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
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
Firefox Start

Google™  Web  Bilder  Groups  News

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
Shopping Cart

The Ultimate Hitchhiker's Guide to the Galaxy - Douglas Adams; Paperback
- In Stock
- Eligible for FREE Super Saver Shipping
- This will be a gift (Learn more)
- Delete · Save for later

Price: $12.99
You save: $7.01 (35%)
Quantity: 1

Subtotal: $12.99

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

Conditions of Use Privacy Notice © 1996-2012, Amazon.com, Inc. or its affiliates
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
  $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 ▽
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.

Billing Information:

Gift Cards & Promotional Codes:

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

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)

Ordering Options
Add options


The Ultimate Hitchhiker's Guide to the Galaxy
by Douglas Adams
$12.99
Quantity: 1

Shipping Address:
Bastian Braun
Universitaet Passau
Instr. 43
Passau, Bayern 94032
Germany
Phone: +491796494588 Change
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
“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.”

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
• 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
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**

<table>
<thead>
<tr>
<th>Framework</th>
<th>Dispatcher</th>
<th>Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Tapestry</td>
<td>Master Dispatcher</td>
<td>–</td>
</tr>
<tr>
<td>Google Web Toolkit</td>
<td>Web.xml</td>
<td>–</td>
</tr>
<tr>
<td>CodeIgniter</td>
<td>routes.php</td>
<td>pre_controller, post_controller</td>
</tr>
<tr>
<td>CakePHP</td>
<td>routes.php</td>
<td>beforeFilter, afterFilter</td>
</tr>
<tr>
<td>Kohana</td>
<td>Bootstrap.php</td>
<td>before, after</td>
</tr>
<tr>
<td>ASP.NET Web Forms</td>
<td>Global.asax</td>
<td>–</td>
</tr>
<tr>
<td>ASP.NET MVC</td>
<td>Global.asax</td>
<td>OnActionExecuting, OnActionExecuted</td>
</tr>
<tr>
<td>ASP.NET Web Pages</td>
<td>Global.asax</td>
<td>–</td>
</tr>
<tr>
<td>Ruby on Rails</td>
<td>ActionDispatch</td>
<td>beforeFilter, afterFilter</td>
</tr>
<tr>
<td>Django</td>
<td>URLconf</td>
<td>Middleware</td>
</tr>
</tbody>
</table>

Bastian Braun
### Survey – Outcome

<table>
<thead>
<tr>
<th>Framework</th>
<th>Version</th>
<th>CFI</th>
<th>RC</th>
<th>Param.</th>
<th>Lang</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Tapestry</td>
<td>5</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>Java</td>
</tr>
<tr>
<td>Google Web Toolkit</td>
<td>2.5</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>Java</td>
</tr>
<tr>
<td>Spring/Web Flow</td>
<td>3.2.2/2.3.0</td>
<td>−/+</td>
<td>−/≈</td>
<td>+</td>
<td>Java</td>
</tr>
<tr>
<td>CodeIgniter</td>
<td>2.1.3</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>PHP</td>
</tr>
<tr>
<td>CakePHP</td>
<td>2.3.0</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>PHP</td>
</tr>
<tr>
<td>Kohana</td>
<td>3.3.0</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>PHP</td>
</tr>
<tr>
<td>ASP.NET Web Forms</td>
<td>4.5</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>C#, VB.NET</td>
</tr>
<tr>
<td>ASP.NET MVC</td>
<td>4</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>C#, VB.NET</td>
</tr>
<tr>
<td>ASP.NET Web Pages</td>
<td>2</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>C#, VB.NET</td>
</tr>
<tr>
<td>Ruby on Rails</td>
<td>1.9.3</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>Ruby</td>
</tr>
<tr>
<td>Django</td>
<td>1.5.1</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>Python</td>
</tr>
</tbody>
</table>
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
• 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 features
    - and no answer to email request

<table>
<thead>
<tr>
<th>A1</th>
<th>Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A3</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A4</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>A5</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>A6</td>
<td>Sensitive Data Exposure</td>
</tr>
<tr>
<td>A7</td>
<td>Missing Function Level Access Control</td>
</tr>
<tr>
<td>A8</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A9</td>
<td>Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
<tr>
<td>Survey: WAF</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>OWASP Stinger 2.2.2</td>
<td>Radware AppWall</td>
</tr>
<tr>
<td>NAXSI 0.49</td>
<td>Armorlogic – Profense</td>
</tr>
<tr>
<td>AQTronix – WebKnight 3.0</td>
<td>Barracuda Networks - Application Firewall</td>
</tr>
<tr>
<td>Trustwave SpiderLabs – ModSecurity 2.7</td>
<td>Bee Ware – i-Suite</td>
</tr>
<tr>
<td>Qualys – Ironbee 0.7</td>
<td>BinarySec - Application Firewall</td>
</tr>
<tr>
<td>Riverbed – Stingray</td>
<td>BugSec – WebSniper</td>
</tr>
<tr>
<td>Trustwave - WebDefend Web Application Firewall 6.1</td>
<td>Cisco - ACE Web Application Firewall</td>
</tr>
<tr>
<td>Imperva – SecureSphere</td>
<td>Citrix - Application Firewall</td>
</tr>
<tr>
<td>Penta Security – WAPPLES</td>
<td>eEye Digital Security – SecureIIS</td>
</tr>
<tr>
<td>Bayshore Networks – Application Protection Platform 2.0</td>
<td>F5 - Application Security Manager 11.4 (?)</td>
</tr>
<tr>
<td>DenyAll - Web Application Firewall 4.1</td>
<td>Forum Systems – Sentry 11.4</td>
</tr>
<tr>
<td>Applicure – DotDefender 4.2</td>
<td>webSecurity - webApp.secure</td>
</tr>
<tr>
<td>Port80 Software - ServerDefender VP 2.2.2</td>
<td>Ergon – Airlock 4.2.6</td>
</tr>
<tr>
<td>Privacyware - ThreatSentry IIS Web Application Firewall</td>
<td>Xtradyne - Application Firewalls</td>
</tr>
</tbody>
</table>