IMPERVA

E-BOOK

Protect Your Applications Against All OWASP Top 10 Risks

Content

Web Applications are the Most Successful Vector for Breaches

When it comes to discovering the weakest link in your company's security defenses, you may need to look no further than your web applications. According to the 2017 Verizon Data Breach Investigation Report, more successful breaches resulted from attacks on web applications than any other type of attack.

That's why the Open Web Application Security Project (OWASP) is focused on researching and identifying the most common web application attacks. An open community and not-for-profit organization, OWASP is dedicated to providing an unbiased source of information on cybersecurity best practices. One of the most valuable awareness projects from OWASP is the OWASP Top 10, which was first released in 2003 and revised most recently in 2017. It provides excellent insight into the most critical security risks to web applications.

In spite of the fact that more than half of the threats on the OWASP 2017 Top 10 list have been in existence for more than a decade, many organizations still lack the processes and technology to protect against these threats. In fact, OWASP confirmed that many applications are still at risk when it gathered and analyzed data on more than 50,000 applications contributed by a variety of organizations, consultants, and vendors. More than 2.3 million vulnerabilities were identified within the applications submitted.

Clearly organizations are struggling to properly address web application security. This eBook goes beyond the guidance from OWASP to provide insight into ways that security teams can use best-of-breed solutions to protect against recently identified OWASP Top 10 threats. These solutions provide layers of defense that work together to significantly mitigate the risk of each Top 10 threat to your organization.

2017 OWASP Top 10

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

Making OWASP Guidance Actionable and Automated

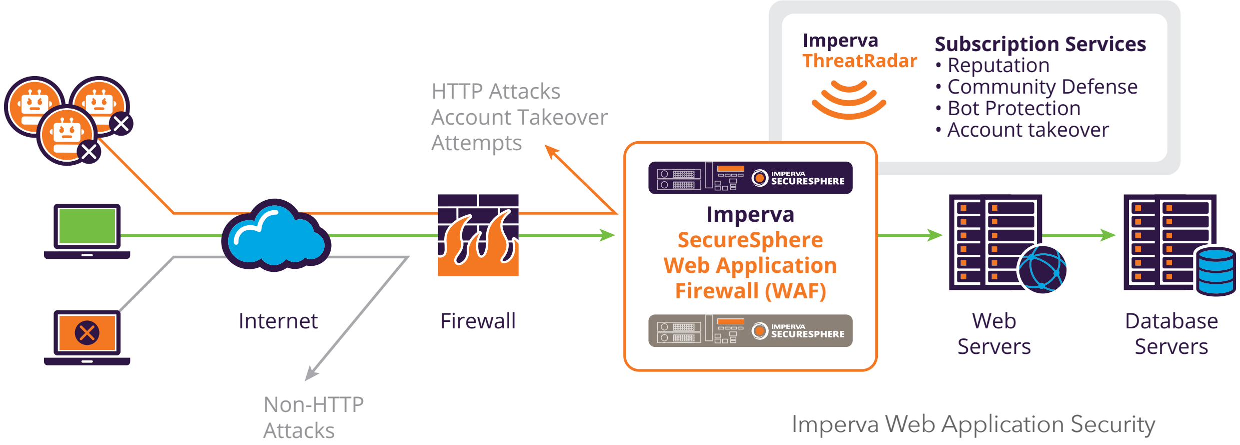
OWASP has provided information on the top web application threats and guidance on how to prevent them since 2003. For the most part, the threats have not changed substantially during that time. Yet in 2016, web application attacks were the most successful vector for breaches. What happened?

While the OWASP Top 10 document describes ways to prevent attacks based on each type of threat, human efforts to practice secure coding, discover flaws, define and follow security best practices, and monitor application usage are limited by enormous volumes of code, the pace of change, scarce resources and limited skillsets.

It's physically impossible to inspect every piece of code—both custom and third party—to determine whether a component is 100 percent vulnerability-free. For this reason, automation of web application security is imperative.

Essential security tools for web applications

Best-of-breed security solutions can protect applications and data—both on-premises and in the cloud—against all online threats, including, but not limited to, the OWASP Top 10. Imperva protects your web applications and data against web attacks, distributed denial of service (DDoS) attacks, site scraping and fraud.

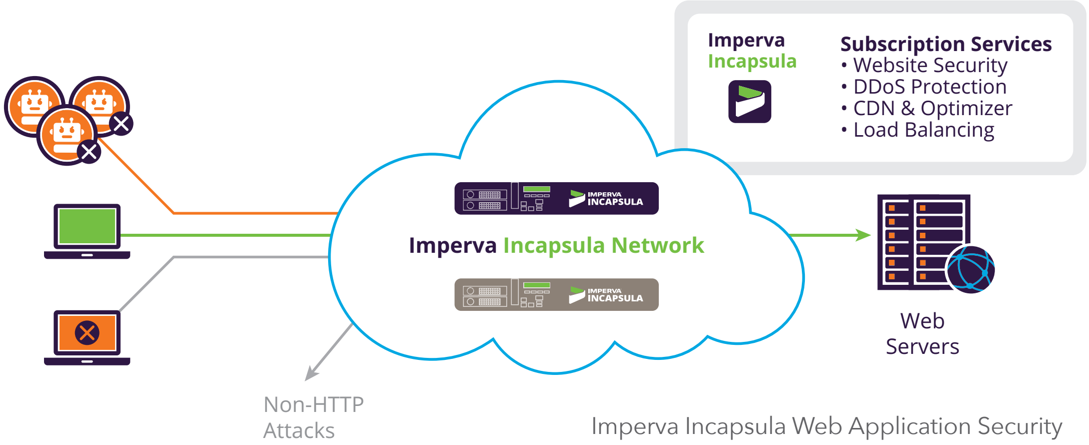


Imperva Web Application Security

Imperva SecureSphere Web Application Firewall (WAF) is an on-premises solution that analyzes all user access to your web applications and protects your applications and data from attacks.

Imperva ThreatRadar arms Imperva SecureSphere Web Application Firewall with globally crowdsourced, real-time threat intelligence to stop known malicious users and industrialized, multi-vector attacks.

Imperva SecureSphere Database Audit and Protection monitors database and user activity to detect and stop unauthorized access of sensitive data.



Imperva Incapsula Web Application Security

Imperva Incapsula Web Security offers a cloud WAF as a standard feature of the Incapsula service that also includes a CDN and optional DDoS protection and load balancing.

A1: Injection

Exploitability: Easy

Prevalence: Common

Impact: Severe

Risk: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection occur when an application sends untrusted data 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.

Protection: In addition to the OWASP recommendation of keeping untrusted data separate from commands and queries, organizations can use Imperva to accurately detect and block multiple types of injection attacks using a variety of techniques.

- A unique SQL injection correlation engine combines information from the web application profile (positive security model) and matches this information with attack signatures (negative security model) using SecureSphere's Correlated Attack Validation engine.
- Pre-defined signatures help block additional injection attacks such as LDAP, XPath, and OS injection.
- Signature recognition, IP reputation and other security methodologies are used by Incapsula's SQL injection correlation engine to identify and block SQL injections.
- Incapsula protects against Remote File Inclusion (RFI) by monitoring user inputs and filtering out malicious requests using a combination of signature, behavioral and reputation-based security heuristics.
- Attacker data (e.g. IP addresses, attack signatures, etc.) is correlated across the entire Incapsula network to quickly pinpoint known malicious users and block their access to protected sites.
- Incapsula IncapRules is a security rules engine that enables granular customization of default security settings and the creation of additional case-specific security policies.

A2: Broken Authentication and Session Management

Exploitability: Easy

Prevalence: Common

Impact: Severe

Risk: Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume (temporarily or permanently) the identities of other users.

Protection: Imperva helps you meet OWASP recommendations for strong authentication and session controls and also helps you stop session attacks such as session hijacking, fixation, and tampering.

- When deployed as a transparent bridge, SecureSphere tracks and enforces session variables, without intruding on an application's session management facility.
- SecureSphere profiles application activity to learn about cookies and correctly identify attacks such as cookie injection or poisoning.
- Strong correlation capabilities allow you to define advanced rules for detection of session hijacking attempts such as simultaneous user authentication from two different IP addresses.
- Application user tracking automatically captures web application user names and associates all subsequent session activity with that specific username to detect successful or failed logins and prevent brute-force attacks.
- Incapsula includes a two-factor authentication (2FA) solution that provides strong, multi-factor authentication for any website protected by Incapsula without requiring application code changes or hardware or software installation.
- The Incapsula IncapRules security rules engine enables granular customization of default security settings and the creation of additional case-specific security policies.

A3: Sensitive Data Exposure

Exploitability: Average

Prevalence: Widespread

Impact: Severe

Risk: Sensitive data exposure has been the most common, impactful attack according to OWASP. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and personally identifiable information (PII). Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Protection: Imperva mitigates exposure of sensitive data by preventing the attacks that lead to a data breach.

- Using data loss prevention (DLP) rules, SecureSphere mitigates data exposure by inspecting outbound traffic for sensitive information such as cardholder data and Social Security numbers. If SecureSphere detects leakage of sensitive data, it blocks web server responses before they reach the end user.
- Imperva also stops malicious users from exploiting web server and application vulnerabilities to gain control and access sensitive data.
- By preventing the attacks that lead to a data breach—such as man-in-the-middle (MITM), SQL injection, and OS command injection attacks—Imperva drastically reduces the opportunity for attackers to access encrypted data.

A4: XML External Entities (XXE)

Exploitability: Average

Prevalence: Common

Impact: Severe

Risk: An XXE attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. Attackers can exploit vulnerable XML processors if they are able to upload XML or include hostile content in an XML document. Such an attack can lead to the disclosure of confidential data, denial of service, server side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.

Protection: Imperva helps protect your organization from XXE attacks against vulnerable XML processors by detecting and blocking the threats using multiple techniques.

- A correlation engine combines information from the web application profile (positive security model) and matches this information with out-of-the-box attack signatures (negative security model) using SecureSphere's Correlated Attack Validation engine.
- Continual ThreatRadar threat intelligence and signature updates help SecureSphere and Incapsula automatically block emerging threats.
- Signature recognition and other security methodologies are used by Incapsula to identify and block XXE injections.
- Attacker data (e.g. IP addresses, attack signatures, etc.) is correlated across the entire Incapsula network to quickly pinpoint known malicious users and block their access to protected sites.

A5: Broken Access Control

Exploitability: Average

Prevalence: Common

Impact: Severe

Risk: When restrictions on what authenticated users are allowed to do are not properly enforced, attackers can exploit these flaws to access unauthorized functionality and/or data. The threats include: unauthorized access to other users' accounts, viewing sensitive files, modifying other users' data, changing access rights, and more.

Protection: Imperva helps you go beyond code review to verify that all data and functions have appropriate controls for detecting and blocking risky or potentially malicious activities.

- Dynamic application profiling learns which URLs and functions require a valid session identifier such as a cookie. If a cookie is not present or if the user has manipulated it, then SecureSphere can block the session, user, or IP address.
- If attackers attempt to access hidden or protected URLs by enumerating different file and directory names, SecureSphere thwarts the attempt to use forceful browsing to circumvent function-level access controls.
- Custom policies can restrict access to certain files by IP address or user name.
- Dynamic application profiling identifies and understands expected behavior for elements of an application to detect attempts to manipulate input values.
- Imperva detects and blocks users from performing activities that are considered a risk to a web environment. Attacks through valid user input against known attack vectors, behaviors, and deviations are blocked.
- In addition to existing usernames and passwords, Incapsula's Login Protect feature adds a second level of authentication based on a one-time passcode sent to the authenticating user via email, text message (SMS), or Google Authenticator mobile application. Login Protect can also be used as a primary method of authentication.

A6: Security Misconfiguration

Exploitability: Easy

Prevalence: Widespread

Impact: Moderate

Risk: Attackers will often try to exploit unpatched flaws or access default accounts, unused pages, unprotected files and directories, and other misconfigurations to gain unauthorized access or knowledge of the system. Security misconfiguration can happen at any level of the application stack, including: network services, frameworks, application servers, web servers, database servers, platforms, and other components.

Protection: Imperva protects against vulnerabilities created by human configuration errors such as incorrect security settings, unpatched software, and others.

- By profiling normal input, SecureSphere can alert on and block deviations and attempts to misuse access. If a developer or network administrator misconfigured something within the environment and an attacker tries to gain access, SecureSphere can detect the deviation from normal usage and block it.
- Integrations with leading web server and application scanners enables SecureSphere to import scan results to instantly mitigate misconfigurations by virtually patching vulnerabilities.
- By applying both generic and application-specific security measures, Incapsula can prevent exploitation of vulnerabilities created by security misconfigurations.
- Incapsula can implement virtual patching on many common applications such as WordPress, Joomla, Drupal, and others to protect against known vulnerabilities and misconfiguration issues.
- With two-factor authentication from Incapsula, misconfigurations such as using default names and passwords can be mitigated by forcing users to successfully pass a second layer of authentication to access sensitive areas of websites.

A7: Cross-Site Scripting (XSS)

Exploitability: Easy

Prevalence: Widespread

Impact: Moderate

Risk: XSS is the second most prevalent issue in the OWASP Top 10 and is found in roughly two-thirds of all applications. Flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create JavaScript. 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.

Protection: Imperva accurately detects and mitigates XSS attacks using both positive (white list) and negative (black list) models. The negative security model explicitly declines known attack signatures and includes XSS signatures, keywords, suspicious patterns and other indicators to correctly detect XSS attacks.

- Dynamic Profiling creates an additional layer of defense using a positive security model of the application structure. It uses the dynamic web application profile to allow only legitimate user input.
- SecureSphere analyzes where the XSS pattern appears (for example, in a web page hyperlink) and whether the XSS pattern is new or a standard part of the web application.
- XSS signatures, policies, and correlation rules are used by Imperva to detect and block attacks.
- Utilizing a combination of algorithms, SecureSphere validates user input and application behavior to accurately detect and mitigate evasion techniques.
- Incapsula uttilizes custom signatures and specific XSS rules with system-wide correlation of attacker data (e.g. IP addresses, attack signatures, etc.) across the entire Incapsula network to quickly pinpoint known malicious users and block their access to protected sites.

A8: Insecure Deserialization

Exploitability: Difficult

Prevalence: Common

Impact: Severe

Risk: Applications and APIs can be vulnerable if they deserialize (take structured data and rebuild it into an object) hostile or tampered-with data supplied by an attacker. While exploitation of deserialization is somewhat difficult, the impact can be severe, with deserialization flaws potentially leading to remote code execution, denial of service, and access control attacks.

Protection: Imperva defends your applications against deserialization attacks using profiling and policies, as well as white- and black-list security models. Our zero-day protection rules spot attacks, giving our security team insight that is then used to publish new, dedicated security rules to provide maximum protection to Imperva SecureSphere and Incapsula WAF customers against vulnerabilities such as the Apache Struts REST Plugin XStream XML Request Deserialization RCE and others.

- SecureSphere out-of-the-box policy rule detects and blocks deserialization attacks using digital signatures.
- Using its profiling mechanism to learn which external web applications are allowed to communicate messages for deserialization to the protected domain, SecureSphere automatically detects attempted injections.
- ThreatRadar Emergency Feed automatically updates attack signatures and provides predefined security policies to block emerging threats.
- Signature recognition is used by Incapsula to identify and block deserialization attacks.
- Virtual patching enables Incapsula to auto-apply a patch on the edge to protect against known vulnerabilities.

A9: Using Components with Known Vulnerabilities

Exploitability: Average

Prevalence: Widespread

Impact: Moderate

Risk: 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. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

Protection: Imperva protects web applications that use third-party components, which may be vulnerable to exploits.

- Using multiple layers of defense, including patented Dynamic Profiling technology, SQL injection and XSS correlation engines, and detection of HTTP protocol violations, SecureSphere identifies known and zero-day attempts to exploit vulnerable components.
- Dynamic Profiling allows only legitimate values to be used as input parameters and methods for URLs.
- Once a new vulnerability is published, the Imperva Defense Center quickly develops a signature or a set of policies to virtually patch the vulnerability.
- For commonly used applications such as WordPress, Joomla, Drupal, and others, Incapsula virtually patches the software to prevent any known vulnerabilities from being exploited by attackers. When a new vulnerability is published, the Incapsula security team quickly develops a signature or set of policies to virtually patch the vulnerability across the entire Incapsula network.
- Through defenses such as virtual patching, SQL injection and XSS correlation engines, detection of HTTP protocol violations, and backdoor shell protection, Incapsula identifies attempts to exploit vulnerable components.
- The Incapsula Research Team monitors external sources such as new vulnerability disclosures and analyzes all traffic going through Incapsula. Any new attack identified on the network is automatically analyzed, and new mitigation rules are propagated to customers.

A10: Insufficient Logging & Monitoring

Exploitability: Average

Prevalence: Widespread

Impact: Moderate

Risk: Rather than a specific type of web application threat or vulnerability, this risk is about the lack of or incompleteness of best practices for detecting and responding to attacks. OWASP states that exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the absence of monitoring and timely response to achieve their goals without being detected.

Protection: In addition to detecting and blocking attacks, Imperva also provides extensive logging and alerting, including customizable reporting, for rapid response to security events. It minimizes false positives by using Dynamic Profiling supported by machine learning.

- Logging and monitoring with rich, graphical reporting capabilities provide detailed, actionable security event information.
- Custom policies can be defined to protect specific application weaknesses from attack.
- Machine learning is used to create a positive security model of an application's profile, avoiding false-positives and improving detection of anomalies by learning the behavior of the common way to interact with the application.
- For complete visibility into all database transactions, including local privileged user access and service accounts, SecureSphere Database Audit and Protection continuously monitors and audits all logins/logouts, updates, privileged activities and more.
- Incapsula provides a detailed analysis of every threat posed to a website including: IP address, user agent, location, and other pertinent session information.
- Weekly graphical reports visualize trends in website traffic, threats, and performance improvements.
- A real-time statistics dashboard enables users to get instant access to live information about their website traffic and performance.
- Proprietary machine learning and classification techniques reduce false positives.
- The IncapRules security rules engine enables granular customization of default security settings and the creation of additional case-specific security policies.

Learn More

The OWASP Top 10 is an excellent resource to understand today's most critical risks for web applications. It gives security teams and developers a structure around which to prioritize and organize their security strategy. It also offers guidance on how to mitigate the threats.

An essential component of any web application strategy is automation. The right security solutions dynamically learn the normal behavior of your applications to identify and act on application vulnerability attacks including the ones in the OWASP Top 10, as well as business logic attacks such as site scraping and account takeover attacks as well as other fraudulent activities.

Learn more about how Imperva can protect your applications against OWASP Top 10 and other threats:

- Incapsula Website Security
- Imperva SecureSphere
- Imperva Blog
- Imperva Incapsula Blog
- Gartner Magic Quadrant for Web Application Firewalls
- The State of Web Application Vulnerabilities
- Imperva App Security Center: OWASP Top 10

About Imperva

Imperva® (NASDAQ: IMPV) is a leading provider of cyber security solutions that protect business-critical data and applications. The company's SecureSphere, CounterBreach, Incapsula and Camouflage product lines enable organizations to discover assets and risks, protect information wherever it lives–in the cloud and on-premises–and comply with regulations. The Imperva Defense Center, a research team comprised of some of the world's leading experts in data and application security, continually enhances Imperva products with up-to-the-minute threat intelligence, and publishes reports that provide insight and guidance on the latest threats and how to mitigate them. Imperva is headquartered in Redwood Shores, California.

Learn more: www.imperva.com, our blog, on Twitter.

EBook-OWASP_Top_Ten_2017_0118-v3

imperva.com

IMPERVA®