Application Security Trends

SQL injection, cross-site scripting, command injection, and cryptographic errors are still wreaking havoc on web applications.

Hewlett Packard Enterprise

Web applications continue to provide an attractive target for malicious attackers looking for an entry point to enterprise systems and data. Well-understood vulnerabilities like SQL injection, cross-site scripting, command injection, and cryptographic errors continue to be rampant in web applications despite a heightened awareness of the threat they pose to enterprise security. Some of these issues, like SQL injection and cross-site scripting flaws, have been around almost as long as the web itself but continue to pose major problems for organizations.

A full 48% of web applications in 2014 that HPE reviewed for its Cyber Risk Report 2015[1] had cross-frame scripting vulnerabilities, 47% had a privacy violation error, while 45% were prone to cookie security issues. The HPE report also showed that 68% of all reported web application vulnerabilities resulted from inadequate input validation.

Over the years, threat actors have looked for and exploited these vulnerabilities with devastating effects. Common attacks have included those that redirect website visitors to malicious sites, escalate privileges, send malicious code and scripts, read data from databases, or modify database data.

The situation could get worse. Data gathered by Verizon for its 2015 Data Breach Investigations Report[2] showed that organized crime groups attacked web applications more frequently than any other threat actor.

Concerns over web application security have pushed organizations like the PCI Security Standards Council to require covered entities to implement specific controls for mitigating the risk posed by vulnerable applications.

PCI rules require all organizations that handle credit or debit card data to do application code reviews and, in many cases, implement a web application firewall for protecting web applications handling payment card data. The rules leave it largely up to the covered entities to decide if they want to do a manual source code review or use automated scanning tools to look for and remediate any web application vulnerabilities.

PCI rules also recommend that organizations put controls in place to detect and prevent tampering of session tokens and to automatically receive signature updates from application vendors.[3]

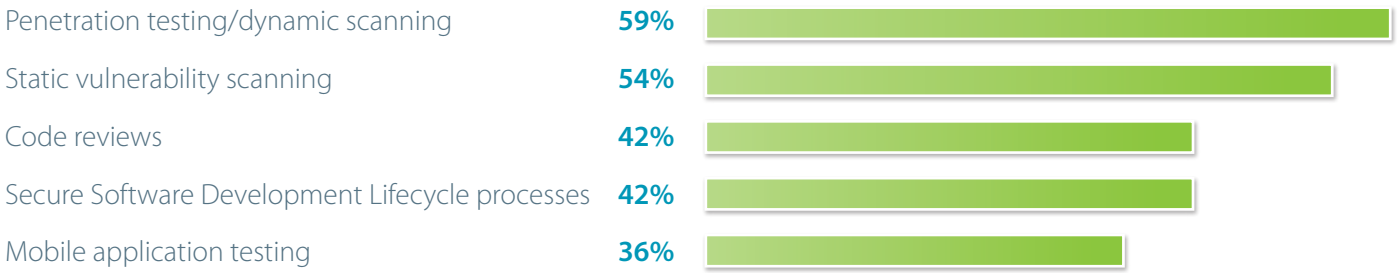
Multiple tools and approaches are available to enterprises to mitigate application security issues. Examples include penetration testing and dynamic scanning of production code, static vulnerability scans of code in development and testing, code reviews, and runtime application self-protection tools.

Implementing a secure software development practice, where security is an integral part of the application development life cycle and not treated as an afterthought, can help mitigate common application security errors over the longer term.

Responses to the UBM Tech survey show that many organizations are already taking application security measures in one form or another. Only 14% of the respondents admitted to not taking any web application security precautions at all.

Dynamic scanning appears to be the most commonly used method for testing application security, with 59% of the respondents saying they have implemented the measures. Static vulnerability scanning is used by 54%, while code reviews and secure software development practices each garnered 42%.

The results of the UBM survey are somewhat similar to the results of a survey conducted by the SANS Institute on the continuous monitoring practices of enterprises.[4] That survey showed that 38% of organizations conduct



↑ Which of the following application-level security products and controls has your organization implemented?

Note: Multiple responses allowed

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

web application vulnerability scans on a weekly or better basis, while 13% have implemented a continuous monitoring capability. When respondents were asked the top three categories of vulnerabilities they discovered most frequently as a result of these scans, they quite expectedly pointed to cross-site scripting, privilege escalation, and information disclosure flaws.

The numbers suggest that a fair number of organizations have implemented measures to address web application security issues. But many are lagging in their efforts. For example, if 59% in the UBM survey are doing penetration tests and dynamic scans, it calls into question why 41% of the respondents aren't taking such measures. Similarly, 58% are not doing either code reviews or secure software development. So while a majority of organizations in total are taking at least some measures to mitigate app security vulnerabilities, not many appear to have implemented multilayered protections around web apps.

Part of the problem could be budget. When asked what proportion of their IT security budget is spent on application security, 37% in the UBM survey said less than 10% while 32% said the amount hovered between 10% and 20%. On the positive side, a substantial 45% said their organizations plan to spend more on application security in the next 12 months, while 30 percent expect their budgets to remain the same.

45%

The percentage of organizations that plan to spend more on application security in the next 12 months.

In addition to limited budgets, a lack of management buy-in and skilled resources appear to be posing a big challenge to better web application security at many organizations. A relatively high 58% of survey respondents said their efforts to launch new application security initiatives or improve upon existing ones were being hampered by a lack of support from management. Fifty-five percent blamed the situation on a lack of skilled manpower.

It's actually somewhat surprising that this number isn't even higher. A recent Forbes study[5] on the cybersecurity industry's market size and employment statistics showed that more than 200,000 cybersecurity jobs in the US are currently unfilled because of a dearth of security skills. By 2019, the number of unfilled jobs is expected to reach a staggering 1.5 million.

[1] *http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/*

[2] *http://www.verizonenterprise.com/DBIR/2015/*

[3] *https://www.pcisecuritystandards.org/*

[4] *https://www.sans.org/reading-room/whitepapers/analyst/vulnerabilities-survey-continuous-monitoring-36377*

[5] *http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/*