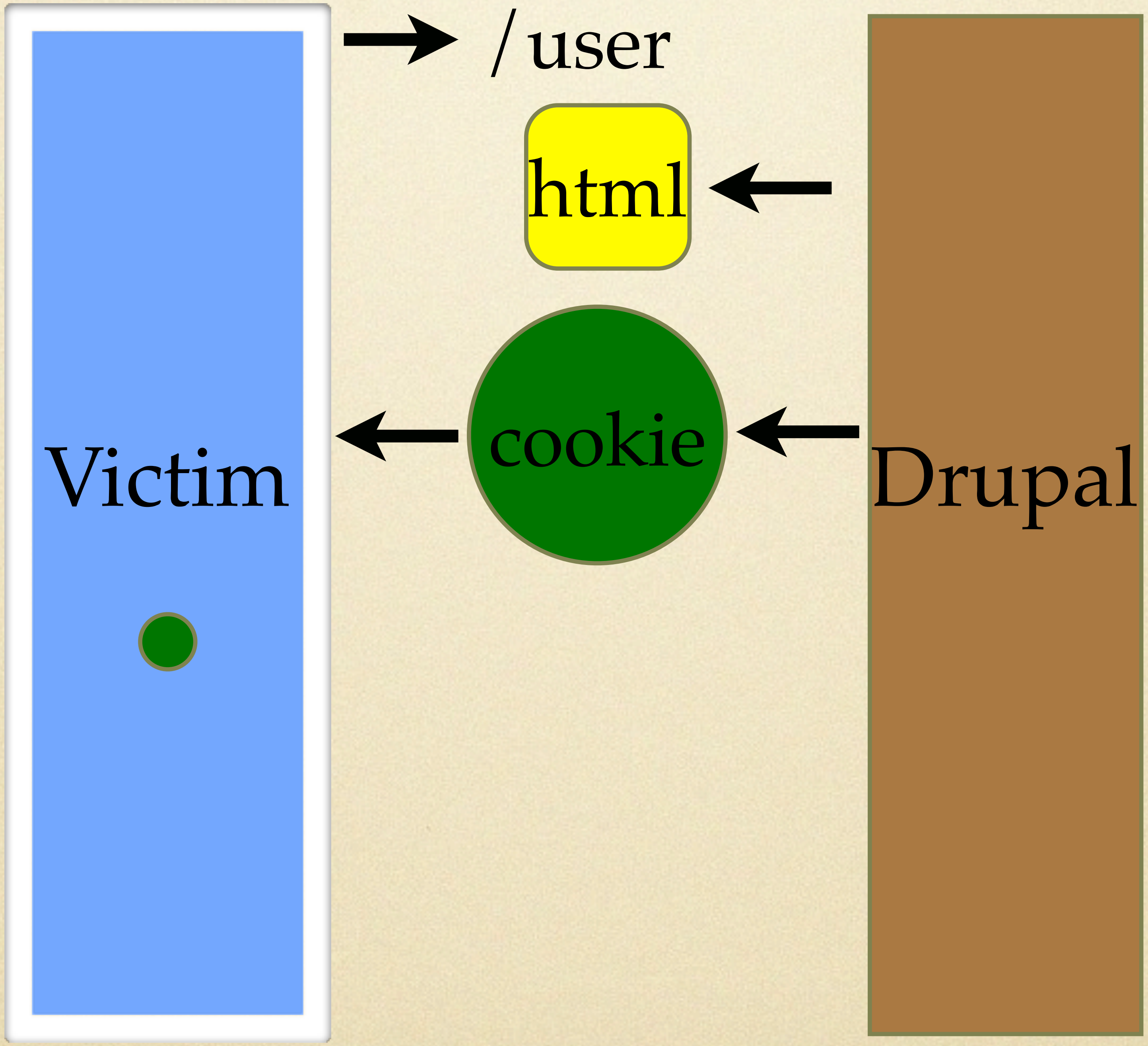
Attacker

comment/reply/1

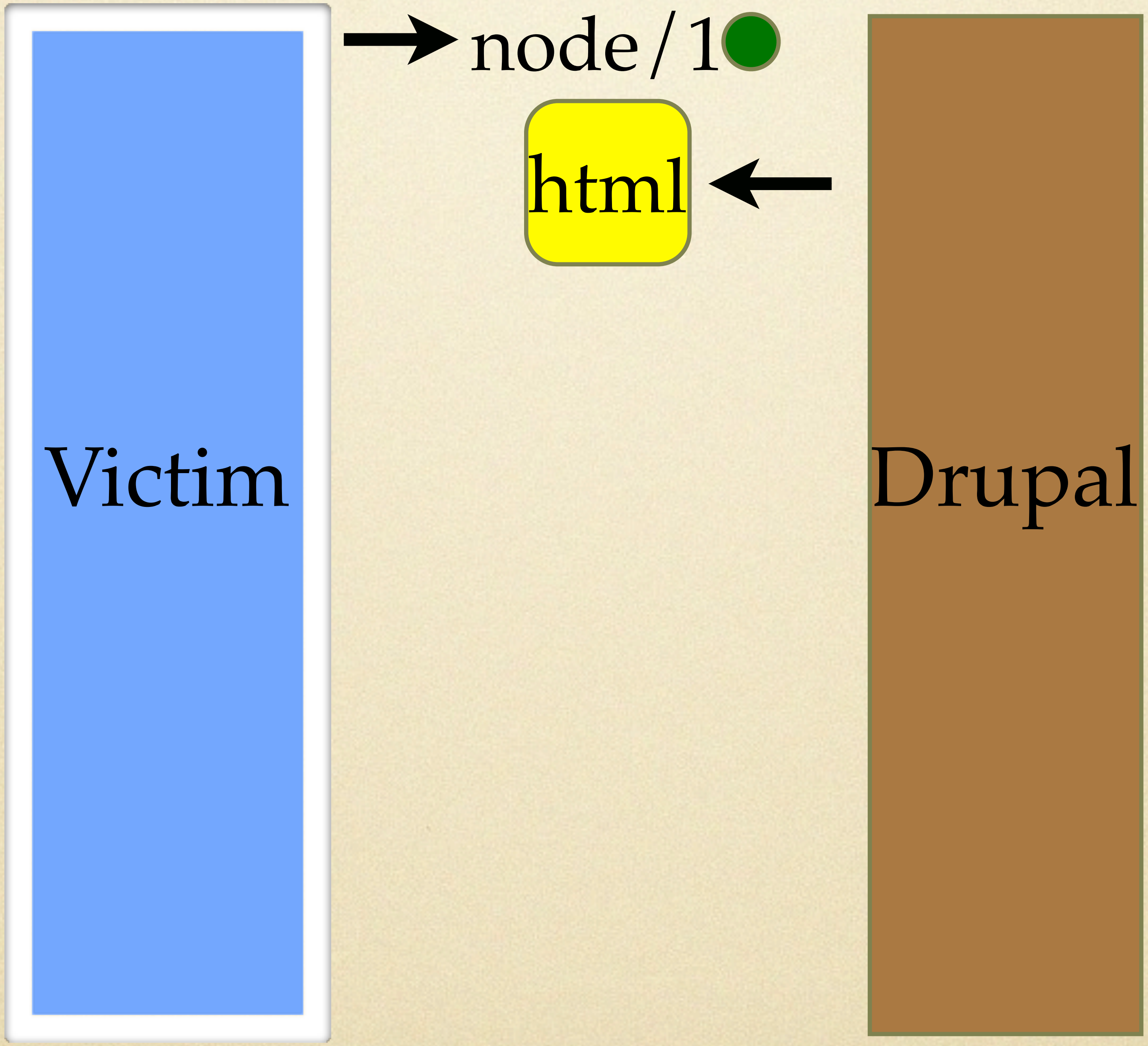
img src=delete/1

Drupal

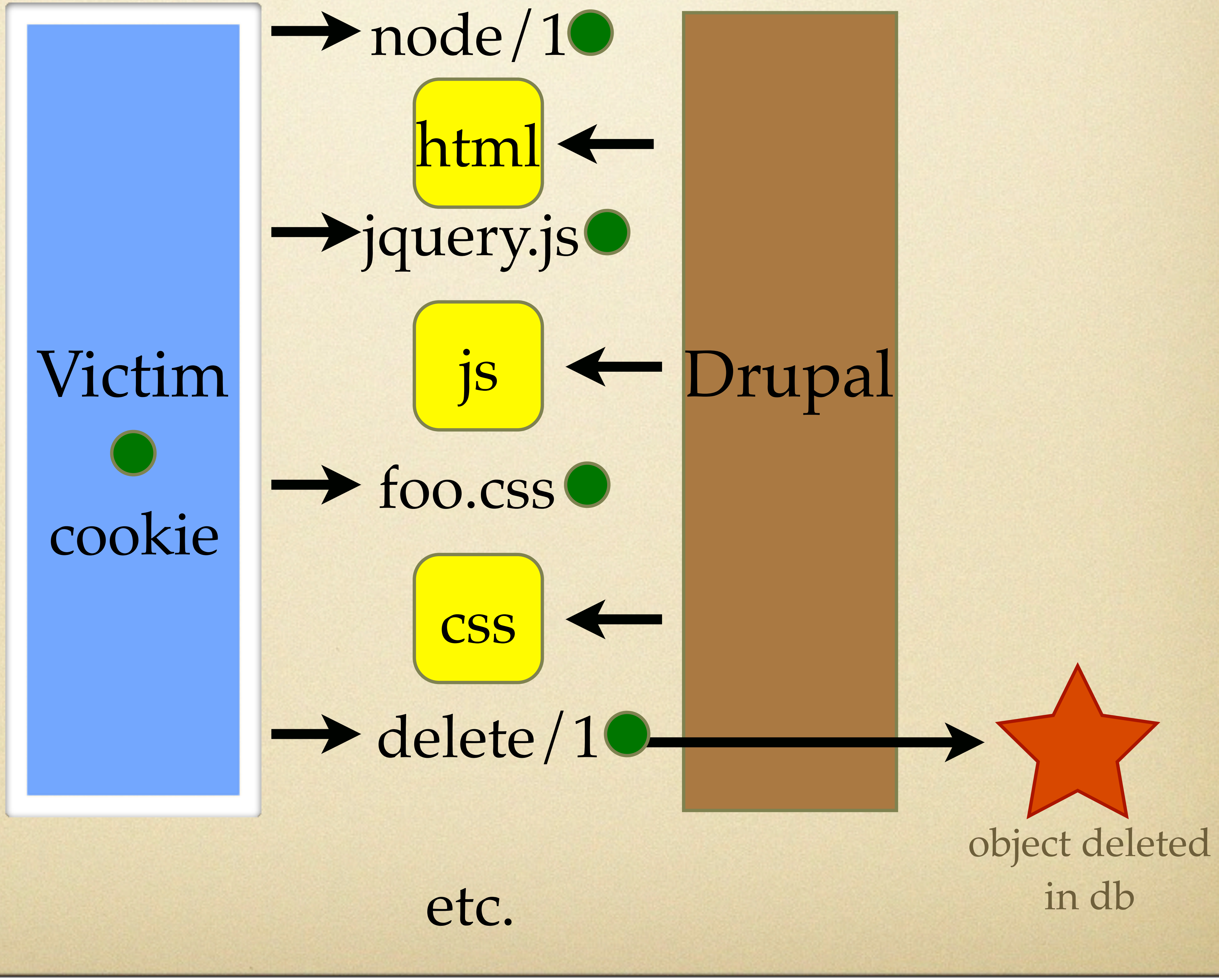
CSRF Flow



CSRF Flow



CSRF Flow


Victim
●
cookie
node/1●
html
jquery.js●
js
foo.css●
css
delete/1●
Drupal
object deleted
in db
etc.

How do you exploit it?

- URL Shorteners
- <img src="http://example.com/delete/2">
- Send a message to a site admin
  - What is my email address or twitter?

Are you my CSRF?

- menu callback with an action verb and not drupal_get_form
- directly use $_POST, $_GET, arg(), menu object
- not using form_submit OR drupal_get_token

Tokens (aka nonce)

- Form API includes tokens by default
- do form, form_validate, form_submit
  - don’t $_POST
- OR: drupal_get_token, drupal_valid_token

CSRF Resources

http://drupalscout.com/tags/csrf

XSS

aka: Cross Site Scripting

code in browser using your session

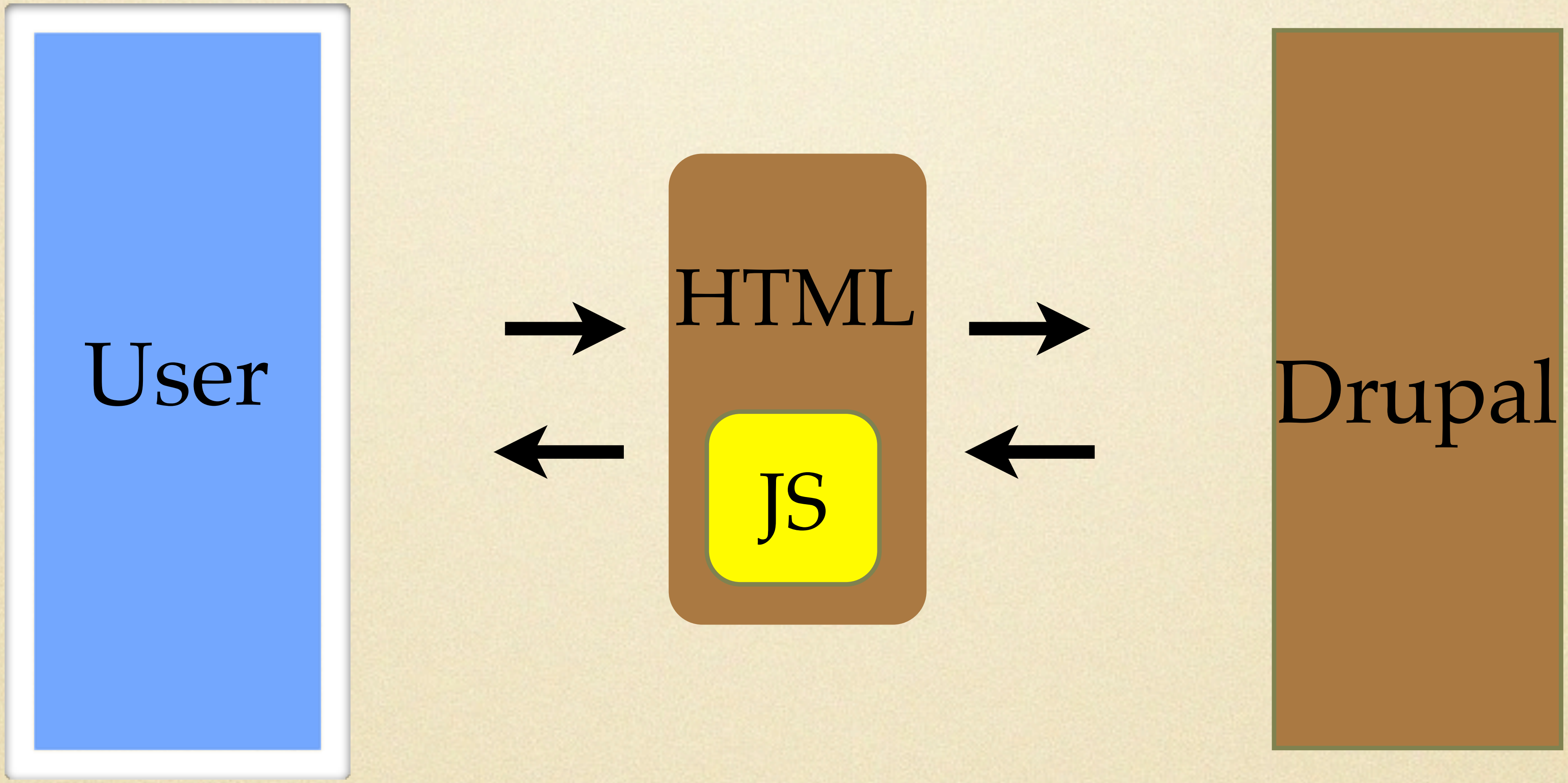
XSS

- Code
- Running in your browser
- Using your cookies on your site
- Requesting, sending, reading responses
- Browser context

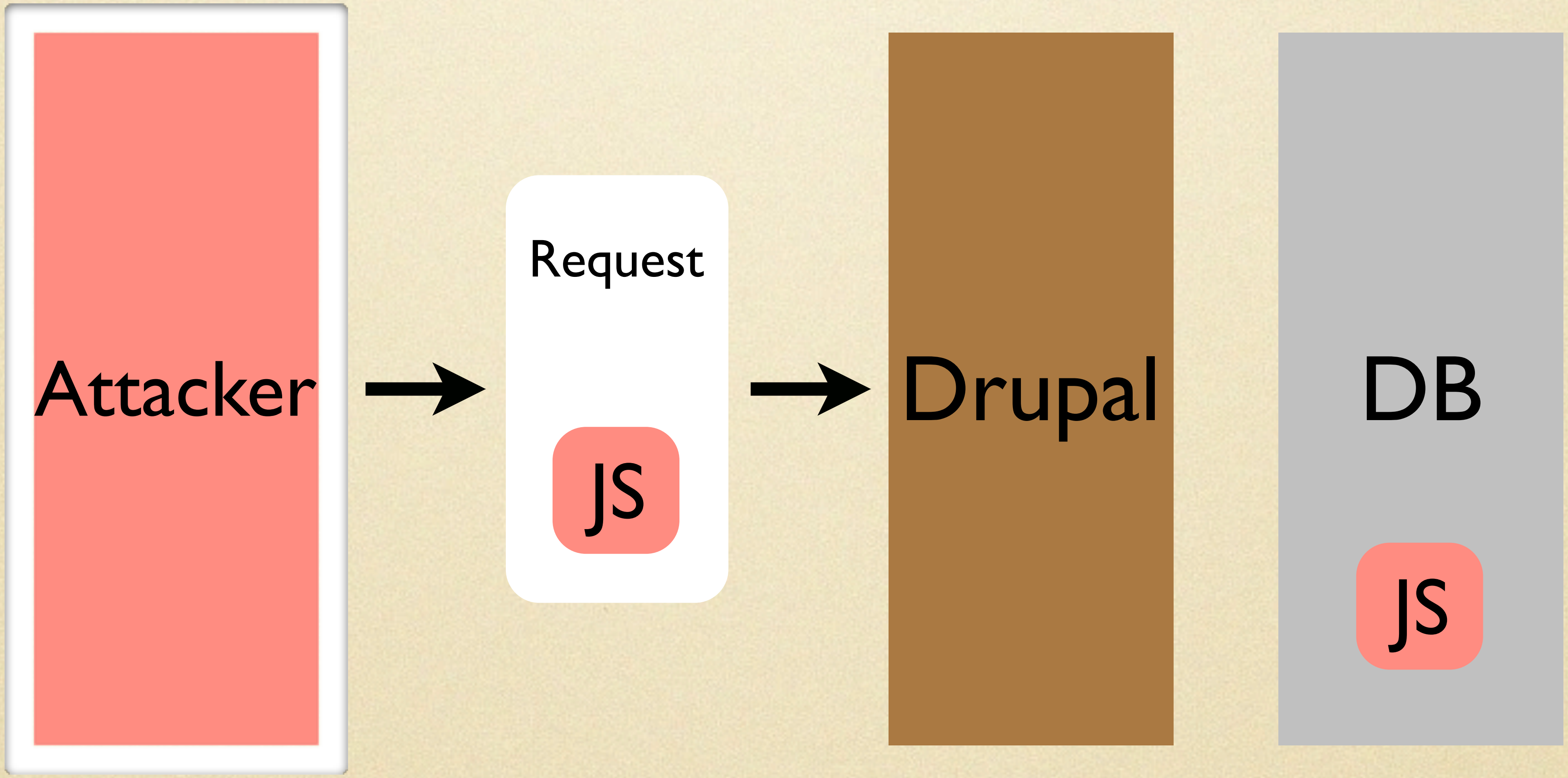
Does that sound familiar?

https://vimeo.com/15447718

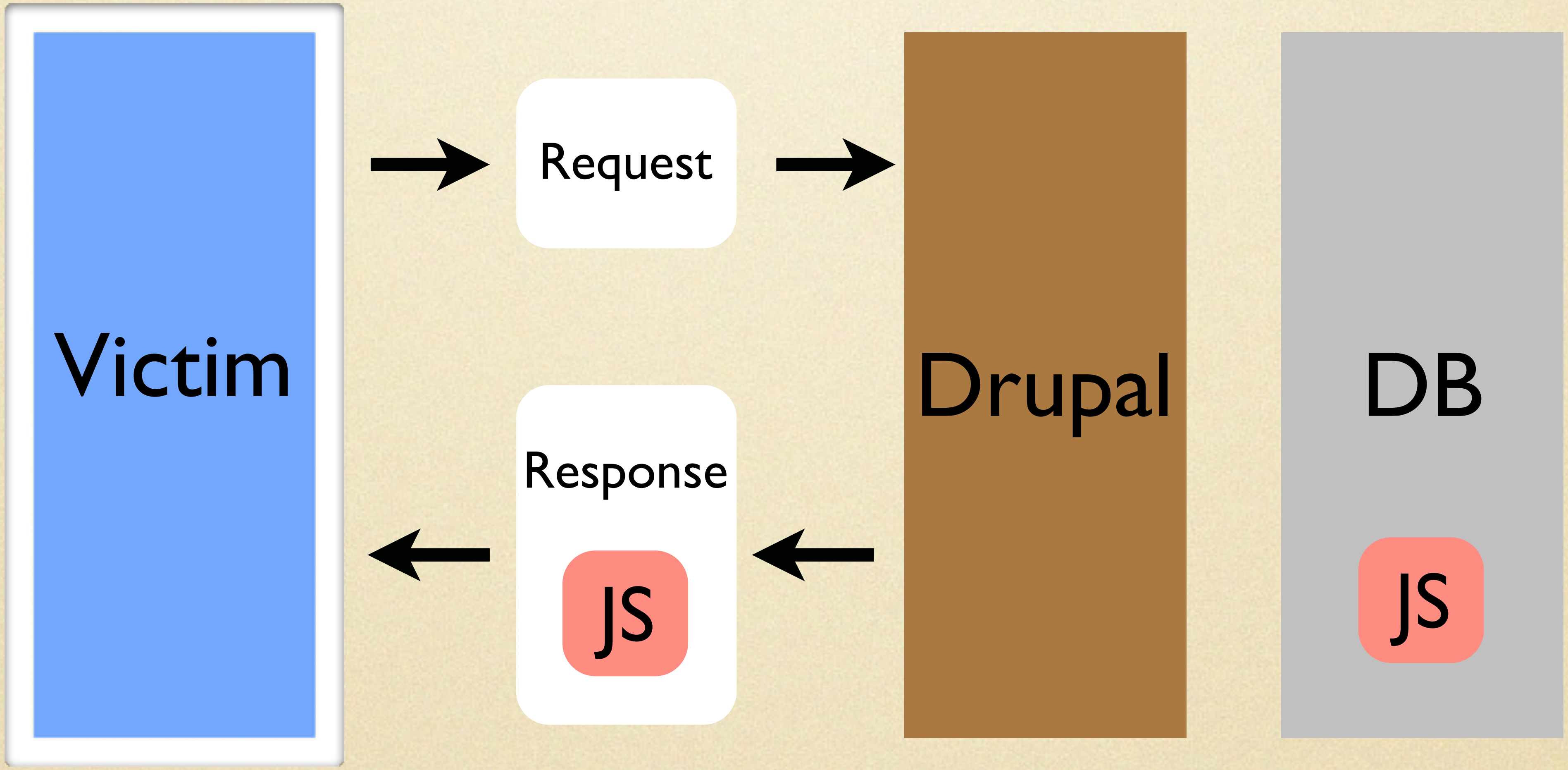
Ajax



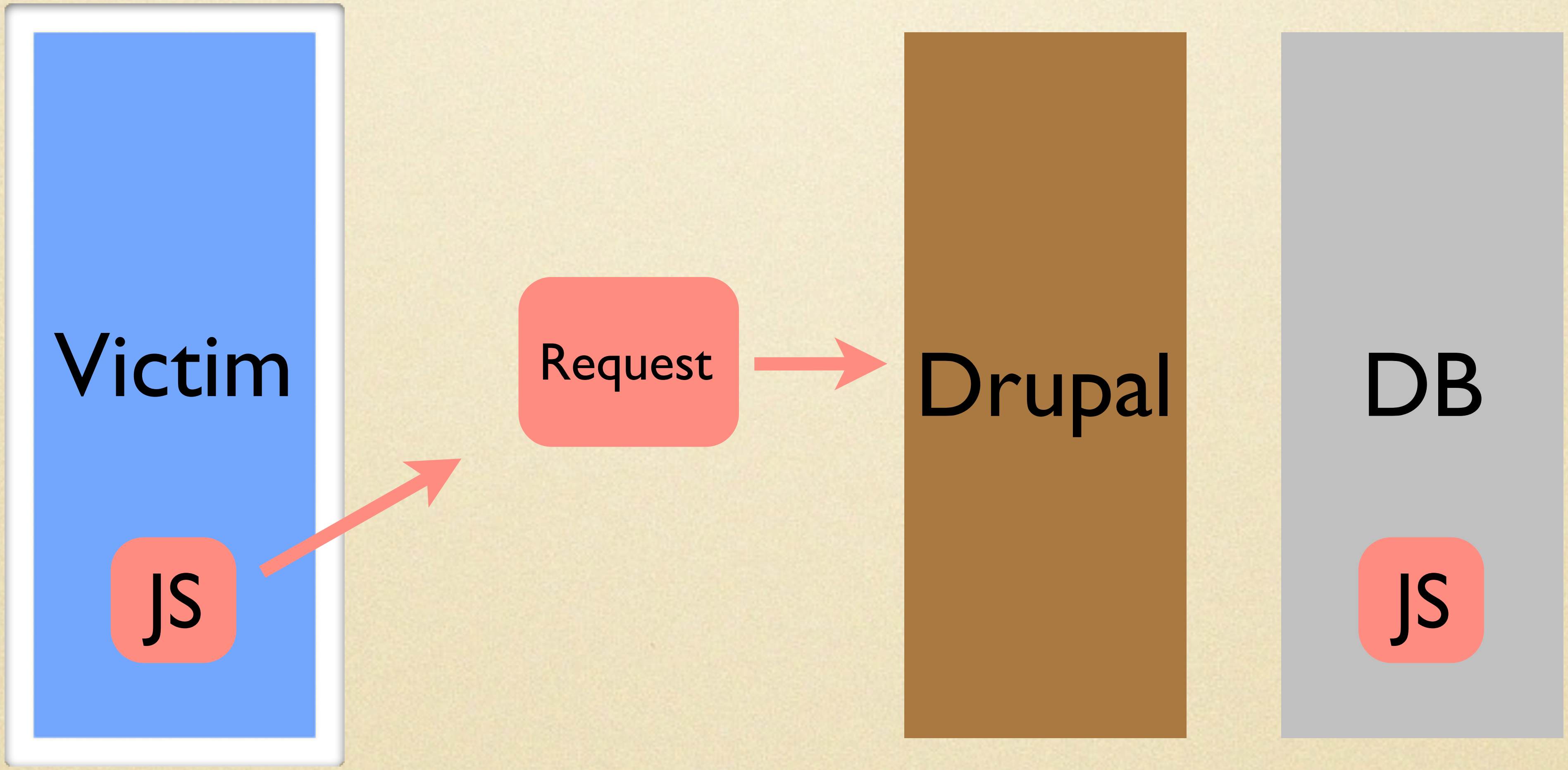
Cross Site Scripting



Cross Site Scripting



Cross Site Scripting



Validate input

“Why would I ever want javascript in a node title?”

-developer who forgot to filter on output

Validate input

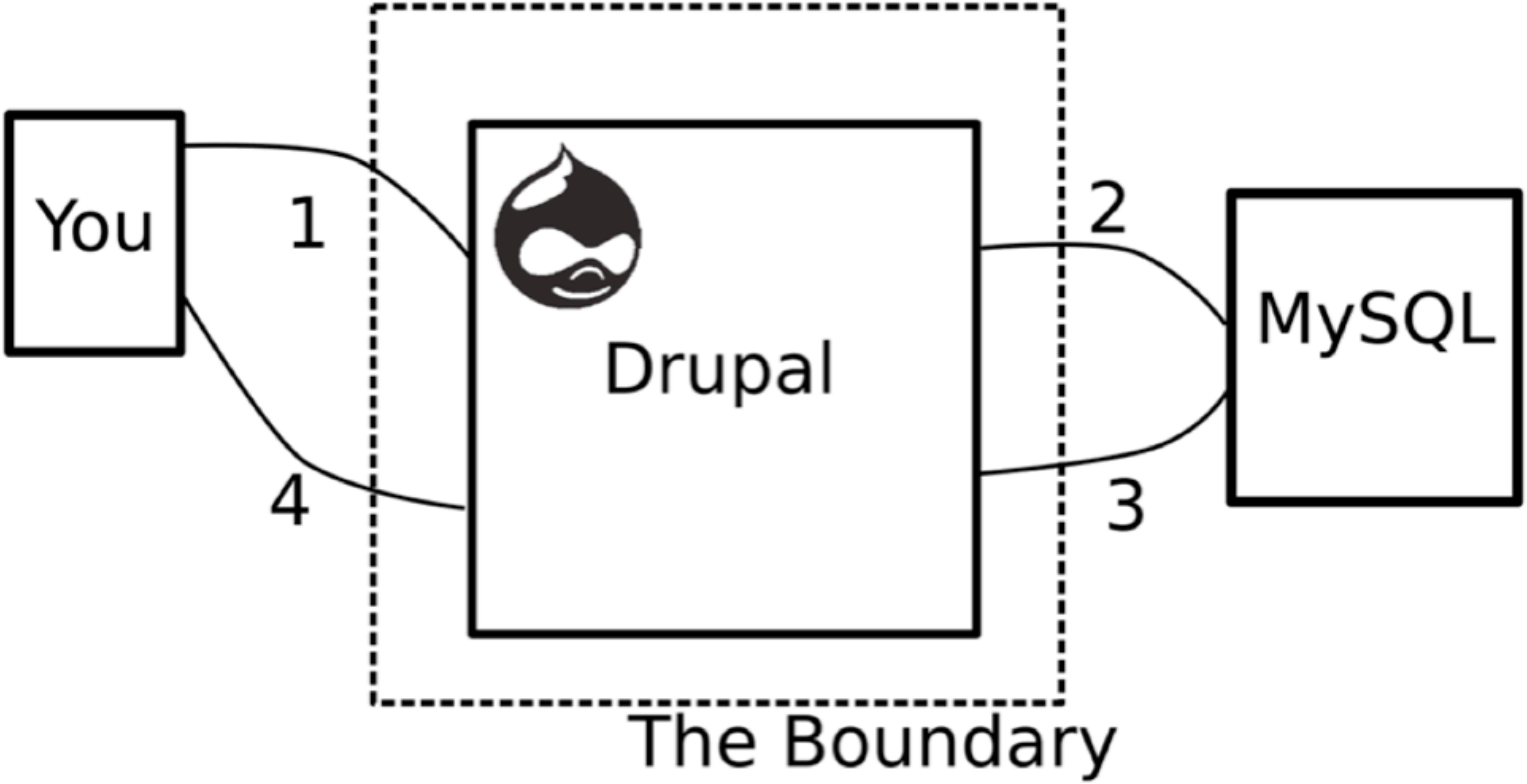
- Is it an email?
- Is it a nid (right type? that they have access to?)

Validation is NOT filtering

Validation is “yes or no” - user fixes it

Filter on output

- “output”
- “filter”
- “on”


You
1
4
Drupal
2
3
MySQL
The Boundary

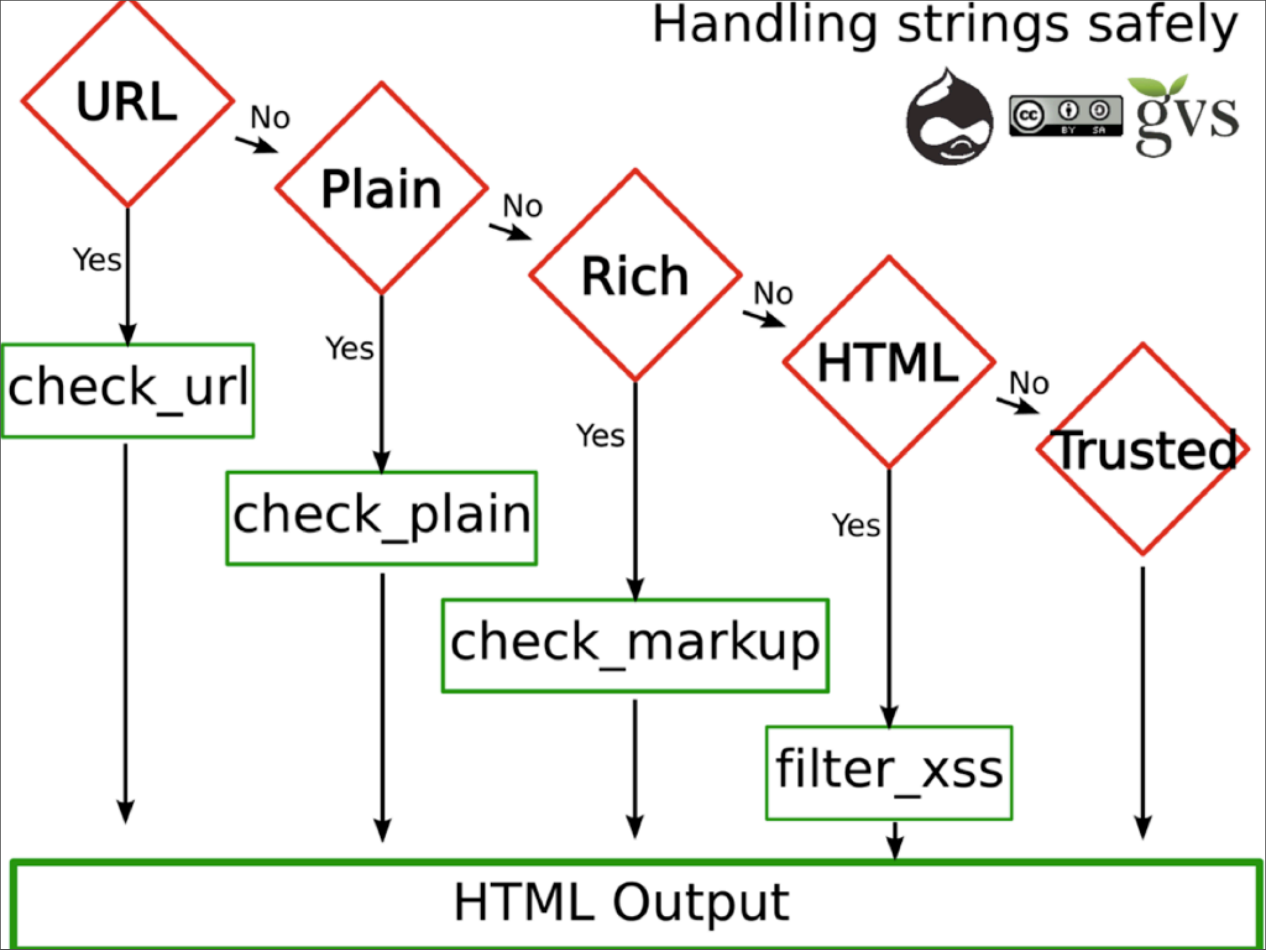
Output Contexts

- Mail context
- Database context
- Web context
- Server context
- http://acko.net/blog/safe-string-theory-for-the-web

Filtering XSS

- Input untrusted data
- Output browser appropriate data
- check_plain, check_markup
- filter_xss, filter_xss_admin
- free: l(), t() @ and %, drupal_set_title

Handling strings safely



Are you my XSS?

- `drupal_set_message($user_data);`
- `$output .= $node->title;`
- FAPI checkboxes, radios, descriptions, etc.

XSS Resources

http://drupalscout.com/tags/xss

Access Bypass

Authentication

Authorization

What is it?

- See something they shouldn’t see
- Do something they shouldn’t do

Stop Access Bypass

- Check before providing the action
- Check before taking action

Where do we check?

- Request arrives
- Find menu callback
- Call it
- Alter that
- Preprocess it
- Theme it

- 'access callback' => TRUE,
- Page callback
- $form['#access'] = whatevs();
- $form['f']['#access'] = whatevs();
- $o = theme(‘username’, $account);

R U my Access Bypass?

- Menu callbacks - kind of important
- node_access()
- $query->addTag('node_access')
- hook_permission/user_access

Resources

- drupal.org/security/writing-secure-code
- groups.drupal.org/best-practices-drupal-security
- drupalscout.com
- crackingdrupal.com

Mostly automated review

- drupal.org/project/security_review
- drupal.org/project/hacked
- drupal.org/project/coder
- drupal.org/project/secure_code_review
- Vuln: github.com/unn/vuln
- More: http://drupalscout.com/node/11

Pen-testing tools

- Too many false positives
- Instead, use Drupal specific tools
- Peer review code
- Contribute code

Automated analysis++

- Acquia Insight
- Near real-time 100+ checks
- Routinely alert you to mistakes

Evaluate our session, please

munich2012.drupal.org/node/733

Thanks!

@greggles
@benswords