Ajax und PHP im Einsatz
Submit und Response war gestern

Dr. Volker Göbbels

Arachnion GmbH & Co. KG

http://www.arachnion.de

Arachnion
Business Solutions

2

Zur Person

- Promotion in Theor. Chemie
- Gründer und Geschäftsführer der Arachnion GmbH & Co. KG
- Spezialisiert auf „komplexe“ Web- und eCommerce-Projekte im Unternehmensumfeld
- Aktiv in der PHP Community

Arachnion
Business Solutions

3

Zu Ihnen

- Wer von Ihnen setzt PHP ein?
- Wer von Ihnen setzt Ajax ein?
- Falls ja, eigene JavaScript Lösung oder externe Library?
- Wer von Ihnen verwendet irgendwelche Sicherheitsmaßnahmen bei Ajax?

Arachnion
Business Solutions

4

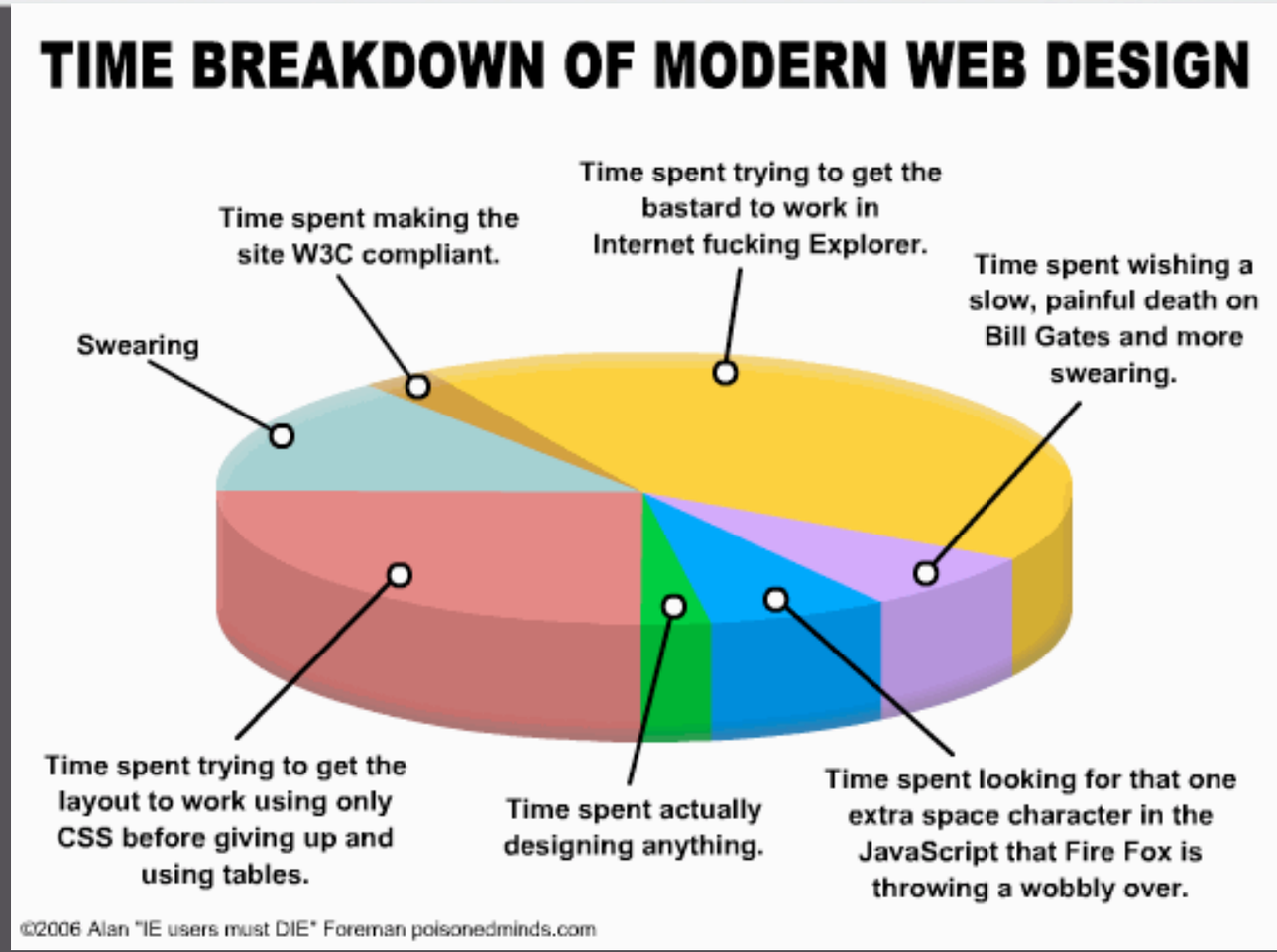
Agenda

- Rationale
- Architektonischer Überblick
- Marktübersicht existierender Ajax Lösungen
- Exemplarische Nutzung einiger Ajax Libraries
- Sicherheitsaspekte im Umgang mit Ajax Anwendungen

Arachnion
Business Solutions

5

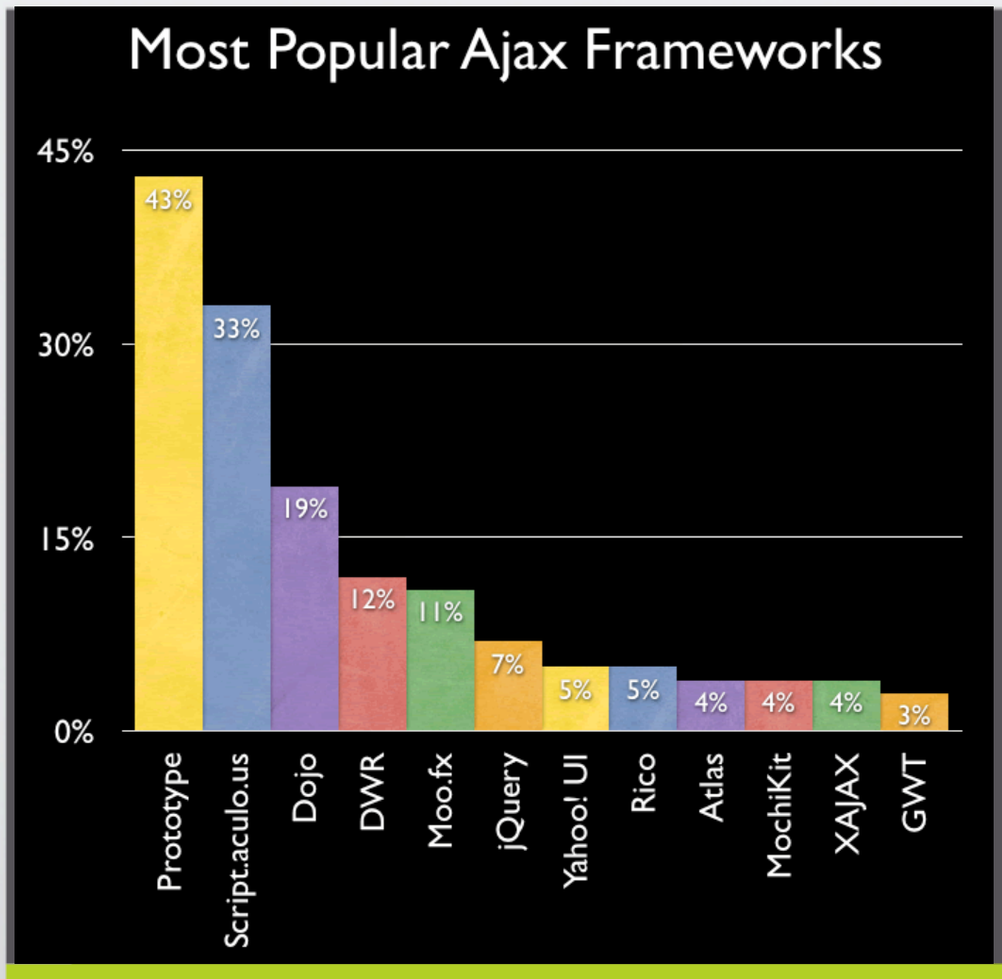
Rationale – Warum eine Library?



Arachnion
Business Solutions

6

Ajaxian.com Umfrage: Frameworks

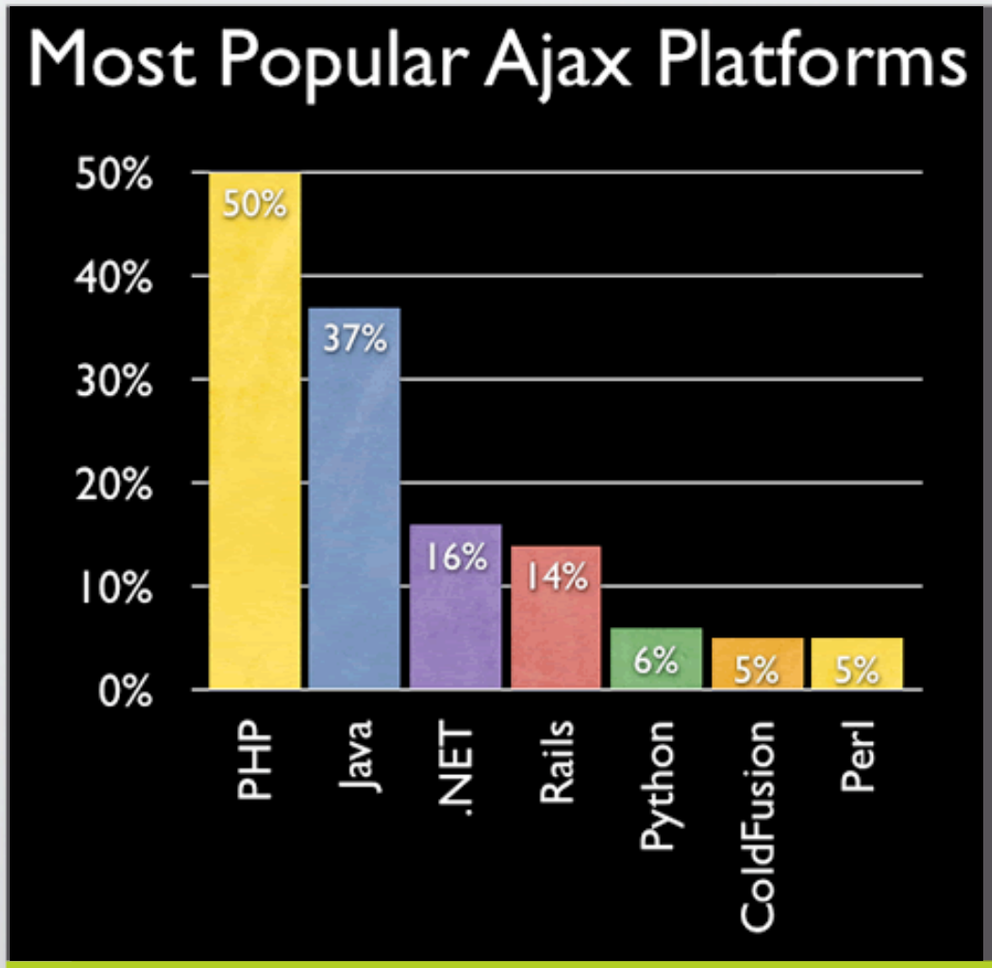


- ✓ 25% setzen XMLHttpRequest direkt ein.
- ✓ 11% setzen JSON an Stelle von XML ein.

Arachnion
Business Solutions

7

Ajaxian.com Umfrage: Plattformen

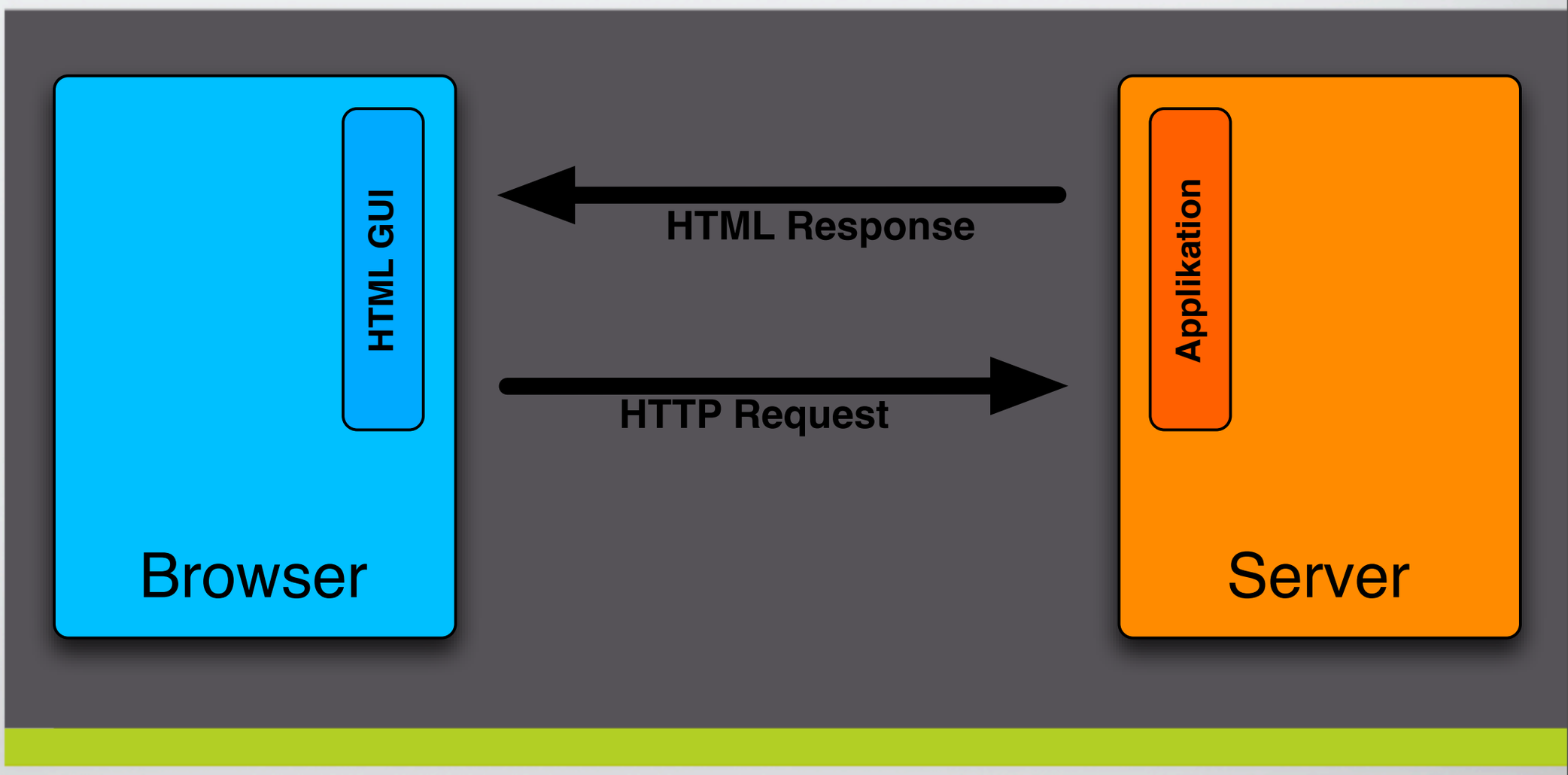


- ✓ 5 Teilnehmer (ca. 0.6%) setzen C++ ein.
- ✓ Ein Teilnehmer setzt Delphi ein,
  ein weiterer Lisp ;)

Arachnion
Business Solutions

8

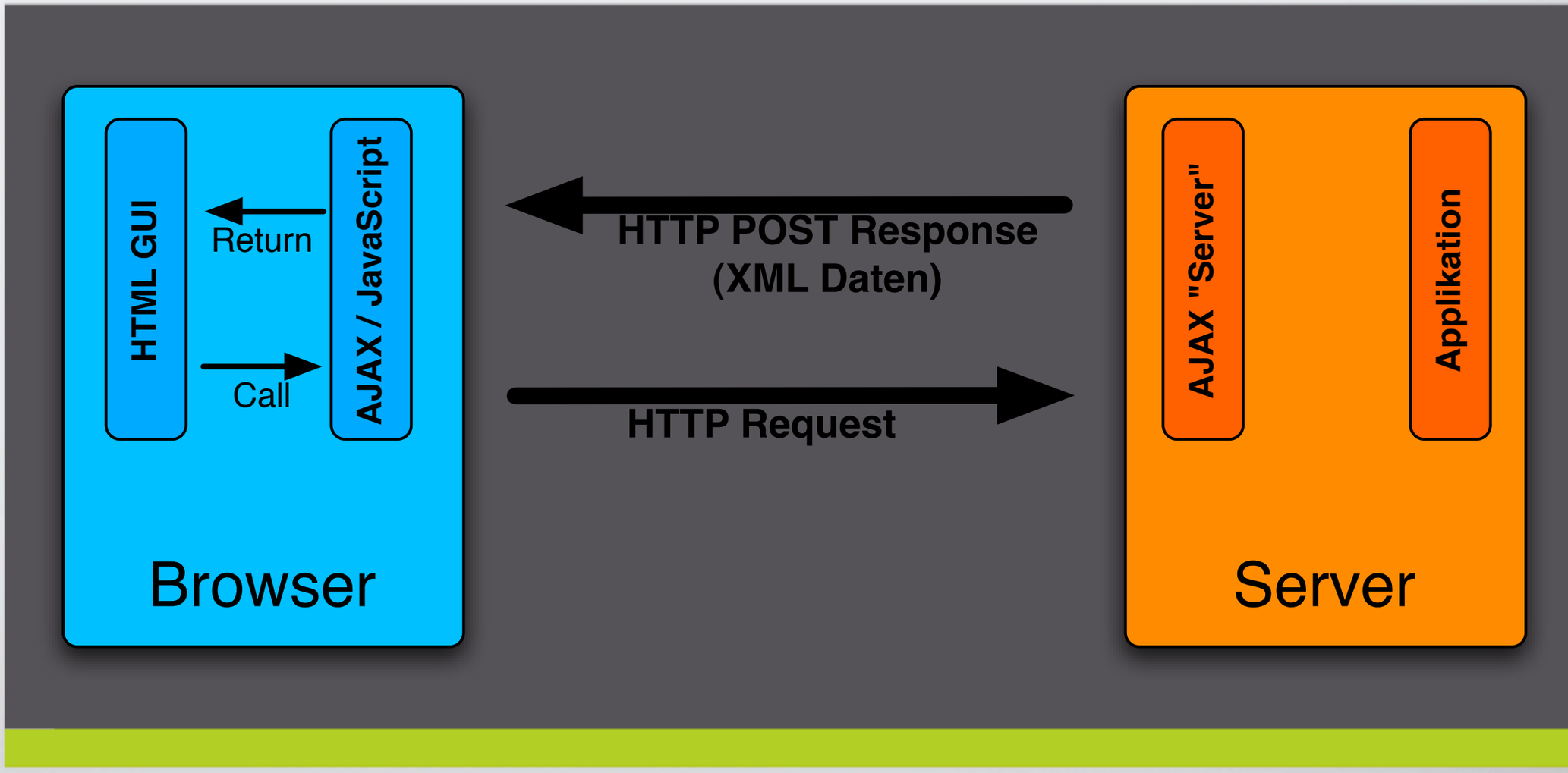
Überblick: „Standard“ Webapplikationen



Arachnion
Business Solutions

9

Überblick: AJAX Webapplikationen



Arachnion
Business Solutions

10

Pro & Contra Ajax / PHP

- Pro: AJAX Applikationen fordern selten komplette Webseiten beim Server an
- Pro: Die ausgetauschten Datenpakete sind deutlich kleiner
- Pro: Browserseitiges JavaScript erlaubt komfortable GUIs
- Pro: Konzentration in PHP auf das „Wesentliche“
- Contra: JavaScript ist browserabhängig
- Contra: Gemischtsprachliche Entwicklung und „Miniatur-

Arachnion
Business Solutions

11

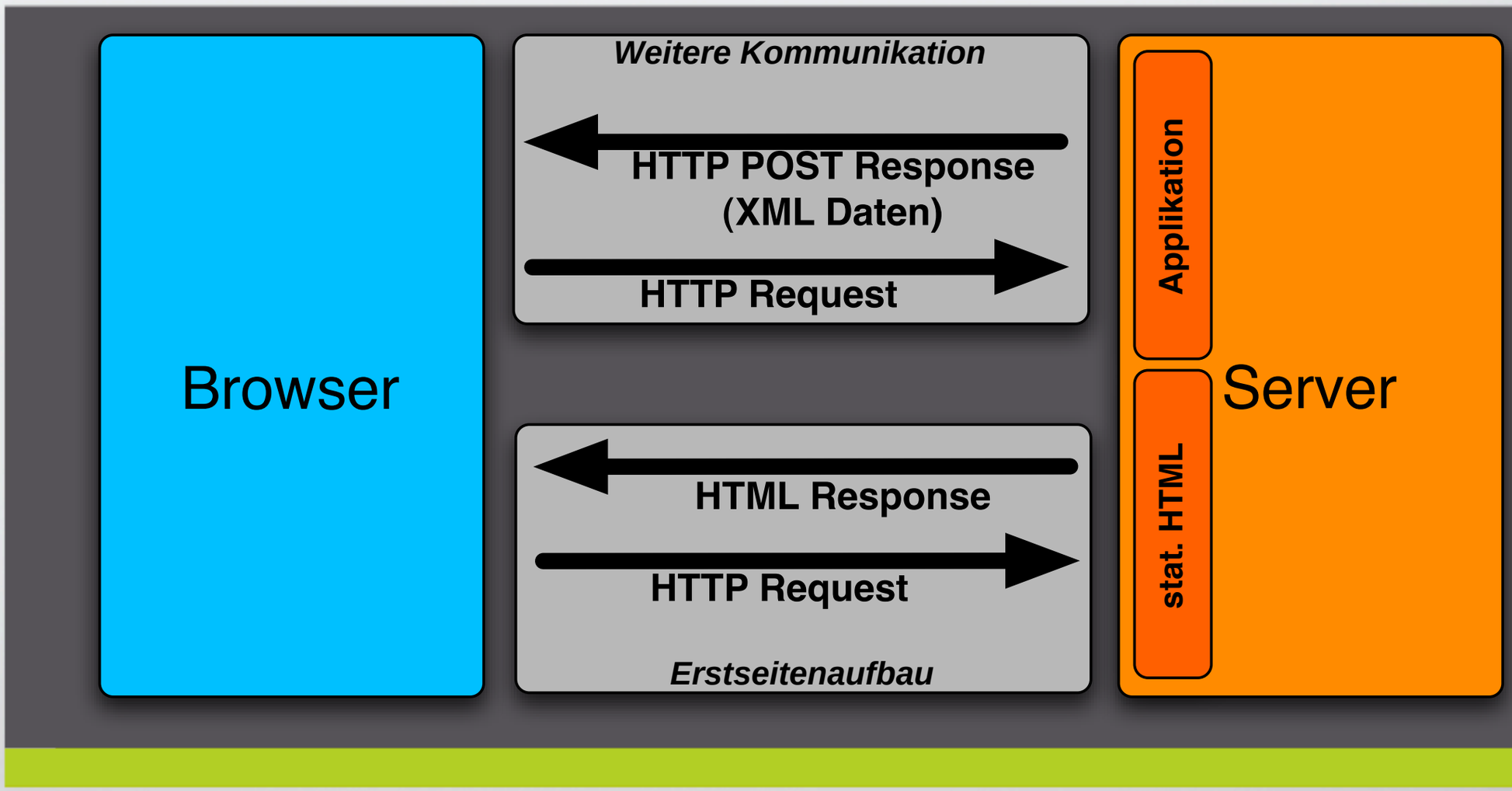
Lösungsansatz: Standardisierte JS/AJAX Libraries

- Browserübergreifendes JavaScript
- Standardisiertes API von Seiten des Browser-GUI und der Serverkomponenten
- Vorgefertigte browserseitige Komponenten aka. Widgets
- 2 Varianten von Libraries
  - reine browserbasierte Bibliotheken, ausschließlich JavaScript
  - serverseitige Bibliothek in Host/Scriptsprache, passender browserseitiger Output wird erzeugt

Arachnion
Business Solutions

12

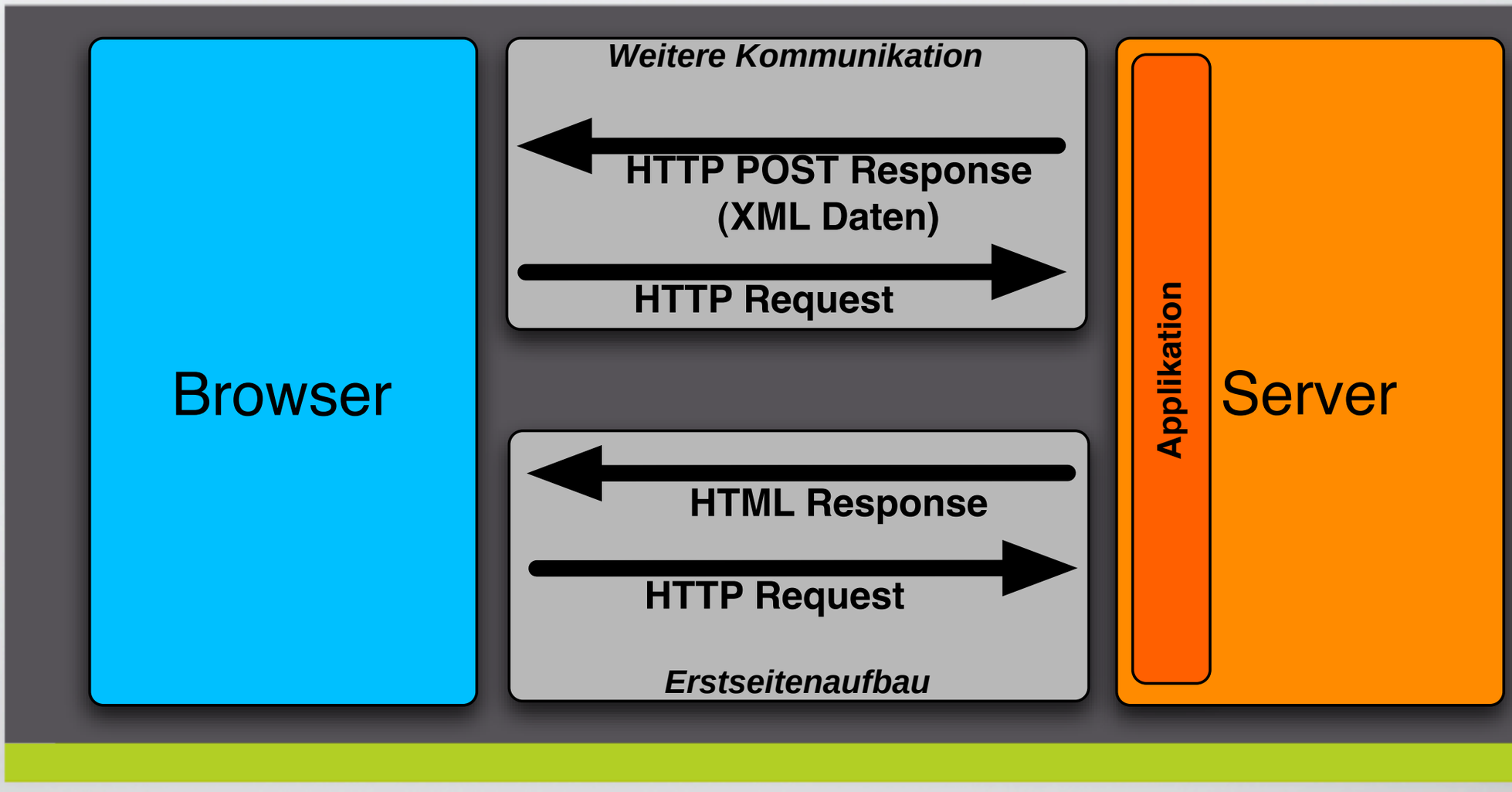
Variante 1: Reines clientseitiges JavaScript



Arachnion
Business Solutions

13

Variante 2: Serverseitige GUI-Erzeugung



Arachnion
Business Solutions

14

Marktüberblick
Vorbemerkungen (1/2)

- Client- / Serverseitige Libraries
- Funktionsumfang
  - Asynchrone Kommunikation (AJAX)
  - Effekte (DHTML)
  - GUI (Widgets)
  - Allgemeine JavaScript-Features
  - Qualität der Dokumentation
- Nur die bekanntesten / wichtigsten / interessantesten

Arachnion
Business Solutions

15

Marktüberblick
Vorbemerkungen (2/2)

- Clientseitige Libraries
  - Dojo, qooxdoo, mochikit, Prototype
- Serverseitige Libraries
  - xajax, sajax, AjaxCore, PEAR::HTML_AJAX

Zu den fett markierten Frameworks folgen Beispiele bzw. praktische Teile.

Arachnion
Business Solutions

16

Historie
Wie entstehen Ajax Frameworks?

- Eigenständiger Ansatz ohne „spezielle“ Ziele
- Umsetzung in anderen Sprachen (PHP, Java, ...)
- Ergänzung bestehender Frameworks/Plattformen (Prototype -> RoR, Atlas -> .NET, mochikit -> TurboGears, ...)
- Mehrsprachige Tools (sajax)

Arachnion
Business Solutions

17

Marktüberblick (Client)
Dojo

- AJAX: AJAX, JSON, iframe-Proxy, ...
- DHTML: Animation, DnD, Fading, Grafik, SVG, ...
- Widgets: Forms, Sortable Table, Editor, Tabs, Trees, Split Pane, Dialog, DatePicker, ColorPalette, Menüs, ...
- Utilities: Datenstrukturen, Regex, DOM, Logger, Kryptographie, Mathematik
- Dokumentation: Teilweise gut, Gerade in Reorganisation
- URL: http://www.dojotoolkit.org

Arachnion
Business Solutions

18

Marktüberblick (Client)
qooxdoo

- AJAX: AJAX (Transport-API)
- DHTML: DnD
- Widgets: Forms, Views (Tab, Page), Menüs, Toolbars, Tree, TreeFullControl, Listview, Table, DateChooser, ColorSelector, ...
- Utilities: -
- Dokumentation: Gut bis befriedigend, ziemlich vollständig

Arachnion
Business Solutions

19

Marktüberblick (Client)
mochikit

- AJAX: AJAX (Async)
- DHTML: DnD, Runde Ecken, Animation, Fading, Puff, Shake, ...
- Widgets: -
- Utilities: DOM, DateTime, String Formatting, Iteratoren, Sortables, ...
- Dokumentation: Sehr gut
- URL: http://mochikit.com

Arachnion
Business Solutions

20

Marktüberblick (Client)
Prototype

- AJAX: AJAX (ajax)
- DHTML: –
- Widgets: Form-Manipulation
- Utilities: Datentypen, DOM, ...
- Dokumentation: Nicht vorhanden
- URL: http://prototype.conio.net

Arachnion
Business Solutions

21

Marktüberblick (Server)
xajax

- AJAX: AJAX
- DHTML: –
- Widgets: –
- Utilities: –
- Dokumentation: Knapp aber brauchbar
- Besonderheit: Coding in JavaScript nahezu unnötig
- URL: http://www.xajaxproject.org/

Arachnion
Business Solutions

22

Marktüberblick (Server)
sajax

- AJAX: AJAX
- DHTML: -
- Widgets: -
- Utilities: -
- Dokumentation: Knapp aber brauchbar
- Besonderheit: Anbindung an PHP, Python, Ruby, ASP, Perl, Lua, ...
- URL: http://www.modernmethod.com/sajax/

Arachnion
Business Solutions

23

Marktüberblick (Server)
AjaxCore

- AJAX: AJAX
- DHTML: -
- Widgets: -
- Utilities: -
- Dokumentation: Knapp aber brauchbar
- Besonderheit: PHP only. Nutzt Prototype.
- URL: http://sourceforge.net/projects/ajaxcore/

Arachnion
Business Solutions

24

Marktüberblick (Server)
PEAR::HTML_AJAX

- AJAX: AJAX
- DHTML: -
- Widgets: -
- Utilities: -
- Dokumentation: Gut
- Besonderheit: PHP only. Integration mit anderen PEAR Packages (z.B. Quickform) möglich.
- URL: http://pear.php.net/package/HTML_AJAX

Arachnion
Business Solutions

25

Praktischer Teil

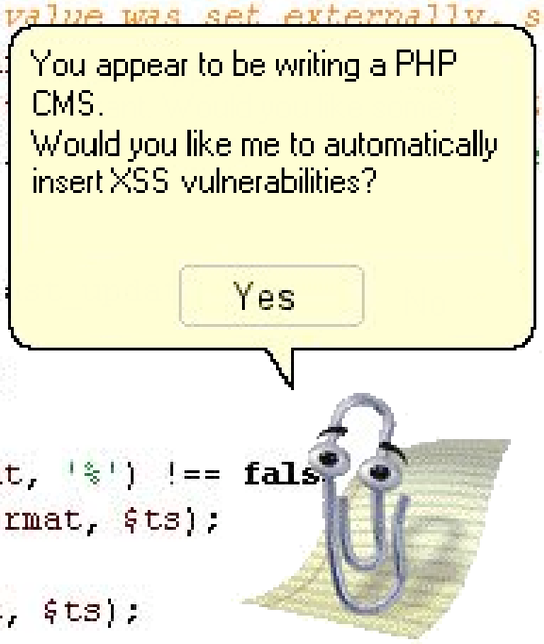
- Client-Frameworks (Web)
  - Dojo Standard
  - Dojo & Smarty Integration
- Server-Frameworks
  - xajax
  - sajax
  - AjaxCore
  - PEAR::HTML_AJAX

Arachnion
Business Solutions

26

Ajax Sicherheit

```
209     public function getDateLastUpdated($format = '%x')
210     {
211
212         if ($this->date_last_updated === null || $this->date_l
213             return null;
214         } elseif (!is_int($this->date_last_updated)) {
215             // a non-timestamp value was set externally, so we
216             $ts = strtotime($th
217             if ($ts === -1 || $
218                 throw new Prope
219             }
220         } else {
221             $ts = $this->date_l
222         }
223         if ($format === null) {
224             return $ts;
225         } elseif (strpos($format, '%') !== fals
226             return strftime($format, $ts);
227         } else {
228             return date($format, $ts);
229         }
```



Arachnion
Business Solutions

27

Ajax Sicherheit
Übersicht

- Es gelten die „allgemeinen Prinzipien“ für Webapplikationen:
  - „Never trust any user input“
  - Authentifizierung & Autorisierung
  - Transport über SSL
- Großer Vorteil: Bei XMLHttpRequests sendet der Browser evtl. gesetzte Cookies mit, das bedeutet, auch das Ajax-Backend kann mit Sessions arbeiten!

Arachnion
Business Solutions

28

Sicherheit
Nevertrust any user input

- Nicht aus $_REQUEST lesen
- Nur $_GET und $_POST entsprechend dem verwendeten Protokoll
- Value-Filtering: intval(), floatval(), strval()
- Strings escapen (SQL-Injection, XSS, ...)
- Authentifizierung
- Verwendung eines Security Scanners wie Chorizo

Arachnion
Business Solutions

29

Sicherheit
Authentifizierung / Autorisierung

- Durch Session-Handling Verwendung aller üblichen Auth-Tools möglich:
  - PEAR::Auth
  - PEAR::LiveUser
  - PHPLib Auth-Klasse
  - PHPGacl
- Beispiel

Arachnion
Business Solutions

30

Zusammenfassung

- Es gibt reichlich Ajax Libraries mit und ohne GUI Elementen
- Fast alle sind noch in konstanter Entwicklung
- Häufig leidet darunter die Dokumentation
- Ajax Frontends führen im Hintergrund Requests aus. Diese können wie jeder Request von einem PHP-Script bearbeitet werden
- Die Sicherheitsmaßnahmen entsprechen denen „normaler“ Webapplikationen

Arachnion
Business Solutions

31

Referenzen

- http://www.ajaxbuch.de/
- http://www.ajax-community.de/
- http://www.ajaxian.com/
- http://ajaxpatterns.org/
- http://www.arachnion.de, vmg@arachnion.de

Arachnion
Business Solutions

32

Ende