GuardRails

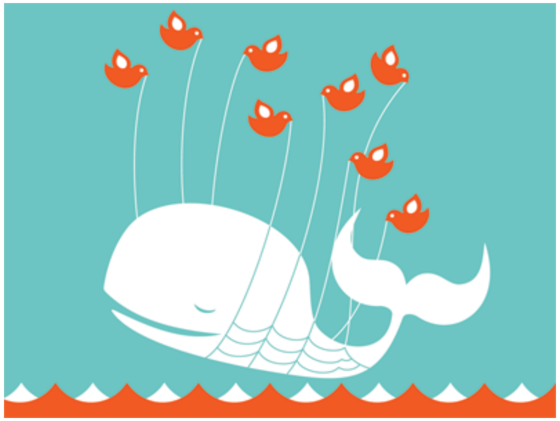
A (Nearly) Painless Solution to Web Application Security

Jonathan Burket, Patrick Mutchler, Michael Weaver, Muzzammil Zaveri

University of Virginia
http://guardrails.cs.virginia.edu

So What?

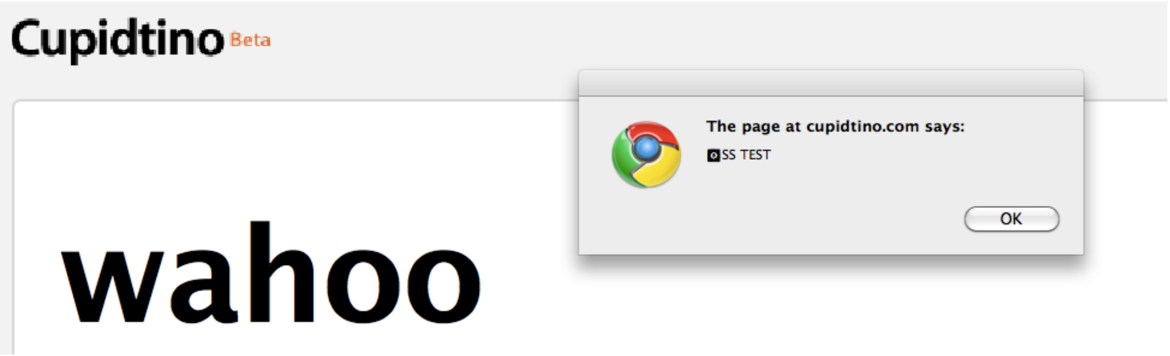
Web applications are easy to create!



BUT.....

amazon.com

Web security is not easy!



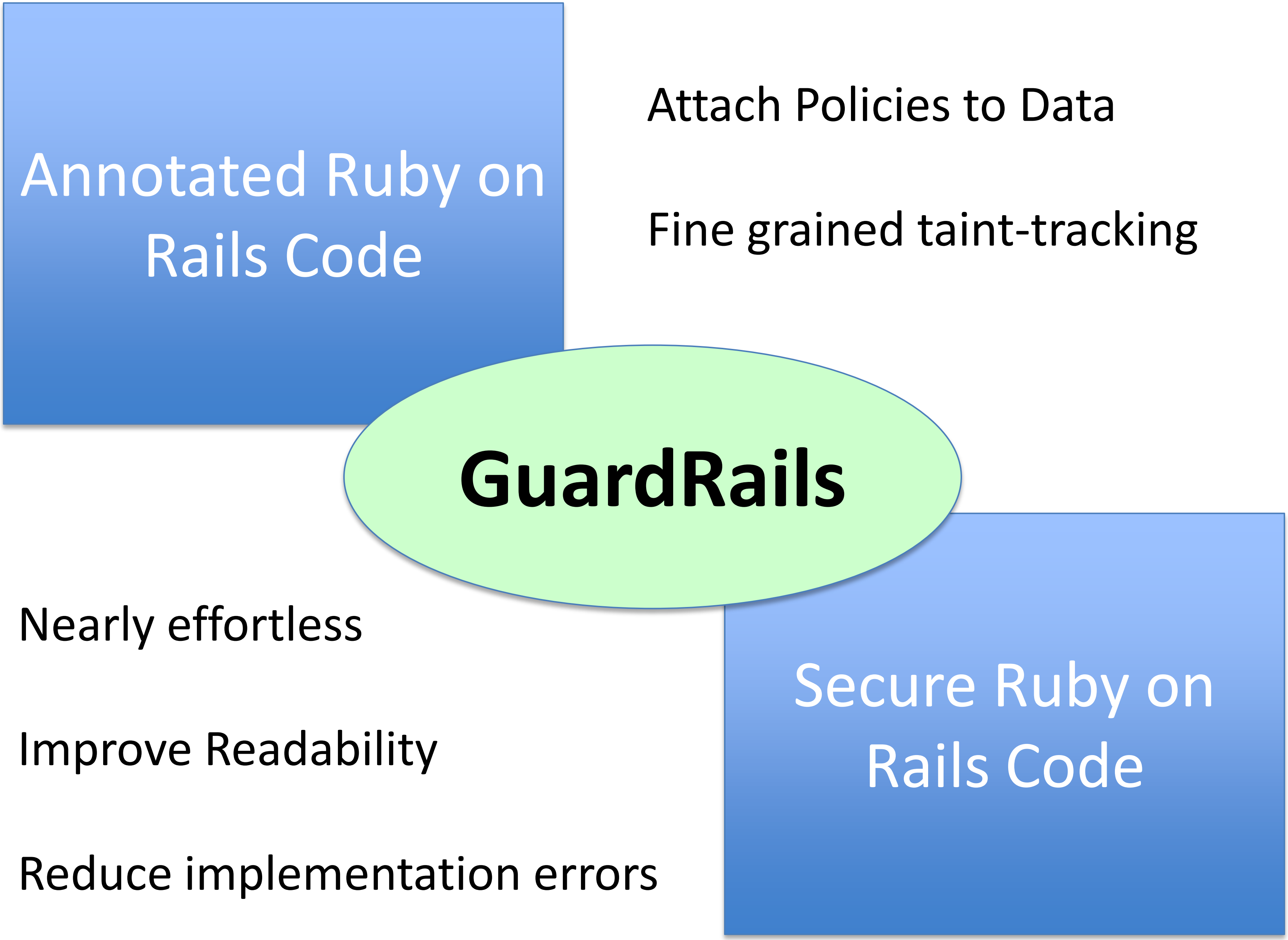
Cupidtino Beta

The page at cupidtino.com says:

SS TEST

wahoo

DIASPORA*



Annotated Ruby on Rails Code

Attach Policies to Data

Fine grained taint-tracking

GuardRails

Nearly effortless

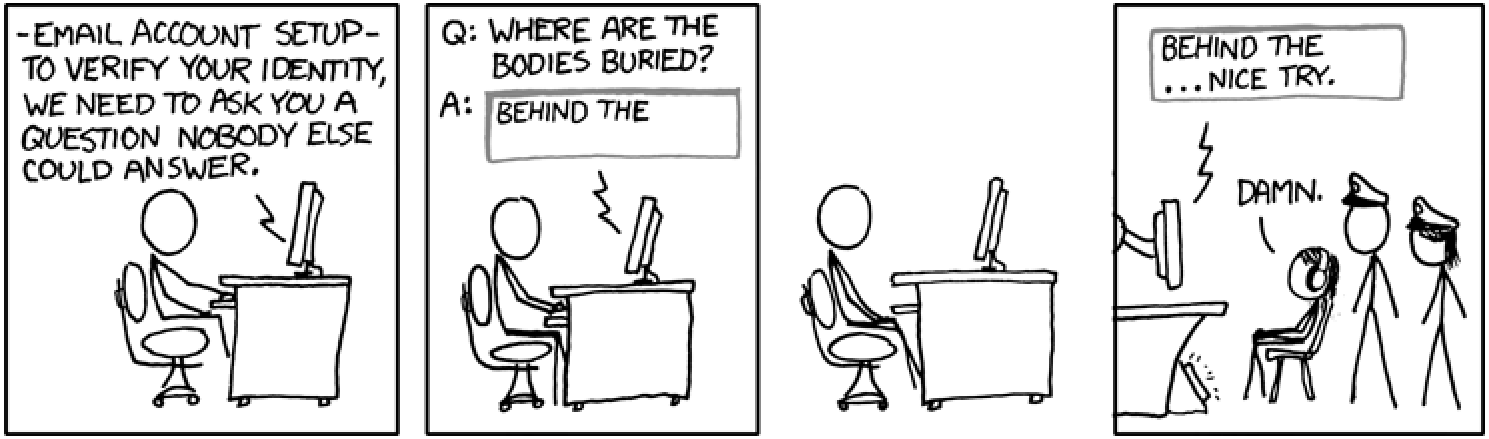
Improve Readability

Reduce implementation errors

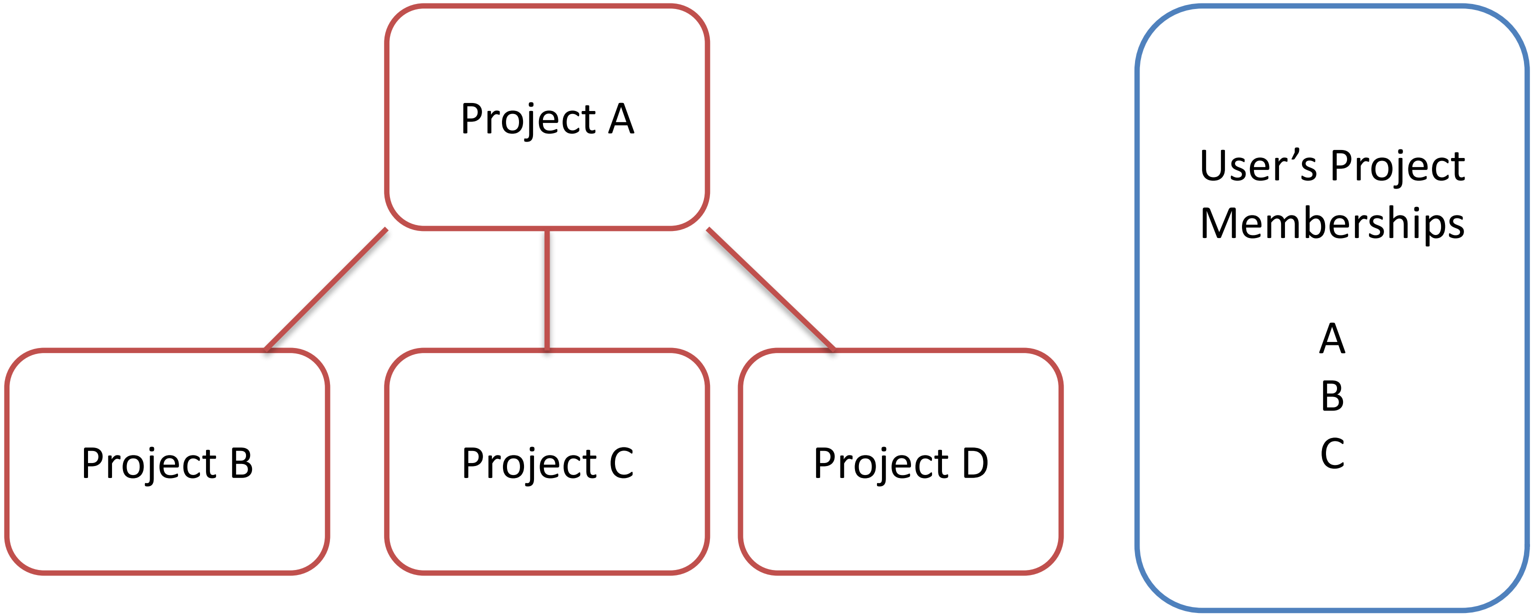
Secure Ruby on Rails Code

Access Control Policies

Patrick Mutchler


-EMAIL ACCOUNT SETUP-
TO VERIFY YOUR IDENTITY, WE NEED TO ASK YOU A QUESTION NOBODY ELSE COULD ANSWER.
Q: WHERE ARE THE BODIES BURIED?
A: BEHIND THE
BEHIND THE
...NICE TRY.
DAMN.

An Example



Project A

Project B

Project C

Project D

User’s Project Memberships

A
B
C

Access Control is Annoying and Tedious

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

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

RedMine

Access Control is Annoying and Tedious

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

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

RedMine

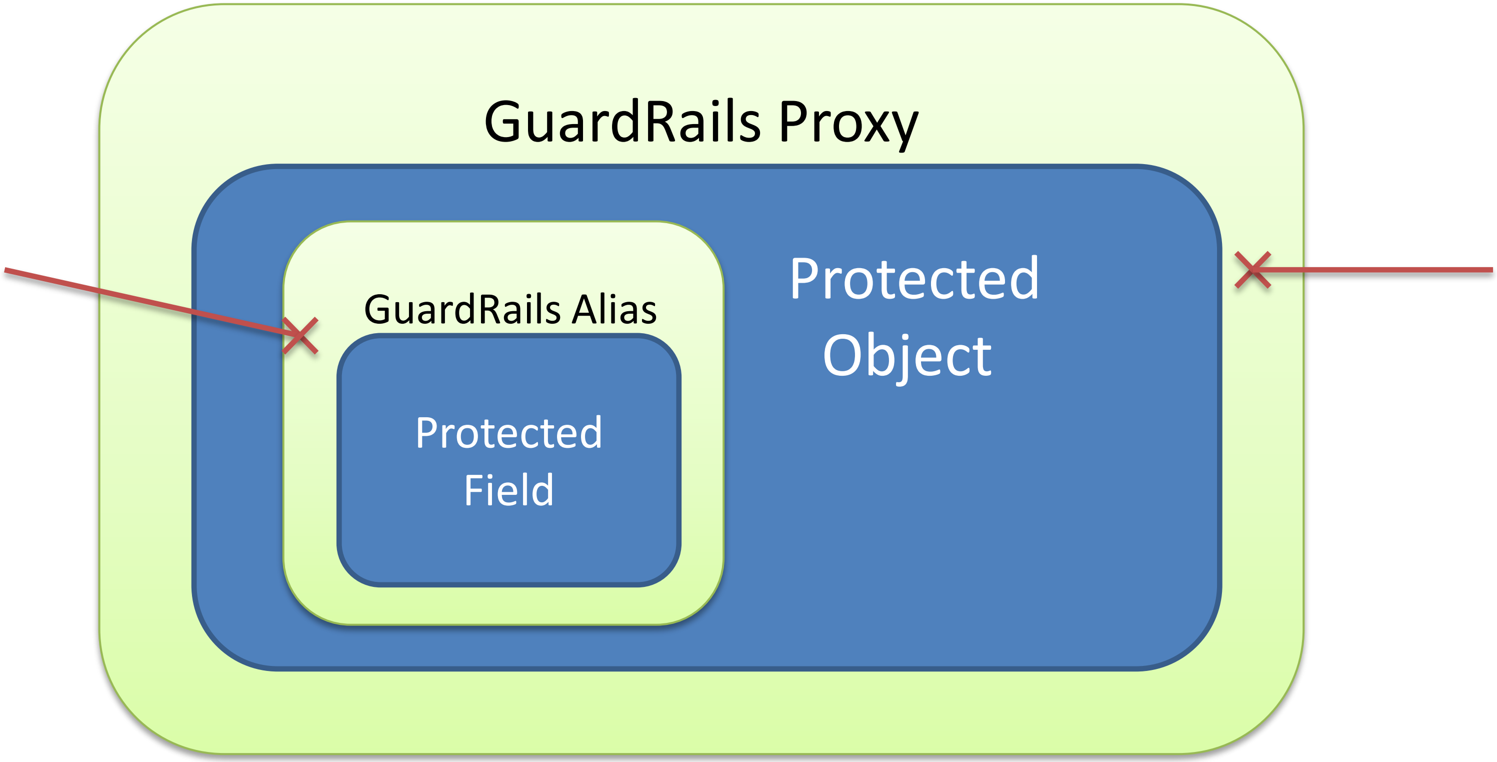
Access Control is Annoying and Tedious

```
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}"]
```

RedMine

Object Oriented Policy Enforcement



Access Control Policies

Read

```
User.find(..)
```

Write

```
@usr.secret= x
```

Append

```
addToMailingList(@usr)
```

Create

```
User.create
```

Delete

```
@usr.destroy
```

Access Control Policy Annotations

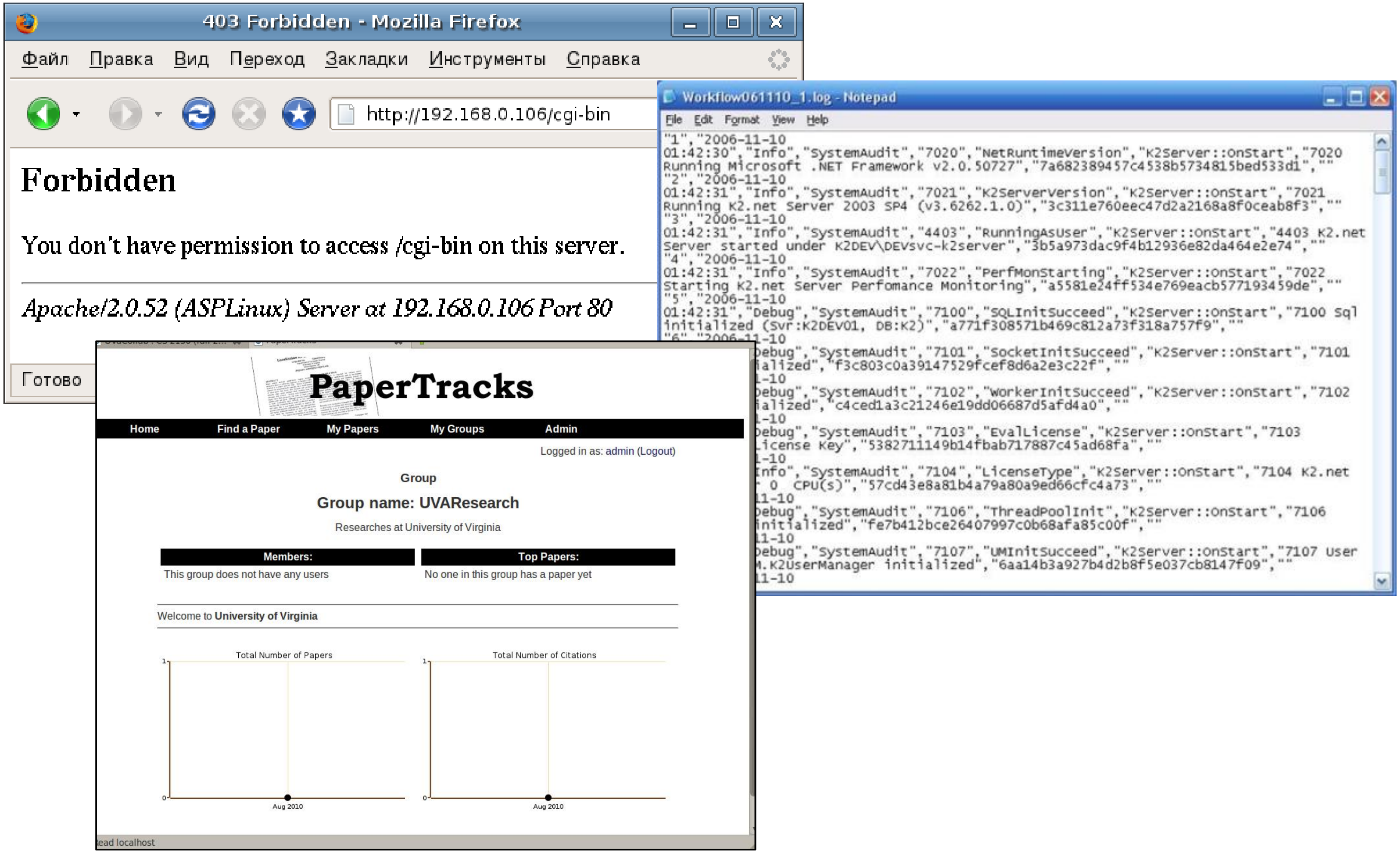
```
# @ (policy_class, targets, expression)
```

```
# @ delete access, :admin

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

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

Policy Violations


403 Forbidden - Mozilla Firefox
Файл Правка Вид Переход Закладки Инструменты Справка
http://192.168.0.106/cgi-bin
Готово

Forbidden

You don't have permission to access /cgi-bin on this server.

Apache/2.0.52 (ASPLinux) Server at 192.168.0.106 Port 80

Workflow061110_1.log - Notepad
File Edit Format View Help

```
"1","2006-11-10
01:42:30","Info","SystemAudit","7020","NetRuntimeVersion","K2Server::OnStart","7020
Running Microsoft .NET Framework v2.0.50727","7a682389457c4538b5734815bed533d1",""
"2","2006-11-10
01:42:31","Info","SystemAudit","7021","K2ServerVersion","K2Server::OnStart","7021
Running K2.net Server 2003 SP4 (v3.6262.1.0)","3c311e760eec47d2a2168a8f0ceab8f3",""
"3","2006-11-10
01:42:31","Info","SystemAudit","4403","RunningAsUser","K2Server::OnStart","4403 K2.net
Server started under K2DEV\DEVsvc-k2server","3b5a973dac9f4b12936e82da464e2e74",""
"4","2006-11-10
01:42:31","Info","SystemAudit","7022","PerfMonStarting","K2Server::OnStart","7022
Starting K2.net Server Perfomance Monitoring","a5581e24ff534e769eacb577193459de",""
"5","2006-11-10
01:42:31","Debug","SystemAudit","7100","SQLInitSucceed","K2Server::OnStart","7100 Sql
initialized (Svr:K2DEV01, DB:K2)","a771f308571b469c812a73f318a757f9",""
"6","2006-11-10
Debug","SystemAudit","7101","SocketInitSucceed","K2Server::OnStart","7101
ialized","f3c803c0a39147529fcef8d6a2e3c22f",""
1-10
Debug","SystemAudit","7102","WorkerInitSucceed","K2Server::OnStart","7102
ialized","c4ced1a3c21246e19dd06687d5afd4a0",""
1-10
Debug","SystemAudit","7103","EvalLicense","K2Server::OnStart","7103
License Key","5382711149b14fbab717887c45ad68fa",""
1-10
Info","SystemAudit","7104","LicenseType","K2Server::OnStart","7104 K2.net
r 0  CPU(s)","57cd43e8a81b4a79a80a9ed66cfc4a73",""
11-10
Debug","SystemAudit","7106","ThreadPoolInit","K2Server::OnStart","7106
initialized","fe7b412bce26407997c0b68afa85c00f",""
11-10
Debug","SystemAudit","7107","UMInitSucceed","K2Server::OnStart","7107 User
M.K2UserManager initialized","6aa14b3a927b4d2b8f5e037cb8147f09",""
11-10
```

Logged in as: admin (Logout)

Group

Group name: UVAResearch

Researches at University of Virginia

Members:	Top Papers:
This group does not have any users	No one in this group has a paper yet

Welcome to **University of Virginia**

Data Policy Example

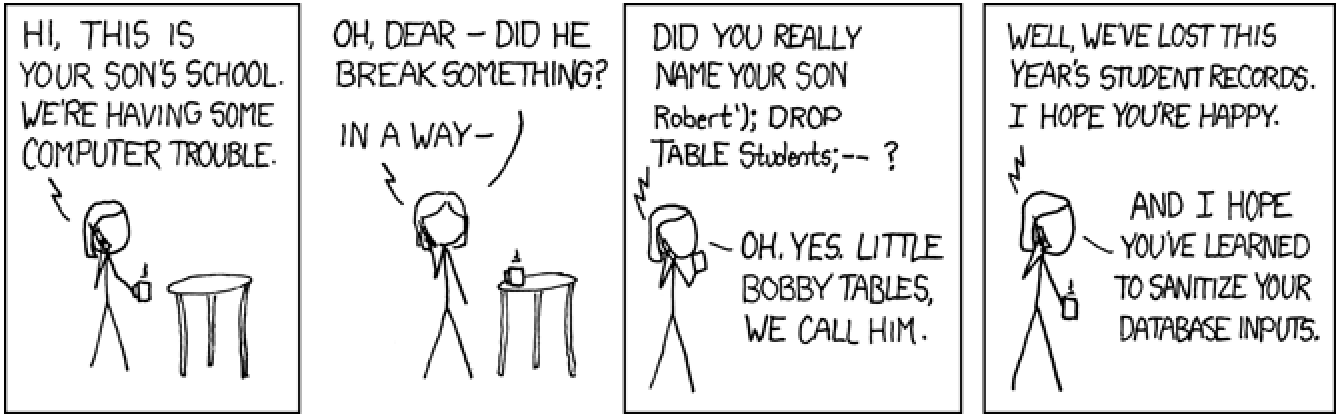
```
def require_user
    unless current_user
    self.notice = I18n.t("page_only_viewable_when_logged_in")
    redirect_to new_user_session_url
    return false
end end

def require_no_user
    if current_user
    self.notice = I18n.t("page_only_viewable_when_logged_out")
    redirect_to root_url
    return false
end end

def store_location # disallow return to login, logout, signup pages
    disallowed_urls = [signup_url, login_url, logout_url]
    ..
```

Dynamic Taint Tracking

Jonathan Burket


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.

xkcd.com

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:

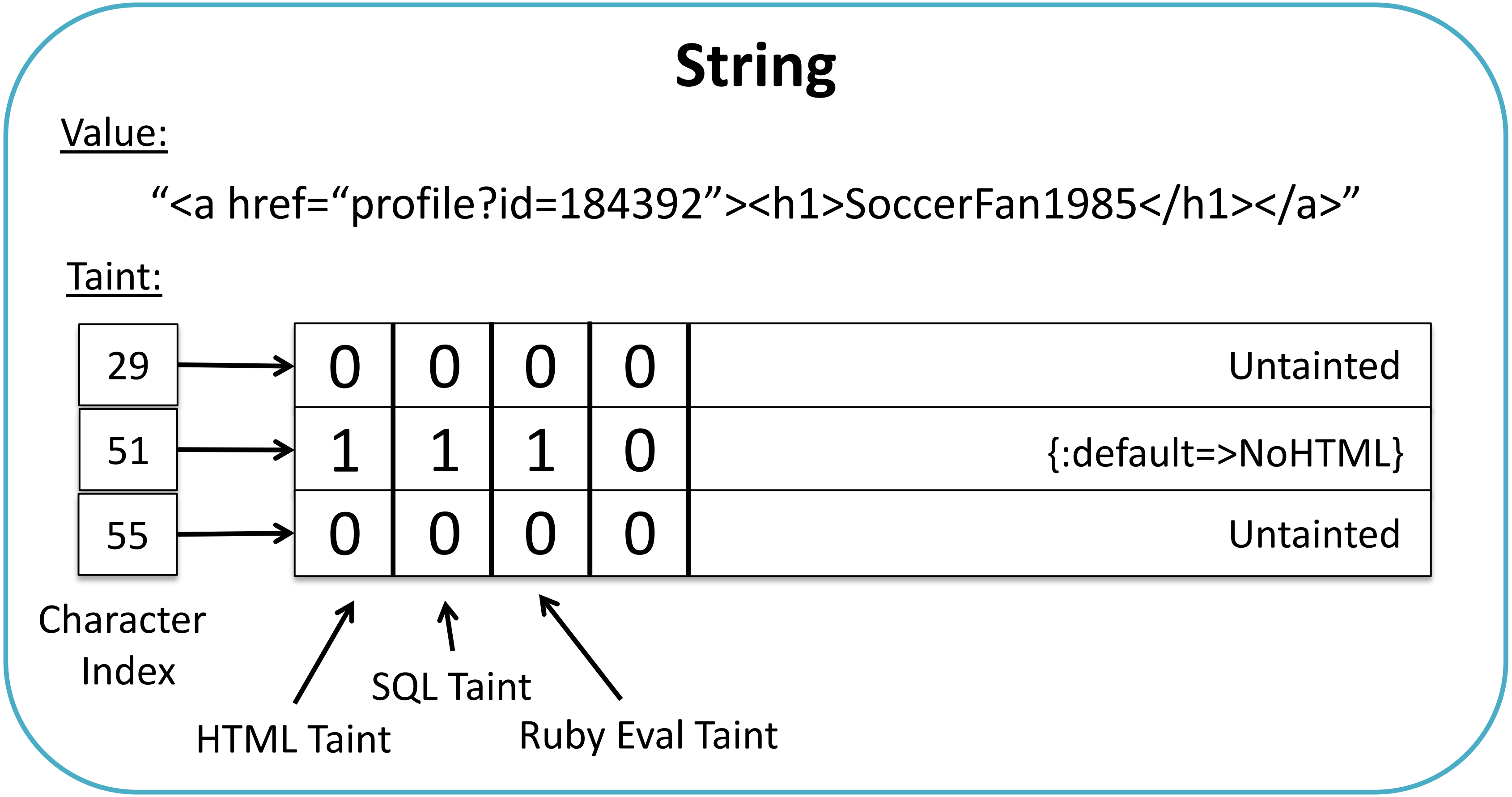
“User: <a href=‘profile_page’>” + user_name + “</a>”

Good: user_name = “DrKevinPhillips”

Bad: user_name = “<script language=‘javascript’>
alert(‘document.cookie’);</script>”

Expressive Taint Status

“<a href=“profile?id=184392”><h1>SoccerFan1985</h1></a>”



String

Value:

“<a href=“profile?id=184392”><h1>SoccerFan1985</h1></a>”

Taint:

29	0	0	0	0	Untainted
51	1	1	1	0	{:default=>NoHTML}
55	0	0	0	0	Untainted

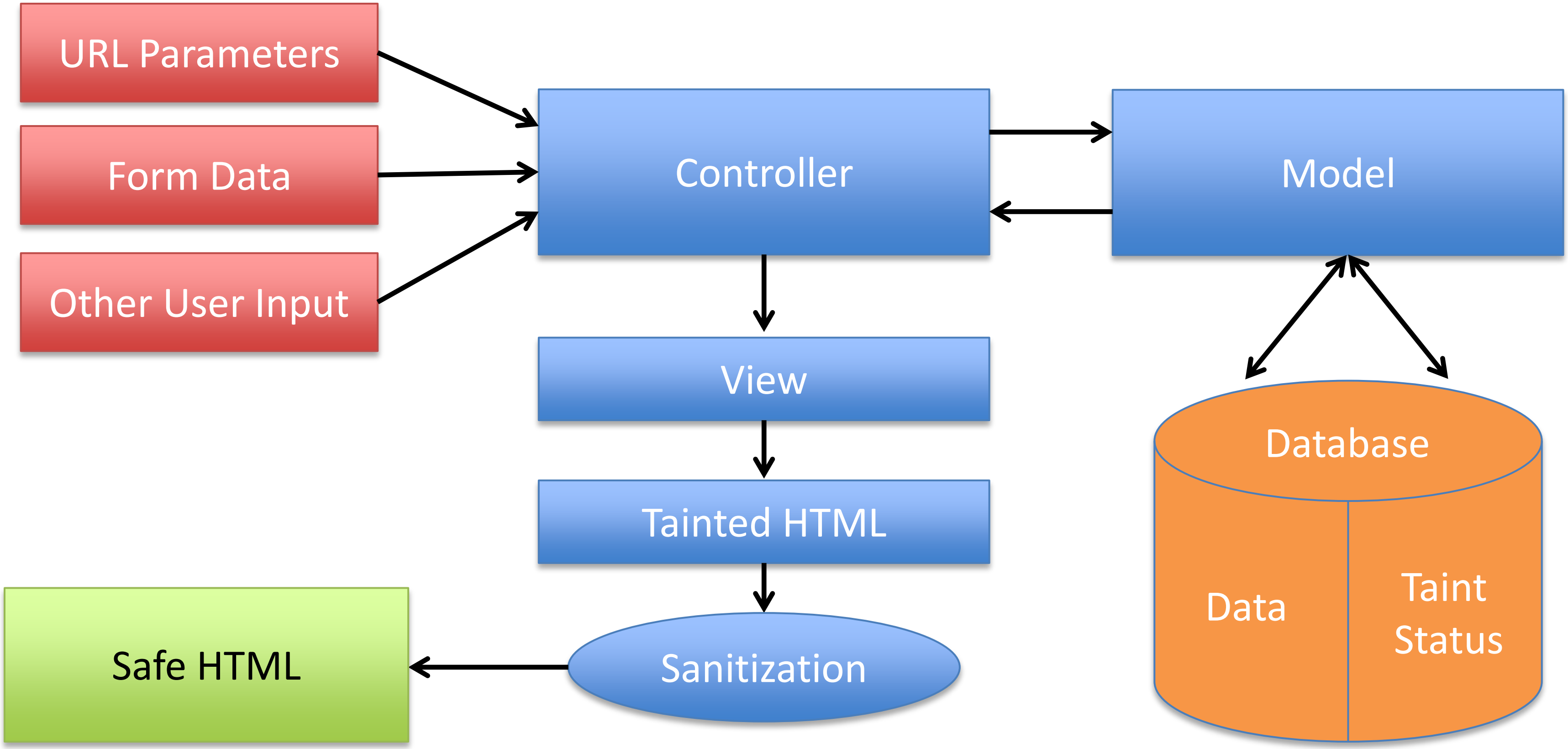
Character Index

HTML Taint

SQL Taint

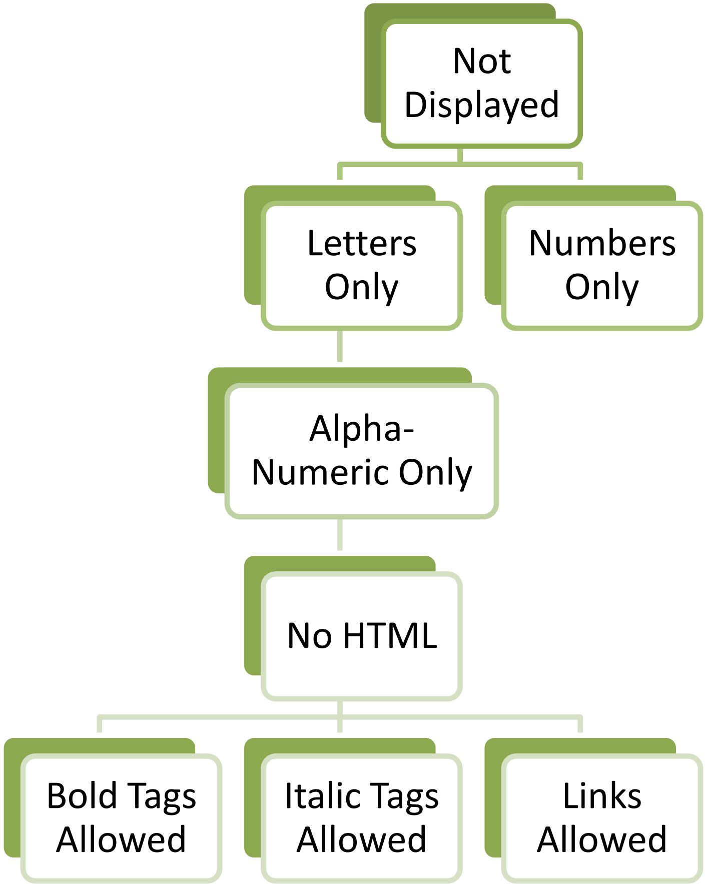
Ruby Eval Taint

Taint Propagation



“**foo**” + “bar” → “**foo**bar”

Taint Lattice



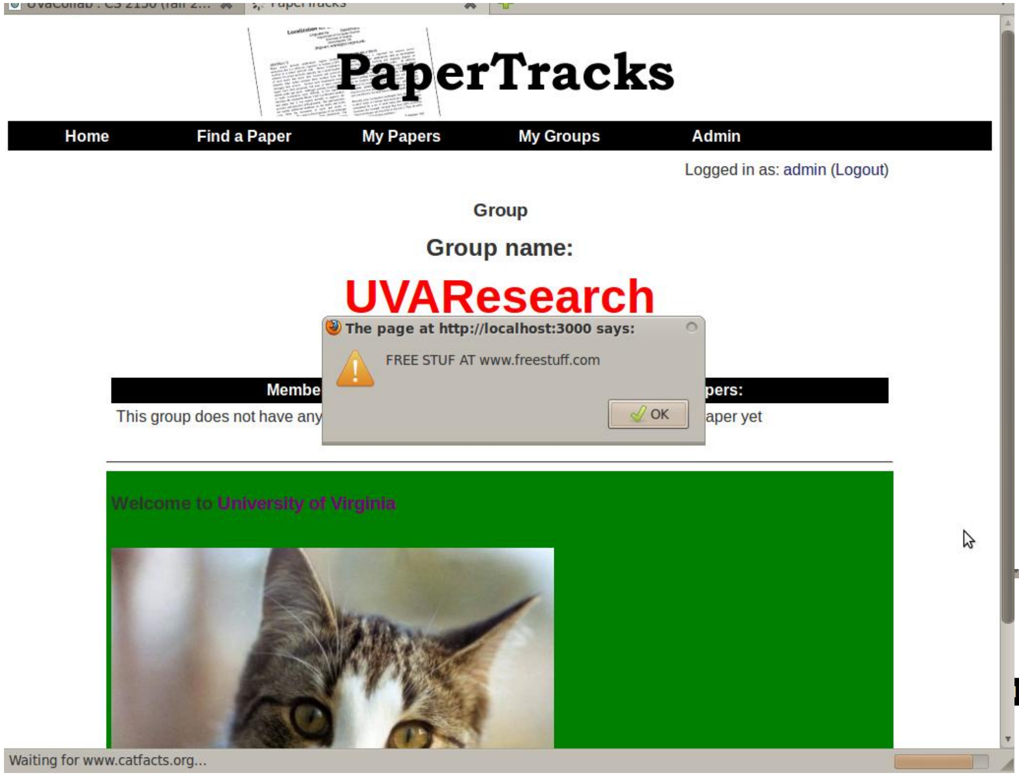
- Combination of taint statuses
- Extendable by developers
- Subtyping

Context-Appropriate Sanitization

```
# @ taint, username, AlphaNumeric


# @ taint, full_name, NoHTML,
        TitleTag: LettersAndSpaces


# @ taint, profile, BoldItalicUnderline,
        "//script[@language='javascript']": Invisible
```



PaperTracks

Logged in as: admin (Logout)

Group

Group name:

UVAResearch

The page at http://localhost:3000 says:

FREE STUF AT www.freestuff.com

Membe

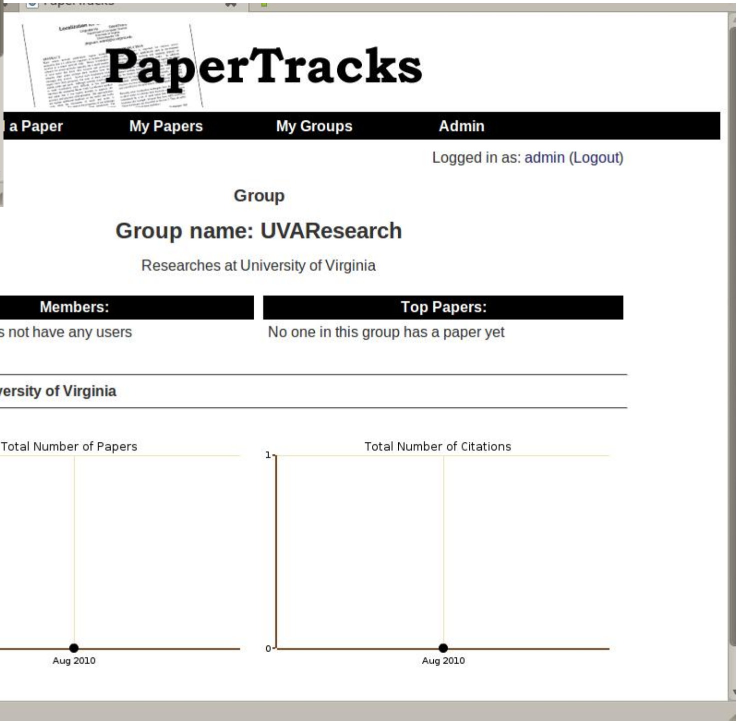
pers:

This group does not have any

aper yet

Welcome to University of Virginia

Waiting for www.catfacts.org...



PaperTracks

Logged in as: admin (Logout)

Group

Group name: UVAResearch

Researches at University of Virginia

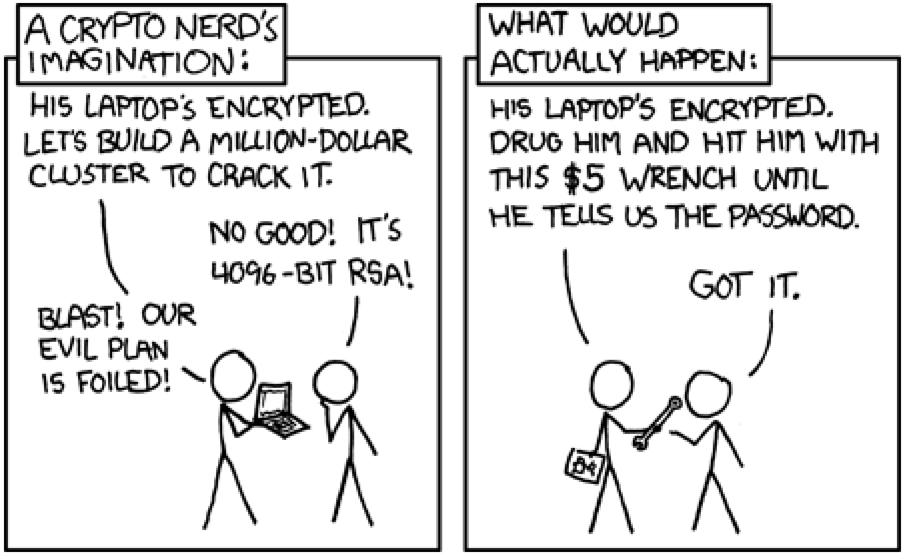
Members:	Top Papers:
This group does not have any users	No one in this group has a paper yet

Welcome to **University of Virginia**

ead localhost

Demo and Early Results

Michael Weaver


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Other real-word examples

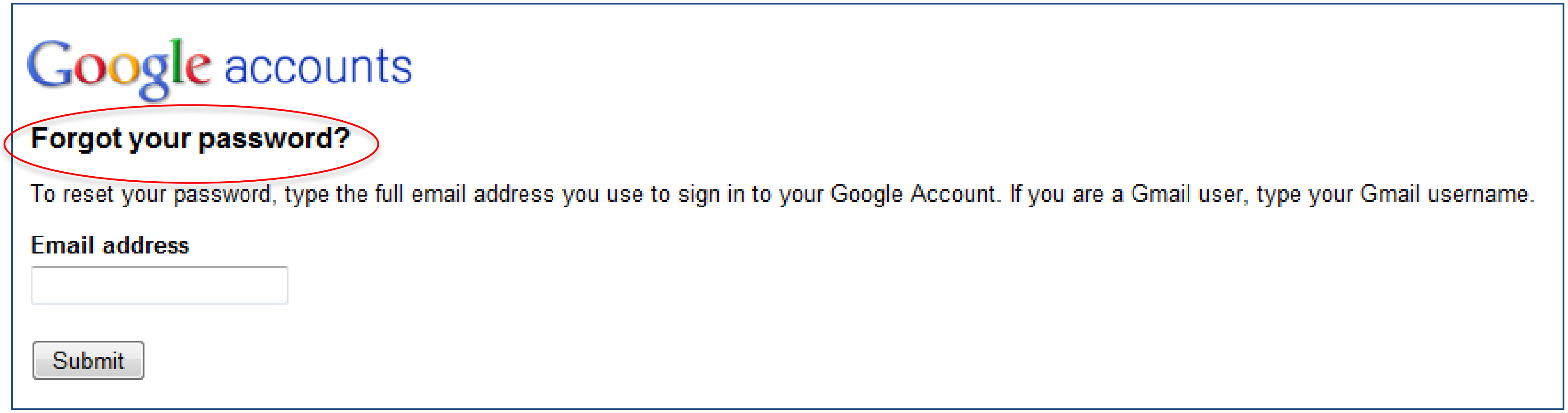
Looking to Try Out GuardRails?

- Our Contact Info: guardrails@cs.virginia.edu
- WebPage: http://guardrails.cs.virginia.edu

Questions?

Access Control Policies

Context-Dependent Policies



Google accounts

Forgot your password?

To reset your password, type the full email address you use to sign in to your Google Account. If you are a Gmail user, type your Gmail username.

Privileged Functions