



PHPIDS

WEB APPLICATION SECURITY 2.0

PHP Usergroup Frankfurt am Main
14. Februar 2008

Autor: Tom Klingenberg

LASTFLOOD®

Web & Applikation

PHP

(PHP: Braucht hier nicht erklärt werden.)

A decorative graphic in the bottom right corner of the slide. It consists of three overlapping semi-circular shapes. The top one is yellow, the middle one is a light green, and the bottom one is a slightly darker green. There is a white, curved gap between the middle and bottom green shapes.

IDS

IDS: Intrusion Detection System

„Einbruchsmeldesystem“

IDS (Fort.)

Dient der Gefahrenabwehr

Klassischer Anwendungsbereich in der Informationstechnologie ist in Netzwerksystemen

IDS Eigenschaften

- Einbruch wird erkannt
 - Identifizierung eines Angreifers
 - Durch seine Handlung / Aktionen

IDS Eigenschaften

- Einbruch wird erkannt
 - Identifizierung eines Angreifers
 - Durch seine Handlung / Aktionen
- Reaktion
 - Aktionen können ausgelöst werden

IDS Eigenschaften

- Einbruch wird erkannt
 - Identifizierung eines Angreifers
 - Durch seine Handlung / Aktionen
- Reaktion
 - Aktionen können ausgelöst werden
- Szenarien
 - Blockieren von Remotehosts
 - Blockieren von Daten
 - Bewerten von Daten

IDS Problemstellen

- Reaktives System
 - „man läuft hinterher“
 - Neue Angriffsvektoren (z. B. DoS)
 - Oftmals Prinzip „Blacklisting“
- False Positives
 - Kann ein Einbrecher genau erkannt werden?
 - Gibt es „den Einbrecher“?

„Intrusion“ bei einer Webanwendung

Wie wird in eine Webanwendung
eingebrochen?



„Intrusion“ bei einer Webanwendung

- 1.) Cross Site Scripting (XSS)
- 2.) Injection Flaws (particularly SQL injection)
- 3.) Malicious File Execution
- 4.) Insecure Direct Object Reference
- 5.) Cross Site Request Forgery (CSRF)

Top 5 aus der *OWASP Top 10 2007*
http://www.owasp.org/index.php/Top_10_2007

PHPIDS

„IDS geschrieben in PHP für PHP
Anwendungen“



PHPIDS

PHPIDS kann mit seinen Features genutzt werden um eine IDS in die eigene Anwendung zu integrieren.

Web 2.0 / PHP / Worum geht es?

- XSS – Cross Site Scripting
- CSRF – Cross Site Request Forgery
- SQL Injections

▶ Zusätzliche Sicherheitsschicht

PHPIDS

- In PHP 5 geschrieben
- Ist ein Script, kein kompiliertes PHP-Modul
- Modular:
 - Eigene Klassen
 - Regeldatei
- Aktuelle Version: 0.4.6 vom 29. Januar 2008
- Lizenz: LGPL

Technische Voraussetzungen

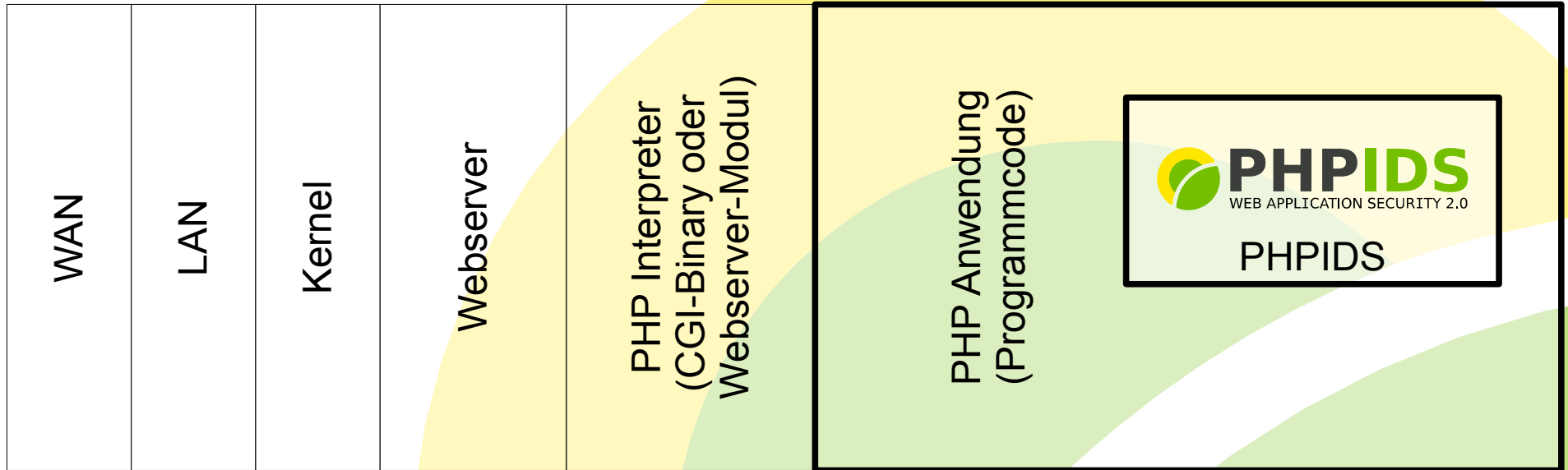
- PHP 5.1.6 oder höher
- LIBXML
 - getestet mit 2.6.21 und höher
 - LIBXML_COMPACT
- PHP PCRE mit Unicode-Unterstützung
 - Patch von *converter.php* möglich falls nicht

PHPIDS Integration

- Einsatz zur
 - Bewertung von Anfragen
 - Filterung von Daten – Frei nach Aschenputtel.
- Als Plugin für:
 - Typo3
 - Wordpress
 - Drupal

PHPIDS Verortung

Anfrage



PHPIDS Verortung (2)

- Schutz als Teil der eigenen Programmlogik
- Ein PHP Anwendungsentwickler kann sich PHPIDS in der eigenen Anwendungslogik zunutze machen.
 - Vergleichbar einem SPAM Filter mit eigener Bewertung (Bayesian).
 - Konträr zu MOD_SECURITY das vor der Anwendung liegt.

PHPIDS Verortung (3 und Schluss)

- IDS zielt auf Benutzereingaben
- Werte von Variablen werden bewertet
- API Beispiel (Auszug):

```
//initialize phpids
$init = IDS_Init::init('config.ini');
...

//starting phpids and fetch results
$request = array($_GET, $_POST);
$ids = new IDS_Monitor($request, $init);
$result = $ids->run();
```

Bewertung von Nutzereingaben

Ist eine Nutzereingabe „Gut oder Böse“? - Wie kann PHPIDS das Entscheiden?

- Methode 1: Impact
 - *dtsch. Der Einschlag*
 - *frz. Le impact*
- Methode 2: PHPIDS Centrifuge
 - *dtsch. Die Zentrifuge*
 - *frz. La centrifugeuse*

Methode 1: Impact

- RegEx Filter
- Bewertung jedes Treffers mittels seines numerischen „Impact Wertes“
- default_filter.xml / default_filter.json
- Prinzip Blacklisting
- Wichtig für die Bewertung der Wirksamkeit

Methode 2: PHPIDS Centrifuge

Generische Angriffserkennung

- Seit PHPIDS 0.4.1 September 2007
- Entstanden als Ergänzung zum Blacklisting
- RegEx kann manche komplexen Angriffsvektoren nicht erkennen
- Basierend auf eigenen Algorithmen, numerische Wertung
- Details im Whitepaper

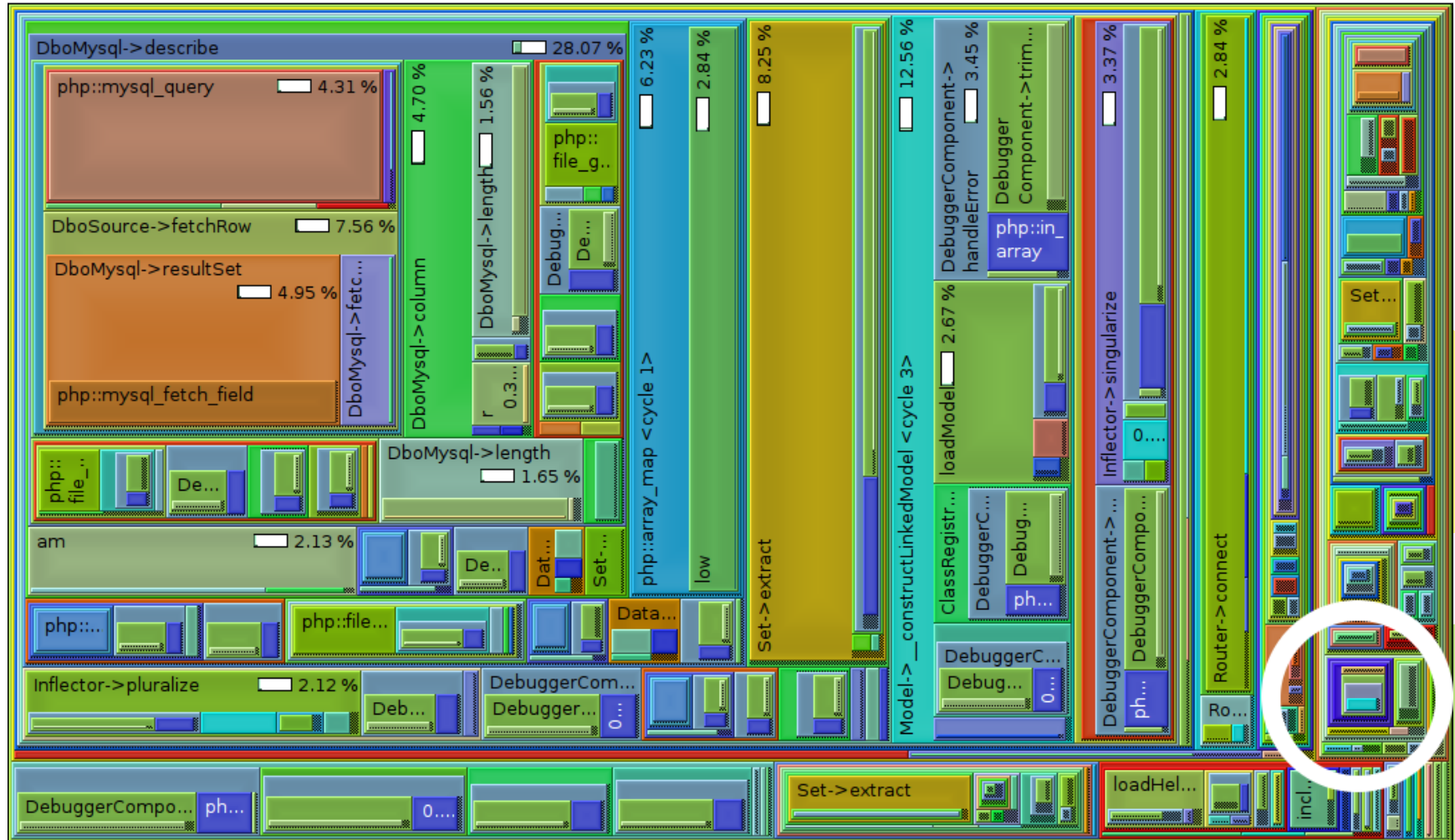
Filtern von Nutzereingaben

- PHPIDS selber filtert nicht - und das ist auch gut so.
- Gefiltert werden sollte immer nach eigener Anwendungslogik.
- Dazu kann das Result von PHPIDS genutzt werden.

Praxis

- Wird in Projekten im echten Leben eingesetzt
- Mit den aktuellen Regeln aus der SVN seit sechs Tagen keine False Alerts mehr (Stand 2008-02-14)

Praxis (2)



xdebug profiler output in KCachegrind from a real world CakePHP application - PHPIDS performance usage resides inside the white circle (~0.54%)

Praxis (3)

Smoketest auf der Projektseite

<http://demo.php-ids.org/>

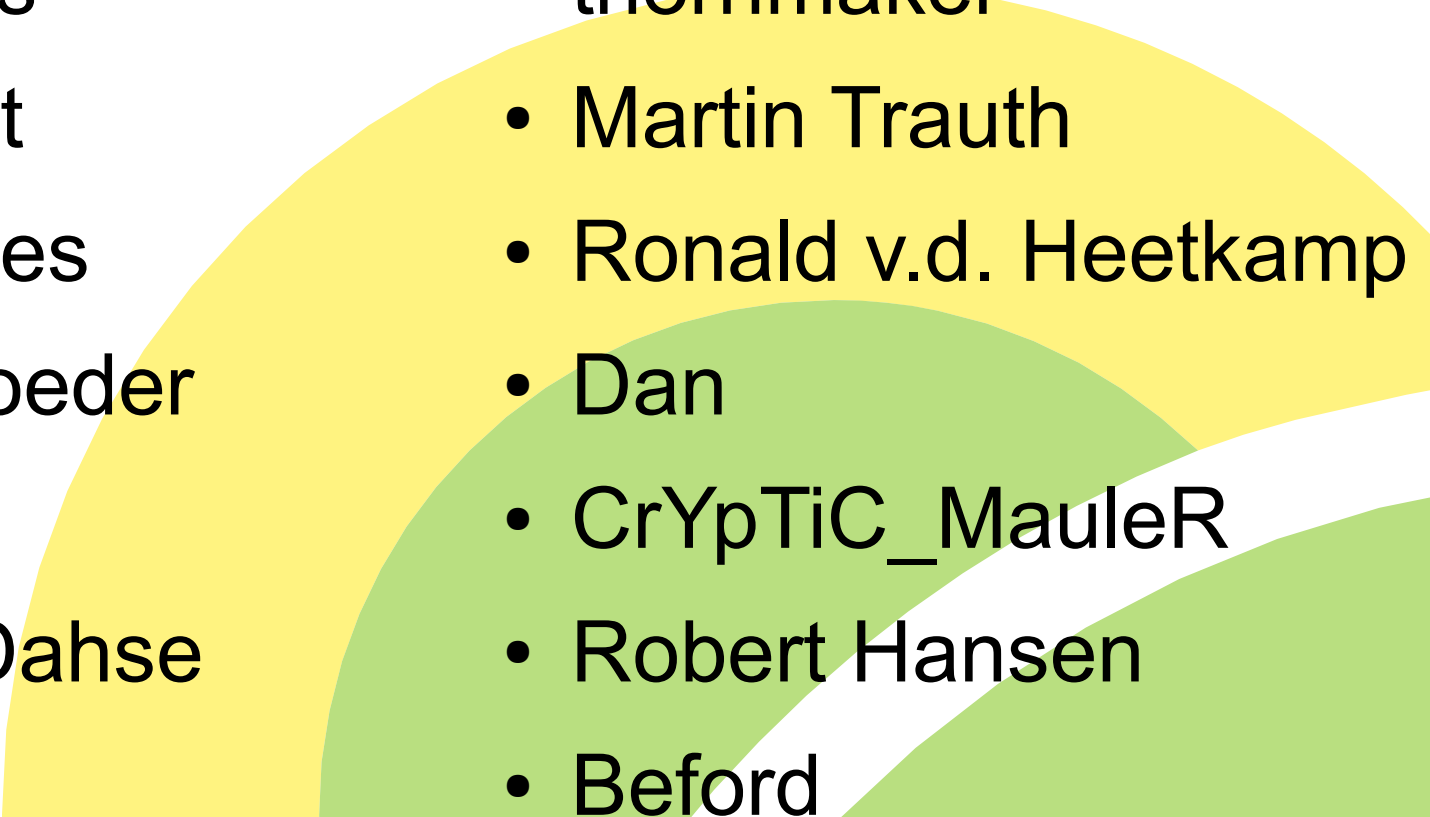
Wordpress Plugin auf der Usergruppen Seite

<http://phpugffm.de/>

Entwickler-Team

- Mario Heiderich <mario.heiderich@gmail.com>
- Christian Matthies <ch0012@gmail.com>
- Lars H. Strojny <lars@strojny.net>

Test / Hack / Contrib

- Kishor
 - Martin Hinks
 - SirDarckCat
 - Gareth Heyes
 - Kevin Schroeder
 - xorrer
 - Johannes Dahse
 - tx
 - Giorgio Maone
 - thornmaker
 - Martin Trauth
 - Ronald v.d. Heetkamp
 - Dan
 - CrYpTiC_MauleR
 - Robert Hansen
 - Beford
- 

Test / Hack / Contrib



... du ?!

Webadressen

- PHPIDS offizielle Webseite:
<http://php-ids.org/>
- PHPIDS Forum:
<http://php-ids.org/forum/>
- PHPIDS Google group:
<http://groups.google.de/group/php-ids/>
- Whitepaper:
In Vorbereitung

Dank

für die Aufmerksamkeit

und Danke an Mario für die Unterstützung!

Fragen?

LASTFLOOD®

Web & Applikation

Tom Klingenberg

<tklingenberg@lastflood.net>