

---

# Security



---

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

---

# Where in the world is Ryan from?

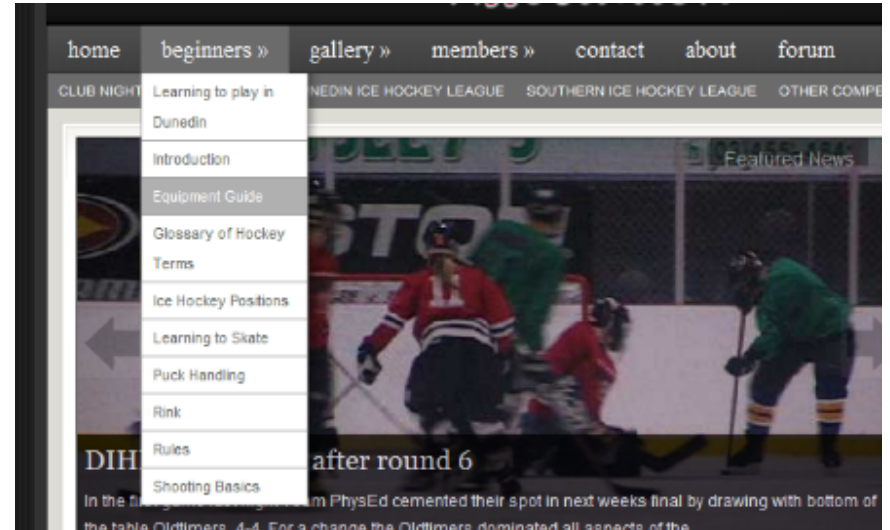
---



# Created a menu plugin

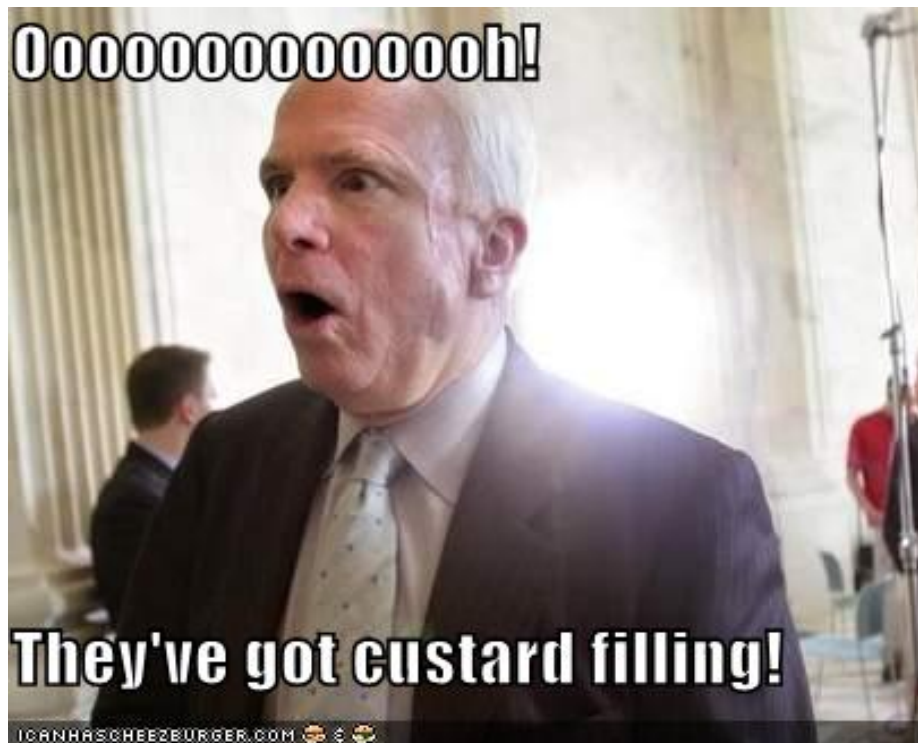
---

- Pre menus in core
- Dropdowns!



# John McCain

---





# Bart Simpson



The image is a screenshot of a website for Nancy Cartwright. On the left, there is a portrait of Nancy Cartwright, a blonde woman with a bright smile, wearing a red long-sleeved top. The background of the website header features a blue sky with white clouds. The name "Nancy Cartwright" is written in a large, elegant, red cursive font across the top. Below the header, there is a navigation bar with four links: "Home", "About Nancy", "The Latest Stuff", and "Links". The "About Nancy" link is highlighted in red. Below the navigation bar, there is a main content area. On the left side of this area, the word "Home" is written in a large, green, serif font. Below it, there is a paragraph of text that is partially obscured by a grid of menu items. The grid consists of several green rectangular buttons with white text. The buttons are arranged in two columns. The first column contains: "Contact Form", "About Nancy" (highlighted in red), "Video Clips", "Newsletters", "Email Sign-up", and "Cartoon Contest". The second column contains: "Credits", "My Mentor" (highlighted in red), "FAQs", "Bio Highlights", and another "My Mentor" button. To the right of the grid, there is a search bar with the placeholder text "Searchterm..." and a "Subscribe" button with social media icons. Below the search bar, there is a section titled "Articles by Date" with a list of years and the number of articles for each year: 2009 (17), 2008 (20), 2007 (29), 2006 (32), and 2005 (25).

*Nancy Cartwright*

Home About Nancy The Latest Stuff Links

Home

Welcome to  
modernize the  
the informat  
a lot always  
have a lot to  
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

Searchterm...

Subscribe

Articles by Date

- ▶ 2009 (17)
- ▶ 2008 (20)
- ▶ 2007 (29)
- ▶ 2006 (32)
- ▶ 2005 (25)

# Security audit

---

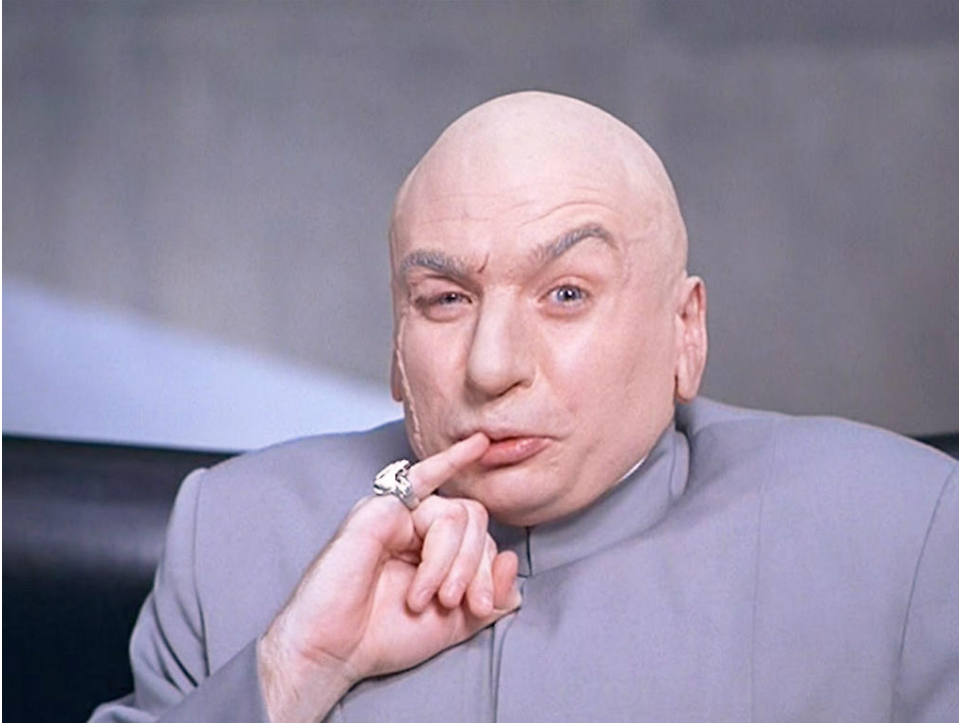
A+

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

---





# 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](#)[Screen Options](#)[Help](#)

Page updated. [View page](#)

### Encryption demo

Permalink: <http://pressabl.net/ryanhellyer/encryption-demo/> [Edit](#)

[View Page](#)[Get Shortlink](#)[Add Media](#)[Add Form](#)[Visual](#)[Text](#)

[b](#) [i](#) [link](#) [b-quote](#) [del](#) [ins](#) [img](#) [ul](#) [ol](#) [li](#) [code](#) [more](#)

[close tags](#)[fullscreen](#)

JwFYwfzR21LpuYH687InnV55SrAIVvD3kTek6248L1DAIzgEqRT8NM  
oeonnes0pk0QKKNs zhv5X09A=

### Publish

[Preview Changes](#)

Status: Published [Edit](#)

Visibility: Public [Edit](#)

Revisions: 2 [Browse](#)

Published on: Jan 19, 2014 @ 14:24 [Edit](#)

Please enter the encryption key

SEO: [?](#)

[Move to Trash](#)[Update](#)

### Page Attributes

# Problems

---

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

# Thank you!

---

- 10up
  - Anthony Cole
  - Mark Jaquith
- 

