



State of Web Application Security

Executive Summary

Sponsored by Cenxic & Barracuda Networks

Independently conducted by Ponemon Institute^{LLC}

Publication Date: February 2011

State of Web Application Security Executive Summary

Presented by Ponemon Institute, February 2011

Ponemon Institute is pleased to present the findings of the *State of Web Application Security* study sponsored by Cenxic and Barracuda Networks. We surveyed 637 IT and IT security practitioners in a variety of industries with an average of 11 years experience in their profession.

The survey focused on the following issues:

- The importance of securing Web-facing applications
- What organizations are doing to augment and secure Web applications
- Perceptions about the use of Web application firewalls (WAFs)
- What organizations are doing to test the vulnerabilities of Web applications

Web applications are vulnerable to hundreds of threat vectors. According to OWASP's Top 10 Web Software Application Security Risks, SQL injection flaws are considered the most critical Web application security risks for organizations followed by cross-site scripting (XSS) flaws. Other serious vulnerabilities include session management, privilege escalation, and cross-site request forgery among many. Some of the consequences from injection flaws include data loss, corruption, denial of access or complete host takeover. Cross-site scripting could allow an attacker to hijack a user's session or deface Websites.¹

The IT practitioners in our study agree that it is important to reduce the risks caused by these threats. According to the findings, 74 percent of respondents believe Web application security is either more critical or equally critical to other security issues faced by their organizations. When asked what the economic impact would be if they had a hacker attack, 25 percent of respondents have no idea. Almost half (47 percent) estimate it can range from \$100,000 to \$500,000 and the average is \$255,000. IT practitioners recognize attacks can be costly due to the potential for the loss of sensitive data, fines due to noncompliance with regulations and business disruption.

Given both the importance of Web application security and the potential for significant economic loss, are the organizations represented in our study taking the necessary measures to protect their Web applications? As shown in this study, only a small percentage of respondents test their Web applications for vulnerabilities. This lack of testing could be attributed in part to the fact only 12% strongly agree that they have ample resources to detect and remediate insecure Web apps.

There are other indications that the state of Web application security is dismal. While 73 percent of the organizations in the study have been hacked at least once in the last 24 months, 72 percent of the respondents test less than 10 percent of their applications. The reasons for this are a lack of budget and expertise.

To make matters worse, 64 percent do not agree that their organization is able to fix Web application vulnerabilities quickly. In fact, 88 percent of respondents say their Web application security budget is less than the organization's coffee budget (about \$30 per employee per month). Sixty-seven percent say it is less than the budget for network security and 51 percent say it is less than the budget for database encryption.

Following is a summary of key findings according to the following themes: Perceptions and concerns about Web application security, methods and standards used to secure Web applications and why the state of Web application security in organizations is at risk.

¹ "Injection Tops List of Web Application Security Risks, Angela Moscaritolo, SC Magazine, April 19,2010

Part 1. Key Findings

Perceptions and concerns about Web application security

Web application security is considered critical. Forty-three percent of respondents say Web application security is equally critical to other security issues faced by their organization and 31 percent say it is more critical. However, only 36 percent say their IT organization has adequate governance and policies over the use of insecure Web applications by end-users across the enterprise and the same percentage say their organizations fix Web application vulnerabilities quickly and efficiently.

Hacks through Websites are the # 1 concern. When asked what type of hacker attack concerns them most, respondents ranked hacks through Websites followed by hacks at the network layer and hacks through desktops, laptops or other connected devices. Fifty-three percent believe it is the responsibility of the Web-hosting provider to secure their organization's Web applications.

Data protection and compliance are the most important reasons for securing Web applications. The top three reasons for securing Web applications are data protection, compliance with regulations and business disruption. The primary means for securing Web-facing applications are network firewalls, reverse proxy and internal pen testing. Other popular tools are Web application firewalls (WAF) and intrusion prevention systems (IPS). Network firewalls are the most popular method used to augment and secure Web applications, which shows a severe lack of knowledge about Web application security.

Attacks on an organization's Web applications can be costly. When asked what the economic impact would be if they had a hacker attack, 25 percent have no idea. Almost half (47 percent) estimate it can range from \$100,000 to \$500,000 and the average is \$255,000. IT practitioners recognize attacks can be costly due to the potential for the loss of sensitive data, fines due to noncompliance with regulations and business disruption.

Methods and standards used to secure Web applications

The majority of WAF users in our study (41 percent of all respondents) consider a full reverse proxy WAF to be more secure. WAF users and the overall sample who believe the reverse proxy WAF is more secure, say it is so because of session termination and reconstruction followed by the ability to scan uploaded documents for malware before they hit the Web application and ICAP connections for incorporating data loss prevention systems.

WAF users consider this method as necessary or critical for their organizations' security infrastructure. Eighty-five percent of WAF users consider this method as critical. In contrast, only 29 percent of the overall sample believes WAFs are critical and 40 percent are uncertain. This result suggests there is a great deal of unfamiliarity with WAFs.

Further, 68 percent of WAF users consider a fully functional WAF as one that optimizes both performance and security. Less than one-third of respondents in the general sample believe this is the case and 43 percent are unsure. This suggests that there is uncertainty about the capabilities and value provided by WAFs. Those respondents who say that a fully functional WAF optimizes both performance and security are almost evenly divided about whether security or performance is more important. Forty-four percent say security is more important and 40 percent say performance is more important.

NIST, SANS 25 and CWE are the top three standards used in the organizations' Web application security. Almost half of respondents (49 percent) say their organization applies NIST standards followed by 39 percent who apply SANS 25 and 29 percent who apply CWE. In the case of OWASP, more than half (57 percent) of respondents are very familiar or somewhat familiar with OWASP organization and principles which is very surprising given that it's the only

non-profit organization focused entirely on Web application security. Of those who are very familiar or familiar with OWASP, 35 percent apply them and 30 percent are unsure.

Why the state of organizations' Web application security is insecure

Only a small percentage of Web applications are tested for vulnerabilities. As mentioned above, 53 percent of respondents agree that they expect Web applications to be secured by the Web hosting provider. That could explain why a small percentage of Web applications are being tested for vulnerabilities. Twenty percent do not test and 40 percent test only 5 percent of their Web applications. The extrapolated average for all Web applications that are being tested by organizations in our study is estimated to be 13 percent. The main reasons for not testing their Web applications are a lack of budget and expertise.

IT organizations' budget for Web application security is less than what it spends on coffee for its employees. Eighty-eight percent of respondents say the coffee budget is bigger (about \$30 per employee per month) and 67 percent say it is less than the budget for network security. Yet, we estimate from the responses that one attack could cost the organization an average of \$255,000.

Web application vulnerability scanning is the most popular method for testing. Forty-nine percent of respondents use this method followed by managed service (19 percent). Proprietary apps and outsourced apps are the categories most often tested. More than half (56 percent) test their Web applications in development and 54 percent test them in testing and quality assurance venues. Only 13 percent test their applications in production.

Organizations are at risk because many Web application vulnerabilities when discovered are not fixed. Or, if they are fixed it can take months. Sixty-four percent of respondents say their organizations have been hacked through insecure Web applications between 1 and 10 times in the past 24 months. However, 20 percent do not know.

Twenty-one percent of respondents do not know how long it takes to fix a single Web application vulnerability. The extrapolated average for all organizations participating is more than two months (68 days).

On average, organizations are devoting approximately 24 percent of their information security efforts to fixing the vulnerabilities of insecure Web applications. The controls in place to protect their Web infrastructure until the Web apps are secure include network firewall, manual process and WAF.

Part 2. Conclusion

We believe the research findings show that the state of Web application security is bleak and requires an immediate response from organizations. While companies and government agencies are constantly being hacked through the Websites, minimal efforts are being made toward securing these websites.

Factors contributing to the insecurity are a lack of budget, expertise and governance procedures. As a result, Web application vulnerabilities are not fixed quickly. According to IT practitioners in our study, 21 percent do not know how long it takes to fix one vulnerability and 6 percent say they are never able to fix these vulnerabilities. Decisions to fix Web application vulnerabilities are made informally (46 percent of respondents) or there is no effort to prioritize (29 percent).

We hope this study creates awareness of a security problem that could have serious financial and reputational consequences for organizations. On a positive note, IT practitioners seem to be aware of the threats to their Web applications. The next step is to convince management to consider making Web application security as important as the coffee budget.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.