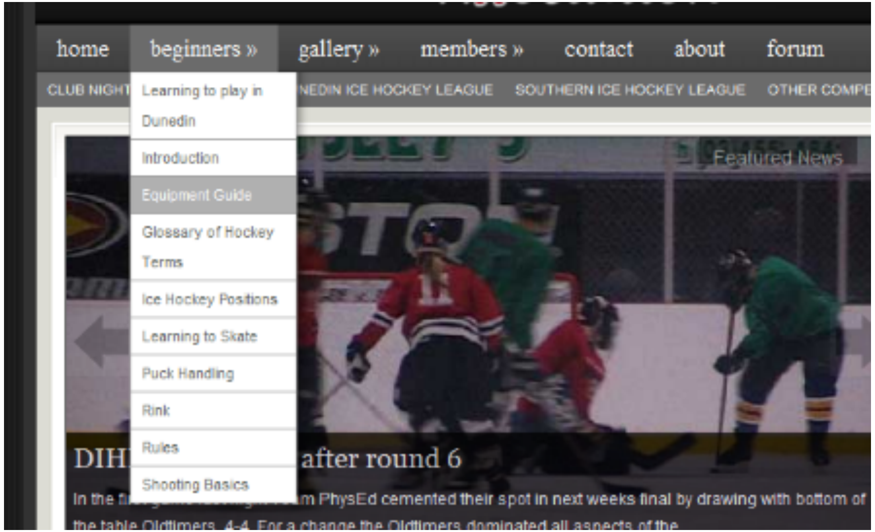
Security

It’s not paranoia when they’re actually out to get you!

Where in the world is Ryan from?

Created a menu plugin

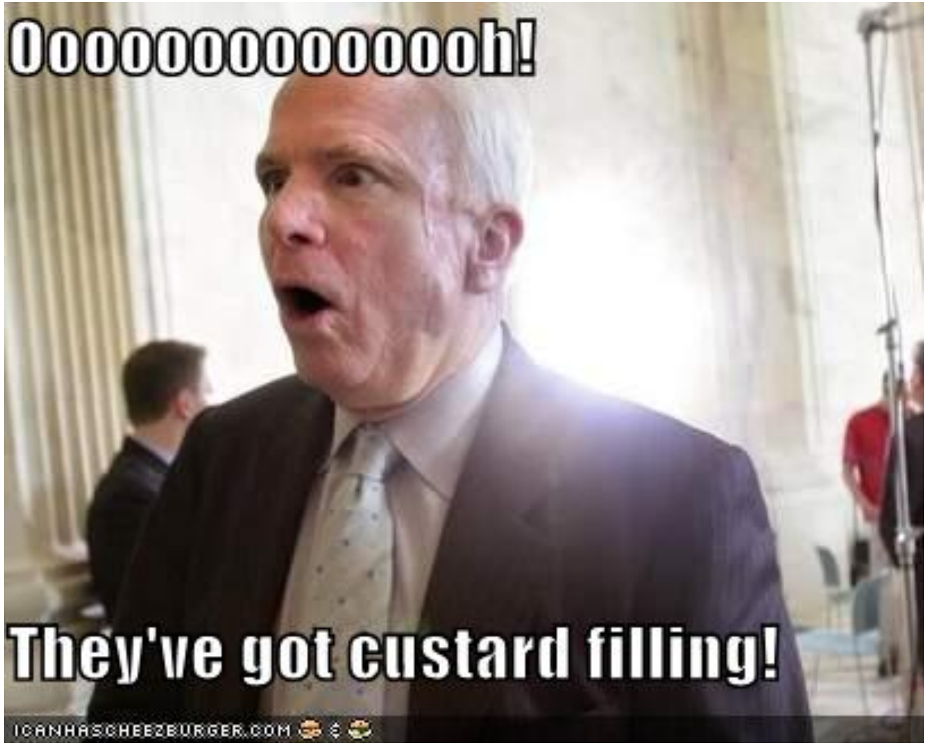
- Pre menus in core
- Dropdowns!



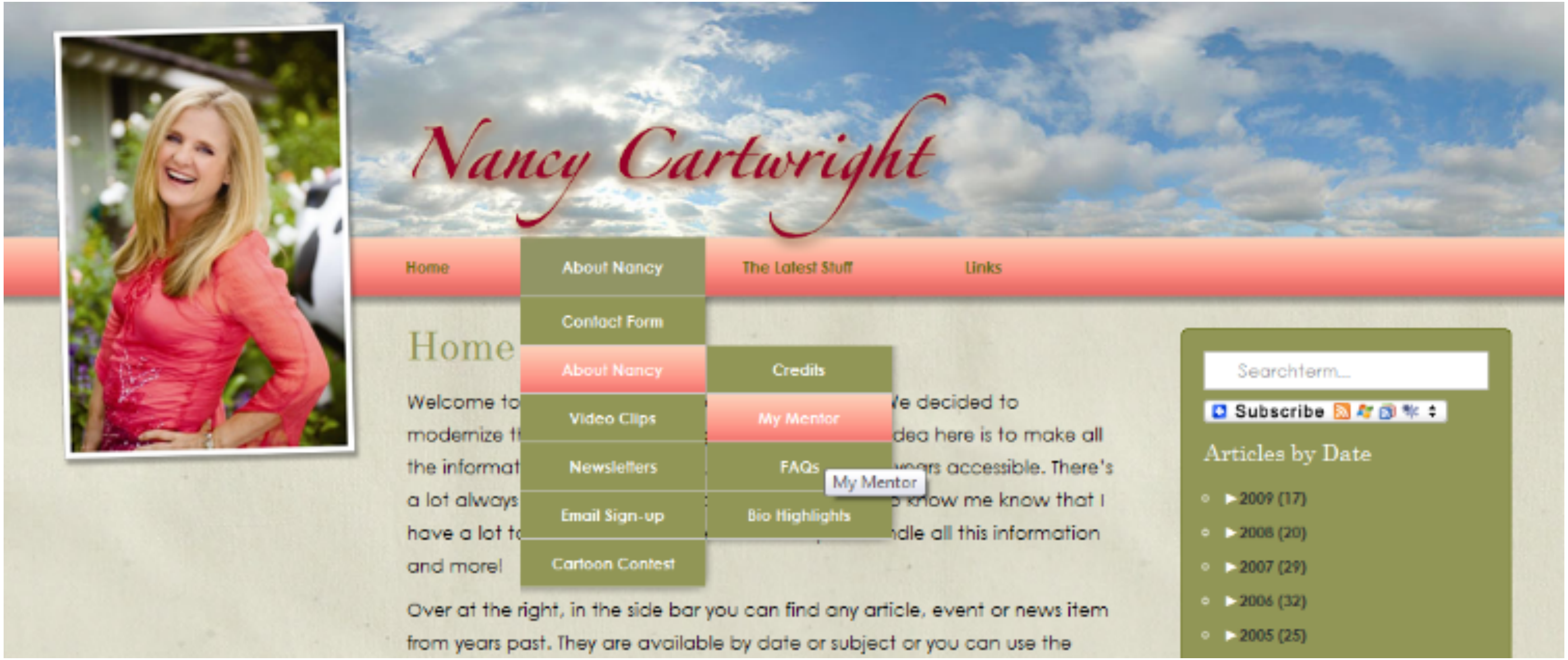
DIH after round 6

In the fi m PhysEd cemented their spot in next weeks final by drawing with bottom of the table Oldtimers 4-4. For a change the Oldtimers dominated all aspects of the

John McCain


Oooooooooooooh!
They've got custard filling!
ICANHASCHEEZBURGER.COM

Bart Simpson



Home

Welcome to
've decided to
modernize t
dea here is to make all
the informat
years accessible. There's
a lot always
know me know that I
have a lot t
ndle all this information
and more!

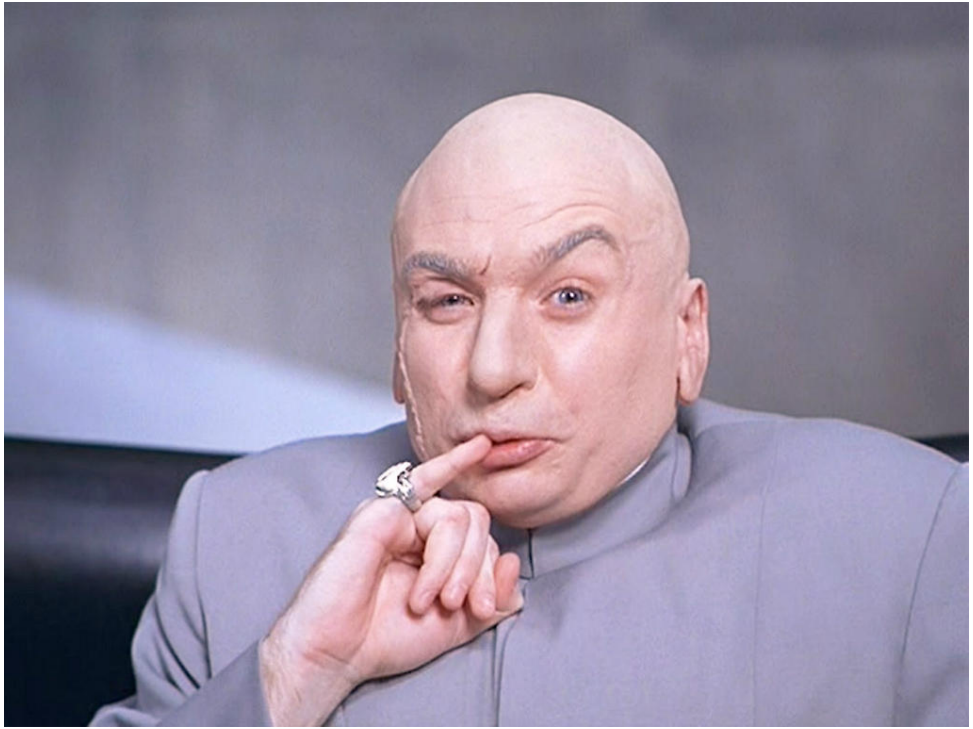
Over at the right, in the side bar you can find any article, event or news item from years past. They are available by date or subject or you can use the

Security audit

A+

No flaws found

Disaster



- Blog post
- Security flaw found
- Public announcement

update_option(‘css’, $_POST[‘css’]

Trust no one!

PARANOIA

That unmistakable feeling everyone is out to get you!

Code injection

- Trusted users … no problem
- Trusted user accounts … big problem

- Code injection via admins is a big problem

XSS

Nerdy interlude

Need to do four things …

1. Check user has permission
2. Check user intended to do it
3. Sanitize/validate user data
4. Escape data before output

How to spot bad code

Impossible to teach in a short lecture :(

```
update_option( ‘bla’, $_GET[‘test’] );
echo get_option( ‘bla’ );
```

```
http://domain.com/?test=<script>alert(‘test’);</script>
```

Trusting outside sources

- $_SERVER
- $_COOKIE
- $_POST
- $_GET
- $_REQUEST
- API data

The rules

- Trust no one
  - Including logged in users
- Validate/sanitize inputs
- Escape outputs

Top 100 plugins on WordPress.org

- In 2011, found (hackable) security flaws in 50%
  - 20% were hackable on most setups

- In 2014, most have been fixed
  - Still need to be careful of elevated permission setups

Quality has gone up for the top 100 plugins :)

WordPress security plugins

Securi Security plugin

Core file verification check!

Minimum Password Strength plugin

New Zealand

Norway

Germany

Lets put our tinfoil hat on

NATIONAL SECURITY AGENCY
UNITE
AMERICA

Scenario

Want to store private data in our website

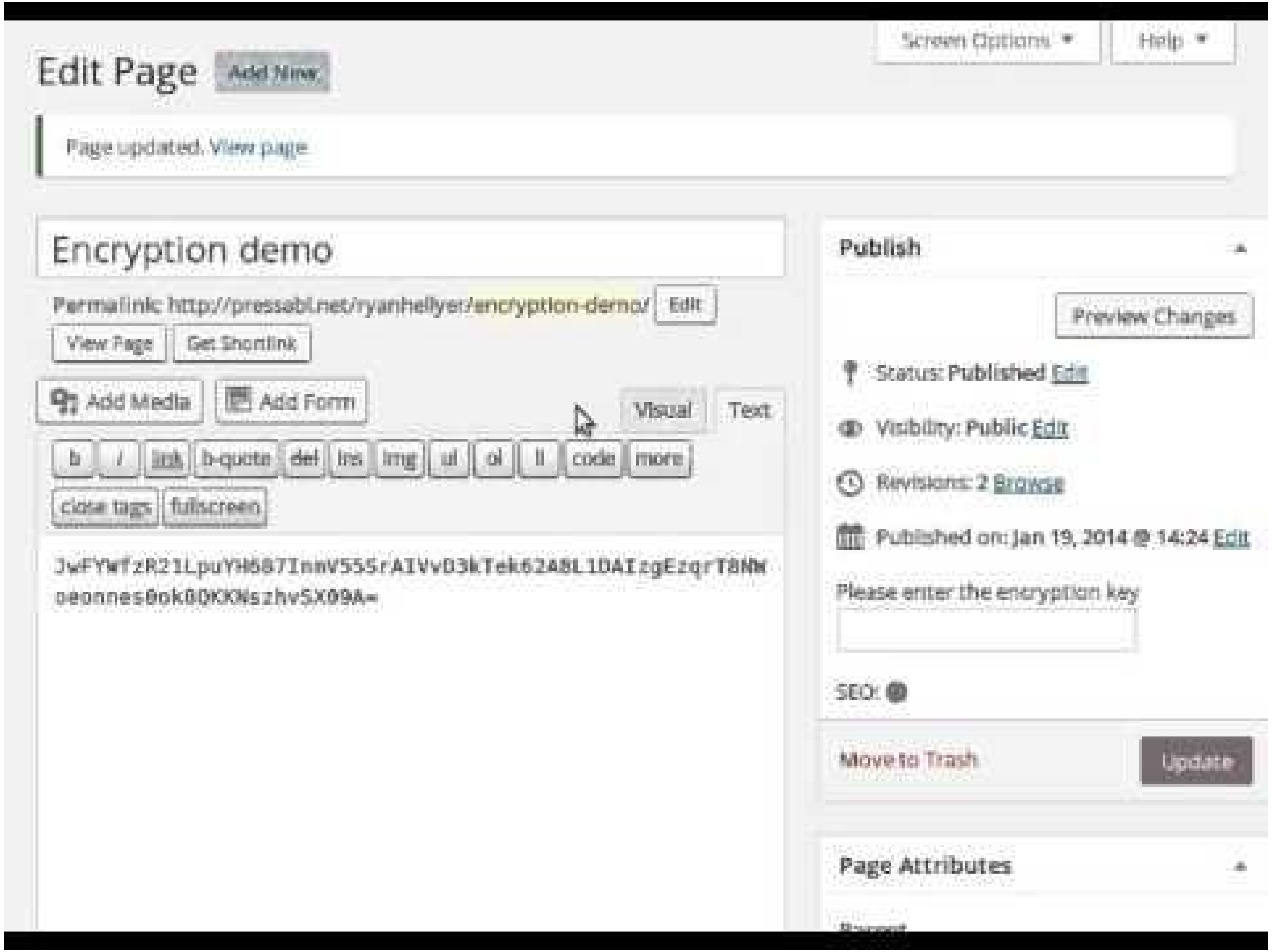
Only certain people to have access

- Use private pages?
- User password protected pages?
- Something better?

Encrypt data

Can’t send unencrypted data back to the server

Browser -> [encryption] -> server -> browser -> [decryption]



Edit Page Add New

Page updated. View page

Encryption demo

Permalink: http://pressabl.net/ryanhellyer/encryption-demo/

```
JwFYWfzR21LpuYH687InmV555rAIVvD3kTek62A8L1DAIzgEzqrT8NW
oeonnes0ok0OKKNszhv5X09A=
```

Publish

Status: Published Edit

Visibility: Public Edit

Revisions: 2 Browse

Published on: Jan 19, 2014 @ 14:24 Edit

Please enter the encryption key

SEO: ●

Page Attributes

Parent

Problems

- Similar to CryptoCat
- Self JavaScript attack
- Solution?
  - browser plugin
- Help wanted!

Thank you!

- 10up
- Anthony Cole
- Mark Jaquith