Look at the top 10 web application security risks worldwide as determined by the Open Web Application Security Project. Then discover how IBM Security AppScan helps website administrators find, correct, and avoid these and other web security threats.

The Open Web Application Security Project (OWASP) is an international organization dedicated to enhancing the security of web applications. As part of its mission, OWASP sponsors numerous security-related projects, one of the most popular being the Top 10 Project. This project publishes a list of what it considers the current top 10 web application security risks worldwide. The list describes each vulnerability, provides examples, and offers suggestions on how to avoid it. The most recent version of the top 10 list, officially published in June 2013, updated the 2010 list. The 2013 Top 10 list is based on data from seven application security firms, spanning over 500,000 vulnerabilities across hundreds of organizations. OWASP prioritized the top 10 according to their prevalence and their relative exploitability, detectability, and impact.

As a further aid in understanding some of these vulnerabilities, the IBM Security Systems Ethical Hacking team has prepared the following videos.

#1 Injection
Warren Moynihan defines injection and lists a few of the many examples of it. He then provides a detailed example of how injection techniques might be used by a hacker to gain access to otherwise protected data. Finally, he illustrates how you can use IBM Security AppScan to find and eliminate this vulnerability.

To view this video, **OWASP top 10 vulnerabilities: #1 Injection**, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

#2 Broken authentication and session management
Broken authentication and session management is one of the most commonly exploited web vulnerabilities. Brennan Brazeau explains how non-secure credentials practices and inadequate
session management techniques let attackers gain access to web applications. He also illustrates how you can use AppScan to identify these potential problems.

To view this video, **OWASP top 10 vulnerabilities: #2 Broken authentication and session management**, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

**#3 Cross-site scripting**

In this video, Security Systems' Moynihan describes how hackers use cross-site scripting (XSS) to send malicious code to websites. He demonstrates techniques that are used to exploit this common vulnerability, and shows how IBM Security AppScan searches for and identifies XSS vulnerabilities on an example website.

To view this video, **OWASP top 10 vulnerabilities: #3 Cross-site scripting**, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

**#4 Insecure direct object reference**

Websites often require users to provide values for their applications' parameters. If these values are not properly vetted, hackers can use them to pass malicious commands to the site. Here, Jonathan Fitz-Gerald demonstrates a possible attack and how you can use AppScan to identify vulnerabilities of this type.

To view this video, **OWASP top 10 vulnerabilities: #4 Insecure direct object reference**, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

**#5 Security misconfiguration**

Misconfigured web servers provide hackers with opportunities to abuse websites. In this video, Paul Ionesco shows how attackers take advantage of testing or debugging features carelessly left enabled. The "least privilege" principle is recommended as a method to mitigate the risk, and AppScan is shown to be effective in seeking out examples.

To view this video, **OWASP top 10 vulnerabilities: #5 Security misconfiguration**, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

**#6 Sensitive data exposure**

John Zuccato reviews the sensitive data exposure vulnerability. Unencrypted data in transport can be vulnerable to attackers listening in on a connection. For example, unencrypted data stored on a server might be at risk through an SQL injection attack. As with other vulnerabilities, AppScan helps identify potential problems.

To view this video, **OWASP top 10 vulnerabilities: #6 Sensitive data exposure**, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.
#7 Missing function level access control

Here, Zuccato examines missing function level access control, occurring when a lower-level-access user is inadvertently allowed access to a part of a website restricted to higher-level access. Administrators who elect to "hide" functions instead of protecting their applications at the function level can create these vulnerabilities. You can use AppScan's "Privilege Escalation" test to find them.

To view this video, OWASP top 10 vulnerabilities: #7 Missing function level access control, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

#8 Cross-site request forgery

Cross-site request forgery (CSRF) is currently ranked #8 on the OWASP top 10 chart and is a commonly exploited vulnerability. Cross-site request forgery is a web application vulnerability that makes it possible for an attacker to force a user to unknowingly perform actions while they are logged into an application. Attackers commonly use CSRF attacks to target cloud storage, social media, banking, and online shopping sites because of the user information and actions available in those types of applications. In this video, a member of the IBM Security Systems Ethical Hacking team explains the vulnerability, explores the risks, tells you how to protect your web applications from the attack, and demonstrates how AppScan Standard discovers the vulnerability.

To view this video, OWASP top 10 vulnerabilities: #8 Cross-site request forgery, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

#9 Using components with known vulnerabilities: Heartbleed and Shellshock in action

Using components with known vulnerabilities is currently ranked #9 on the OWASP top 10 chart. Heartbleed and Shellshock are recent examples of this threat. There is a wealth of reusable software components available to application developers. Many of these components are open source, developed with voluntary contributions, and available for free. Developers can quickly build feature-rich applications using these third-party components. While the benefit of taking such an approach is obvious, companies need to account for the cost of security bugs if they use third-party components.

To view this video, OWASP top 10 vulnerabilities: #9 Using components with known vulnerabilities: Heartbleed and Shellshock in action, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

#10 Unvalidated redirects and forwards

Unvalidated redirects and forwards is currently ranked #10 on the OWASP top 10 chart and is a commonly exploited vulnerability type. Web applications frequently redirect and forward users to
other pages and websites. Without proper validation, attackers can redirect victims to malicious sites or use forwards to access unauthorized pages.

To view this video, OWASP top 10 vulnerabilities: #10 Unvalidated redirects and forwards, please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

**Conclusion**

These are only a few of the security vulnerabilities modern web applications are subject to. However, by following the tips provided in these videos and other help available from IBM Security Systems, and by using advanced security software such as IBM AppScan, website administrators can find, correct, and avoid these and other web security threats.
Related topic

- Webinar: Avoiding Application Attacks: A Guide to Preventing the OWASP Top 10 from Happening to You

© Copyright IBM Corporation 2015
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)

OWASP top 10 vulnerabilities