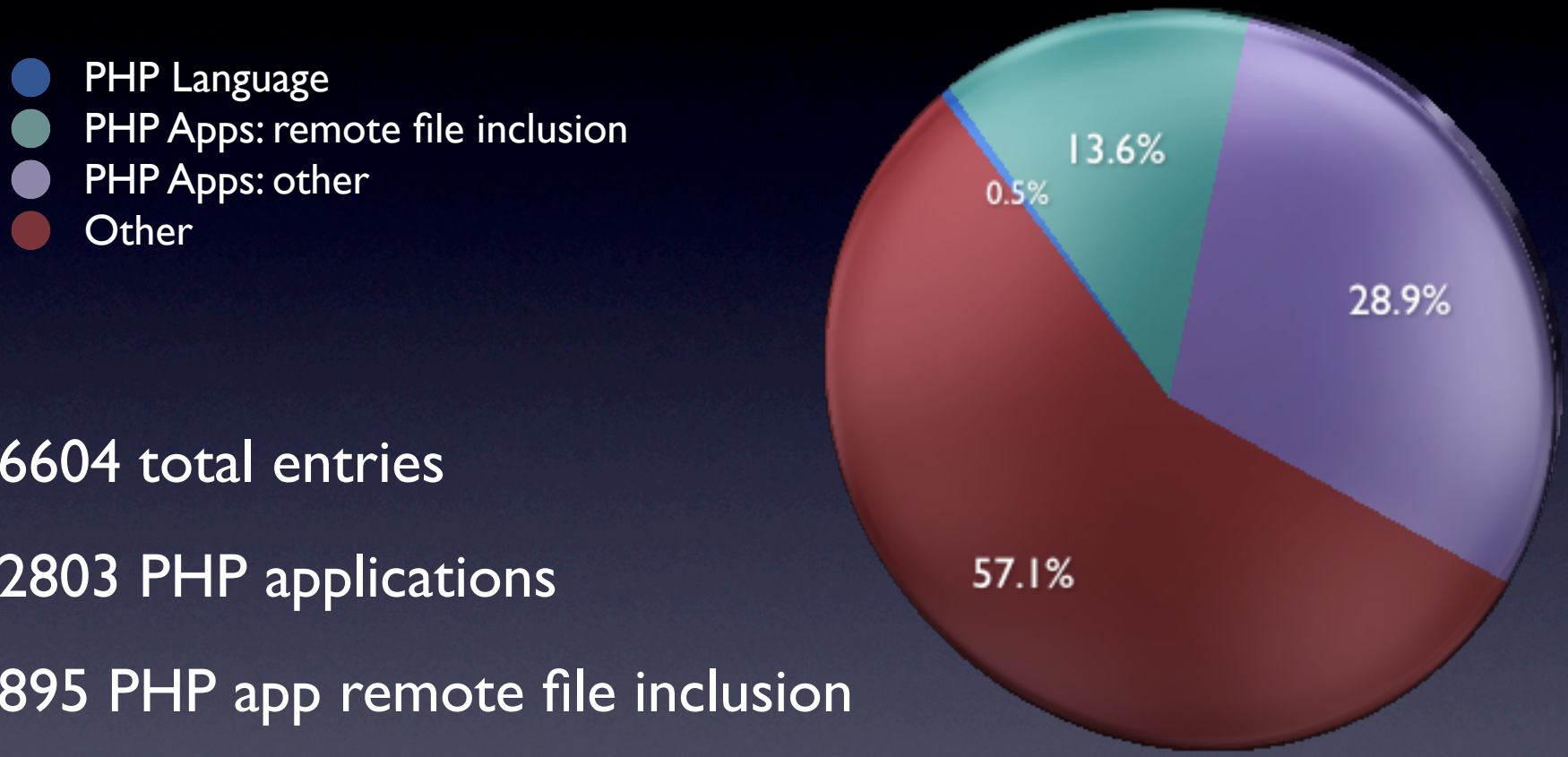
Secure PHP Development with Inspekt

Ed Finkler <coj@funkatron.com>

DC PHP Conference – 11/08/2007

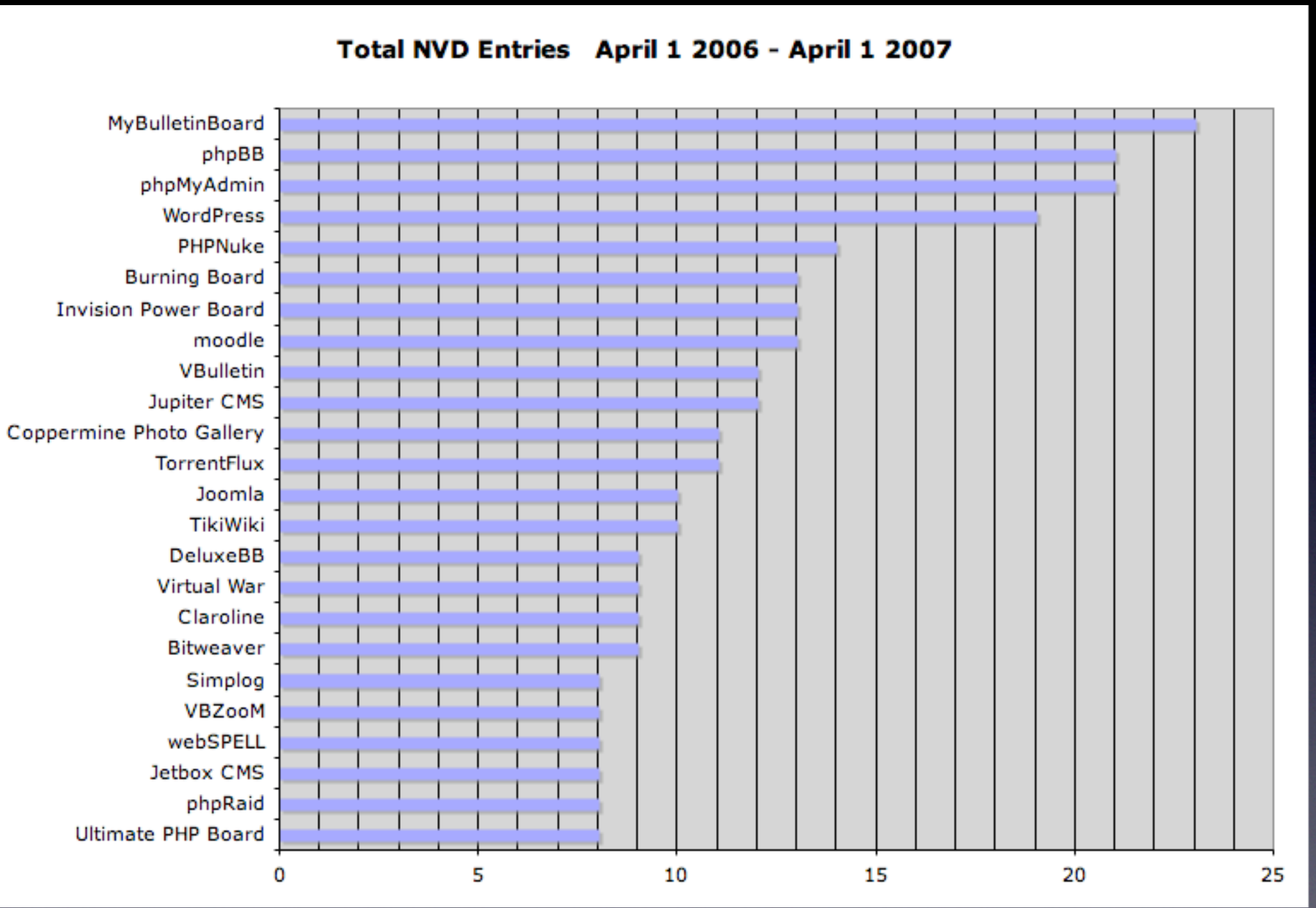
Be afraid

NIST NVD: 2006 data

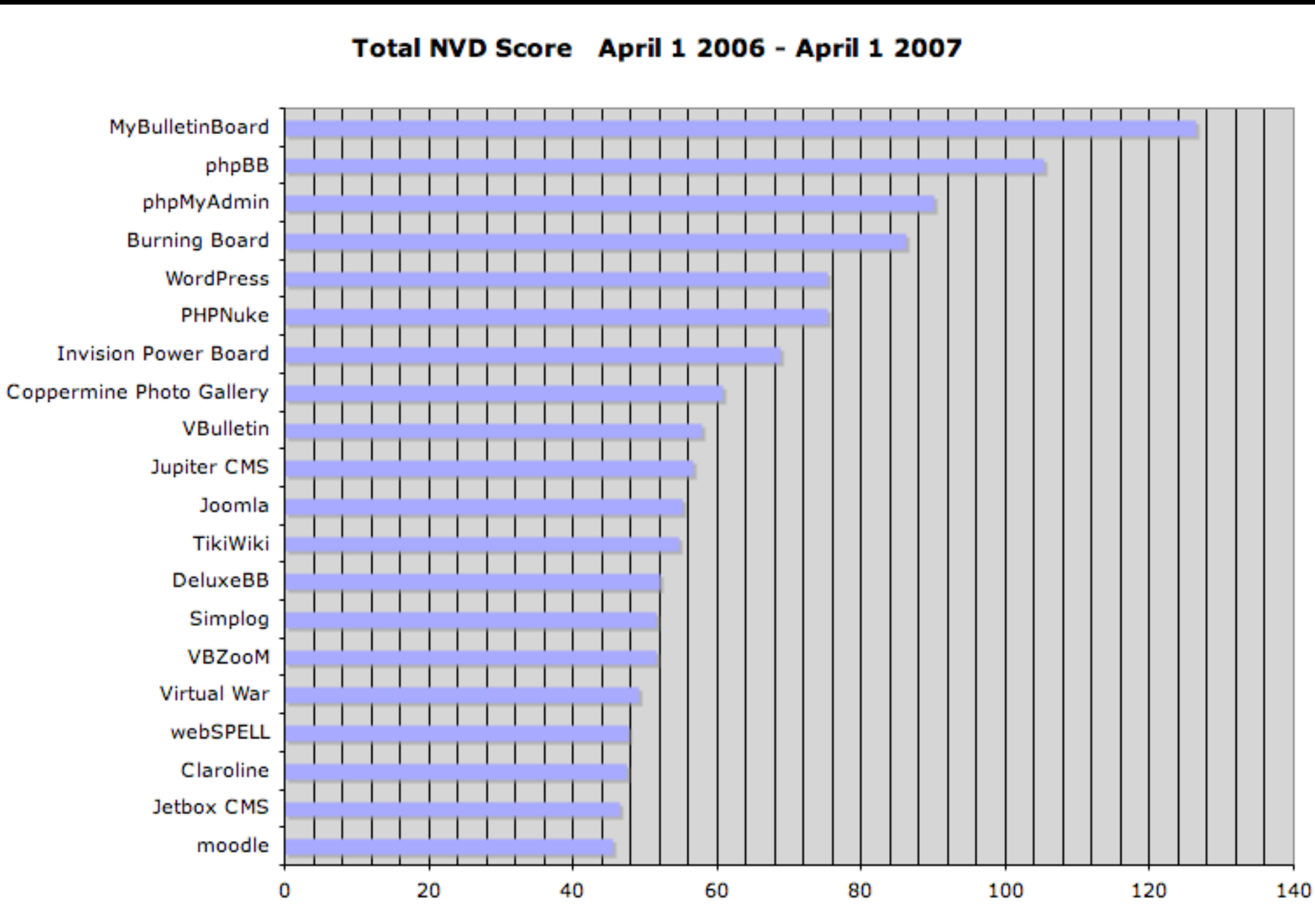


- 6604 total entries
- 2803 PHP applications
- 895 PHP app remote file inclusion
  - Almost blocked by disabling allow_url_fopen (allow_url_include in 5.2+)

Ed Finkler <coj@funkatron.com>



Ed Finkler <coj@funkatron.com>



Ed Finkler <coj@funkatron.com>

Well, that sucked

- PHP has a very shallow learning curve
  - Great for adoption
  - Not so great for security

Dealing with input

- The problem of direct access
  - Default action is insecure
    - Security is more work than insecurity
  - Error-prone

```php
<?php

/**
 * Classic direct access approach to obtaining input
 * By default, this is raw, dangerous
 */
$id = $_POST['id'];

// casting as int
$id = (int)$_POST['id'];

// escaping for mysql
$id = mysql_real_escape_string($_POST['id']);

```

Dealing with input

- The importance of architecture in security
  - Single point of defense vs multiple points
  - Need to apply same fixes multiple times
    - More instances == more errors

> "We have fine HTML filtering with KSES. The filtering has never been a problem, it's just places where it's been not [sic] applied." – *Matt Mullenweg*

Guiding principles

- Simple and straightforward
  - Secure development needs to be as easy as possible
  - Don't require complex setup process
  - Clearly delineates from old habits
  - Needs to make creation of secure apps *easier*, and creation of insecure apps *harder*

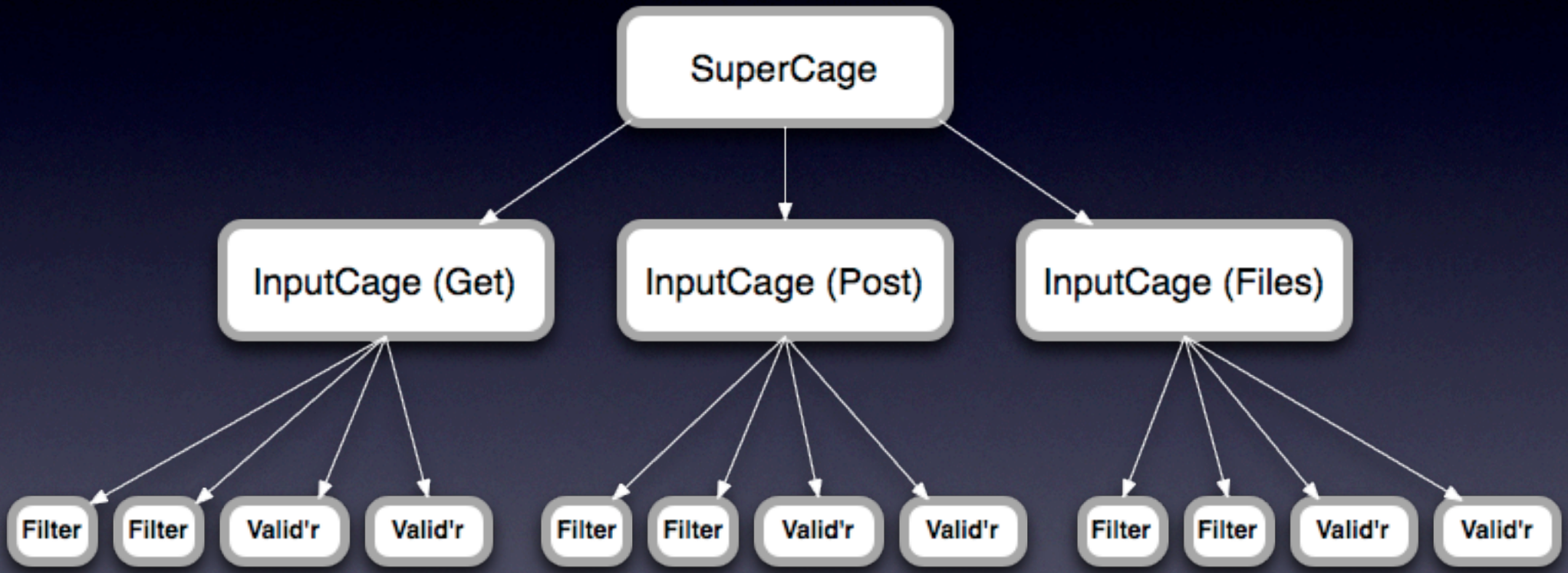
Inspekt's ancestry

- Original Zend_Input_Filter
  - Chris Shiflett
  - PHP5-only
    - This was a bigger issue pre-PHP4 deprecation
  - No support for multidimensional arrays
  - Relied on Zend Framework

Inspekt's ancestry

- **Inspekt changes**
  - PHP4 and 5
  - Supports multidimensional arrays
    - Both access and application of filters
  - No external dependencies

Inspekt Hierarchy



Ed Finkler <coj@funkatron.com>

Features

- **Validators and Filters**
  - Validators examine data and return information about data
  - Filters modify data and return modified version
  - if passed an array, filters will walk the array recursively
    - makes less sense for validators

Filters and validators

```
Inspekt::foo($bar);
```

Filters

getAlnum
getAlpha
getDigits
getDir
getPath
getInt
noPath
noTags

Validators

isAlnum
isAlpha
isBetween
isCcnum
isDate
isDigits
isEmail
isFloat
isGreaterThan
isHex
isHostname
isInt
isIp
isLessThan
isOneOf
isPhone
isRegex
isUri
isZip

Features

- **Input cage**
  - Encapsulates an array inside object
    - Existing array nullified
  - Access to data via filter/validator methods

Features

- **Input cage**
  - Helper methods to quickly create cages for input arrays

```
Inspekt::makeFooCage()
```

makeCookieCage
makeEnvCage
makeFilesCage
makeGetCage
makePostCage
makeServerCage
makeSessionCage

```
$postCage->getAlnum('username')
```

Features

- **SuperCage**
  - Creates an object with 7 input cages as properties
  - Created by helper method

```
Inspekt::makeSuperCage()
```

Features

- **SuperCage**
  - correspond to 7 superglobals
    - env
    - files
    - get
    - post
    - cookie
    - session
    - server

```
$supercage->post->getAlnum('username')
```

Features

- **Scoping issues and singletons**
  - Superglobals have advantage of automatic global scoping
  - Singleton pattern is best solution
    - requires call to create cage in each new scope

Ways to use Inspekt

- **Bootstrapping w/ Supercage**
  - Apply Inspekt before anything else can access input
    - require on each page
    - auto_prepend

Ways to use Inspekt

- **Apply to arbitrary array**
  - `Inspekt_Cage::Factory($array)`
- **Static calls to filter and validator methods**
  - `Inspekt::getAlnum($mixed)`

Future

- **1.0 Release by Dec 1**
  - Ability to auto-filter via config files
  - PEAR channel distribution
  - Human-generated docs for all functionality

Post 1.0 (*may change*)

- Drop PHP4 support
  - bug fixes would still be applied, but no new features
  - lots of wins in PHP5
- Integration with HTML Purifier (htmlpurifier.org)
- New filters/validators
- **New contributors???**

More information

- inspekt.org
- funkatron.com
- owasp.org