imperva

Unveiling Unseen Requirements: Empowering Organizational Security & Control from the Core

Shailes Nanda, CISSP – Principal EMEA Security Engineer
shailes.nanda@imperva.com

TODAY'S APPLICATIONS & APIS REMAIN UNDER CONSTANT ATTACK

DDoS Attacks

LAYER 3/4
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

DDoS Attacks

LAYER 7
NS Query floods
SlowLoris attack
HTTP(S) GET request floods
HTTP(S) POST request floods
SMTP request flood

OWASP Top 10 Attacks

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

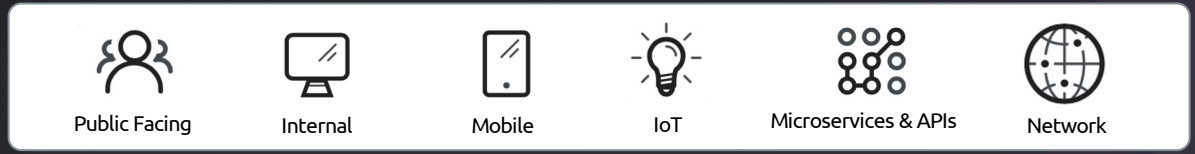
OWASP Automated Threats

Account Aggregation
Account Creation
Ad Fraud
CAPTCHA Defeat
Card Cracking
Carding
Cashing Out
Credential Cracking
Credential Stuffing
Denial of Inventory
Denial of Service
Expediting
Fingerprinting
Footprinting
Scalping
Scraping
Skewing
Sniping
Spamming
Token Cracking
Vulnerability Scanning

Supply Chain & Zero Day Attacks

Insider threats
Unknown attacks
Internal facing apps

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



OWASP API Top 10 Attacks

Broken object level authorization
Broken user authentication
Excessive data exposure
Lack of resources & rate limiting
Broken function level authorizatio
Mass assignment
Security misconfiguration
Injection
Improper assets management
Insufficient logging & monitoring

Client-side Attacks

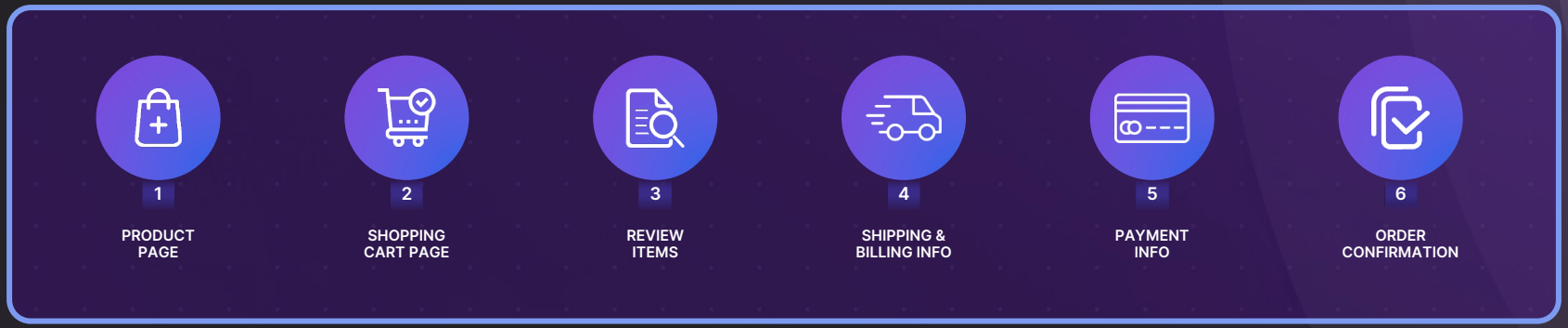
Formjacking
Credit card skimming
Card skimming
Digital Skimmers
Magecart
JavaScript supply chain attacks

Serverless Attacks

Event injection
Denial of wallet
Business logic manipulation

INJECTIONS
Command Injection
Cross-Site Scripting
Cross-Site Request Forgery
CSS & HTML Injection
Database Access Violation

Protecting required for business logic attacks



What is business logic?

Business logic is the custom rules or algorithms that handle the exchange of information between a database and user interface

Business logic vulnerabilities are flaws in the design and implementation of an application that allow an attacker to manipulate legitimate functionality to achieve a malicious goal

Imperva

Known for Web Application Firewall

Evolving Critical Infrastrucure Protection

External

Script Kiddies

Disgruntled Employees

Good and Bad Bots

Legitimate Compromised User

Sponsored Attack

- DDOS
- GBLS
- CDN
- WAAP
- ABP/
- ATOS
- CSP
- API

80

443

FW, NGFW, IPS, Anti-Malware
-Application aware? App Layer 7?

Technical Attacks
-XSS, SQLi, OWASP

Biz Logic Attacks
-Bots, DDoS
-Site Scraping

Fraud IP Reputation
ATO

WAAP/API

- AWS
- Azure
- GCP
- On Prem

Analytics & Insights

Big Data

- Hadoop
- Mongo
- Hive, HBase, HDFS

Files

- Financial
- PII / PHI
- Credit Card
- IP

Databases

- Oracle
- MS SQL
- DB2
- mySQL
- Terradata
- etc.

Data Security & Audit

RASP

Analytics & Insights

Internal

Malicious User

Employee

Compromised User

The Imperva Difference – App Security + Delivery

Before:

- Used multiple vendors for security, bot mitigation, DDoS and CDN.
- Required application delivery rules that respond rapidly to market demands and as part of DevSecOps.
- High cost to security operations due to maintaining multiple vendors solutions.
- Limited capability to manage changes due to time delay in activating changes.

After:

- **Imperva Cloud Application Security provides a vertically integrated solution that unify capabilities to address all use-cases with single onboarding.**
- **Imperva Cloud Application Security enforced policy in real-time enabling advanced automation to drive more value in operations.**
- **Unique single stack approach enabled 90% savings on content served (bandwidth) by offloading it through Imperva Cloud Application Security CDN.**

The Imperva Difference – Data Security

A global bank improved their ability to detect, respond, and recover from potential anomalies while meeting their NIST–based compliance requirements.

The scope of the analysis was ~7.2B bank transactions during a 60 day period.

Before: Native Audit & Splunk

- 85,000 incidences in 60 days
- ~10,000 alerts per week
- 2 FTE
- 10% of alerts investigated
- 0 significant incidents discovered

After: Imperva

- 723 incidences in 60 days
- ~60 incidents per week
- 2 FTE
- 100% of incidents investigated
- 6 significant incidents discovered

Results

- Machine learning no tuning
- Manageable # of alerts
- Equivalent FTE
- All incidents investigated
- 914k DB records accessed by 1 person

Thank you