This machine is a seen
DO NOT POWER DOWN!!
Security Vulnerability

This machine is aaser
DO NOT POWE"
"" DOWN!!
Security Vulnerability

Web Applications
Process Innovations For Security Vulnerability Prevention In Open Source Web Applications

Diploma Thesis Presentation
Florian Thiel 2009/05/25
“How to make open source web applications more secure without resorting to forks and rewrites”
Focus

SQL Injection

XSS
Hi, this is your son's school. We're having some computer trouble.

Oh, dear - did he break something?

In a way -

DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?

Oh, yes. Little Bobby Tables, we call him.

Well, we've lost this year's student records. I hope you're happy.

And I hope you've learned to sanitize your database inputs.
“SELECT firstname FROM Students
WHERE (login = ‘%s’ AND password = ‘%s’);
% (login, password)
"SELECT firstname FROM Students WHERE (login = '%%s' AND password = '%%s');" % (login, password)

SELECT firstname FROM Students WHERE (login = 'Robert'); DROP TABLE Students; --

AND password = "";
Threat to:

• Integrity
• Confidentiality
• Accountability
• Availability
if ($this->date_last_updated === null || $this->date_last_updated === true)
  return null;

else if (!is_int($this->date_last_updated)) {
  // a non-timestamp value was set externally, so we
  // validate it:
  $ts = strtotime($this->date_last_updated);
  if ($ts === -1 || $ts === time())
    throw new PropertyException('date_last_updated');
}
else {
  $ts = $this->date_last_updated;
}

if ($format === null) {
  return $ts;
}
else if (strpos($format, '%') !== false)
  return strftime($format, $ts);
else {
  return date($format, $ts);
}
if ($this->date_last_updated === null || $this->date_l
    return null;
} elseif (!is_int($this->date_last_updated)) {
    // a non-timestamp value was set externally, so we
    $ts = strtotime($this->date_last_updated);
    if ($ts === -1 || $ts)
        throw new PropertyTypeException($this,
            'Can not convert to date', $this->get_property_name(), $this->get_value());
    }
} else {
    $ts = $this->date_last_updated;

    if ($format === null) {
        return $ts;
    elseif (strpos($format, '%') !== false)
        return strftime($format, $ts);
    else {
        return date($format, $ts);
    }
}
http://www.phpnuke.org/user.php?
 op=userinfo&uname=
 <script>alert(document.cookie); </script>
<h3 class="storytitle">
<a href="<?php the_permalink() ?>"
rel="bookmark">
<?php the_title(); ?></a>
</h3>

WordPress, wp-content/themes/classic/index.php
Threats:

• Account Theft
• User Tracking
• Misinformation
(1) technology is mature enough
Failure to sanitize data into a different plane
Process Innovations For Security Vulnerability Prevention In Open Source Web Applications
Process Innovations For Security Vulnerability Prevention In Open Source Web Applications
(2) architecture matters

- web browser
- database
- application
- ...
Process Innovations For Security Vulnerability Prevention In Open Source Web Applications
Process Innovations For Security Vulnerability Prevention In Open Source Web Applications
// remap urls in post_content

$wpdb->query( $wpdb->prepare( "UPDATE {$wpdb->posts} SET post_content = REPLACE(post_content, '%s', '%s')", $from_url, $to_url))
// remap urls in post_content
$wpdb->replace($wpdb->posts,
    'post_content', $from_url, $to_url);
// remap urls in post_content
// @RawSQLUse, simple_code
$wpdb->query($wpdb->prepare("UPDATE {$wpdb->posts} SET post_content = REPLACE(post_content, '%s', '%s')", $from_url, $to_url))
Process Innovations For Security Vulnerability Prevention In Open Source Web Applications
Process Innovations For Security Vulnerability Prevention In Open Source Web Applications
Mambo CMS
echo T_('The current stable version is') . "<strong>" . p($server->version) . "</strong><BR />";
// @EncodeForHTML, plain
html
JavaScript
attribute
URL
CSS
Mambo CMS

// @EncodeForHTML, plain
html
JavaScript
attribute
URL
CSS

(3) annotations may help (although it's hard)
Licensing Issue
Legacy Constraint
Structural Conservatism
Fear Of Loss Of Power
Use Of Inferior Method
• Prepared Statement
• ORM
Technology Improvement Planned

ha·bá·ri
spread the news

Mambo CMS

Drupal

TYP03

zikula

Joomla!™...because open source matters
(4) concepts are useful for understanding projects’ behavior
Findings

(1) technology is mature enough
(2) architecture matters
(3) annotations may help (although it’s hard)
(4) concepts are useful for understanding projects’ behavior
(5) delayed technology use?
Thank You!
Study Issues

- annotation introduction
- generality of annotation approach
- relevance of concepts
Further Research

• annotation approach
• usefulness of annotations
• other web app vulnerabilities
• concepts
• “age” of applications