Defense in Depth - API Edition

Shahn Backer | Snr. Solutions Architect | F5
API Growth

20 M
users

1.13 B
requests made

Greater the Growth.. Greater the Attention

Breach Story 1: Large Telco

- 10 Million customer exposed
- One attacker wanted $1 million in cryptocurrency (Later apologized and claimed to have deleted data)
- Reports suggest breach due to an API available online without authentication

Source: The Guardian
Understand The Exposure

OWASP API Top 10
OWASP API Top 10 (2019)

- Broken Object Level Authorization
- Broken User Authentication
- Excessive Data Exposure
- Lack of Resource & Rate Limiting
- Broken Function Level Authorization
- Mass Assignment
- Security Misconfiguration
- Injection
- Improper Assets Management
- Insufficient Logging and Monitoring
# OWASP API Top 10 (2019)

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>API1:2019</td>
<td>Broken Object Level Authorization</td>
<td>Identity &amp; Access</td>
</tr>
<tr>
<td>API2:2019</td>
<td>Broken User Authentication</td>
<td>Identity &amp; Access</td>
</tr>
<tr>
<td>API3:2019</td>
<td>Excessive Data Exposure</td>
<td>Application Security</td>
</tr>
<tr>
<td>API4:2019</td>
<td>Lack of Resource &amp; Rate Limiting</td>
<td>Network &amp; Infra</td>
</tr>
<tr>
<td>API5:2019</td>
<td>Broken Function Level Authorization</td>
<td>Identity &amp; Access</td>
</tr>
<tr>
<td>API6:2019</td>
<td>Mass Assignment</td>
<td>Identity &amp; Access</td>
</tr>
<tr>
<td>API7:2019</td>
<td>Security Misconfiguration</td>
<td>Network &amp; Infra</td>
</tr>
<tr>
<td>API8:2019</td>
<td>Injection</td>
<td>Application Security</td>
</tr>
<tr>
<td>API9:2019</td>
<td>Improper Assets Management</td>
<td>Identity &amp; Access</td>
</tr>
<tr>
<td>API10:2019</td>
<td>Insufficient Logging and Monitoring</td>
<td>Application Security</td>
</tr>
</tbody>
</table>
Understanding Security Controls
# Reactive vs Proactive vs Predictive

## Schools of security controls

<table>
<thead>
<tr>
<th></th>
<th>Reactive</th>
<th>Proactive</th>
<th>Predictive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Premise</strong></td>
<td>Time taken by attacker to cause damage is greater than time taken to detect and react</td>
<td>Process and activities performed periodically to identify and eliminate vulnerabilities</td>
<td>Using contextual analysis to identify threats before they become incidents</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>Adding IPs to Deny-list after 10 failed logon attempts</td>
<td>Payload inspection by a WAF/WAAP</td>
<td>Behavioral – Malicious user detection</td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td>Stop-gap when all controls fail</td>
<td>Real runtime protection</td>
<td>Advance warning and protection</td>
</tr>
<tr>
<td><strong>Powered By</strong></td>
<td>Logs and telemetry data indicating attacks</td>
<td>Real time analysis of traffic</td>
<td>Machine learning on telemetry data</td>
</tr>
</tbody>
</table>
Types of Controls
Negative vs Positive vs Assistive

Positive Security
1. Allow known good
2. Enforcing Swagger
   • HTTP VERB/Method
   • URL Endpoint
3. Allow API and non-API traffic on the same base URL

Negative Security
1. Rate limiting
2. Malicious Payload check
3. IP intelligence

Assistive (Machine Learning/AI)
1. API Discovery
2. Anomaly detection
Defense in Depth for APIs
Defense-in-Depth for APIs

SECURITY AND VISIBILITY THAT COUNTS

Perimeter defense
- DDoS protection
- Rate-limiting
- Bot defense

Network defense
- SSL Decryption
- Intrusion Prevention
- Firewall monitoring

Application defense
- WAAP
- Anomaly detection
- Shadow API discovery

Data defense
- Modern authentication
- Advanced access control
- Sensitive data masking

Policy and Procedures
- Risk management
- Audit and monitoring
Deploying the Controls
Deploying Security Controls for API

API Security (WAAP)
- App Security (L7)
- API Discovery
- Network Security (L3-L4 DoS)
- Anycast/GSLB

API Management
- Developer portal
- G/W management
- Visibility
- Versioning
- Documentation

API GW CLUSTER
- Routing, Billing
- AuthN/AuthZ

API Security (API Key or OAuth)
- Access Control
Demo

Shadow APIs Detection and Mitigation
Shadow APIs & How to tackle them

Threat mitigation techniques
• Allow/Deny request
• Rate Limits
API Security Maturity Model at Runtime

- Reactive Security
- Proactive Security
- Predictive Security

- AI/ML Enabled
- Behavioral App/API Security
- WAAP + MCN
- Access Control

Shift-Right