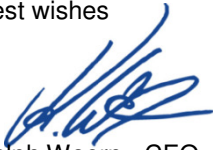


Dear reader,

the OWASP Top Ten provides a powerful awareness document for web application security and is used as basis for the PCI-DSS standard requirements 6.3.7b, 6.5, 6.6 and 11.3.2. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. The OWASP Top Ten was first released in 2003, updates were made in 2004 and 2007, and now the 2010 release has been published.

To help you to consider the changes caused by the new OWASP Top Ten for your audit preparation we have summarized in this newsletter the basic information so that you can inform yourself easily about the changes and how your organization is affected by this changed OWASP set in regard to PCI DSS. This information will provide you with a brief overview of the OWASP changes, for more information please download the detailed document from www.owasp.org.

Best wishes



Ralph Woern - CEO

+++ PCI Council publishes OWASP Top Ten +++

Why are these changes important for you?

For you as a company interested in PCI certification and compliance it is important that you adapt your processes and development regarding PCI certification to this new release. This is due to PCI-DSS requirement 6.5 (regarding software development and documentation), which requires the use of the most actual OWASP Top Ten to match the PCI requirements. Furthermore the PCI-DSS requirements 6.3.7b (regarding code reviews), 6.6 (regarding external code reviews and application firewalling) and 11.3.2 (regarding penetration testing) are affected by this change of the OWASP Top Ten.

What has changed?

First of all, the OWASP Top 10 is now based on risk, not on most common weaknesses as they were before. To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization. Together, these factors determine the overall risk. On the first glance, you will notice that the ordering of the topics has changed. When looking closer you will see that two new issues have been added and two issues dropped from the list.

Which details are of special interest?

- A6 (new) – "Security Misconfiguration". This issue was A10 in the OWASP Top 10 from 2004, named "Insecure Configuration Management", but was dropped in 2007 because it wasn't considered to be a software issue. However, from an organizational risk and prevalence perspective, it clearly merits re-inclusion in the Top 10; so now it's back: Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application. We are sure that you are still testing and validating your configurations before deploying them into the production environment, but in preparation for your next audit double check that all configuration changes are treated and documented accordingly as required by PCI-DSS.
- A10 (new) – "Unvalidated Redirects and Forwards". This issue is making its debut in the Top 10. The evidence shows that this relatively unknown issue is widespread and can cause significant damage. Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages. For this reason adapt your software development and validation processes to include validation of all Forwards and Redirects you use on your web application.

Two topics have been removed from the list, even when they are still important, so do not underestimate them regarding the security risk posture of your company:

- A3 (previous) – "Malicious File Execution". This is still a significant problem in many different environments. However, its prevalence in 2007 was inflated by large numbers of PHP applications having this problem. PHP now ships with a more secure configuration by default, lowering the prevalence of this problem.
- A6 (previous) – "Information Leakage and Improper Error Handling". This issue is extremely prevalent, but the impact of disclosing stack trace and error message information is typically minimal. With the addition of Security Misconfiguration this year, proper configuration of error handling is a big part of securely configuring your application and servers.

Summary

So, summarizing, for your next PCI onsite assessment make sure that you have all according processes and documentation prepared accordingly to these changed requirements, which are now part of the current PCI set of requirements.

Imprint

Acerigo AG
Wilhelmsplatz 8
70182 Stuttgart (Germany)
+49 (0)7 11/6 20 30-300
Residence:
Stuttgart - Amtsgericht Stuttgart HRB 724100.

Executive Board: Ralph Woern, Dr. Stephan Engelke

Editorial:
Christina Wolf
christina.wolf@acerigo.com