UNIVERSITÄT PASSAU

Institute of IT-Security and Security Law

WebSand

# A Doorman for Your Home – Control-Flow Integrity Means in Web Frameworks

**Bastian Braun**

**bb@sec.uni-passau.de**

***joint work with Christian v. Pollak***

**OWASP AppSec EU 2013, 22/08/13**

# Background

- A web application is a reactive system
  - reacts on incoming requests
  - reaction includes response + possibly change of data
  - a sequence of (action,reaction) pairs is a control flow
- Examples
  - booking & payment
    - eCommerce (ebay, amazon), banking, flights, railway tickets
  - configuration
    - registering, (re)set password
  - several domains involved
    - payments via Paypal

# Background

- **Web applications require step-by-step operation**
  - **Assumption: users start only at entry page & only click on hyperlinks and buttons**
- **Steps happen by processing HTTP requests**
  - **http://www.example.de/users.php?action=add &name=doe&firstname=john**
- **Factors: method, HTTP parameters, *past steps***
- **Control flow = sequence of requests (i.e., steps) in the same user context**

Mozilla Firefox Startseite - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.google.de/firefox?client=firefox-a&rls=org.mozilla:de:off

Google

Erste Schritte Aktuelle Nachrichten

# Firefox Start

Google™ Web Bilder Groups News

Erweiterte Suche
Einstellungen

Suche: Das Web Seiten auf Deutsch Seiten aus Deutschland

Google-Suche

Über 100 Suchmaschinen können in die Firefox-Suchleiste integriert werden, für den schnellen Zugriff auf Ihre Lieblingssuchmaschinen.

Firefox Hilfe und Erweiterungen Über Mozilla CDs & Merchandise Unterstützen Sie Mozilla

Fertig

Mozilla Firefox Startseite - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.example.de/shopping.php?show=cart

Erste Schritte Aktuelle Nachrichten

amazon

Your Amazon.com | Today's Deals | Gift Cards | Help

FREE Two-Day Shipping
Join Amazon Prime Today

Shop by Department

Search All Go

Hello. Sign in
Your Account

1 Cart

Wish List

Get up to a $75 Amazon.com Gift Card
when you get a new credit card
by applying from Amazon.com Learn more

Add $12.01 of eligible items to your order to qualify for FREE Super Saver Shipping. See details

Subtotal (1 item): $12.99

This order contains a gift

Proceed to Checkout

or

Sign in to turn on 1-Click ordering.

## Shopping Cart

Items to buy now

| | Price | Quantity |
|---|---|---|
| The Ultimate Hitchhiker's Guide to the Galaxy - Douglas Adams; Paperback<br>In Stock<br>Eligible for FREE Super Saver Shipping<br>This will be a gift (Learn more)<br>Delete · Save for later | $12.99<br>You save:<br>$7.01 ( 35%) | 1 |

Subtotal: $12.99

Customers Who Bought The Ultimate Hitchhiker's Guide... Also Bought

The Restaurant at the End of the...
› Douglas Adams
(146)

Mozilla Firefox Startseite - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.example.de/shopping.php?action=login

Erste Schritte Aktuelle Nachrichten

amazon.com

SIGN IN SHIPPING & PAYMENT GIFT-WRAP PLACE ORDER

## Sign In

**Enter your e-mail address:**

**I am a new customer.**
(You'll create a password later)

**I am a returning customer, and my password is:**

Sign in using our secure server

Forgot your password? Click here

Has your e-mail address changed since your last order?

Mozilla Firefox Startseite - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.example.de/shopping.php?action=shipping

Erste Schritte Aktuelle Nachrichten

amazon.com

SIGN IN SHIPPING & PAYMENT GIFT-WRAP PLACE ORDER

## Choose your shipping options

**Shipping Details** (Learn more)

**Choose a shipping speed:**

- (●) Standard International Shipping (averages 18-32 business days)
- ( ) AmazonGlobal Expedited Shipping (averages 8-14 business days)
- ( ) AmazonGlobal Priority Shipping (averages 2-4 days)

**Item:** Need to Change quantities or delete?

**Shipping to:** Bastian Braun, Universitaet Passau, Innstr. 43, Passau, Bayern, 94032 Germany

- **The Ultimate Hitchhiker's Guide to the Galaxy** - Douglas Adams
  $12.99 - Quantity: 1
  Condition: New
  Sold by: Amazon.com LLC

**Does your order contain gift items?**

[ ] Ordering a gift? Check this box to see gift options before checkout.

Continue

Mozilla Firefox Startseite - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.example.de/shopping.php?action=payment

amazon.com

SIGN IN SHIPPING & PAYMENT GIFT-WRAP PLACE ORDER

How would you like to pay?

http://www.example.de/shopping.php?action=confirmation

Your credit and debit cards | Name on card | Expires on

MasterCard ending in | Bastian Braun

Continue

(You can review this order before it's final.)

More payment options

Credit or Debit Cards

Amazon.com accepts all major credit and debit cards.

Add a new card

http://www.example.de/shopping.php?action=check_payment

Gift Cards & Promotional Codes

Apply

Enter a gift card or promotional claim code.

Amazon.com Store Card

Access to exclusive financing offers. No annual fee. Zero fraud liability. Learn more »

Apply now

Mozilla Firefox Startseite - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.example.de/shopping.php?action=confirmation

Erste Schritte Aktuelle Nachrichten

amazon.com

SIGN IN SHIPPING & PAYMENT GIFT-WRAP PLACE ORDER

## Review Your Order

By placing your order, you agree to Amazon.com's privacy notice and conditions of use

**Important message**

Check this box to default to these delivery and payment options in the future.

**Shipping Address:**
Bastian Braun
Universitaet Passau
Innstr. 43
Passau, Bayern 94032
Germany
Phone: +491796494588 Change

**Billing Information:**

**Gift Cards & Promotional Codes:**

Apply

Place your order in EUR

**Order Summary**

Amazon Currency Converter is **Enabled.** (Learn More)

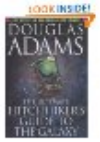
| | |
|---|---|
| Items: | EUR 10,51 |
| Shipping & Handling: | EUR 6,45 |
| Total Before Tax: | EUR 16,96 |
| Estimated Tax To Be Collected: | EUR 0,00 |

**Order Total: EUR 16,96**

Switch currency

See Exchange Rate

**Estimated delivery: Oct. 26, 2012 - Nov. 16, 2012**




**The Ultimate Hitchhiker's Guide to the Galaxy**
by Douglas Adams
$12.99
**Quantity:** 1 Change
Sold by: Amazon.com LLC
Add gift options

**Choose a shipping speed:**

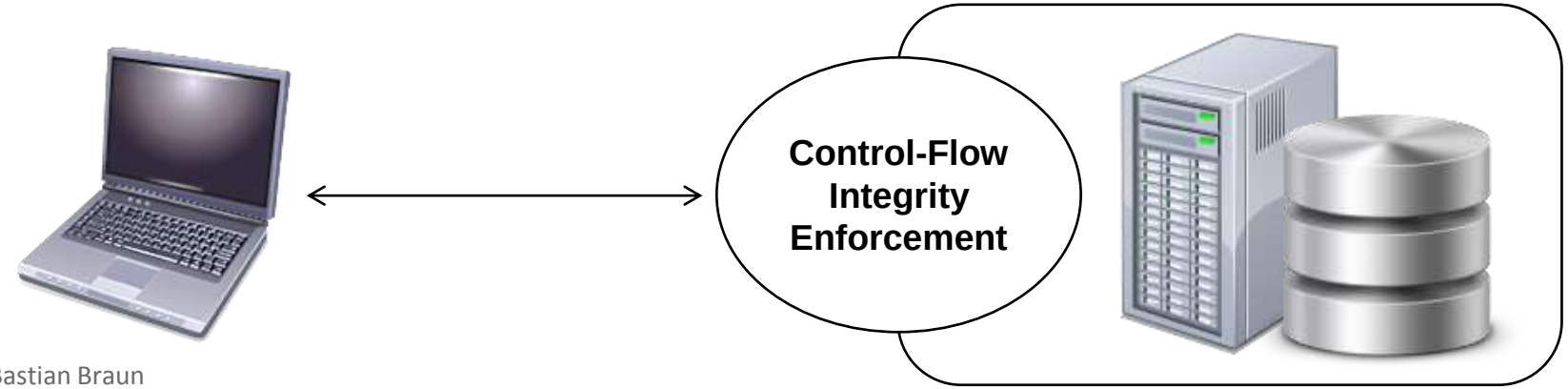
- (●) Standard International Shipping (averages 18-32 business days)
- ( ) AmazonGlobal Expedited Shipping (averages 8-14 business days)
- ( ) AmazonGlobal Priority Shipping (averages 2-4 days)

# Real-World Examples

- **Race Conditions** [Paleari et al., 2008]
- **HTTP Parameter Manipulation** [Citigroup, 2011; UNESCO, 2011]
- **Unsolicited Request Sequences** [Wang et al., 2011]
- **Compromising Use of the 'Back' Button** [Hallé et al., 2010]
- **Session Puzzling** [Chen, 2011]
- **Facebook OAuth Access Token Leak** [Goldshlager, 2013]

# Root Causes

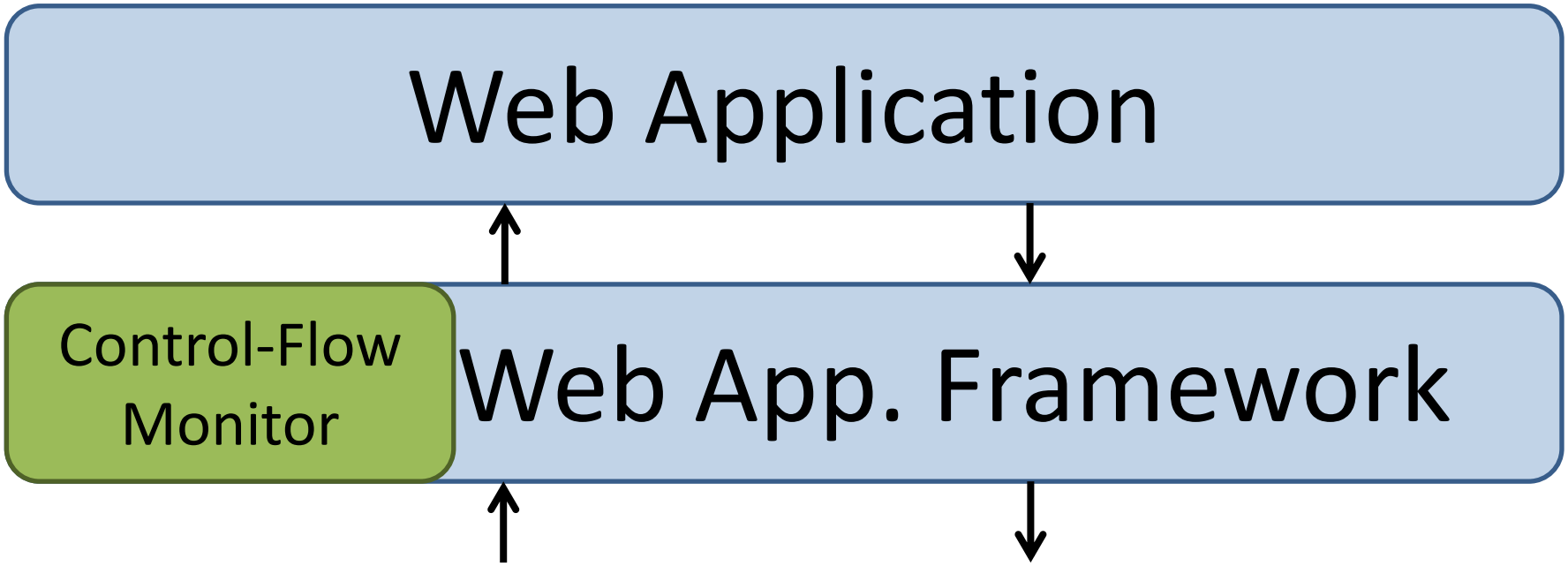
- In all cases
  - no explicit control-flow definition
  - no central enforcement
  - user behavior differs from expectations
    - i.e. user did not only click on provided links
  - access control fails or can not help
    - e.g. by guessable URLs or permitted actions
  - Needed: central policy enforcement point



# Survey

"A framework is a set of classes that embodies an abstract design for solutions to a family of related problems, and supports reuses at a larger granularity than classes."

[src:Johnson, R.E., Foote, B.: Designing Reusable Classes.
In: Journal of Object-Oriented Programming. Volume 1. (1988)]



# Survey

- Top 10 web application frameworks according to BuiltWith
  - Apache Tapestry
  - Google Web Toolkit
  - Spring
  - CodeIgniter
  - CakePHP
  - Kohana
  - ASP.NET
    - Web Forms, MVC, Web Pages
  - Ruby on Rails
  - Django*

# Survey

- 3 security features inspected for each framework
  - message sequence enforcement
  - race condition protection
  - request integrity / parameter data type enforcement
- Methodology: check
  - manuals
  - config options
  - flow of request processing through framework components

# Survey – Outcome

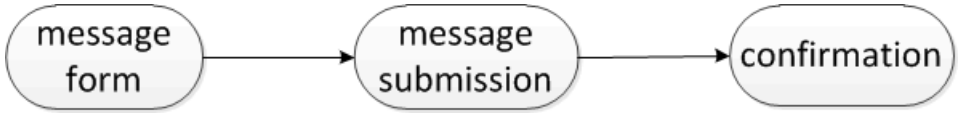
- **Message sequence enforcement**
  - **only 1 out of 11 provides support**
  - ***Spring* + *Web* module + *Web Flow* extension**
    - **inserts controller into MVC**
    - **accepts policy as XML or Java**
    - **implements flow graph with states & transitions**
    - **adds new request parameters**
      - `flowExecutionKey` & `eventID`
    - **allows multi-tabbing**
    - **“Back” button protection**

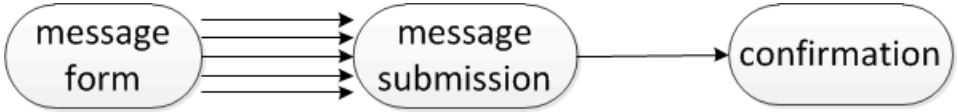
# Survey – Outcome

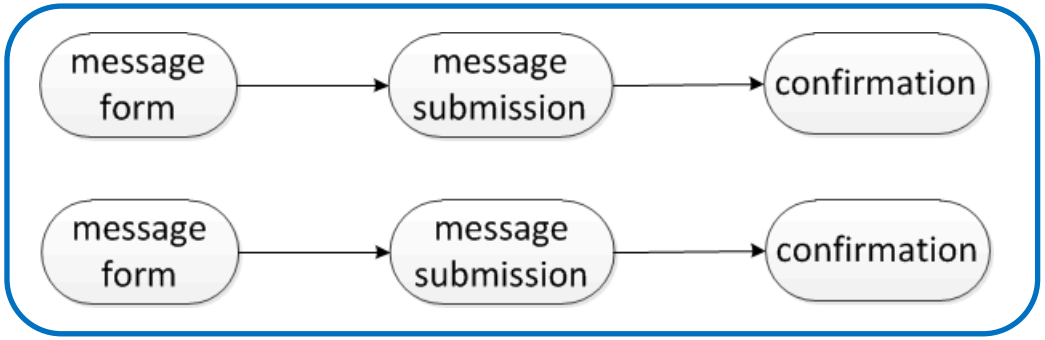
- **Message sequence enforcement: problem**
  - **cross-workflow parameter exchange**
  - **Example:**
    - **start workflows A & B**
    - **obtain “payment successful” token in A for cheap purchase**
    - **append this token to request in B to forge payment of expensive goods**
  - **application-specific parameter binding necessary, no framework support**
    - **can happen across tabs (same session) and across browsers (different sessions)**

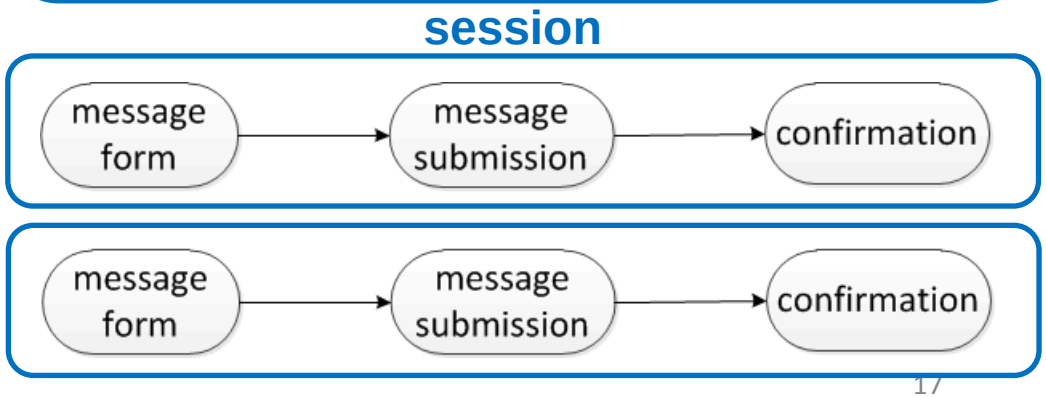
# Survey: Race Condition Exploits

- Different attack levels exist
  - in-tab / in-workflow
    - same user account
    - same session ID
    - same workflow ID
  - multi-tab
    - same user account
    - same session ID
    - different workflow IDs
  - multi-browser
    - same user account
    - different session IDs
    - different workflow IDs



# Survey – Outcome

- **Race condition protection**
  - **again only Spring offers protection**
    - **probably a side effect of message sequence enforcement**
    - **only ‘in-tab’ protection, i.e. within one workflow**
  - **no framework protects against race condition attacks from parallelized workflows**
  - **… nor against attacks from parallelized sessions**

# Survey – Outcome

- **Parameter data type enforcement**
  - **mainly depends on underlying programming language**
    - **e.g. Java-based frameworks raise exceptions depending on type cast**
  - **all frameworks offer regular expression filtering**
    - **spoofed requests never reach controller if value does not match**
  - **this feature must be explicitly used by developer**
    - **no enforcement by default**

# Survey – Outcome

- **Dispatchers + Filters: single points of enforcement**

| Framework | Dispatcher | Filters |
|---|---|---|
| Apache Tapestry | Master Dipatcher | – |
| Google Web Toolkit | Web.xml | – |
| CodeIgniter | routes.php | pre_controller, post_controller |
| CakePHP | routes.php | beforeFilter, afterFilter |
| Kohana | Bootstrap.php | before, after |
| ASP.NET Web Forms | Global.asax | – |
| ASP.NET MVC | Global.asax | OnActionExecuting, OnActionExecuted |
| ASP.NET Web Pages | Global.asax | – |
| Ruby on Rails | ActionDispatch | beforeFilter, afterFilter |
| Django | URLconf | Middleware |

# Survey – Outcome

| Framework | Version | CFI | RC | Param. | Lang |
|---|---|---|---|---|---|
| Apache Tapestry | 5 | – | – | + | Java |
| Google Web Toolkit | 2.5 | – | – | + | Java |
| Spring/Web Flow | 3.2.2/2.3.0 | –/+ | –/≈ | + | Java |
| CodeIgniter | 2.1.3 | – | – | + | PHP |
| CakePHP | 2.3.0 | – | – | + | PHP |
| Kohana | 3.3.0 | – | – | + | PHP |
| ASP.NET Web Forms | 4.5 | – | – | + | C#, VB.NET |
| ASP.NET MVC | 4 | – | – | + | C#, VB.NET |
| ASP.NET Web Pages | 2 | – | – | + | C#, VB.NET |
| Ruby on Rails | 1.9.3 | – | – | + | Ruby |
| Django | 1.5.1 | – | – | + | Python |

# Conclusion

- No framework offers security by design
  - all have at least single points of enforcement
  - 7 out of 11 even have customizable filters
    - implementation effort necessary
- Spring Web Flow provides basic protection
  - request sequence within workflow
  - race condition within workflow
- No framework has cross-workflow protection
  - neither concerning request sequence nor race conditions
- No framework has by design parameter data type integrity
  - but all have regex support

# Are We Lost?

- **Maybe WAFs can help…**

# Plus: WAF Survey

- Inspected 28 Web Application Firewalls
  - based on public documentation
  - all claim protecting against OWASP Top 10
  - 1 seems to be extensible for CFI protection
    - Ironbee
  - 1 provides only vague description of feaures
    - and no answer to email request

| | |
|---|---|
| A1 | Injection |
| A2 | Broken Authentication and Session Management |
| A3 | Cross-Site Scripting (XSS) |
| A4 | Insecure Direct Object References |
| A5 | Security Misconfiguration |
| A6 | Sensitive Data Exposure |
| A7 | Missing Function Level Access Control |
| A8 | Cross-Site Request Forgery (CSRF) |
| A9 | Using Components with Known Vulnerabilities |
| A10 | Unvalidated Redirects and Forwards |

# Survey: WAF

| | |
|---|---|
| OWASP Stinger 2.2.2 | Radware AppWall |
| NAXSI 0.49 | Armorlogic – Profense |
| AQTronix – WebKnight 3.0 | Barracuda Networks - Application Firewall |
| Trustwave SpiderLabs – ModSecurity 2.7 | Bee Ware – i-Suite |
| *Qualys – Ironbee 0.7* | BinarySec - Application Firewall |
| Riverbed – Stingray | BugSec – WebSniper |
| Trustwave - WebDefend Web Application Firewall 6.1 | Cisco - ACE Web Application Firewall |
| Imperva – SecureSphere | Citrix - Application Firewall |
| Penta Security – WAPPLES | eEye Digital Security – SecureIIS |
| Bayshore Networks – Application Protection Platform 2.0 | F5 - Application Security Manager 11.4 *(?)* |
| DenyAll - Web Application Firewall 4.1 | Forum Systems – Sentry 11.4 |
| Applicure – DotDefender 4.2 | webScurity - webApp.secure |
| Port80 Software - ServerDefender VP 2.2.2 | Ergon – Airlock 4.2.6 |
| Privacyware - ThreatSentry IIS Web Application Firewall | Xtradyne - Application Firewalls |

# Questions?


THANK YOU !