FortiWeb and the OWASP Top 10
Mitigating the most dangerous application security threats
Introduction

The Open Web Application Security project (OWASP) Top Ten provides 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 as identified by a variety of security experts from around the world who have shared their expertise to produce this list.

The U.S. Federal Trade Commission strongly recommends that all companies use the OWASP Top Ten and ensure that their partners do the same. In addition, the U.S. Defense Information Systems Agency has listed the OWASP Top Ten as key for best practices.

In the commercial market, the Payment Card Industry (PCI) standard has adopted the OWASP Top Ten and lists it as a key requirement as part of section 6 – “Develop and maintain secure systems and applications” mandating that all web applications be developed according to security guidelines to protect against the OWASP Top 10.

Web Application Security Challenges

Web applications are attractive targets to hackers as often they are public facing applications that are required to be open to the internet as they provide major e-commerce and business driving tools for organizations. Connected to backend databases web applications are perfect for hackers as these databases are the primary repository for card holder data, company data and other sensitive information.

According to the SANS attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet. Web application vulnerabilities such as SQL injection and Cross-Site Scripting flaws in custom-built applications account for more than 80% of the vulnerabilities being discovered.

The difficulty in protecting web applications is their architecture and dynamics. While network security is simple – define security policies to allow/block specific traffic to and from different networks/servers, applications consist of hundreds and sometimes thousands of different elements - URLs, parameters and cookies.

Manually creating different policies for each of these items is almost impossible and obviously does not scale. On top of this, web applications change frequently with new URLs and parameters being added making it difficult for security administrators to update their security policies.

FortiWeb Web Application Firewall

Combining both Web Application Firewall and XML Firewall capabilities in a single platform the FortiWeb solution allows enterprises to protect against application level attacks targeted at the Web application and web services infrastructure. Using advanced techniques to provide against SQL injection, Cross site scripting and a range of other attacks helps to prevent identity theft, financial fraud and corporate espionage which can result in significant damage.

FortiWeb provides flexible and reliable protection to address the OWASP Top Ten by utilizing a range of in-depth security modules and technologies. Sophisticated attacks are blocked using a multi layered security approach. Incorporating a positive and a negative security module based on bi-directional traffic analysis and an embedded behavioral based anomaly detection engine FortiWeb can protect against a broad range of threats without the need for network re-architecture and application changes.

FortiWeb Incorporates two security models in order to protect both known and unknown vulnerabilities:

Positive Security Model

FortiWeb uses Positive Security Model to protect against any known and especially unknown vulnerabilities. Once a new web application policy is defined, FortiWeb starts monitoring traffic flowing to the application and based on a behavioral analysis technology called Auto-Learn FortiWeb builds a dynamic baseline of allowed elements for the application. By analyzing user behavior FortiWeb understands how the web application should be accessed. Authorized URLs are created with the relevant parameters for each of the URLs. Parameters constraint characteristics are profiled as well to provide an overall picture of the web application structure and what constitutes as normal user behavior.
Using a sophisticated engine FortiWeb only adds normal behavior to the profile making sure any abnormal activity is discarded.

The Auto-Learn profiling capability is completely transparent and does not require any changes to the application or network architecture. FortiWeb does not scan the application in order to build the profile, but rather analyzes the traffic as it monitors it flowing to the application.

By creating a comprehensive security model of the application FortiWeb can now protect against any known or unknown vulnerabilities, zero day attacks such as SQL Injection, Cross Site Scripting, and other application layer attacks.

Figure 1 and 2 FortiWeb Traffic Analysis based on Positive Security Model

Negative Security Model

FortiWeb includes a full application signature dictionary to protect against known application layer attacks. A sophisticated engine scans both inbound and outbound traffic, matching elements with pre-defined known exploits.

A comprehensive flexible engine also allows customers to write their own signatures using a sophisticated regular expression engine which provides the ability to create new and customized signatures for every application and vulnerability.

FortiWeb’s signature dictionary is updated regularly and automatically via FortiGuard, a Security Subscription Service which delivers continuous, automated updates and offers dynamic protection based on the work of the Fortinet® Global Security Research Team, which researches and develops protection against known and potential security threats.

The negative security layer is extended with an HTTP RFC enforcement layer making sure any access to the protected application is done according to the HTTP standard. FortiWeb provides an enhanced policy configuration with multiple rules to protect against buffer overflows, encoding based attacks and any other attack that tries to manipulate the HTTP protocol.
Additional FortiWeb Functionality Helps Protect against OWASP Top 10

Data Leak Prevention and Information Disclosure

FortiWeb extends monitoring and protection to outgoing traffic such as credit card leakage and information disclosure. Providing multiple policies for information disclosure FortiWeb immediately alerts any web application abnormalities that may be caused by an attack or by poor application configuration. Rules can be extended to rewrite information disclosure such that users are not exposed to any sensitive application data. Additional credit card leakage rules make sure any outgoing traffic does not include credit card numbers.

FortiWeb also allows customers to create their own custom rules providing an entire solution for Data Leak Prevention.

Web Vulnerability Scanner

FortiWeb is the only vendor that provides a Vulnerability Scanner module within the web application firewall that automatically scans and analyzes the protected web applications and detects security weaknesses, known and unknown vulnerabilities.

Together with the web application firewall FortiWeb completes a comprehensive solution for PCI DSS requirement 6.6 and 6.5 allowing organizations to scan their applications, identify vulnerabilities and protect them in real time from the same platform.
Enforcing access to the application according to the correct business logic is an important part of web application security. Applications that do not enforce this open themselves to Cross Site Request Forgery (CSRF) attacks. For example, e-commerce applications should not allow access to the shipping or payments stage directly, without prior access to the ordering pages.

By defining a Page Access rule on FortiWeb CSRF attacks are immediately blocked helping with OWASP Top Ten A5 requirement.

Additionally, FortiWeb offers a Start Page policy as well which defines the entry point to the application helping with requests that try to circumvent authentication or any other environment that requires users to start browsing at a specific page.

**OWASP Top Ten and FortiWeb Mitigation Technique**

The table below lists the OWASP Top Ten and the corresponding FortiWeb mitigation techniques.

<table>
<thead>
<tr>
<th>OWASP Top Ten</th>
<th>Explanation</th>
<th>FortiWeb Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A1. Injection</strong></td>
<td>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 unauthorized data.</td>
<td>Auto-Learn profiling automatically builds an allowed baseline allowing a comprehensive request validation feature to enforce strict URL and parameter control. Enhanced application signature detection engine adds a secondary layer for abnormal characters and known injection strings.</td>
</tr>
<tr>
<td><strong>A2. Cross-Site Scripting (XSS)</strong></td>
<td>XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and 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.</td>
<td>Application signature detection engine includes various XSS signatures. Request validation process ensures only relevant characters can be submitted.</td>
</tr>
</tbody>
</table>
### A3. Broken Authentication and Session Management

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

Enforces session management with strict cookie control. Provides various Authentication Offload capabilities (supporting Local, LDAP and NTLM) to minimize application security flaws.

### A4. Insecure Direct Object References

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.

Auto-Learn profiling builds a comprehensive profile of allowed elements within the application. Any attempt to manipulate a parameter will trigger an alert and immediately be blocked. Hidden Fields Rules detect and block any attempt by the client to alter a hidden parameter value.

### A5. Cross-Site Request Forgery (CSRF)

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.

Strict reference page enforcing provides protection against sophisticated CSRF attacks. Also, page access rules allow customers to define URL order. Common CSRF attacks attempt to submit a specific crafted request. For example, FortiWeb enforces a page order sequence that will block the request if it didn’t go through the proper payment order sequence and as such - invalid.

### A6. Security Misconfiguration

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.

1) Using Auto-Learn FortiWeb will block any attempt made by an attacker to exploit a misconfigured web application.  
2) Through monitoring application responses, FortiWeb is able to identify any application failure.  
3) Vulnerability Scanner module scans the protected applications, finds inherent misconfigurations and quickly turns them to security rules.

### A7. Insecure Cryptographic Storage

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.

Extended monitoring and protection for all outgoing traffic prevents sensitive information leakage such as credit card numbers, Social Security numbers and many other types of information disclosure.
A8. Failure to Restrict URL Access

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.

Authentication Offload allows organizations to use FortiWeb to authenticate different URLs in different Realms. Administrators can define URL groups that require specific authentication while other URLs open to the public. Using FortiWeb’s authentication capability ensures correct URL access rights are enforced.

A9. Insufficient Transport Layer Protection

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.

FortiWeb, when deployed as a reverse proxy, adds a SSL layer and enforces SSL v3 only and cipher size higher than 128 bits to maintain strong encryption.

A10. Unvalidated Redirects and Forwards

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.

Auto-Learn profiling indentifies when parameters are used in a different manner then supposed to. Validation enforcement makes sure characters that are usually associated with redirects and forwards are not allowed as part application usage.

Summary

The OWASP Top Ten provides a great starting point for customers to measure their application security and prioritize their risk. Mandated by the Payment Card Industry (PCI) standard as a key requirement as part of section 6 and widely adopted by many organizations the OWASP Top 10 is an important guideline that helps companies focus on application security.

FortiWeb’s integrated Web Application Firewall and Vulnerability assessment scanner allow customers to protect against high risk attacks such as defined in the OWASP Top Ten and many others.