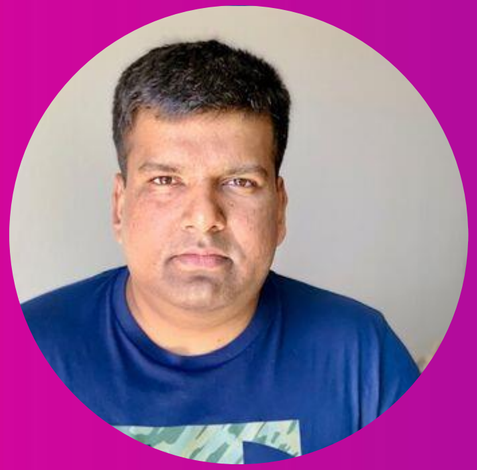
Pro Workshop

TOP API SECURITY THREATS & SOLUTIONS

Who We Are

The Presenters



INTESAR MOHAMMED

CEO | Security Researcher
@ CyberSecuriti.ai

Work Experience & Publications in APIs and Security

5 Patents in Security & Cloud

Leadership roles at VMware, Cisco, HyperGrid

Agenda

Session Timeline

TOP EXPLOITS

Top exploits targeting the API layer

DEMO

Detection techniques

Q&A

HOW APIS TRANSFORMING THE INDUSTRY

- **Building Blocks**

  APIs are the new building blocks for automation wave

- **Programmable Interface**

  APIs provides an easy and flexible programmable interface allowing a large number of client applications quickly consume and process functionality

- **API Economy**

  Most SaaS & Cloud businesses requires APIs for industry adoption. Salesforce generates 50% revenue through APIs and Expedia over 90%. Cloud services revenue from APIs is going grow to 65% by 2023

DevOps Adoption

API POWERED

Most organizations today are building Apps and Services powered by API

DEVOPS RUSH

In their rush towards adopting DevOps and releasing products faster, they've forgotten to include security leaving the products vulnerable

MAJORITY ATTACK

Majority of reported cyber attack have targeted the API layer and business logic flaws in general

PRIVACY LAWS

To make matters even worse the new CCPA and GDPR privacy laws now require organizations to report accidental exposure/breaches and pay compensation to the customers

#1 Unprotected Endpoints

COMMON FLAW

5% of the API endpoints are left unprotected.

EASY TO DETECT

- No special tools are required.
- You can use curl for discovery

Live Demo

DETECT UNPROTECTED ENDPOINTS

#2 ABAC

BUSINESS LOGIC FLAWS

A typical 100 endpoint API has over 200 data operations (create, read, modify, actions, delete, etc.)

DATA ACCESS CONTROLS

As organizations race towards DevOps and releasing new features faster, often the continuous security is overlooked

Live Demo

DETECT ABAC VULNERABILITIES

ABAC Breach Case Studies

USPS.COM

- 60M Customer Records Lost
- GET: /customers/{id}
  - Any authenticated user can request data from the above endpoint by using a valid customer-id

VULNERABILITY DISCOVERY

- Sign up two accounts User-A & User-B

- Invoke GET: /customers/{User-A} as User-A -> Response {UserA data}

- Invoke GET: /customers/{User-A} as User-B -> Response
  {No Data} - No vulnerability
  {UserA data} - vulnerability

IS IMPLEMENTING ACCESS-CONTROLS EASY?

Imagine Box.com APIs

- Consider this endpoint
  https://api.box.com/2.0/files/file_id

- Private file
- Shared file
- Public file
- Org public file
- Public URL or ID
- Auto expiring ID

#3 RBAC

PRIVELEGE ESCALATIONS

Misconfigured role to endpoint mapping can give escalated or admin access to the regular users

Live Demo

DETECT RBAC VULNERABILITIES

RBAC Breach Case Studies

MICROSOFT OUTLOOK.COM

- 6% Outlook inboxes were breached
- Hackers stole support agent credentials

RBAC DESIGN FLAW

- The support agent role had access to message subjects and compose-send operation
- No access to read the message body, forward and delete messages - This made perfect sense
- Had access to add forwarding rules - This is how the hackers breached!

OWASP WEB/MOBILE

INJECTION

STORED INJECTION

SENSITIVE DATA EXPOSURE

DoS

OLD FRAMEWORKS WITH KNOWN VULNERABILITIES

XSS

INSUFFICIENT LOGGING

INSECURE COMMUNICATION

Q&A

intesar@fxlabs.io

Thank You!