A Data-Centric Web Application Security Framework

Jonathan Burket, Patrick Mutchler, Michael Weaver, Muzzammil Zaveri, and David Evans
University of Virginia
http://guardrails.cs.virginia.edu

Web applications are easier to create than ever!

Securing web applications is not nearly as easy!

DIASPORA*
amazon.com
"<script>alert(document.cookie);</script>
**Design Goals**

**Top Priority:**
- Automatically enforce security policies

**Other Objectives:**
- Preserve application functionality
- Easy for developers to use

**Lesser Goals:**
- Minimize performance cost

**Our Philosophy**

Security policies should be attached to the data
- Security policies should be enforced automatically

**Annotated Ruby on Rails Code** → **GuardRails** → **Secure Ruby on Rails Code**
if include_subprojects && !active_children.empty?
ids = [id] + active_children.collect{|c| c.id}
conditions = ["#{Project.table_name}.id IN (#{ids.join(',')})"]
Access Control Policy Annotations

```
# @ (policy_type, [target], [handler], mediator)
# @ :read, :self, lambda{|user|self.is_public or user.memberships.include? self.id}
```

In Project model file:
```
# @ :read, lambda{|user| self.is_public or user.memberships.include? self.id}
class Project < ActiveRecord::Base
  # Project statuses
  STATUS_ACTIVE = 1..
```

Dynamic Taint Tracking

Protects against injection attacks

SQL Injection:
```
"SELECT profile FROM users WHERE username='' + user_name + ''"
Good:  user_name = "jazzFan26"
Bad:   user_name = "", DROP TABLE users--"
```

Cross-Site Scripting:
```
"User: <a href='profile_page'>" + user_name + "</a>"
Good:  user_name = "DrKevinPhillips"
Bad:   user_name = "<script language='javascript'>
        alert('document.cookie');</script>"
```
### Expressive Taint Status

```
<a href='profile?id=184392'>evil</a>SoccerFan1985</a></span>
```

**String**

<table>
<thead>
<tr>
<th>Character Index</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td><code>&lt;Transformer::Identity&gt;</code></td>
</tr>
<tr>
<td>51</td>
<td><code>&lt;Transformer::Default&gt;</code></td>
</tr>
<tr>
<td>55</td>
<td><code>&lt;Transformer::Identity&gt;</code></td>
</tr>
</tbody>
</table>

**Taint Propagation**

**Transformers**

The Default Transformer

- `<HTML => {` ("/script" => NoDisplay, :default => NoHTMLAllowed)
- `:SQL => SQLSanitize, :Ruby_eval => NoDisplay)`

**Transformer Annotations**

```
# @ taint, target, transformer
```

- `@ taint, :username`,
  `(HTML => AlphaNumericOnly)`
- `@ taint, :full_name`,
  `(HTML =>
   {TitleTag => LettersAndSpacesOnly, :default => NoHTML})`
- `@ taint, :profile`,
  `(HTML =>
   {"/script" => Invisible, :default => BoldItalicUnderlineOnly})`
Try GuardRails

Alpha Release Now Available!
Our Web Page: http://guardrails.cs.virginia.edu
Full source code can be downloaded from GitHub

Contact Info: guardrails@cs.virginia.edu
Questions?

Alpha Release Now Available!
Our Web Page: http://guardrails.cs.virginia.edu
Full source code can be downloaded from GitHub

Contact Info: guardrails@cs.virginia.edu