Threat Prevention Coverage – OWASP Top 10

Analysis of Check Point Coverage for OWASP Top 10 Website Vulnerability Classes

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. OWASP mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.
Adopting the OWASP Top Ten is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

The OWASP Top Ten is a list of general vulnerability classes, so the level of coverage that security products provide against such vulnerabilities cannot be easily defined or measured.
IPS products, such as Check Point IPS blade, usually detect well-known vulnerabilities rather than track the behavior of custom web applications, which means this list, and the classification of vulnerabilities into classes, is not designed in the way IPS products categorize vulnerabilities. This document provides, however, some notes regarding Check Point's protection against these vulnerability classes, focusing mainly on Check Point IPS blade.

The document was authored by Danny Lieblich, benefited from comments from several Check Point researchers, and was edited by Gil Sasson. Feel free to send any comments about the document to Gil.

References:
OWASP: https://www.owasp.org/
OWASP 2010 Top 10:
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2010
OWASP 2013 Top 10:
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013

Injection (2010 – no. 1, 2013 – no. 1)

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

IPS blade includes several generic protections against injection vulnerabilities:

- SQL injection
- LDAP injection
- Command Injection
- HTTP Command Injection

SQL and Command Injection Attacks are blocked by looking for keywords. Keywords are traced in form fields either in GET or POST request, inside the URL or the HTTP request body. Keyword lists are preconfigured, and users only need to set the security level on HIGH/MEDIUM/LOW. When a higher security level is used, keywords that are less indicative of an attack are also examined.

In addition, Check Point IPS blade currently offers ~250 protections against specific well-known SQL injection vulnerabilities, and ~80 more other command injection and other injection-related vulnerabilities.

Broken Authentication and Session Management (2010 - no. 3, 2013 – no. 2)

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

Organizational applications intended for internal users could protect themselves against such implementation flaws by using Check Point's authentication and Identity Awareness features, performing the authentication at the Firewall (which could in turn query an external database, such as LDAP, Windows, RADIUS, Citrix, RSA SecurID, etc.). In addition, Check Point IPS blade offers protections against some known attacks on specific servers which exploit known authentication and session management vulnerabilities.

Cross-Site Scripting (XSS) (2010 – no. 2, 2013 – no. 3)

Cross-Site Scripting flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Check Point IPS blade offers a generic Cross-Site scripting protection, which rejects any occurrence of HTTP request containing banned HTML tags and escape sequences that may be used for scripting, as well as ~130 XSS protections against specific vulnerabilities, which look for multiple keywords that can be used for scripting code, JavaScript and VBScript commands, event that can trigger scripting engine, and HTML attributes and tags.

Insecure Direct Object References (2010 - no. 4, 2013 – no. 4)

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
No security product other than the application itself could track which user is authorized to access which data. Therefore, this type of vulnerabilities is outside the scope of network devices, and probably any other external security software.

Security Misconfiguration (2010 – no. 6, 2013 – no. 5)

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

Check Point IPS blade offers a "Header Spoofing" feature, which allows an administrator to hide the identity of the Web server from scripts looking for vulnerable Web servers. IPS blade also offers protections against misconfigured applications, such as attempt to use the default credentials of some well-known applications, or attempts to use some deprecated protocols, methods, options and parameters.

In addition, Web servers that are not kept up-to-date with the current security patches would still be protected against many of the vulnerabilities which these patches solve by the Check Point IPS blade's various protections.

Sensitive Data Exposure (2013 – no. 6)

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Check Point IPS blade contains ~150 protections against specific vulnerabilities involving information disclosure.

Missing Function Level Access Control (2013 – no. 7)

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

Organizational applications intended for internal users could control access rights to the various functionalities by using Check Point's authentication and Identity Awareness features.

Cross-Site Request Forgery (CSRF) (2010 – no. 5, 2013 – no. 8)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Check Point IPS blade offers protections against several specific CSRF vulnerabilities in WordPress, Oracle, Adobe, Trend, Symantec, and other products.

Using Components with Known Vulnerabilities (2013 – no. 9)

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Network security products may only inspect the traffic that passes over the network. If the use of the vulnerable component results in unique traffic for that component, it may be identified regardless of the application that uses that component. However, if the vulnerable component is an infrastructure used in different ways by different applications, and does not result in distinct traffic that can be identified, it is outside the scope of a network security device.

Invalidated Redirects and Forwards (2010 – no. 10, 2013 – no. 10)

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.

Check Point IPS blade offers protections against several known redirection vulnerabilities in Apache, IIS, IE, Forefront, Wordpress, and other products.

Insecure Cryptographic storage (2010 – no. 7)

Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

Check Point products include built-in support for encryption protocols, and provide the highest level of security and management capabilities for encryption functions, so that the burden of implementation cryptographic functionality is shifted from the Web application developer to Check Point.

Organizational applications intended for internal users could use Check Point's VPN / Remote Access features in order to enable encrypted and authenticated access to sensitive data, while not exposing it to external attackers. This can be done either by an IPSec VPN tunnel or by a clientless SSL/TLS VPN. As for users' credentials for authentication performed at the Firewall, they could be stored securely on an external server (LDAP, Windows, RADIUS, Citrix, RSA SecurId, etc.) queried by the Firewall. In addition, Check Point offers Full Disk Encryption as well as other media encryption solutions to help protect sensitive data from unauthorized direct access.

Failure to restrict URL Access (2010 – no. 8)

Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.

Check Point's authentication and Identity Awareness features could be used to restrict access to certain URLs for specific authenticated internal users only, instead of relying only on the web application's own authentication. In addition, IPS protections such as Directory Traversal protections and Null HTTP Encoding prevent URL manipulation that could fool URL-base authorization mechanisms.

Insufficient Transport Layer Protection (2010 – no. 9)

Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.

Check Point Security Management Server allows the security administrator to require that certain connections must be authenticated or encrypted. Encryption and authentication could be carried out by the Firewall, including checking certificates' integrity and validity, and using strong and secure authentication and encryption algorithms.

In addition, Check Point's IPS blade includes many protections against vulnerabilities in SSL clients and servers, and attempt to exploit vulnerabilities in the SSL protocol.

