UNIVERSITY of VIRGINIA

GuardRails

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

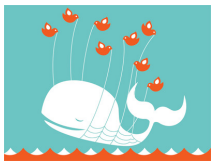
RAILS

Sinatra

Web applications are easier to create than ever!

django The web framework for ponies with magical powers.

CakePHP



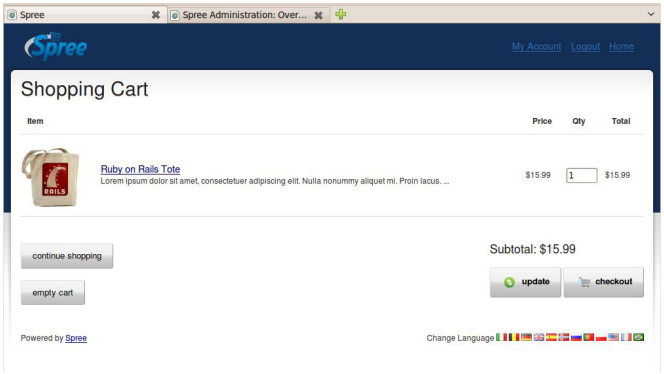
Cupidtino Beta

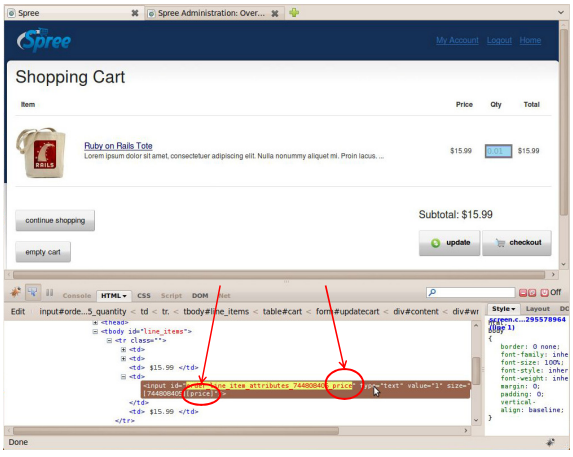
wahoo

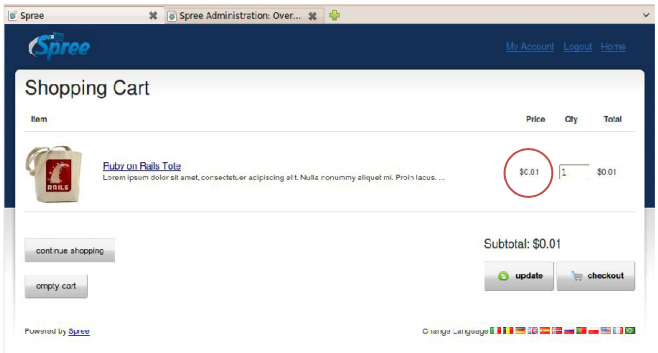
Securing web applications is not nearly as easy!

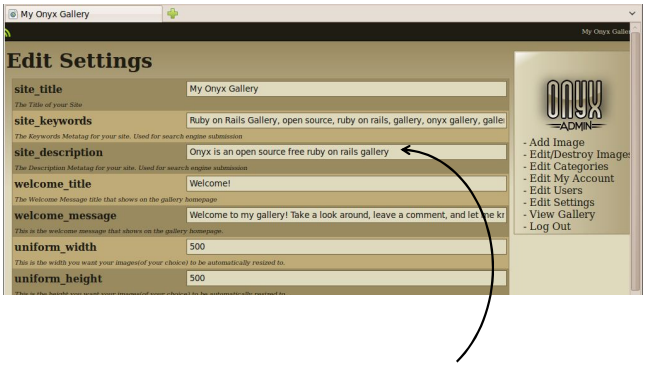
DIASPORA*

amazon.com

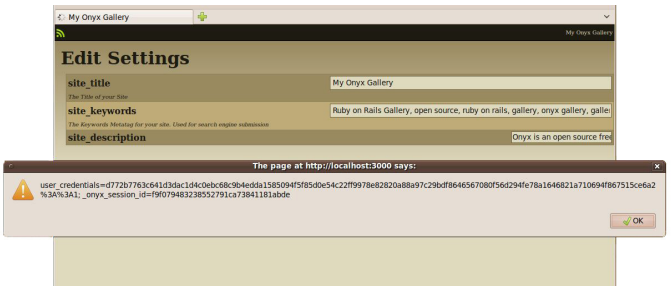


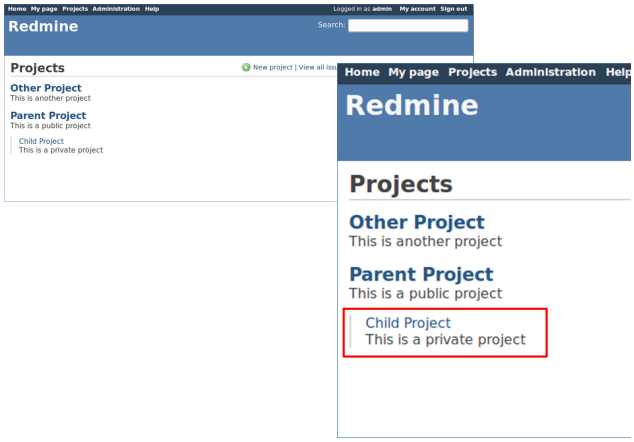


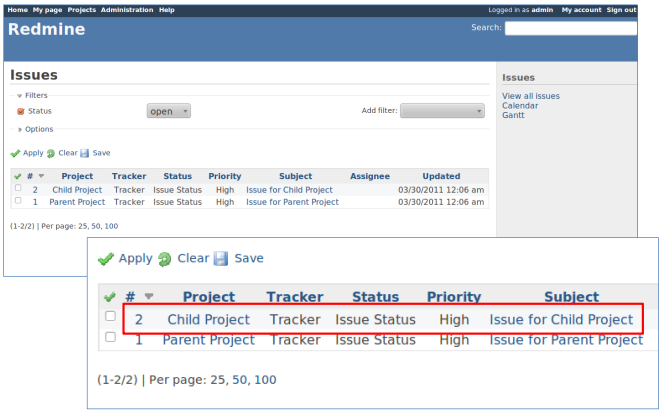


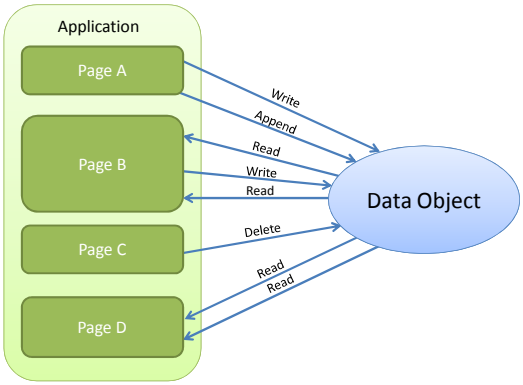


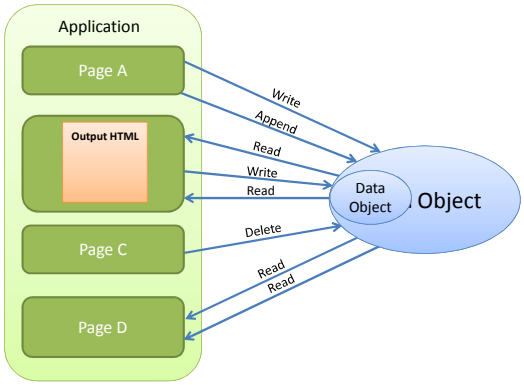
"><script>alert(document.cookie);</script>

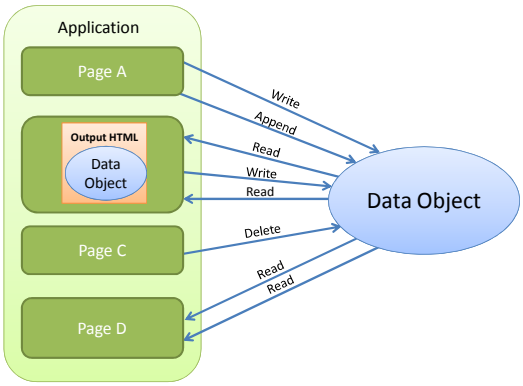


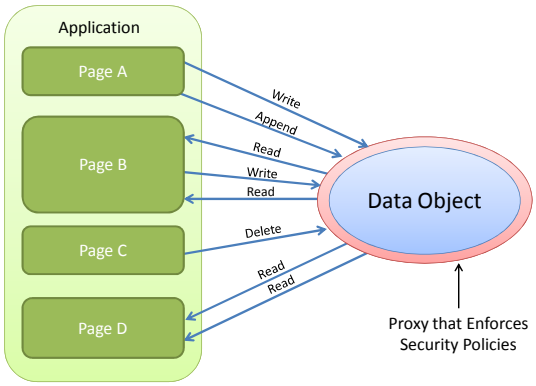


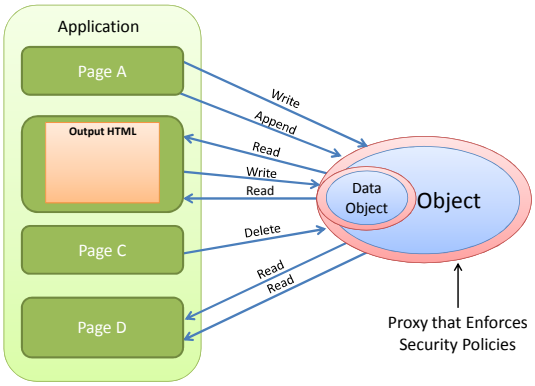








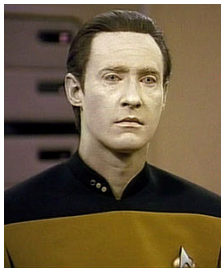


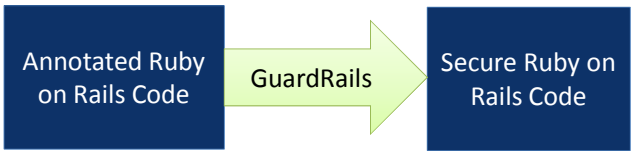


Our Philosophy

Security policies should be attached to the data

Security policies should be enforced automatically





Design Goals

Top Priority:

Automatically enforce security policies

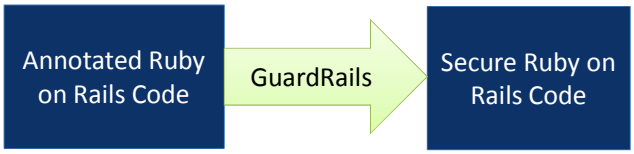
Other Objectives:

Preserve application functionality

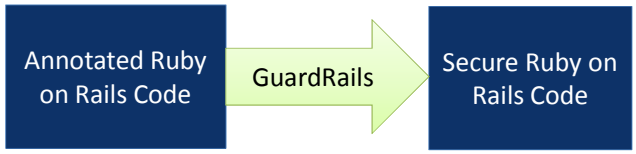
Easy for developers to use

Lesser Goals:

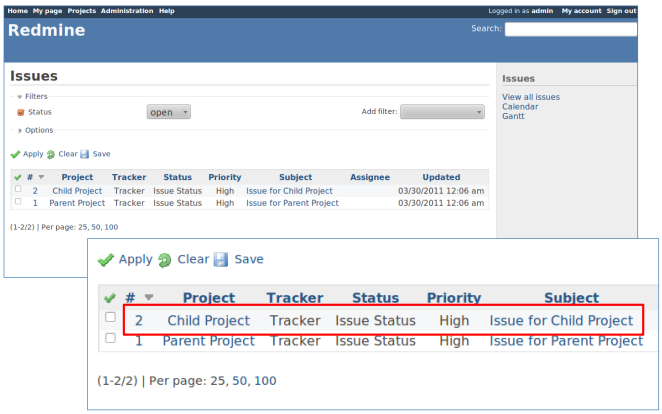
Minimize performance cost



Access Control Policies
Fine Grained Taint-Tracking



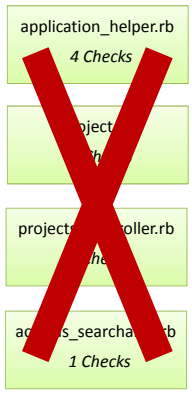
Access Control Policies
Fine Grained Taint-Tracking




```
if include_subprojects && !active_children.empty?
      ids = [id] + active_children.collect {|c| c.id}

      conditions = ["#{Project.table_name}.id IN
            (#{ids.join(',')})"]
```


```
if include_subprojects && !active_children.empty?
      ids = [id] + active_children.collect {|c| c.id}

      conditions = ["#{Project.table_name}.id IN
            (#{ids.join(',')})"]
```


```
if include_subprojects && !active_children.empty?
      ids = [id] + active_children.collect {|c| c.id}

      conditions = ["#{Project.table_name}.id IN
            (#{ids.join(',')}) AND
            #{Project.visible_by}"]
```



1 GuardRails Annotation

```
# @ :read, :self,
lambda{|user|self.is_public
or user.memberships.include? self.id}
```

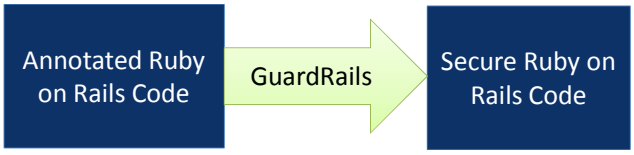
In *Project* model file:

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


Access Control Policy Annotations

 # @ (policy_type, [target], [handler], mediator)

```
# @ :delete, :self, :admin

# @ :write, :password, lambda{|user|user.id == self.id }

# @ :append, :members, lambda{|user| user.belongs_to?(self)}
```

Access Control Policies
Fine Grained Taint-Tracking

Dynamic Taint Tracking

Protects against *injection attacks*

SQL Injection:

```
"SELECT profile FROM users WHERE username='" + user_name + "'"
```

Good: user_name = "jazzFan26"

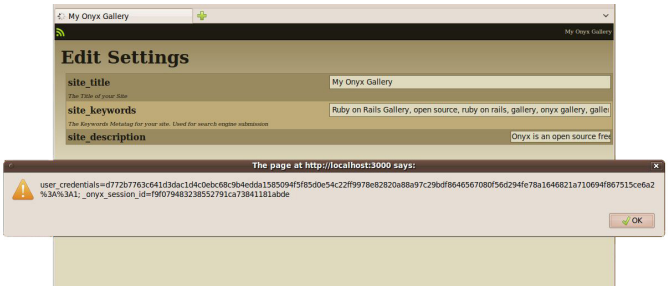
Bad: user_name = "'; DROP TABLE users--"

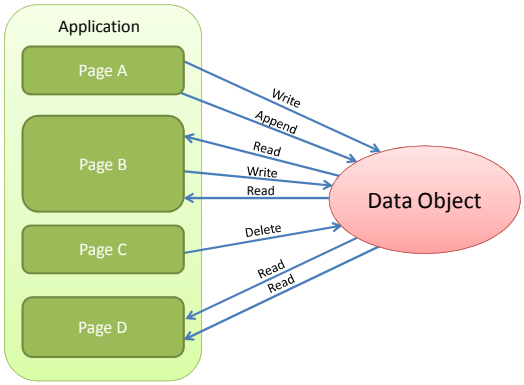
Cross-Site Scripting:

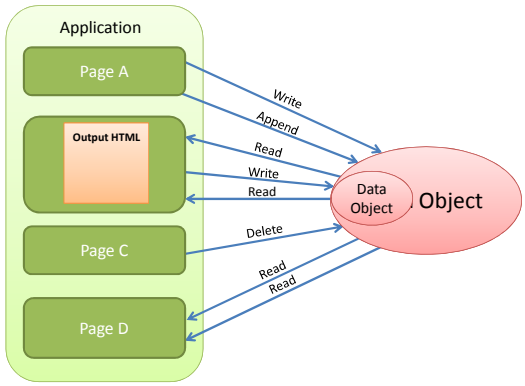
```
"User: <a href='profile_page'>" + user_name + "</a>"
```

Good: user_name = "DrKevinPhillips"

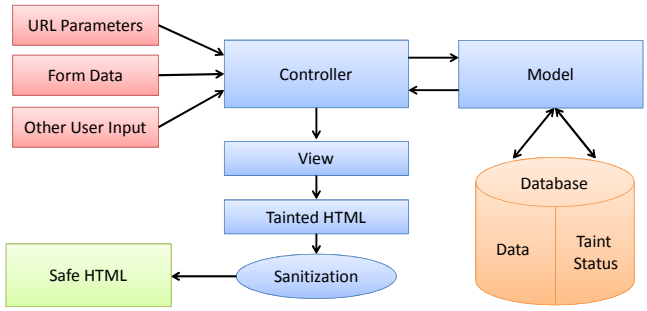
Bad: user_name = "<script language='javascript'>
alert('document.cookie');</script>"







Taint Propagation



Expressive Taint Status

"<evil>SoccerFan1985</evil>"

String

Value:

"<evil>SoccerFan1985</evil>"

Taint:

29	<Transformer::Identity>	Different *Chunks*
51	<Transformer::Default>	
55	<Transformer::Identity>	

Character Index

Transformers

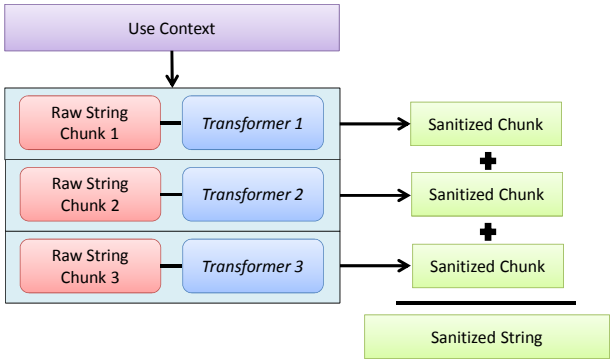
Use Context

The Default Transformer

{:**HTML** => {
"//script" => NoDisplay,
:**default** => NoHTMLAllowed
},
:**SQL** => SQLSanitize,
:**Ruby_eval** => NoDisplay}

Appropriate Sanitization Routine

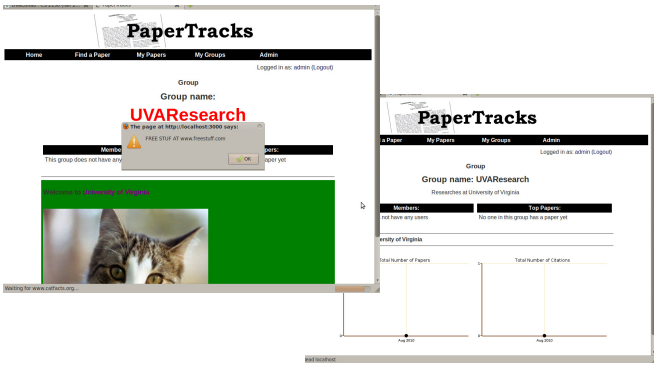
Transformers

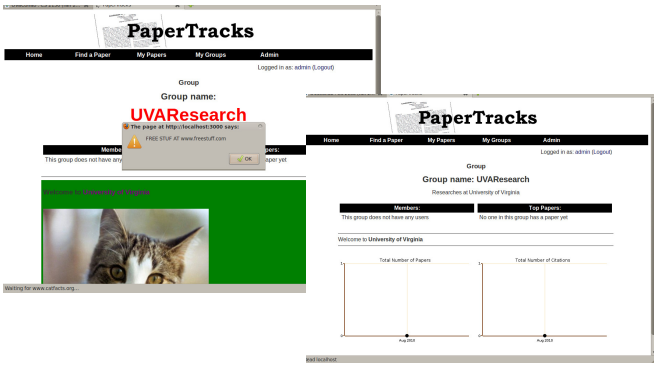


Transformer Annotations

 # @ taint, target, transformer

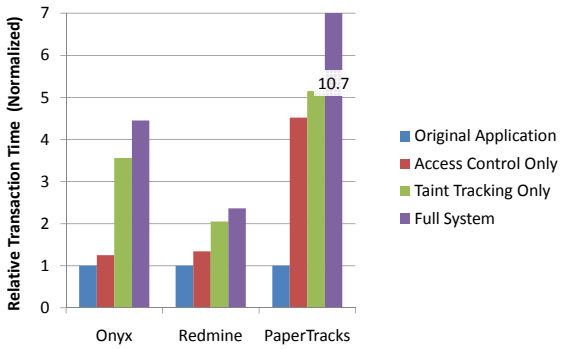
```
# @ :taint, :username,
    {:HTML => AlphaNumericOnly}

# @ :taint, :full_name,
    {:HTML =>
        {TitleTag => LettersAndSpacesOnly,
        :default => NoHTML}}

# @ :taint, :profile,
    {:HTML =>
        {"//script" => Invisible,
        :default  => BoldItalicUnderlineOnly}}
```





Test Application	Application Type
Onyx Image Gallery	Image Gallery (680 lines)
Substruct	E-Commerce (5556 lines)
RedMine	Project Management (30747 lines)
spree	E-Commerce (11561 lines)

Performance Notes



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