Cobalt
Pen Testing as a Service

OWASP Top 10 is a Good Start. Now What?

By Caroline Wong

One of the most hotly debated topics in cybersecurity surrounds the simple question, "Have we gotten any better?" With the constant onslaught of new vulnerabilities, attack methods and near daily headlines warning of new threats to our most critical infrastructure or detailing the latest successful attack on confidential information, it can sometimes feel as though we are barely treading water, let alone actually moving forward.

In 1998, a group of hackers by the name of L0pht testified on Capitol Hill that computers were not safe. They argued that the internet would not get any safer because the people building the technologies that powered it had no incentive to care about security. Furthermore, the government lacked both the knowledge and the will to do anything about it. It was a dire warning that was somehow simultaneously ignored and quickly shown to be true. Within a few years of that testimony, their assertion became obvious to even the most casual computer users when worms like ILOVEYOU, Code Red and Nimda began to wreak havoc on email programs and computers around the world. Computer security could no longer be ignored - and even though we were quick to get excited about useful technologies like anti-virus, intrusion detection and firewalls, we always knew that any real improvement would require us to start building more secure software. In fact, one of the first impactful responses to the onslaught of disruptive security events in the late 90s/early 2000s was Bill Gates' now famous 2002 Trustworthy Computing memo directing Microsoft to focus on building more secure and trustworthy products. Application security has been a part of cyber security from our industry's beginning. And so it is fair to ask "have we gotten any better?"

The Inception of the OWASP Top 10

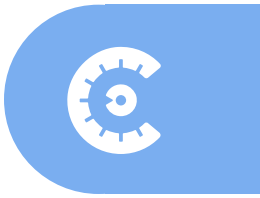
A few years after the Trustworthy Computing memo, the Open Web Application Security Project (OWASP) began publishing the OWASP Top 10, a list of common security risks found in web applications. Originally released in 2004 and updated every few years since, OWASP began publishing the list as a way to educate the development community about application security risks.

Over time, the OWASP Top 10 has arguably evolved into the most well known de facto application security benchmark. As such, whenever a new version is released, it is often a flashpoint for discussion on whether or not application security is improving.

> The most recent version of the OWASP Top 10 was published in October 2017 and is notable for the large amount of community input that went into shaping the list. The top 10 application security risks were selected and prioritized based not only on their prevalence, but also a consensus estimate of their risk by the project's volunteer contributors who considered each issue's exploitability, detectability and impact. Early versions of the 2017 OWASP Top 10 generated substantial feedback from application security experts, which ultimately shaped its final publication. Further, the 2017 list was based on a much larger data call than prior versions. This included over 40 data submissions from firms that specialize in application security, as well as an industry survey that was completed by more than 500 individuals. According to OWASP, this data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real-world applications and APIs.

OWASP has updated the Top 10 just about every three years since its 2004 release. With each new version, what is often most striking to many experts is how little the list meaningfully changes over time. Its most recent release in 2017 was no different and the newest top 10 risks are for the most part very familiar. We are still finding largely the same types of vulnerabilities and they are still being successfully exploited to compromise systems. On the surface, this would seem to tell us that our progress has been stagnant. And yet, in speaking to many who have been on the front lines in application security for a long time, it appears there may be more to the story.

In fact, application security professionals are reporting progress within their companies. Many organizations have invested in secure development education and training, and some are being rewarded with higher levels of engagement in security from their engineering teams. We're also seeing increasing levels of executive support for appsec programs as awareness of the importance of software security has grown in recent years. Industry organizations like OWASP and the Software Assurance Forum for Excellence in Code have been widely sharing free tools, resources and lessons learned from companies like Microsoft that have a long history of working on software security problems.



OWASP Top 10 -2013		OWASP Top 10 -2017
A1 - Injection	→	A1: 2017 - Injection
A2 - Broken Authentication and Session Managament	→	A2: 2017 - Broken Authentication
A3 - Cross-Site Scripting (XSS)	↘	A3: 2017 - Sensitive Data Exposure
A4 - Insecure Direct Object References [Merged +A7]	U	A4: 2017 - XML External Entites (XXE) [NEW]
A5 - Security Misconfiguration	↘	A5: 2017 - Broken Access Control [Merged]
A6 - Sensitive Data Exposure	↗	A6: 2017 - Security Misconfiguration
A7 - Missing Function Level Access Contr [Merged +A4]	U	A7: 2017 - Cross-Site Scripting (XSS)
A8 - Cross-Site Request Forgery (CSRF)	X	A8: 2017 - Insecure Deserialization [NEW, Community]
A9 - Using Componentrs with Known Vulnerabilities	→	A9: 2017 - Using Components with Known Vulnerablities
A10 - Unvalidated Redirects and Forwards	X	A10: 2017 - Insufficient Logging & Monitoring [NEW, Comm.]

Has the Application Security Industry Improved?

So “have we gotten better?” It seems it depends on where you sit. And if you are an application security professional, you are sitting in a place central to the improvement of the security of applications within your specific organization. Of course industry engagement and progress is important, but it is what happens within your four walls that is critical.

The OWASP Top 10 is an excellent awareness and education effort, and a useful resource that can help you assess and understand the security challenge in front of you. But it was never designed to be a simple checklist for a once-a-year vulnerability scan or a complete risk assessment for any individual organization. In our Pen Testing as a Service (PTaaS) work with clients, we also find that the OWASP Top 10 vulnerabilities are some of the most prevalent.

This tells us that all companies should at least be looking for the OWASP Top 10 on a regular basis.

Cobalt Top 10 Finding Types (2017)	OWASP Top 10 -2017
Misconfiguration	A1: 2017 - Injection
Cross-Site Scripting (XSS)	A2: 2017 - Broken Authentication
Authentication and Sessions	A3: 2017 - Sensitive Data Exposure
Sensitive Data Exposure	A4: 2017 - XML External Entites (XXE)
Missing Access Control	A5: 2017 - Broken Access Control
Cross-Site Request Forgery (CSRF)	A6: 2017 - Security Misconfiguration
Components with Known Vulnerablities	A7: 2017 - Cross-Site Scripting (XSS)
Insecure Object References	A8: 2017 - Insecure Deserialization
Redirects and Forwards	A9: 2017 - Using Components with Known Vulnerablities
SQL Injection	A10: 2017 - Insufficient Logging & Monitoring

**Data from Cobalt's pen testing as a service platform, based on 250+ pen tests conducted in 2017

But frequency of occurrence doesn't tell the whole story. Recognizing this, OWASP does not rely solely on prevalence data, but also an assessment by security experts of risk. They seek to determine how exploitable the issues are, if they are defensible, and the potential impact of their compromise. This is how they determine which security issues are plaguing web applications across industries. Manual penetration testing can do the same thing, but at the organizational level. The key to doing so is applying metrics to your pen testing and application security efforts. This amplifies the value of your penetration testing results and provide the decision support necessary for doing things better in the future.

The OWASP Top 10 contains a list of common web application security risks, however each organization will have its own unique "Top 10" list. **If you know what yours is, you can and should use this information to eliminate entire categories of security vulnerablities** by putting into place focused developer training, writing custom static code analysis rules, integrating tests for these types of security vulnerablities into QA testing, etc.

Goal	Prioritize remediation of security defects
Question	What types of security vulnerablities were found in the most recent penetration test? What's the category with the greatest number of instances found? What's the category with the next greatest number of instances found?
Metric	Count the number of security defects of each vulnerabulity type

For more information on applying metrics to your penetration testing program, download Cobalt's 2018 Pen Test Metrics report

One of the major benefits of manual pen testing is that it doesn't give you just information on what vulnerabilities exist, but also can prove how exploitable they are and which assets they endanger. Looked at over time, manual pen test results can help an organization identify which types of security issues are creating the most risk in its unique environment. For some organizations, this may mirror the OWASP Top 10. For others, they may find their own Top 10 differs.

Once you identify your organization's Top 10, the real effort begins.

Determining your Organization's Top 10 Vulnerabilities

If a high risk security issue shows up often enough that it is endemic to an application, an organization should consider implementing a focused effort on reducing that issue earlier in the development process. Some issues may be resolved with a change in design. Others may require a focused training and education effort for all or parts of the product development team. An organization may identify a need to tweak its static analysis tools or invest in in new automated testing tools. Some issues may be caught earlier by directing peer review teams or quality control to look specifically for the issue's appearance and flag it for engineers. While these are common strategies, targeting a particular security issue that is endemic to your organization requires an approach tailored to your organization's culture.

There are a number of free and useful industry resources to help organizations of all sizes initiate or improve their application security programs. OWASP offers advice on preventing each of the Top 10 security risks within the OWASP Top Ten publication itself. Its website also offers free resources on secure development techniques. SAFECode is another non-profit industry organization that offers both free secure development program advice and free training modules for products teams.

So let's make a challenge out of it. The goal is to make more progress reducing the frequency and risk of the Top 10 security issues that your organization has identified as the ones most plaguing your company's applications. If your organizational top 10 list changes more than the next version of OWASP Top 10 list, you win. Here is how to get started:

1. If you are not looking for the OWASP Top 10 in your manual pen testing or vulnerability scanning programs, start today.

2. Once you find security issues, use the OWASP Top 10 to help your organization begin to classify found security issues and rate their risk in your organization. Track this data and use it to start to identify the risk patterns in your organization. Finding numerous security issues outside the Top 10? Great, classify them as well and rate their risk and add them to your own list.

3. Using this data, build your company Top 10. You may find it aligns closely with the OWASP Top 10 or you may find the list differs. The important thing is only to try to identify which security issues are creating the most risk for your applications.

4. Tackle the list. Implement a strategy to eliminate or greatly reduce the prevalence of your most critical risks.

5. Measure your progress over time. Is your list changing over time?

6. At the next OWASP Top 10 release, will you be able to show progress on your Top 10? If so, go ahead and brag to your management team - your application security programs are working.

It's impossible to completely eliminate all risk and vulnerabilities in software. However, you can stop playing whack-a-mole and begin a more a strategic metrics-based approach to reducing the biggest risks to your application security. The first step is to identify what security issues are creating the most risk in your organization. The OWASP Top 10 provides a great starting point for creating an organizational benchmark and tracking progress over time. But it is only a starting point. The list won't change if we don't.

About the Author

Caroline Wong is the Vice President of Security Strategy at Cobalt.

Wong's close and practical information security knowledge stems from broad experience as a Cigital Consultant, a Symantec Product Manager, and day-to-day leadership roles at eBay and Zynga. She is a well-known thought leader on the topic of security metrics and has been featured at industry conferences including RSA (USA and Europe), OWASP AppSec and BSides.

Wong authored the popular textbook Security Metrics: A Beginner's Guide, published by McGraw-Hill in 2011. Wong graduated from UC Berkeley with a BS in electrical engineering and computer sciences and holds a certificate in finance and accounting from Stanford University Graduate School of Business.