

$$\frac{RSS}{n}$$


Search Dark Reading



<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>	<p>  </p>
--	--	--	--	---	--	--	--	--	--	--	--	--	---

[Home](#)  
[News & Commentary](#)  
[Authors](#)  
[Slideshows](#)  
[Video](#)  
[Radio](#)  
[Reports](#)  
[White Papers](#)  
[Events](#)  
[Black Hat](#)  
[SECURITY JOBS](#)

Analytics  
Attacks / Breaches  
App Sec  
Careers & People  
Cloud  
Endpoint  
IOT  
Mobile  
Operations  
Perimeter  
Risk  
Threat Intelligence  
Vulns / Threats

## Vulnerabilities / Threats



Kelly Jackson Higgins  
News

Directly



9 comments

[Comment Now](#)
[Login](#)

[f Like](#) 138 [t Tweet](#) [in Share](#) 302 [G+1](#) 53

## The Programming Languages That Spawn The Most Software Vulnerabilities

PHP, ASP Web scripting languages breed more vulnerabilities than Java, .NET programming platforms, Veracode's new state of software security report says.

The wave of WordPress and Drupal vulnerability warnings and patches over the past couple of years, as well as the never-ending discovery of SQL injection bugs in Web applications, can actually be traced back to their underlying scripting language -- PHP.

Some 86% of applications written in PHP contained at least one cross-site scripting (XSS) vulnerability and 56% came with at least one SQL injection bug, according to new research released today from Veracode, which studied applications written in the most pervasive programming languages -- PHP, Java, Microsoft Classic ASP, .NET, iOS, Android, C and C++, JavaScript, ColdFusion, Ruby, and COBOL. The data is based on its cloud-based scans and code analysis of more than 50,000 applications in the past 18 months.

Some 64% of applications written in Classic ASP and 62% of those written in ColdFusion had at least one SQL injection bug. Meantime, .NET and Java fare the best, with far fewer instances of security flaws in their applications: 29% of .NET apps and 21% of Java apps were found with at least one SQL injection bug.

Chris Wysopal, founder and CTO of Veracode, says PHP's problems are one of the reasons SQL injection -- one of the most abused yet easiest vulns to fix -- just won't die. "When I see a breach, one of the things that sticks out in my head is 'I'll bet that was a PHP site.'" Wysopal says. "What keeps some of these vulnerabilities alive and well is using languages that are harder to program securely.

"I had always suspected that scripting languages are worse. Now we have solid data to show we are getting twice the number of serious issues on those languages," he says.

It comes down to how these programming languages are designed, and their use. While Java and .NET have built-in functions to reduce the risk of buffer overflows, XSS, and SQL injection, PHP and ASP don't come as well-equipped and have fewer security APIs. According to [Veracode's report](#), it traditionally has been difficult to write apps in PHP that "bind parameters in SQL queries," making it more prone to SQL injection flaws.

"It's harder to program in those languages [scripting languages]. There are not as many built-in functions," Wysopal says. "And .NET and Java programs are typically used by computer science graduates who learned those languages in school. A lot of the scripting languages like ColdFusion and ASP came out of the Web dev world, where you're designing websites and starting to learn coding, [and] to make sites more interactive."

These languages also fail the OWASP Top 10: four out of five apps written in PHP, Classic ASP, and ColdFusion failed at least one of the application security standard's benchmarks. Veracode points out that this has a big impact on the Net overall, as some 70% of content management systems on the Web are PHP-based WordPress, Drupal, and Joomla. So "organizations seeking to use these CMSes should carefully plan their deployments," Veracode said in its report.

"If I put on my attacker hat and want to break into a site, I'm going to find PHP sites," Wysopal says.

Developers are basically stuck with the language and platform their organization chooses. "It's

not often that a developer gets to select that," he says. "They are kind of [limited] by the environment and language they need to build their applications on."

That's not to say they can't be better trained to write secure code. Veracode also studied vulnerability remediation rates, which showed a 30% improvement in vuln fixes in organizations that employ secure coding training for its developers.

### Mobile

Veracode also found mobile applications in both Android and iOS contain rampant cryptographic weaknesses. There isn't much daylight between Android and iOS app crypto bugs, either: some 87% of Android apps were found with the bugs, and 81% of iOS apps.

Wysopal says it came down to four issues: insufficient entropy or "randomness;" not checking SSL certificates; not encrypting sensitive information to disk; and using outdated crypto algorithms. "Developers are not understanding how to write crypto properly," he says.

*Kelly Jackson Higgins is Executive Editor at DarkReading.com. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise ... [View Full Bio](#)*

[Comment](#) | [Email This](#) | [Print](#) | [RSS](#)

### More Insights

#### Webcasts

How Technology Is Transforming Manufacturing

Operationalizing Threat Intelligence to Battle Persistent Actors

#### More Webcasts

#### White Papers

TCPA Compliance: Are you at Risk?

Solving Security Challenges in the Cloud

#### More White Papers

#### Reports

[InformationWeek & Dark Reading Report] 2015 Strategic Security Survey Results

Research: 2014 Strategic Security Survey

#### More Reports

### Comments

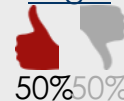
[Newest First](#) | [Oldest First](#) | [Threaded View](#)



[ryanwinchester](#),

User Rank: Apprentice  
12/10/2015 | 11:09:07 AM

[Login](#)



**Re: Developers get to choose their languages often**  
I'm self-taught PHP developer and even I know to use prepared statements.

These days, the only people who are writing insecure PHP are the people who don't care to. The language is not what it used to be.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[TerryB,](#)  
User Rank: Ninja  
12/4/2015 | 1:34:30 PM

[Login](#)  
   
50%50%

### Re: Developers get to choose their languages often

>>PHP is quite easy to develop secure applications in, you just need to know how to do it.

Based on this article, I'd say people as knowledgeable as you on PHP are in the minority. InfoWeek just had an article talking about hottest IT freelance jobs, PHP was at top of list. How many of these freelancers do you think know their stuff like you versus learned the language in a two year tech school (or self taught) because it was easier than learning Java?

PHP reminds me of RPG in the pre internet days, when COBOL ruled the world. RPG (Report Program Generator) was conceived to be a quick and dirty way to create reports on IBM servers, versus the verbose COBOL. But then people started writing complex CRUD apps with it, including entire ERP systems. You talk about some of the worst code you have seen (or tried to maintain) in your life.

PHP had similar origins. In the early days of HTTP apps, when security was an afterthought, it was intended to be a quick and dirty way of getting a CGI app created. Especially in UNIX world, which had no built in languages or databases. But then, as you say, people began building online banking/e-commerce sites with it, when security mechanisms were not even baked into the platform yet.

You'd like to think modern developers are all getting educated now on SQL injection and XSS exploits regardless of programming languages they use. But I suspect their focus is on producing working apps as they learn, not doing deep dives into the language features to verify they are secure.

I'll be honest, I use Sencha's Extjs and Touch now, though strictly for internal company use. But it never even occurred to me to research whether Extjs handled XSS, and how it did it. I did so after reading this article, even though in my use case I don't have to worry about XSS.



Always being a developer on IBM servers, I've always avoided using scripting languages like PHP and coding SQL statements for the database I/O. By using compiled programs and stored procedures at the backend, you completely eliminate the possibility of SQL injection, don't have to chase whether the "drivers" are protected against such exploits. The problem is, the UNIX world doesn't have such luxuries and the world wants to use cheap commodity servers and free databases with no integration with underlying o/s.

That makes things pretty tough on developers for those platforms. But glad to hear people like you that actually know what they are doing exist in PHP world. :-)

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[dawgbone,](#)  
User Rank: Apprentice  
12/4/2015 | 11:26:27 AM

[Login](#)  
   
50%50%

### Re: Developers get to choose their languages often

Except of course languages like PHP have come a long way in terms of having fixed these issues. The problem lies in the fact that many of the resources that exist out in the world are a). Old and b). Badly written.

For instance, PHP fixed SQL injection issues long ago with the PDO driver and prepared statements. One of the very first google results for "PHP insert into database" returns a tutorial using the deprecated mysql driver (and flat insert statments with no talk of

sanitization).

The one knock you can make on PHP in this is:

Why let people still use the mysql driver?

The good news is they finally have. It's now been completely removed in PHP7. The argument against removing it before was that while it took a lot of steps, it was possible to create secure applications using the mysql driver and breaking all of those wasn't a popular idea.

The biggest issue is that because there is so much content on the web on PHP, and a lot of it is massively out of date, we've had new programmers come in and create applications with security holes. PHP is quite easy to develop secure applications in, you just need to know how to do it.

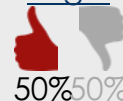
[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[kcisobderf](#),

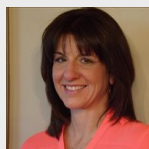
User Rank: Apprentice  
12/4/2015 | 10:21:10 AM

[Login](#)



Re: Developers get to choose their languages often  
Not hobbyist, H1-B. I agree with the rest of it, though.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[Kelly Jackson Higgins](#),

User Rank: Strategist  
12/4/2015 | 9:11:03 AM

[Login](#)



Re: Link Broken  
The link is now working--thanks!

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[RobThaBlob](#),

User Rank: Apprentice  
12/4/2015 | 8:17:02 AM

[Login](#)



Link Broken  
The link to the actual report is broken.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[ahetal](#),

User Rank: Apprentice  
12/4/2015 | 6:48:19 AM

[Login](#)



Re: Developers get to choose their languages often  
"PHP has shown no interest in revising aspects of their framework" - this is wrong in every sense. PHP is a language not a framework.



" they are designed to be used by the least-skilled programmers of all" - and this is applied to all the languages that are listed as the most safe of them all.

the lower you get in the coding level, the less safe the language becomes.

to me, the less safe of them all would be assembly.

you can do everything in assembly, thus, with more power comes more responsibility.

most of the guys I know who work with those "not safe" languages either are not experienced enough to do it, or they don't have the time to do it as it should be done. on the other side, if you use one of those "safe languages" "designed to be used by the least-skilled programmers of all", you don't have to worry about it.

problem is, almost nobody worries about it, no matter what language they work with.

and so we blame the language, not the poor coding. (fanboys love to do it.)

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[googlymoogly](#),  
User Rank: Apprentice  
12/3/2015 | 1:35:10 PM

[Login](#)  
   
100%

**Re: Developers get to choose their languages often**

ColdFusion has had the cfqueryparam tag for over a decade. It makes databinding easy. It makes addressing that aspect of sql injection easy. For it to not be used says nothing about ColdFusion. It does show that a lot of developers using it are off in their little bubble worlds and lacking essential technical skills.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[ajones980](#),  
User Rank: Strategist  
12/3/2015 | 1:19:10 PM

[Login](#)  
   
0% 100%

**Developers get to choose their languages often**

I'm not at all surprised by Veracode's findings - and the languages on the 'worst' list all have the same thing in common - they are designed to be used by the least-skilled programmers of all, and were initially targeted at hobbyist, or at least non-specialist, developers. They attract poorly-skilled developers and the results are predictable. But it's not just a marketing issue, it's also a question of how the language / framework owners react to security issues in their software. Classic ASP was written before Microsoft got religion about security - and was largely deprecated as a result of moving to a much more secure ASP.NET world. ColdFusion, I'm not familiar with, but hey, Adobe, right? Not the best reputation in town. PHP has shown no interest in revising aspects of their framework which make it difficult to securely develop.

I am surprised with the claim that developers don't get to choose the languages in which they develop - my experience is the polar opposite. Sure, they are initially hired to work with specific languages and frameworks that are already in use, but when a new project comes along, the first stage seems to be selection of the framework in which to develop it. And very often, those choices seem driven more by fashion / religion than by a comparison of the desired product's features and functionality and the framework's capabilities. Expect to see new unsecure PHP apps developed by the shovelful.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)

## Related Content

Sponsored by  Check Point  
SOFTWARE TECHNOLOGIES LTD.

### RESOURCES

### WEBINARS

### VIDEOS



#### Multi-Layered Defense for an Evolving Threat Landscape

ESG Analyst Jon Oltsik discusses the key elements of a defense-in-depth strategy to protect



#### What to Look for When Choosing a Sandboxing Solution

Featuring Insights from "Gartner's Market Guide for Network Sandboxing" to help you select your next sandbox.



#### NSS Breach Detection Systems Test Report

Real-world results from independent testing group NSS Labs evaluates today's leading sandboxing



#### Zero-Day Protection Redefined with SandBlast

Today's modern malware often utilizes sophisticated evasion techniques to avoid detection... can you defeat them?



#### Boston Properties - A Study in Defeating Unknown Malware

Discover how one of the largest developers and managers of office space protects their systems from advanced threats.



# CHECK POINT ONE STEP



## AHEAD

[LEARN MORE](#)

Check Point®  
SOFTWARE TECHNOLOGIES LTD.



[Subscribe to Newsletters](#)

Live Events

Webinars





More UBM Tech  
Live Events

Cloud Communications Track at  
Enterprise Connect 2016

Virtualization & Data Center Track at  
Interop Las Vegas

Interop 2016 Storage Track

## White Papers

- [TCPA Compliance: Are you at Risk?](#)
- [Where Efficiency Meets Compliance: Using Data To Drive Revenues And Reduce TCPA Risk](#)
- [Solving Security Challenges in the Cloud](#)
- [Threat Vectors: Are You Prepared?](#)
- [5 REASONS ENDPOINT SECURITY MUST MOVE TO THE CLOUD](#)

[More White Papers](#)

## Video



Cartoon



[All Videos](#)



"WE PROMISE ANONYMITY, TRUST, AND DISCRETION FOR YOUR RELATIONSHIPS. WE DIDN'T SAY ANYTHING ABOUT YOUR DATA."

Latest Comment: [At least they offer discretion for relationships :D](#)

[Cartoon Archive](#)

## Current Issue



### E-Commerce Security: What Every Enterprise Needs to Know

The mainstream use of EMV smartcards in the US has experts predicting an increase in online fraud. Organizations will need to look at new tools and processes for building better breach detection and response capabilities.

[Download This Issue!](#)

[Subscribe Now!](#)

[Back Issues](#) | [Must Reads](#)

[Flash Poll](#)

What's missing from your incident response plan? (Pick all that apply.)

- ☐ Access to activity logs
- ☐ An up-to-date network diagram
- ☐ Blueprint for public disclosure
- ☐ Hostname-IP address maps
- ☐ IR fire drills before the event

- ☐ Plan for finding malicious files after the breach
- ☐ We don't have an incident response plan
- ☐ Other (Please explain in the comments)

[Submit](#)[All Polls](#)[Slideshows](#)



## The Employee Password Habits That Could Hurt Enterprises

 1 comments | [Read](#) | [Post a Comment](#)

[Security Geek Gift Guide](#)

 2

[7 Elements Of Modern Endpoint Security](#)

 4

[More Slideshows](#)

### Twitter Feed



**Jean Paul Ballerini** @jpballerini

1h

The Jean Paul Ballerini Daily is out! [paper.li/jpballerini/13...](http://paper.li/jpballerini/13...) Stories via [@PaulemBidault](#) [@DarkReading](#) [@markjohnston\\_au](#)

[Show Summary](#)



**Unit 42** @Unit42\_Intel

9 Dec

[#Unit42](#) finds [#BackStab](#) Attack Takes Indirect Route To Mobile Data [bit.ly/1NKxiZm](http://bit.ly/1NKxiZm) [@DarkReading](#) [@ErickaChick](#)

 Retweeted by Enrique Pernas

[Show Summary](#)



**McAfee Labs** @McAfee\_Labs

5h

Intelligence sharing among security vendors is set to increase in 2016. More of our predictions, on [@DarkReading](#): [ubm.io/1UaaR5a](http://ubm.io/1UaaR5a)

 Retweeted by KunalVM

[Show Summary](#)



**Kimberly** @StopMalvertisin

3h

[@DarkReading](#) Hey, why a 403? [pic.twitter.com/HNtP6nEfou](http://pic.twitter.com/HNtP6nEfou)



### Bug Report

Enterprise Vulnerabilities  
From DHS/US-CERT's National Vulnerability Database

[CVE-2013-7445](#)

[Published: 2015-10-15](#)

The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...

[CVE-2015-4948](#)[Published: 2015-10-15](#)

netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.

[CVE-2015-5660](#)[Published: 2015-10-15](#)

Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.

[CVE-2015-6003](#)[Published: 2015-10-15](#)

Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.

[CVE-2015-6333](#)[Published: 2015-10-15](#)

Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID CSCuw46076.

## Dark Reading Radio

Archived Dark Reading Radio

[Millennials & The Cybersecurity Skills Shortage](#)

UPCOMING!

Monday, December 21, 1pm EST  
[The Cyber Security Year In Review](#)

[FULL SCHEDULE](#) | [ARCHIVED SHOWS](#)

InformationWeek  
**DARK**Reading

[About Us](#)

[Contact Us](#)

[Customer Support](#)

[Sitemap](#)

[Reprints](#)

[Twitter](#)

[Facebook](#)

[LinkedIn](#)

[Google+](#)

[RSS](#)



### UBM TECH BRANDS

Black Hat

Cloud Connect

Dark Reading

Enterprise Connect

Fusion

GDC

GTEC

Gamasutra

HDI

[Terms of Service](#) | [Privacy Statement](#)

Interop

Network Computing

No Jitter

Tower & Small Cell Summit

Copyright © 2015 UBM Tech, All rights reserved

<b>COMMUNITIES SERVED</b> Enterprise IT Enterprise Communications Game Development Information Security IT Services & Support	<b>WORKING WITH US</b> Advertising Contacts Event Calendar Tech Marketing Solutions Contact Us Licensing
--	--