radware

ANALYZING THE OWASP TOP 10

TOP APPLICATION SECURITY THREATS & HOW TO MITIGATE THEM

Cars require seatbelts. Pill bottles need safety caps. Applications need web application firewalls, and for good reason. The web application threat landscape is in a constant state of flux. From DevOps to new attack vectors, these changes can leave security professionals scrambling to safeguard their most prized digital assets to secure the customer experience.

The Open Web Application Security Project (OWASP) Top 10 list is an invaluable tool for accomplishing this. Since 2003, this top ten list seeks to provide security professionals with a starting point for ensuring protection from the most common and virulent threats, application misconfigurations that can lead to vulnerabilities, as well as detection tactics and remediations.

But just like the adaptive threat landscape it seeks to define, this list is updated to continue to serve as an industry benchmark for the application security community. This piece provides an overview of the 2017 OWASP Top 10 list, changes between the 2013 and 2017 version and technical capabilities security professionals should consider when evaluating web application firewalls (WAFs).

OWASP TOP 10 – 2013	OWASP TOP 10 – 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication
A3 – Cross-Site Scripting (XSS)	A3 – Sensitive Data Exposure
A4 – Insecure Direct Object References **[Merged + A7]**	A4 – XML External Entities (XXE) **[NEW]**
A5 – Security Misconfiguration	A5 – Broken Access Control **[MERGED]**
A6 – Sensitive Data Exposure	A6 – Security Misconfiguration
A7 – Missing Function Level Access Control **[Merged + A4]**	A7 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Insecure Deserialization **[NEW, COMMUNITY]**
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Insufficient Logging & Monitoring **[NEW, COMMUNITY]**

Source: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

#1 THREAT: INJECTIONS

2013 RANK: 1

Injection flaws, such as SQL, NoSQL, OS and LDAP injection, have been a perennial favorite among hackers for some time, which is why it's no surprise that this threat is still at the top of the list. An injection flaw occurs when suspicious data is inserted into an application as a command or query. This hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

The most common code injection are SQL Injections, which is an attack that is accomplished by sending malformed code to the database server. It's a simple, quick and easy attack type that almost anyone with Internet access can accomplish; SQL Injection scripts are available for download and are easily acquirable.

COUNTERMEASURE: POSITIVE PROTECTION

Many web application security solutions leverage a negative security model, which defines what is disallowed while implicitly allowing everything else. Since attack signatures may generate false positives by detecting legitimate traffic as attack traffic, such rules tend to be simplistic, trying to detect the obvious attacks. The result is protection against the lowest common denominator.

A positive security model, which defines the set of allowed types and values, is required to provide proper protection where signature-based protection cannot fill the gap. In the case of SQL Injections, a positive security model screens user input for known patterns of attacks and leverages logic to tell the difference between legitimate user input and injection flaws.

#2 THREAT: BROKEN AUTHENTICATION

2013 RANK: 2

When an application's functions are not implemented correctly, the door is left open for criminals to break in. Attackers can compromise passwords, keys, or session tokens or exploit other implementation flaws to assume other users' identities temporarily or permanently. Sessions should be unique to individual users, and without some session management, an attacker can sneak in disguised as a user to access valuable data

COUNTERMEASURE: CHALLENGE AND VALIDATE

Securing these application in terms of access control is no easy task. Authenticating users by having them provide their identity and challenging them to verify their identity is a key first step. Single sign-on and multi-factor authentication is a key first step that reduces the risk of compromised accounts.

Second is a web application firewall that proactively encrypts session parameters between network and client, proactively inspects login attempts and thwarts HTTP sessions via code-encrypting, cryptographic capabilities.

#3 THREAT: SENSITIVE DATA EXPOSURE

2013 RANK: 6

Many web applications and APIs contain vulnerabilities due to coding, thereby exposing sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

COUNTERMEASURE: ENCRYPTION, EITHER ON THE MOVE OR SITTING IN PLACE

Encryption is key, both for data at rest or in transit. Leading web application firewalls provide inspection/ encryption of data, including SSL inspection and protection capabilities to eliminate security blind spots.

This includes, but is not limited to, SSL traffic decryption and encryption, masking server identities and veiling sensitive information such as credit card numbers and social security numbers. An adaptive WAF that leverages auto policy generation and machine-learning capabilities to automatically create and apply security configurations and policies is also critical. Finally, any enterprise-grade firewall should support the encryption of ingress and egress traffic across both on-premise and cloud-based infrastructures.

#4 THREAT: XML EXTERNAL ENTITIES

NEW IN 2017

Many older or poorly configured XML processors evaluate external entity references within XML documents. Attackers can use external entities for attacks, including remote code execution and to disclose internal files, SMB file shares, conduct internal port scanning and to launch DoS attacks.

COUNTERMEASURE: AN INTEGRATED APPROACH

Static application security testing (SAST) is a tried and true way to discover this issue by inspecting dependencies and configuration. Its brethren, Dynamic Application Security Testing (DAST) are tools to detect vulnerabilities in application in its running state.

A WAF should be able to parse and inspect protcols and structured documents, including HTTP/HTTPS traffic, POST requests and XML JSON schemas. In addition, the aforementioned machine-learning algorithms can learn XML and JSON structures and schemas for enforcement as part of the validation phase and create security policies.

#5 THREAT: BROKEN ACCESS CONTROL

MERGED RISKS 4 & 7 2013

Improperly configured or missing restrictions on authenticated users allow them to access unauthorized functionality or data. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

COUNTERMEASURE: FASTEST TIME TO PROTECTION

Penetration testing is essential for detecting non-functional access controls; other testing methods only detect where access controls are missing. The problem is it can take several weeks to test, produce and assess these reports, and then implement necessary security changes. This problem can be exasperated when four out of five organizations report at least a medium degree of manual work to make security policy updates to their WAF, according to Radware's 2017-2018 Global Application & Network Security Report.

Any web application firewall should serve as a catalyst for stemming unauthorized access via authentication gateway functionality, single sign-on, user tracking and access controls to the web application based on user role and profile information.

#6 THREAT: SECURITY MISCONFIGURATION

2013 RANK: 5

Security misconfiguration remains one of the most commonly seen web application security issues to this day. This risk refers to improper implementation of controls intended to keep application data safe, such as insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and perhaps most importantly, not patching or upgrading systems, frameworks, libraries, applications and components.

COUNTERMEASURE: THE ABILITY TO LEARN

As notable ransomware and malware outbreaks in recent years (i.e. WannaCry) has proven, system upgrades are critical. An “adaptive” WAF will leverage auto policy generation and machine-learning capabilities to automatically create and apply security filters and enforcement rules where security is misconfigured. It evaluates the structure of a web application, sets relevant security filters and analyzes traffic properties from a production environment to build a dynamic network profile, thereby maximizing security while minimizing false positives.

#7 THREAT: CROSS-SITE SCRIPTING (XSS)

2013 RANK: 3

Cross-site scripting (XSS) flaws occur whenever an application includes untrusted data in a new webpage without proper validation or updates an existing webpage with user-supplied data using a browser API that can create HTML or JavaScript. These flaws give attackers the capability to inject client-side scripts in the application to hijack user sessions, deface websites or redirect the user to malicious sites.

COUNTERMEASURE: A CHECKLIST

Against cross-site scripting attempts, make sure any web application firewall can checkoff the following: signature- and rule-based protection with updated signatures (similar to a blacklist) and the ability to identify scripting patterns and blocking malicious requests.

#8 THREAT: INSECURE DESERIALIZATION

NEW IN 2017

Insecure deserialization often leads to remote code execution to tamper or delete serialized objects or elevate privileges. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay or injection attacks.

COUNTERMEASURE: BEST OF BOTH WORLDS

Identify web application firewalls that provide the best of both worlds: they combine negative (defining what is forbidden and accepting the rest) and positive security models (defining what is allowed and rejecting the rest). This winning combination should leverage various WAF access control filters such as cookie encryption, XML/JSON parsing, parameters enforcement and more.

#9 THREAT: USING COMPONENTS WITH KNOWN VULNERABILITIES

2013 RANK: 9

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Developers frequently don’t know which open source or third-party components are in their applications, making it difficult to update components when new vulnerabilities are discovered. These components can undermine application defenses and enable various attacks and impacts.

COUNTERMEASURE: KNOW WHERE THE HOLES EXIST

Any web application firewall that provides integration with programs such as Microsoft’s Server Update Services allows the WAF to protect against exploitations of components with known vulnerabilities by screening client requests and server responses. In addition, security updates and threat intelligence feeds are essential to keep security teams in the know and facilitate quicker responses. for real-time responses to maximize protection and reduce exposure.

#10 THREAT: INSUFFICIENT LOGGING & MONITORING ! NEW IN 2017

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response systems, allows attackers to run amok, attacking further systems, tampering, extracting or destroying data. Many studies show that time to detect is measured in weeks or months, typically detected by external parties rather than internal processes or monitoring.

COUNTERMEASURE: SUITE SOLUTIONS VERSUS BEST-OF-BREED

To address the issue of internal processes, think like an attacker and internally test and audit to discover if your organization has sufficient monitoring. If your organization lacks this "white hat hacker" expertise, be sure that any cyber security vendor you partner with provides DDoS mitigation expertise via a team of battle-hardened security experts.

These same experts should also play a role in the second biggest concern: real-time monitoring and detection. Timely detection of malicious malware or snooping hackers comes down to best-of-breed versus suite offerings. Stopping cyber-attacks in near real-time is best accomplished via a single vendor attack mitigation system. Many organizations leverage best-of-breed mitigation tools from different vendors. This hodgepodge collection results in poor communication and detection. Suite WAF/DDoS solutions can more effectively communicate, setting network traffic baselines and comparing data points to quickly detect when something is awry, in addition to providing enterprise-grade monitoring and management dashboards/analytics.

The OWASP Top 10 is not intended as "one list to rule them all," but rather serves as a great starting point for application security programs and web application firewall evaluation. It serves as a benchmark for empowering improved people, processes and technology.

Successful organizations must establish and use repeatable processes and security controls, testers should establish continuous application security testing, application managers need to take charge of the application lifecycle and the organization as a whole needs to have an application security program in place that effectively coordinates across all facets of its infrastructure.

To that end, selecting the right WAF vendor to partner with is a critical step in executing these concepts. Be sure any WAF solution your organization is evaluating not only meets your organization's existing security needs, but is flexible enough to adapt to future infrastructure environments, business needs and attack vectors.

LEARN ABOUT RADWARE'S WEB APPLICATION FIREWALL AND CLOUD WAF SERVICE.