



Tainted-Object- Propagation- Analyse

Oliver Klee
pixy@oliverklee.de

für PHP 5

Motivation

Cross-site-Scripting (XSS)

X □ - REGIERUNGonline - SEITE EMPFEHLEN - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.bundesregierung.de/Webs/Breg/DE/SeiteEmpfehlen/mailvers Google

English Français Kontakt Impressum Übersicht Suchbegriff >>

Die Bundesregierung

Startseite

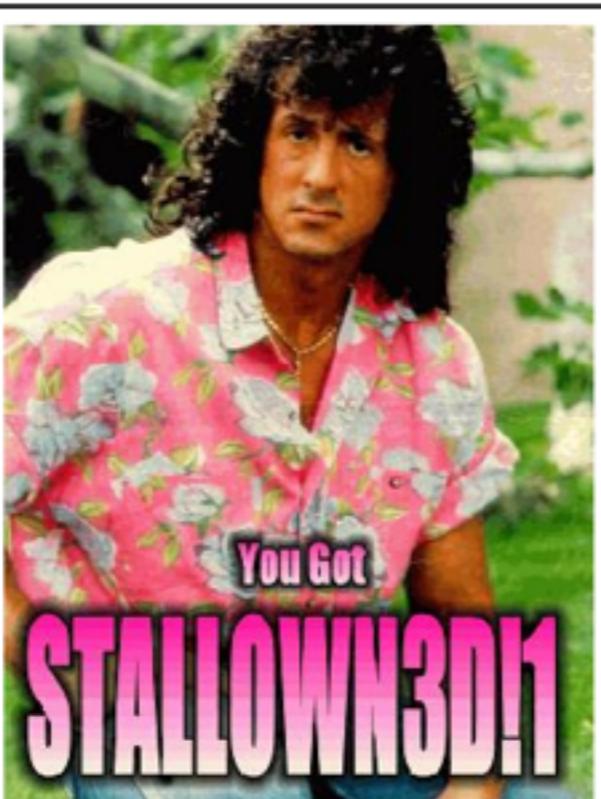
- Bundesregierung
- Reformprojekte
- Regierungspolitik A-Z
- Europa
- Dialog Nachhaltigkeit
- Nachrichten
- Grundgesetz / Gesetze
- Publikationen / Fotos
- Magazine

Sie sind hier: Startseite > Seite empfehlen

Seite empfehlen

Titel

Surfen ohne Risiko: www.FragFinn.de



: der Bundesregierung Zum Seitenanfang ^

SQL-Injection (SQLi)

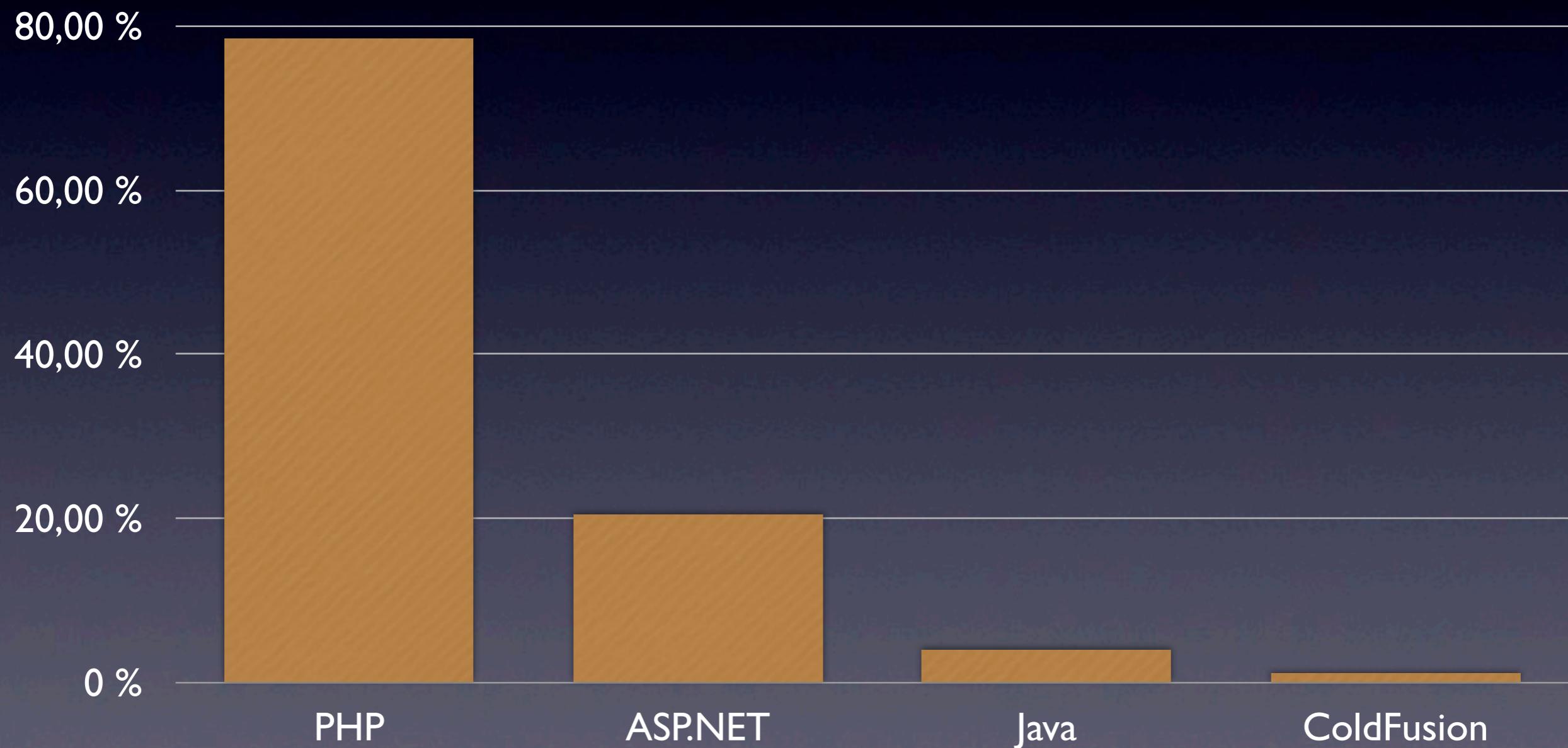


<http://xkcd.com/327/>

PHP ist weit verbreitet



benutzte Server-Programmiersprache



PHP ist . . .

eine Skriptsprache
objektorientiert
dynamisch

PHP ist . . .

eine Skriptsprache
objektorientiert
dynamisch

```
class Foo {}
```

PHP ist . . .

eine Skriptsprache
objektorientiert
dynamisch

```
class Foo {}  
$foo = new Foo();
```

PHP ist . . .

eine Skriptsprache
objektorientiert
dynamisch

```
class Foo {}  
$foo = new Foo();  
$foo = 42;
```

PHP ist . . .

eine Skriptsprache
objektorientiert
dynamisch

```
class Foo {}  
$foo = new Foo();  
$foo = 42;  
$variableName = 'foo';
```

PHP ist . . .

eine Skriptsprache
objektorientiert
dynamisch

```
class Foo {}  
$foo = new Foo();  
$foo = 42;  
$variableName = 'foo';  
echo $$variableName;
```

Pixy ist der Scanner der Wahl

	Typ	Open Source	läuft	Recall	Precision
SWAAT	String-Matching	?	✓	✗	✗
Code Secure Verifier	Datenfluss-Analyse	✗	keine Testversion	?	?
PHP-SAT	Datenfluss-Analyse	✓	✗	?	?
Pixy	Datenfluss-Analyse	✓	✓	✓	✓
YASCA ohne Plugins	Pattern-Matching	✓	✓	✗	✗

Pixy



Autor: Nenad Jovanovic (TU Wien, Dissertation)
Betreuer: Christopher Krügel

(Associate-Professor an der University of California, Santa Barbara)

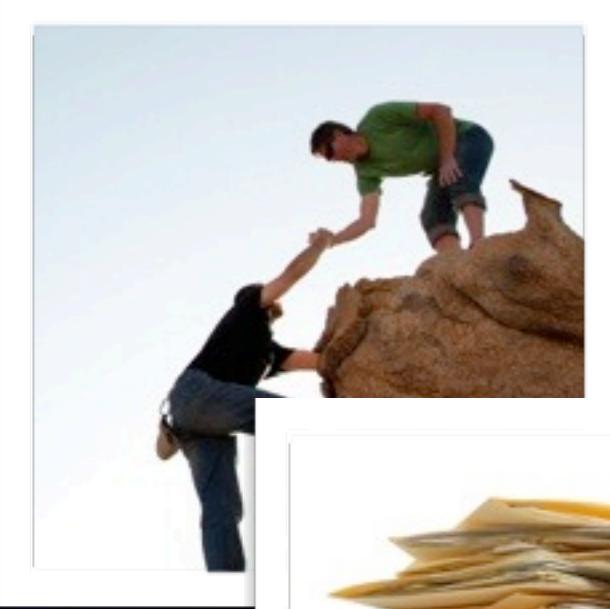


Autor: Nenad Jovanovic (TU Wien, Dissertation)
Betreuer: Christopher Krügel

(Associate-Professor an der University of California, Santa Barbara)



**6 Publikationen auf
Konferenzen und Workshops**



Autor: **Nenad Jovanovic** (TU Wien, Dissertation)
Betreuer: **Christopher Krügel**

(Associate-Professor an der University of California, Santa Barbara)

**6 Publikationen auf
Konferenzen und Workshops**

2006-2007 entstanden



Autor: Nenad Jovanovic (TU Wien, Dissertation)
Betreuer: Christopher Krügel

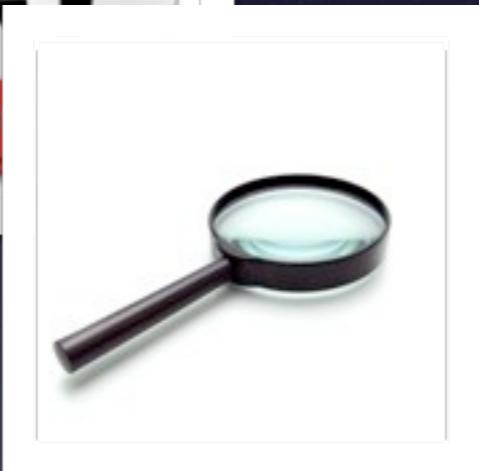
(Associate-Professor an der University of California, Santa Barbara)



6 Publikationen auf
Konferenzen und Workshops



2006-2007 entstanden



scannet
Tainted-Object-Propagation
ausgefeilte **Alias-Analyse**
scannet nur PHP 4.x



Autor: Nenad Jovanovic (TU Wien, Dissertation)
Betreuer: Christopher Krügel

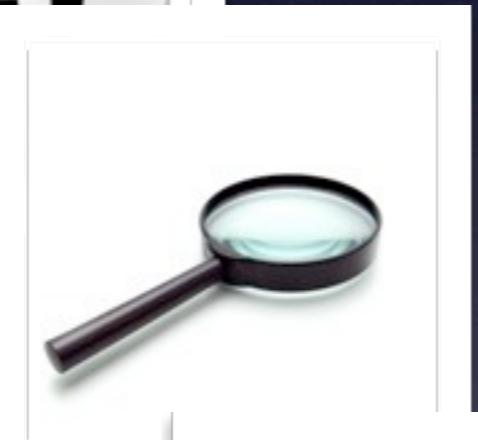
(Associate-Professor an der University of California, Santa Barbara)



6 Publikationen auf
Konferenzen und Workshops



2006-2007 entstanden



scannet
Tainted-Object-Propagation
ausgefeilte **Alias-Analyse**
scannet nur PHP 4.x



in Java 5/6
sehr wenig JavaDoc

Tainted-Object- Propagation

Tainted-Object-Propagation-Analyse benutzt Datenflussanalyse

```
$name = $_GET['name'];  
  
echo '<p>Hello ' . $name . ' !</p>';
```

Tainted-Object-Propagation-Analyse benutzt Datenflussanalyse

Source



```
$name = $_GET['name'];
```

```
echo '<p>Hello ' . $name . ' !</p>';
```

Tainted-Object-Propagation-Analyse benutzt Datenflussanalyse

Source



```
$name = $_GET['name'];
```

```
echo '<p>Hello ' . $name . ' !</p>';
```

Sink



Tainted-Object-Propagation-Analyse benutzt Datenflussanalyse

Source



```
$name = $_GET['name'];
```

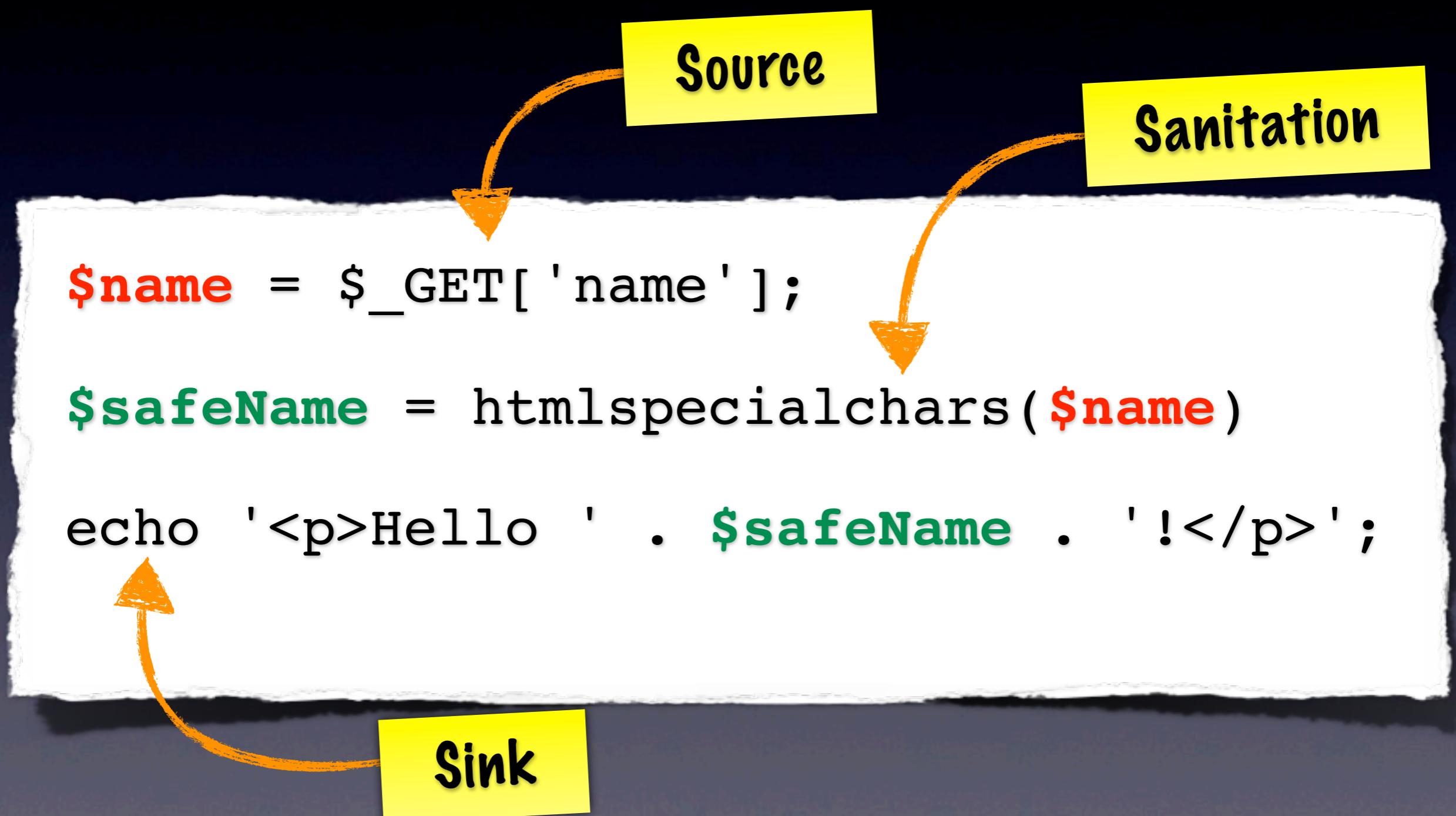
```
$safeName = htmlspecialchars($name)
```

```
echo '<p>Hello ' . $safeName . ' !</p>';
```

Sink



Tainted-Object-Propagation-Analyse benutzt Datenflussanalyse



Aliase und Referenzen in PHP

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

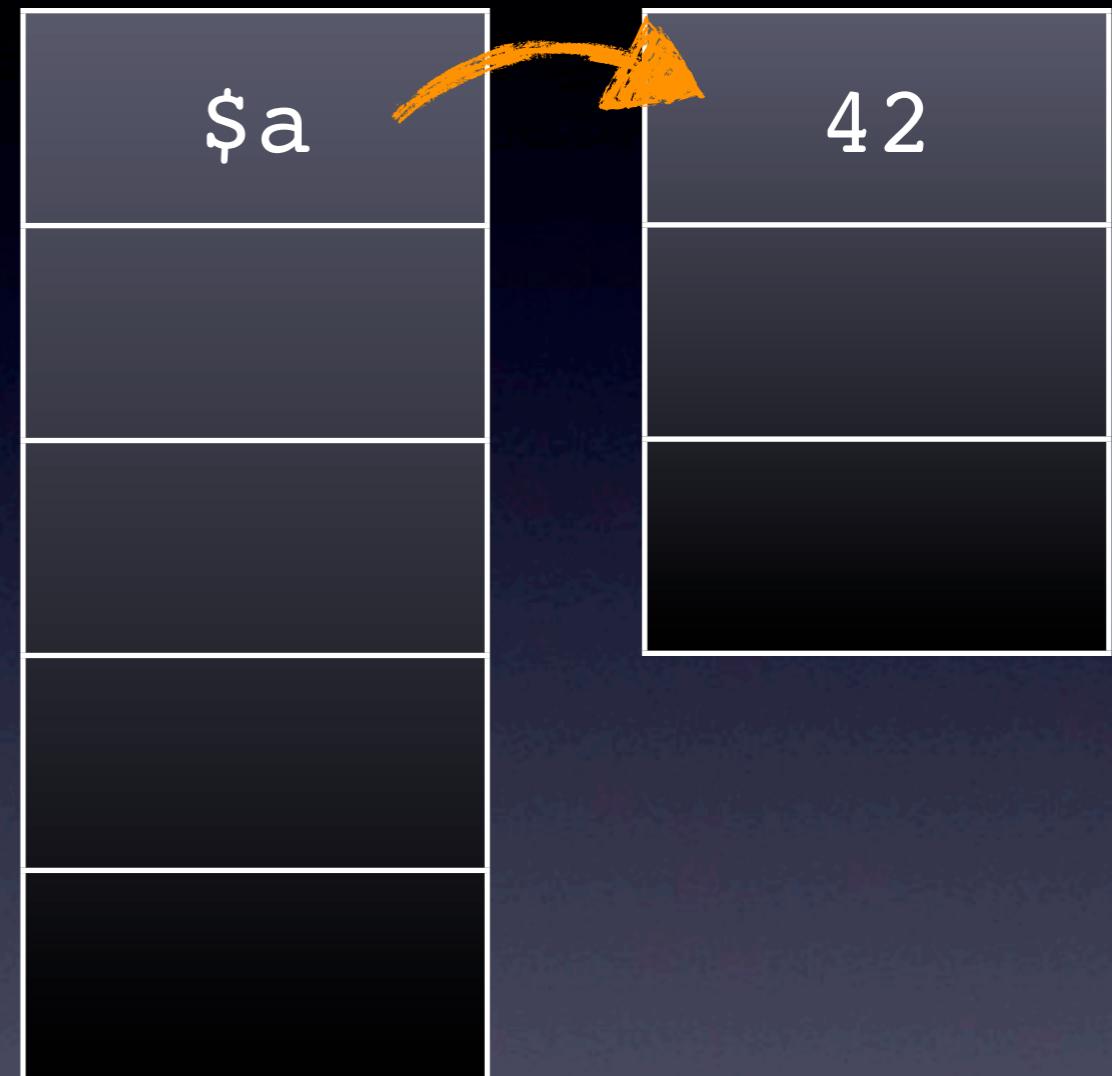
PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

PHP 7.4 - 8.1 | 2023 | 10 Minuten

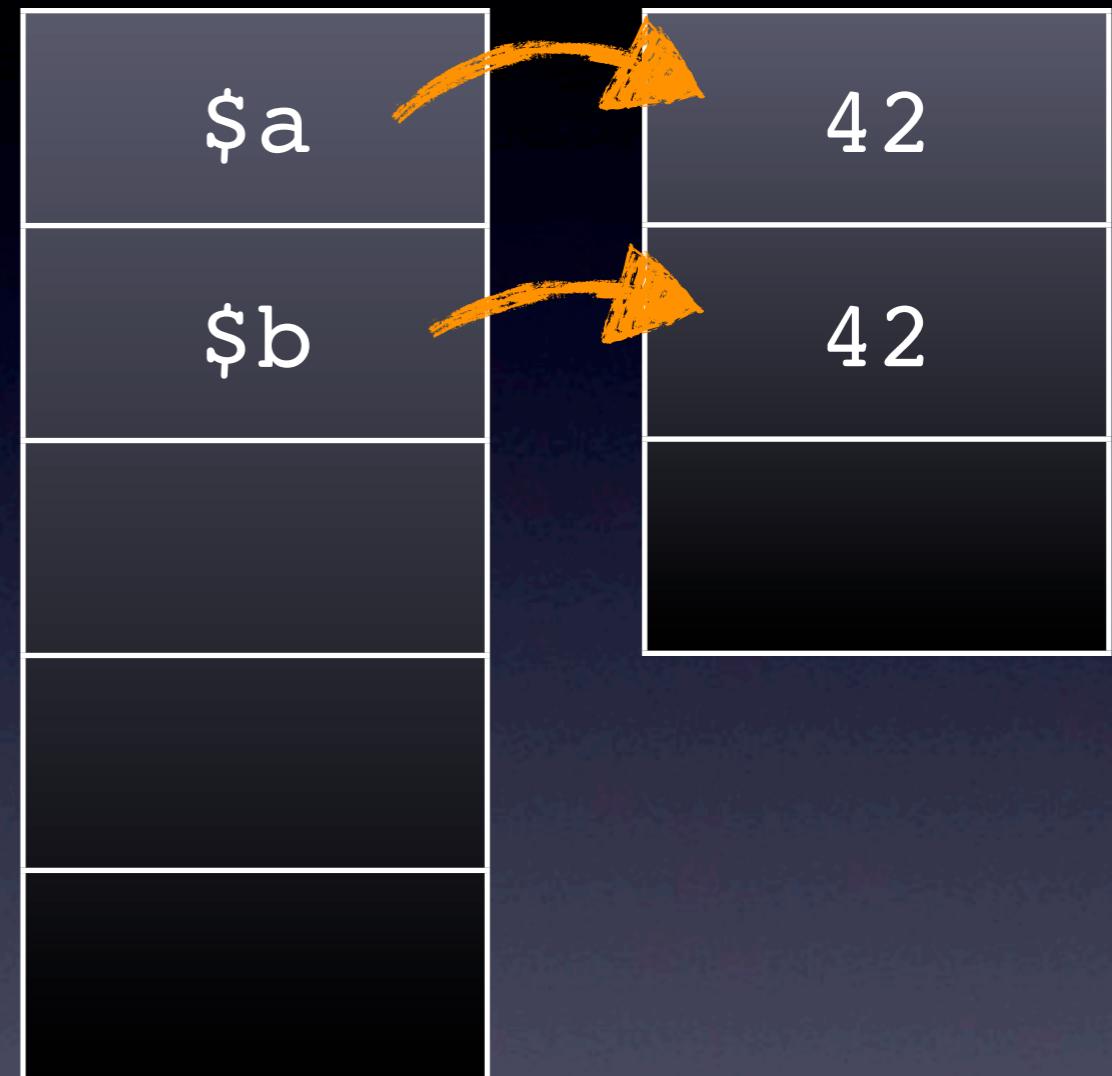
Referenzen in PHP sind keine Pointer

```
$a = 42;
```



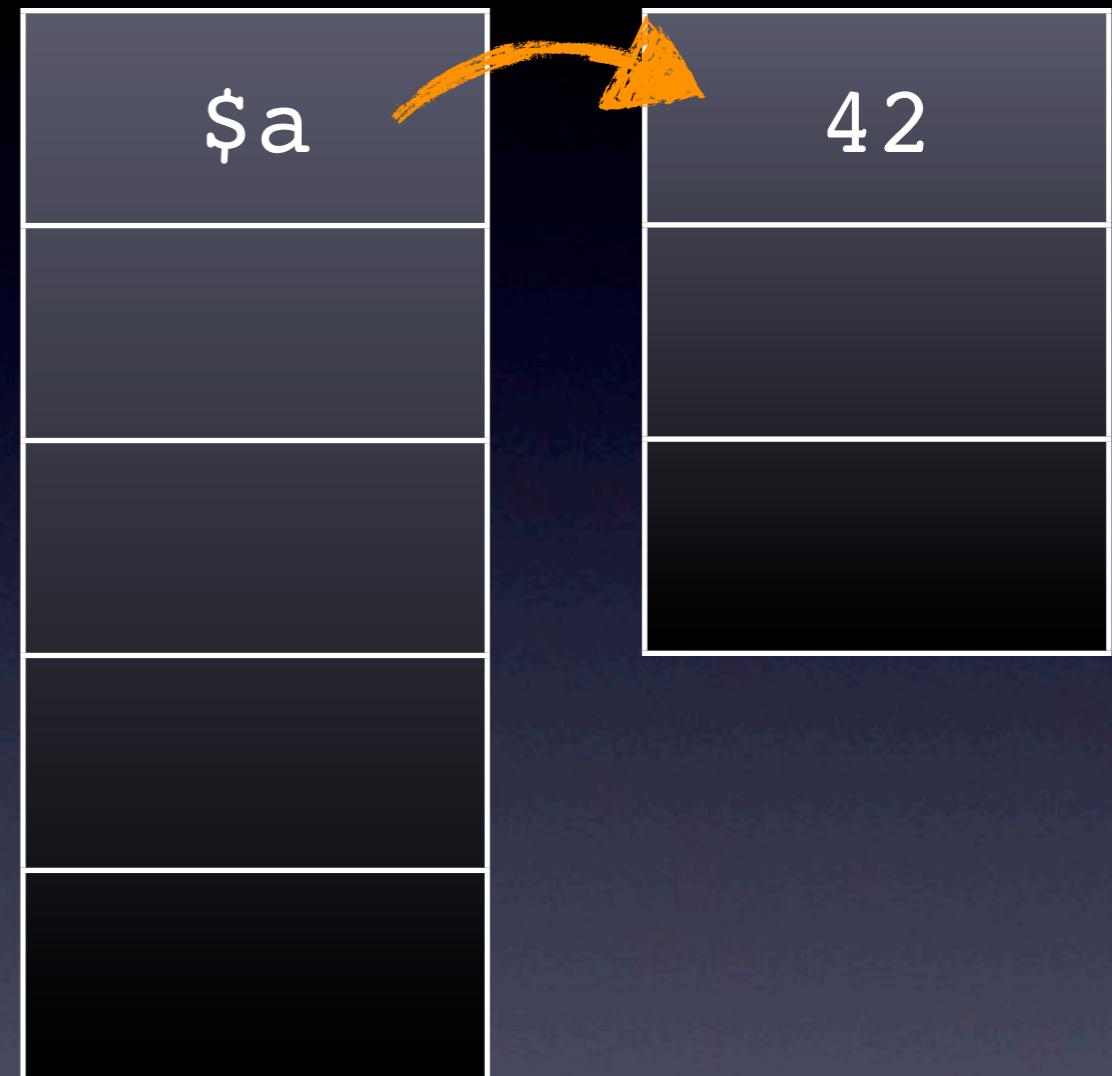
Referenzen in PHP sind keine Pointer

```
$a = 42;  
$b = $a;
```



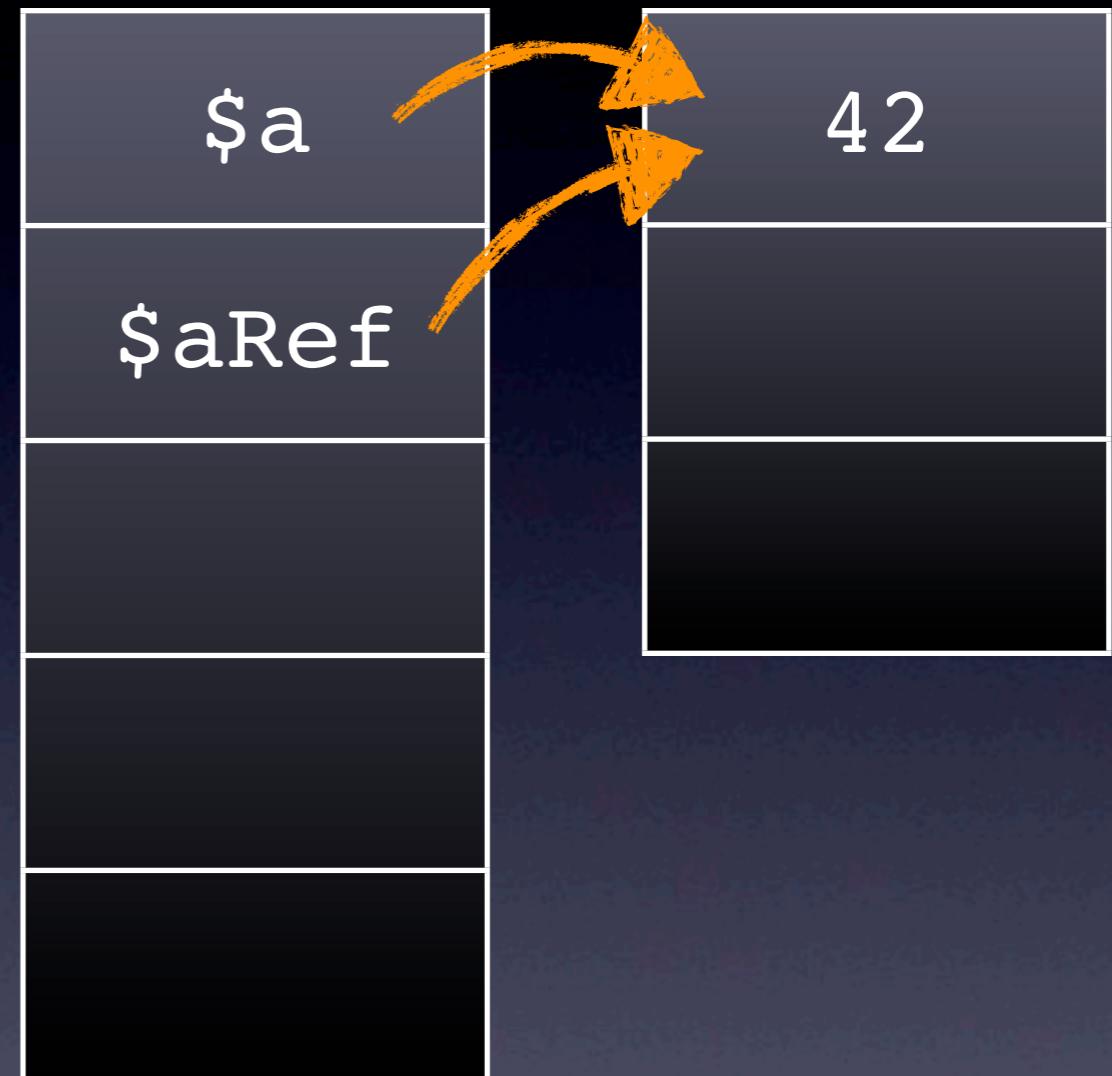
Referenzen in PHP sind keine Pointer

```
$a = 42;
```



Referenzen in PHP sind keine Pointer

```
$a = 42;  
$aRef = &$a;
```



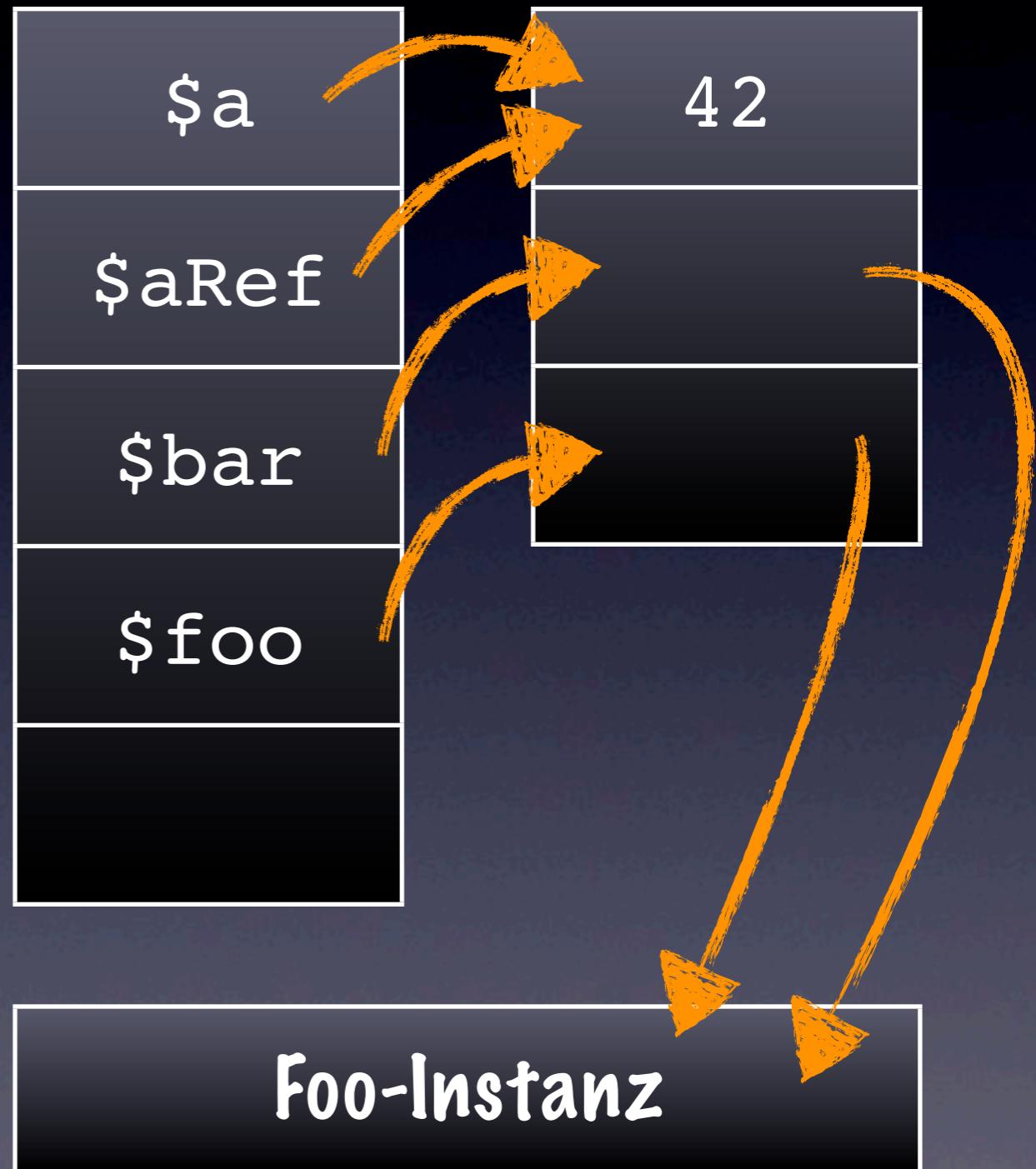
Referenzen in PHP sind keine Pointer

```
$a = 42;  
$aRef = &$a;  
$foo = new Foo();
```



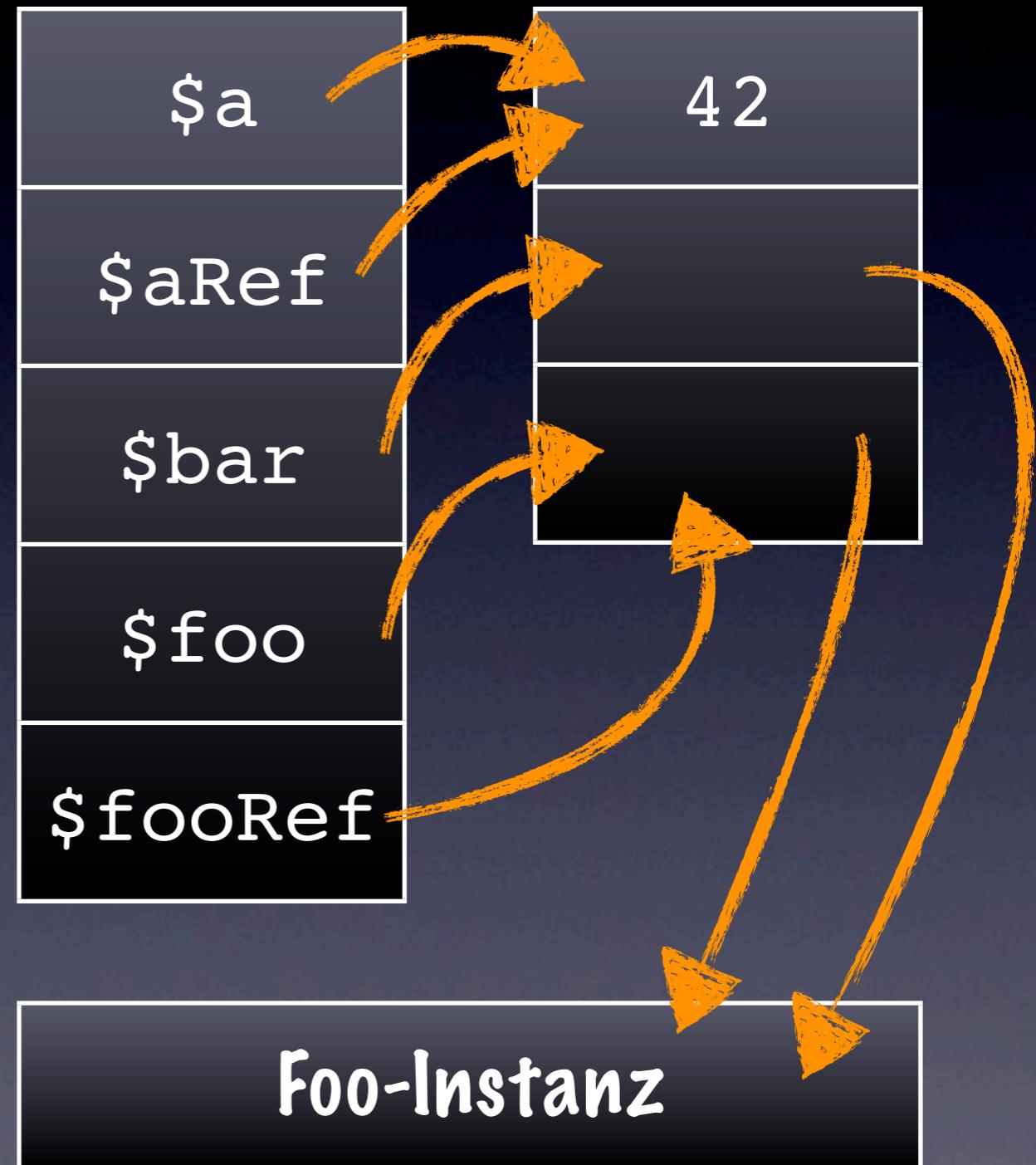
Referenzen in PHP sind keine Pointer

```
$a = 42;  
$aRef = &$a;  
$foo = new Foo();  
$bar = $foo;
```



Referenzen in PHP sind keine Pointer

```
$a = 42;  
$aRef = &$a;  
$foo = new Foo();  
$bar = $foo;  
$fooRef = &$foo;
```



Es gibt Must- und May-Aliase

```
...
$a = &$b;

if (...) {

    $c = &$d;

    $e = &$d;

}

...
...
```

Es gibt Must- und May-Aliase

```
...  
$a = &$b;
```

```
if (...) {
```

```
$c = &$d;
```

```
$e = &$d;
```

```
}
```

```
...
```

Es gibt Must- und May-Aliase

...

\$a = &\$b;

if (...) {

\$c = &\$d;

\$e = &\$d;

}

...

must{} may{}

Es gibt Must- und May-Aliase

```
...  
$a = &$b;  
  
must{} may{}  
  
must{(a,b)} may{}  
  
if (...) {  
  
    $c = &$d;  
  
    $e = &$d;  
  
}  
  
...  
...
```

Es gibt Must- und May-Aliase

```
... must{} may{}  
$a = &$b;  
must{(a,b)} may{}  
if (...) {  
  
    $c = &$d; must{(a,b) (c,d)} may{}  
    $e = &$d;  
  
}  
  
...
```

Es gibt Must- und May-Aliase

```
... must{} may{}  
$a = &$b; must{(a,b)} may{}  
if (...) {  
  
    $c = &$d; must{(a,b) (c,d)} may{}  
    $e = &$d; must{(a,b) (c,d,e)} may{}  
}  
  
...
```

Es gibt Must- und May-Aliase

```
... must{} may{}  
$a = &$b; must{(a,b)} may{}  
if (...) {  
  
    $c = &$d; must{(a,b) (c,d)} may{}  
    $e = &$d; must{(a,b) (c,d,e)} may{}  
}  
... must{(a,b)} may{(c,d) (c,e) (d,e)}
```

Ziele

PHP 5.X als Ziel



PHP 5.X als Ziel

neue Schlüsselwörter

```
$dateTime =  
date_create_from_format(  
    'Y-m-d' , '5-Dec-2012'  
) ;
```

PHP 5.X als Ziel

neue Schlüsselwörter

```
$dateTime =  
date_create_from_format(  
    'Y-m-d', '5-Dec-2012'  
) ;
```

Type-Hinting

Pass-by-Reference per
Default für Objekte

```
function bar(Foo $foo) {  
    ...  
}
```

```
class Foo {}  
$foo = new Foo();  
bar($foo);
```

PHP 5.X als Ziel

neue Schlüsselwörter

```
$dateTime =  
date_create_from_format(  
    'Y-m-d', '5-Dec-2012'  
) ;
```

Klassenkonstanten

```
class Foo {  
    const ANSWER = 42;  
}
```

Type-Hinting

Pass-by-Reference per
Default für Objekte

```
function bar(Foo $foo) {  
    ...  
}
```

```
class Foo {}  
$foo = new Foo();  
bar($foo);
```

PHP 5.X als Ziel

neue Schlüsselwörter

```
$dateTime =  
date_create_from_format(  
    'Y-m-d', '5-Dec-2012'  
) ;
```

Klassenkonstanten

```
class Foo {  
    const ANSWER = 42;  
}
```

Type-Hinting

Pass-by-Reference per
Default für Objekte

```
function bar(Foo $foo) {  
    ...  
}
```

Sichtbarkeit

```
class Foo {  
    protected function bar() {}  
}
```

```
class Foo {}  
$foo = new Foo();  
bar($foo);
```

PHP 5.X als Ziel

neue Schlüsselwörter

```
$dateTime =  
date_create_from_format(  
    'Y-m-d', '5-Dec-2012'  
) ;
```

Klassenkonstanten

```
class Foo {  
    const ANSWER = 42;  
}
```

Type-Hinting

Pass-by-Reference per
Default für Objekte

```
function bar(Foo $foo) {  
    ...  
}
```

Sichtbarkeit

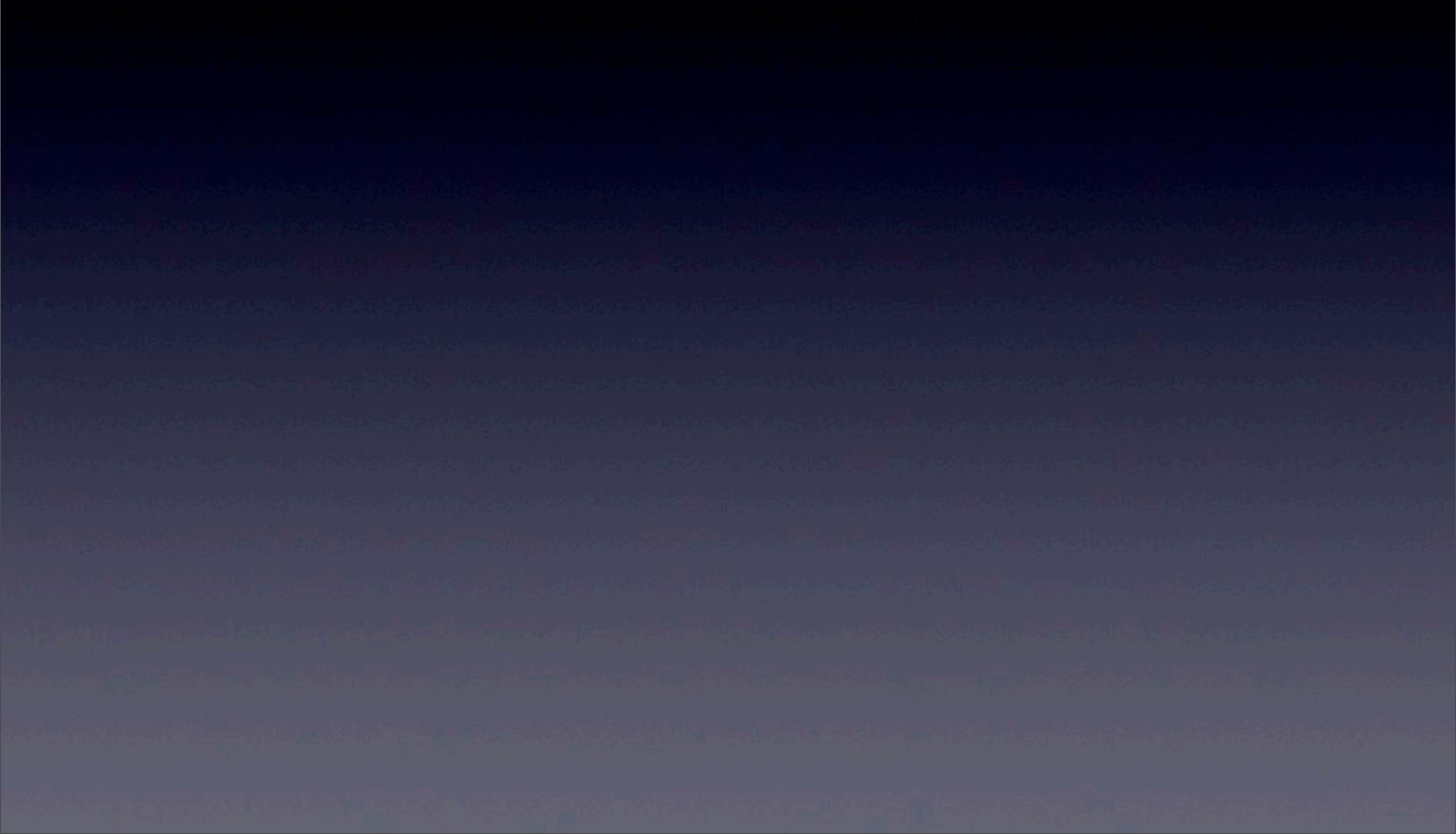
```
class Foo {  
    protected function bar() {}  
}
```

```
class Foo {}  
$foo = new Foo();  
bar($foo);
```

Autoloader

```
// nicht mehr nötig  
// require_once('Foo.php');  
$foo = new Foo();
```

Pixy bietet viele Baustellen



Pixy bietet viele Baustellen

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy bietet viele Baustellen

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

Pixy bietet viele Baustellen

Forschungs-
Ziele

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

technische
Ziele

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Autoloader

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Autoloader

Java 7

Pixy bietet viele Baustellen

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

PhpParser

Scanner/Lexer
(jFlex)

Parser
(CUP)

Pixy

TAC
Kontrollflussgraph (CFG)
Datenflussgraph (DFG)
Alias-Analyse
Tainted Object Propagation

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Autoloader

Java 7

JavaDoc

Pixy-Rework wird evaliert

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Autoloader

Java 7

JavaDoc

Pixy-Rework wird evaliert

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

Open-Source-Projekte parsen:
TYPO3 CMS, Drupal, WordPress, Contao

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Autoloader

Java 7

JavaDoc

Pixy-Rework wird evaliert

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

Open-Source-Projekte parsen:
TYPO3 CMS, Drupal, WordPress, Contao

Anzahl der Java-Warnungen

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Autoloader

Java 7

JavaDoc

Pixy-Rework wird evaliert

Forschungs-
Ziele

PHP 5-
Schlüsselwörter

Sicherheits-
Auswirkungen von
PHP5-Neuerungen

Alias-Analyse für
Pass-by-Reference

Sicherheitslücken suchen in
TYPO3 CMS, Drupal, WordPress, Contao

Open-Source-Projekte parsen:
TYPO3 CMS, Drupal, WordPress, Contao

Anzahl der Java-Warnungen

technische
Ziele

PHP5 ohne
Fehlermeldung
parsen

Autoloader

Java 7

JavaDoc