imperva

EBOOK

# 15 Ways Your Website is Under Attack

## Web applications are under constant attack.

Web applications are the home of your business on the internet. The functionality within your website, the structure of your technology stack, and the code used to build it are under constant attack from bad actors attempting to compromise your business. Understanding these types of attacks will help you prevent fraud, data theft, and online automated abuse while providing a roadmap on how to protect your business.

Remember that any comprehensive Web application and API (WAAP) security platform should protect from many or all of these attacks rather than focus on only one or two categories.

## **QUICK GUIDE** – HOW YOUR WEB APPLICATIONS ARE UNDER ATTACK

| | ATTACK CLASSIFICATION | WHY? | WHO? | SECURITY SOLUTION REQUIRED | IMPERVA |
|---|---|---|---|---|---|
| **1** | **OWASP Top Web Attacks** | Exploit business through web app code vulnerabilities. | Criminals | Web App Firewall | ✓ |
| **2** | **OWASP Top 10 API Attacks** | Exploit business through API vulnerabilities. | Criminals | API Protection | ✓ |
| **3-6** | **DDoS Attacks (Includes Ransom DDoS)**<br>3. DDoS Of IP address<br>4. DDoS Of Website<br>5. DDoS Of Network<br>6. DDoS Of DNS | Bring down the IP address, web application, network or DNS to prevent access. | Criminals and competitors | DDoS Protection | ✓ |
| **7-10** | **Automated Bot Attacks**<br>7. Credential stuffing attacks<br>8. Scraping attacks<br>9. Scalping attacks<br>10. 18 Other unique bot attacks | Exploit functionality and proprietary data published on websites to abuse the business and customers in anti-competitive and criminal ways. | Criminals, competitors and business partners | Bot Protection | ✓ |
| **11** | **Client Side Attacks** | Continuous real-time single record data theft. | Criminals | Client-Side Protection | ✓ |
| **12-13** | **Supply Chain Attacks**<br>12. Software supply chain<br>13. Javascript services | Exploit business through compromised third party services or code within consumer-off-the-shelf software or open source libraries including formjacking, magecart and Solarwinds. | Criminals | Client-Side Protection & Runtime Protection (RASP) | ✓ |
| **14** | **Legacy Application Zero Day Attacks** | Exploit vulnerable code in legacy applications in proprietary code, and any unprotected internal apps from insider threats. | Criminals | Runtime Protection (RASP) | ✓ |
| **15** | **Serverless Workloads Attacks** | Exploit vulnerable code within serverless workloads in public clouds. | Criminals | Serverless Protection | ✓ |

# 1. OWASP Top 10 attacks that target code vulnerabilities

## Attack explanation

The widely acknowledged OWASP Top 10 lists the risks that are most prevalent on web applications. Attackers target any security vulnerabilities incorporated during software development. The focus is on any code level weaknesses and taking advantage of them to compromise the organization.

## Attackers goals

Criminals attack websites looking to perform data theft, compromise the network, deface content, redirect traffic, and deploy malware.

## Protecting from OWASP top 10 risks

While fixing vulnerabilities within the code is ideal, this reality is almost impossible to achieve. Web Application Firewalls (WAF) were created to solve this code vulnerability problem while also helping organizations meet compliance requirements. For example: PCI compliance for businesses processing payment and credit cards.

> **Imperva's Web Application Firewall** is included in **Imperva's *Cloud Application Security*** Platform and protects from known and unknown attacks, is simple to deploy, always on, and blocks out of the box. Deployed by thousands of companies globally, Imperva's WAF is a perennial leader in Gartner's Magic Quadrant.

### OWASP TOP 10 WEB APPLICATION SECURITY RISKS

1. Injection
2. Broken authentication
3. Sensitive data exposure
4. XML external entities (XXE)
5. Broken access control
6. Security misconfiguration
7. Cross-site scripting (XSS)
8. Insecure deserialization
9. Using components with known vulnerabilities
10. Insufficient logging & monitoring

Source: **OWASP TOP 10 Web Application Security Risk**

# 2. OWASP API security Top 10 attacks

## Attack explanation

APIs are foundational components of modern mobile, SaaS, and web applications. Their adoption fueled web application innovation. By design they expose application logic and personally identifiable information (PII). Because of these attributes, and because they are largely unprotected, attackers increasingly target APIs.

## Attackers goals

Criminals attack APIs to achieve a multitude of nefarious goals including data theft, compromising the network, defacing content, redirecting traffic, deploying malware, and denial of service.

## Protecting from OWASP top 10 API risks

API security is a challenge for any organization. Protecting APIs with a positive security model is an advantage for any business.

> **Imperva's *API Security*** is included in **Imperva's *Cloud Application Security* Platform** and protects your APIs with an automated positive security model, detecting vulnerabilities in your applications, and shielding them from exploitation.

### OWASP API SECURITY TOP 10

API1: Broken object level authorization

API2: Broken user authentication

API3: Excessive data exposure

API4: Lack of resources & rate limiting

API5: Broken function level authorization

API6: Mass assignment

API7: Security misconfiguration

API8: Injection

API9: Improper assets management

API10: Insufficient logging & monitoring

Source: **OWASP API Security Top 10**

# 3 thru 6. DDoS attacks

## Attack explanation

DDoS attacks equate to loss of business. There are four distinct targets that are typically under DDoS attack–DDoS of individual IP addresses, DDoS of Website, DDoS of the Network, and DDoS of Domain Name Servers (DNS).

## Attackers goals

The primary goal of DDoS attacks is business disruption. With hundreds of thousands of dollars lost per hour of downtime, DDoS attacks have a significant economic impact. Any successful attack will bring down the businesses service. Beyond the typical criminal groups who launch diversionary DDoS attacks while attacking a different vulnerability, DDoS attacks are also unfortunately used by nefarious competitors to bring rival websites down, steal business, and gain market share.

## Protecting from DDoS attacks

DDoS solutions must ensure business continuity, with guaranteed uptime, and no performance impact. DDoS Protection must stop layer 3, 4, and 7 attacks and protect a businesses IP addresses, websites, network, and DNS.

> **Imperva's *DDoS Protection*** is included in **Imperva's *Cloud Application Security Platform*** and is the right defense against any DDoS attack. With an industry leading 3-second SLA to stop any attack of any size, Imperva ensures 99.999% uptime against any of today's modern DDoS attacks.

### LAYER 3/4 ATTACKS

- UDP floods
- NTP amplification
- DNS amplification
- Tsunami SYN flood
- CharGEN amplification
- Memcache amplification
- SSDP amplification
- SNMP amplification
- GRE-IP UDP floods
- CLDAP attacks
- ARMS (ARD)
- Jenkins
- DNS Water Torture
- SYN floods
- TCP RST floods SSL
- negotiation floods
- TCP connect() floods
- Fragmented attacks
- TCP ACK floods
- CoAP
- WS-DD
- NetBIOS

### LAYER 7 ATTACKS

- NS Query floods
- SlowLoris attack
- HTTP(S) GET request floods
- HTTP(S) POST request floods
- SMTP request flood

# 7 thru 10. Automated bot attacks

## Attack explanation

Sometimes known as bad bot attacks, OWASP classifies 21 unique automated threats that are considered the most consistently damaging to businesses. A quarter of all internet traffic is bad bots. Three of these automated threats are most prevalent—credential stuffing, scraping, and scalping attacks.

## Attackers goals

Bot attacks are considered some of the hardest to defend against because they are sophisticated and their behavior is created to appear human.

- CREDENTIAL STUFFING - Every website with a login page is a victim of these attacks by criminals seeking to perform account takeover of user accounts.
- SCRAPING - From stealing proprietary content like product descriptions and prices, competitors scrape content for every product continuously to win in the marketplace.
- SCALPING - From concert tickets to sneakers to gaming consoles, scalping bots (aka. Grinchbots and Sneakerbots) hoard items to resell on secondary markets. Launched by arbitrage experts, these bots negatively impact the human customer experience and force customers to pay exorbitant mark-ups to purchase limited edition or high demand items.
- 18 OTHER BAD BOT THREATS - include gift card abuse, carding, and spamming malware links into product review forms.

## Protecting from automated bot attacks

Detecting bots is difficult because the sophisticated ones try to appear human and evade detection. Your bot management solution must protect from every OWASP automated threat and be accurate in detecting the difference between human and bot traffic on your website, mobile apps, and APIs.

> **Imperva's *Advanced Bot Protection*** is included in **Imperva's *Cloud Application Security Platform*** and is acknowledged by Forrester as a two time industry leader in Bot Management and detects all of the OWASP automated threats. It helps reduce fraud and minimizes the business impact of price scraping and account takeover bots. Today it is used by companies to mitigate the world's most difficult bot problems on websites, mobile apps and APIs.

### AUTOMATED THREATS

- OAT-020 Account Aggregation
- OAT-019 Account Creation
- OAT-003 Ad Fraud
- OAT-009 CAPTCHA Defeat
- OAT-010 Card Cracking
- OAT-001 Carding
- OAT-012 Cashing Out
- OAT-007 Credential Cracking
- OAT-008 Credential Stuffing
- OAT-021 Denial of Inventory
- OAT-015 Denial of Service
- OAT-006 Expediting
- OAT-004 Fingerprinting
- OAT-018 Footprinting
- OAT-005 Scalping
- OAT-011 Scraping
- OAT-016 Skewing
- OAT-013 Sniping
- OAT-017 Spamming
- OAT-002 Token Cracking
- OAT-014 Vulnerability Scanning

Source: **OWASP Automated Threats Handbook**

# 11. Client side attacks

## Attack explanation

This supply chain attack exploits the growth of JavaScript services used in modern web applications. From chatbots to payment processors, attackers compromise the source code of these services and steal data from any website where the compromised code is used.

## Attackers goals

Performing a continuous single record data breach wherever the compromised code is deployed allows for stealthy data theft of credit cards and PII on multiple websites.

## Protecting from client side attacks

Many businesses are blind to data being transferred by third party JavaScript services because they are added by developers or marketing. Any solution should identify any new services added and prevent unauthorised communications.

> **Imperva's *Client-side Protection*** is included in **Imperva's *Cloud Application Security Platform*** and protects from formjacking, card skimming and magecart attacks. Discovers any new services added and blocks unauthorised services from being able to transfer data.

**CLIENT SIDE ATTACKS**

- Formjacking
- Credit card skimming
- Card skimming
- Skimmers
- Magecart
- JavaScript supply chain attacks

# 12 thru 13. Supply chain attacks

## Attack Explanation

Supply chain attacks exploit any vulnerabilities in third party services used in modern web applications. Examples include:

- SOFTWARE SUPPLY CHAIN ATTACKS (EG. SOLARWINDS) - Zero days or backdoors installed in consumer-off-the-shelf software or open source libraries used within any applications.
- CLIENT-SIDE SUPPLY CHAIN ATTACKS - Compromise of JavaScript services used on websites globally.

## Attackers goals

Software supply chain attacks like Solarwinds can deploy malware, allow espionage, and wreak havoc. Client-side supply chain attacks create continuous single record data breaches if payment processors are compromised.

## Protecting from supply chain attacks

For software supply chain attacks, businesses should consider embedding security within the application using a Runtime protection (RASP) solution. This provides zero-day protection for any 3rd party code. Client-side supply chain attacks must identify any data being transferred by third party JavaScript services. Any solution should identify any new services added and prevent unauthorised communication.

> **Imperva's *Client-side Protection*** is included in **Imperva's *Cloud Application Security Platform*** and protects from supply chain attacks like formjacking, card skimming and magecart. **Imperva's *Runtime Application Self-Protection (RASP)*** helps businesses protect legacy applications from within. RASP is capable of detecting and preventing zero-day attacks in real-time.

### SUPPLY CHAIN ATTACKS

**Software Supply Chain**

- Backdoors
- Zero days
- Target server
- Target client
- Malware distribution
- Data theft

**JavaScript Supply Chain**

- Formjacking
- Credit card skimming
- Card skimming
- Skimmers
- Magecart
- Data theft

# 14. Legacy application zero day attacks

## Attack explanation

Many legacy applications have zero day vulnerabilities that cannot be fixed. Protecting them from attacks is difficult because a signature of the attack is unavailable. Insiders using the application bypass other security tools and can successfully compromise legacy internal facing applications.

## Attackers goals

Similar to goals of OWASP Top 10 attacks, stealing intellectual property, personally identifiable information, financial data, and compromising the business.

## Protecting from legacy application attacks

Self protecting code or Runtime protection is the security solution to protect legacy applications, software supply chain attacks, and prevent insider threats attacking internal facing apps. Runtime Protection must detect zero day attacks and secure applications from within no matter where or how they are deployed, on-prem, in the cloud or via containers.

> **Imperva's *Runtime Application Self-Protection (RASP)*** helps businesses protect legacy applications from within. RASP is capable of detecting and preventing zero-day attacks in real-time.

### LEGACY APPLICATION ZERO DAY ATTACKS

- Insider threats
- Unknown new attacks
- Internal facing app attacks

**Techniques**

- Clickjacking
- HTTP Response Splitting
- HTTP Method Tampering
- Large Requests
- Malformed Content Types
- Path Traversal
- Unvalidated Redirects
- Software Supply Chain Attacks

**Injections**

- Command Injection
- Cross-Site Scripting
- Cross-Site Request Forgery
- CSS & HTML Injection
- Database Access Violation
- JSON & XML Injection
- OGNL Injection
- SQL Injection

**Weaknesses**

- Insecure Cookies & Transport
- Logging Sensitive Information
- Unauthorized Network Activity
- Uncaught Exceptions
- Vulnerable Dependencies
- Weak Authentication
- Weak Browser Caching
- Weak Cryptography

# 15. Serverless workload attacks

## Attack explanation

The migration to the cloud has seen more companies adopt Function-as-a-service (FaaS). The problem is that many incorrectly assume the cloud provider provides security while attackers see the opportunity to attack unprotected code within complex serverless workloads.

## Attackers goals

The Cloud Security Alliance's 12 most critical risks for serverless applications outlines what vulnerabilities are targeted and stealing data and exploiting the business remain the constant goals of bad actors.

## Protecting from serverless workload attacks

Serverless Protection must provide run-time security in the cloud, handle ephemeral workloads on functions that are rapidly created and decommissioned, and protect against widely used libraries from creating software supply chain risks.

> **Imperva's *Serverless Protection*** is an innovative security solution for applications deployed in Amazon Web Services (AWS). It wraps around the function code and protects against zero day exploits.

### CLOUD SECURITY ALLIANCE'S 12 MOST CRITICAL RISKS FOR SERVERLESS APPLICATIONS

- SAS-1: Function Event Data Injection
- SAS-2: Broken Authentication
- SAS-3: Insecure Serverless Deployment Configuration
- SAS-4: Over-Privileged Function Permissions & Roles
- SAS-5: Inadequate Function Monitoring and Logging
- SAS-6: Insecure Third-Party Dependencies
- SAS-7: Insecure Application Secrets Storage
- SAS-8: Denial of Service & Financial Resource Exhaustion
- SAS-9: Serverless Business Logic Manipulation
- SAS-10: Improper Exception Handling and Verbose Error Messages
- SAS-11: Obsolete Functions, Cloud Resources and Event Triggers
- SAS-12: Cross-Execution Data Persistency
- Weak Authentication
- Weak Browser Caching
- Weak Cryptography

# How Imperva helps stop these attacks

Imperva Application Security provides multi-layered protection to make applications and websites always available, always user-friendly and always secure. The company's flagship Web Application & API Protection (WAAP) solution stops advanced cybersecurity threats from a unified platform with multiple market-leading products: Web Application Firewall (WAF), DDoS protection, Runtime Application Self-Protection (RASP), API security, Advanced Bot Protection, Client-Side Protection, Serverless Protection, Content Delivery Network and Attack Analytics.

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.

## Protect your business. Easily.

For a free 30 day trial of Imperva's Cloud Application Security platform, go to www.imperva.com.

## About Imperva

Imperva is the cybersecurity leader whose mission is to protect data and all paths to it. Imperva protects the data of over 6,200 customers from cyber attacks through all stages of their digital journey. Imperva Research Labs and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy and compliance expertise into our solutions.