API Security

The New Frontier

Dave Ferguson
Director of Product Management, Qualys, Inc.
Agenda

The Rise of APIs
A Different Top 10 List from OWASP
Swagger / OpenAPI
Qualys API Security
The Rise of APIs

REST APIs are everywhere
  • 83% of all web traffic is API traffic

Web & mobile apps, IoT devices

Popularity of microservice architectures
  • Better resiliency, scalability, reusability

Public APIs
  • Unlock data for new revenue streams

Vendor/product APIs
# API Security Top 10

1. Broken Object Level Authorization (BOLA)
2. Broken User Authentication
3. Excessive Data Exposure
4. Lack of Resources & Rate Limiting
5. Broken Function Level Authorization
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Assets Management
10. Insufficient Logging & Monitoring
Swagger / OpenAPI

**Swagger** is a specification to describe an API
Name changed to **OpenAPI** starting with version 3
  - OAS = OpenAPI Specification

**About Swagger/OAS files:**
  - Either JSON or YAML format
  - Typically available from dev teams
  - Often auto-generated by tools
Example: Uber API

<table>
<thead>
<tr>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /products</td>
</tr>
<tr>
<td>Product Types</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Estimates</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /estimates/price</td>
</tr>
<tr>
<td>Price Estimates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Estimates</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /estimates/time</td>
</tr>
<tr>
<td>Time Estimates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /me</td>
</tr>
<tr>
<td>User Profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /history</td>
</tr>
<tr>
<td>User Activity</td>
</tr>
</tbody>
</table>
"/estimates/time": {   "get": {     "summary": "Time Estimates",     "description": "Get trip time estimate",     "parameters": [       { "name": "start_latitude", "in": "query", "required": true, "type": "number", "format": "double" },       { "name": "start_longitude", "in": "query", "required": true, "type": "number", "format": "double", "minimum": -90.0, "maximum": 90.0 },       { "name": "product_id", "in": "query", "type": "string", "maxLength": 30, "pattern": "{0-9a-zA-Z','}"    ]   }
Swagger Global Security Directives

```
"schemes": [
  "http",
  "https"
],

"security": [
  {
    "securityDefinitions": {
      "myBasicAuth": {
        "type": "basic"
      },
      "myApiKey": {
        "type": "apiKey",
        "name": "api_key",
        "in": "header"
      },
      "myOAuth2": {
        "type": "oauth2",
        "authorizationUrl": "https://auth.petstore.com/oauth/form",
        "flow": "implicit",
        "scopes": {
          "write:pets": "create or modify pet data",
          "read:pets": "read pet data"
        }
      }
    },
  }
],
```
Qualys API Security

Static Assessment of your Swagger / OpenAPI file
- Get a score and recommended changes

Conformance Scan
- Test the API endpoints for behaviors that violate the Swagger file "contract"

Vulnerability Scan
- This is a current feature of Qualys Web Application Scanning (WAS)
DEMO: Qualys API Security
Final Thoughts

The use of APIs will continue to expand

Insecure APIs are a growing threat

API security requires a different approach compared to web applications

Qualys API Security will help developers secure APIs from design to development to production
Thank You

Dave Ferguson
dferguson@qualys.com