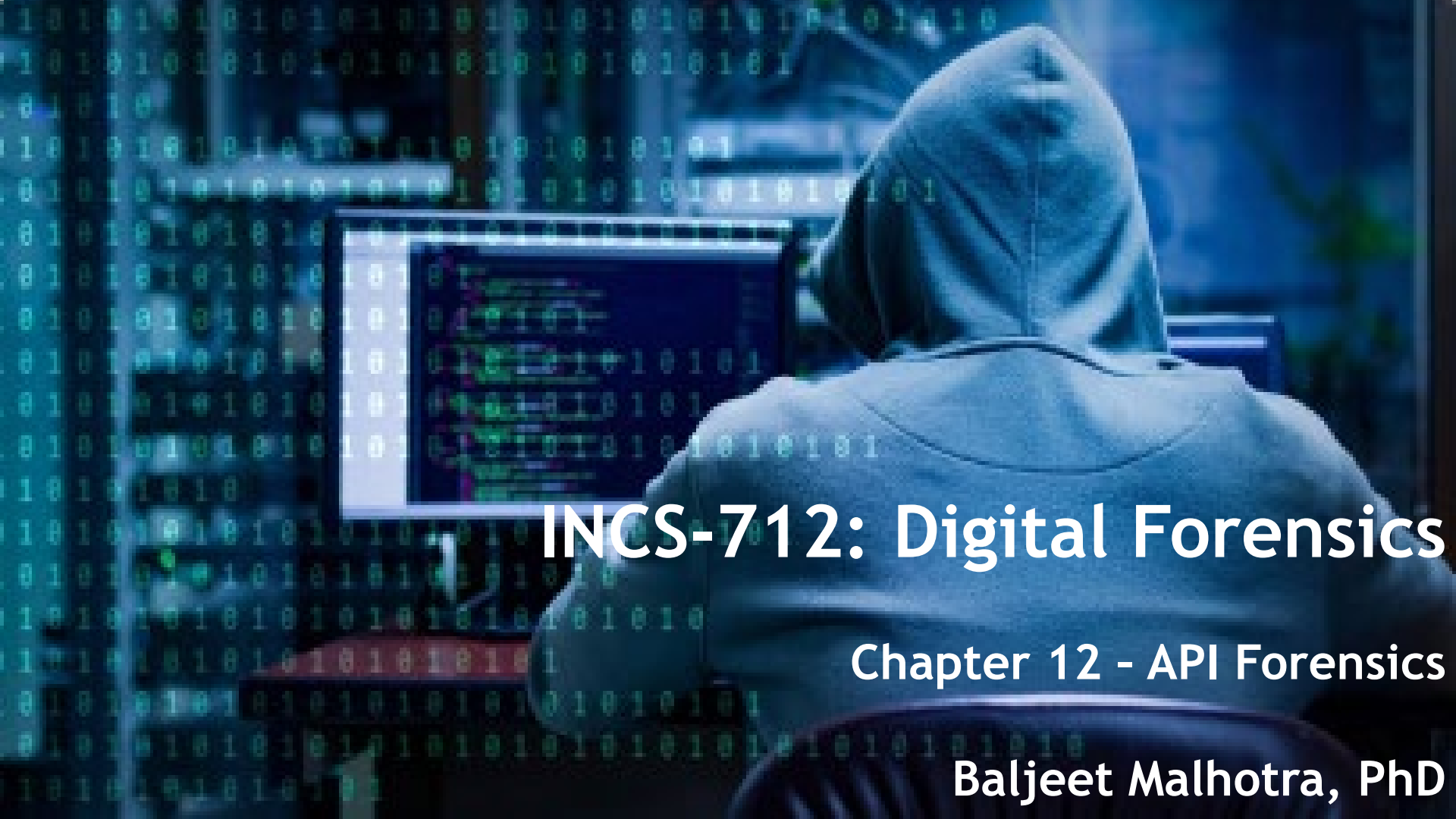
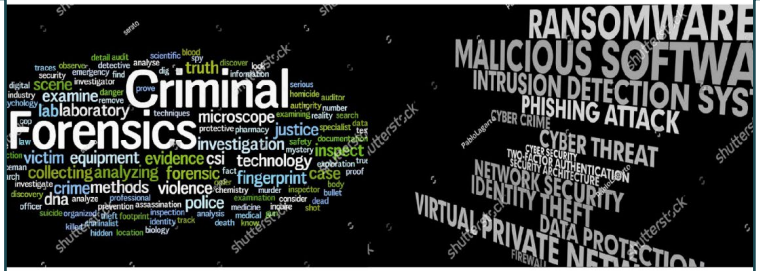


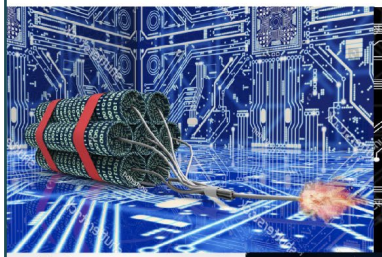
INCS-712: Digital Forensics

Chapter 12 - API Forensics

Baljeet Malhotra, PhD

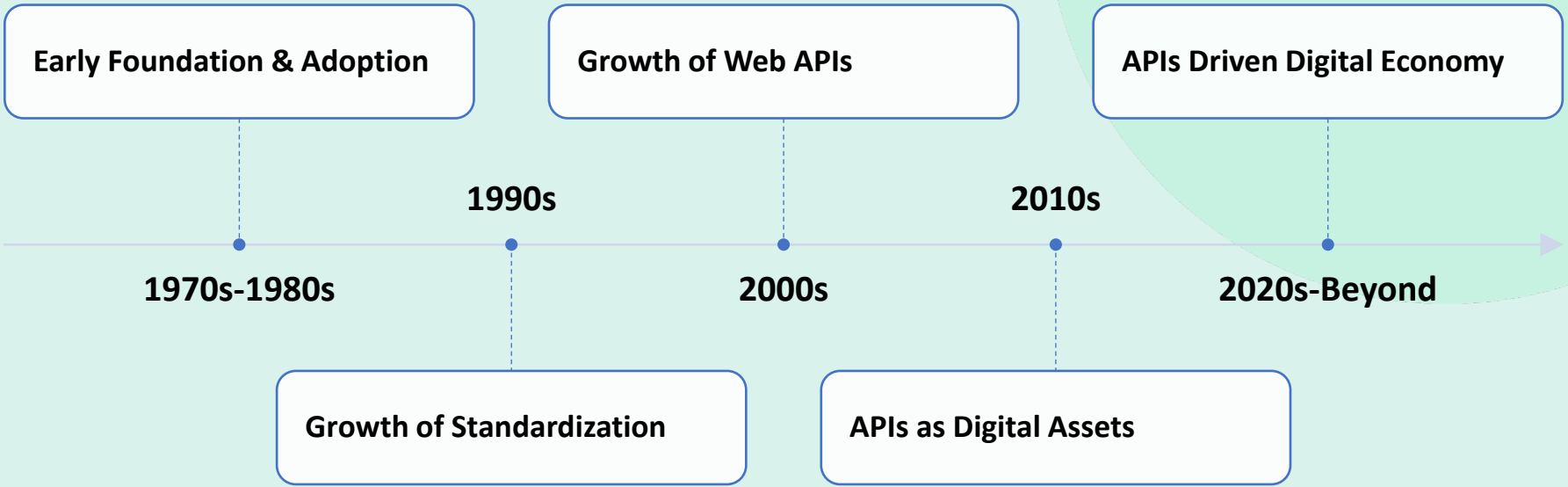


API Security Blueprint

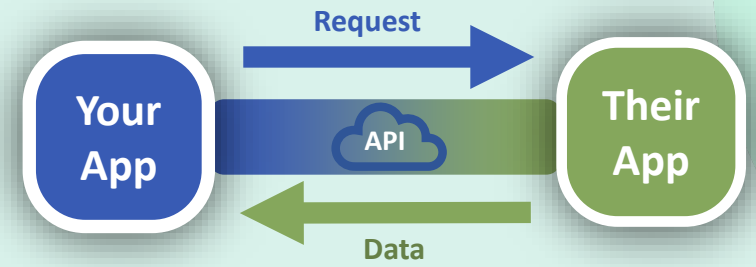


- **30 mins: Introductions and Overview**
  - Brief History of APIs
  - Importance of APIs in Digital Ecosystem
  - Motivations for Securing APIs
- **30 mins: Basics of API Security**
  - Examples of API Breaches/Impacts
  - Understanding API Attacks/Patterns
- 15 mins: ..... {Case Study}
- **25 mins: Advanced API Security**
  - OWASP Top 10: Authentication and Authorization
  - OWASP Top 10: Injections and Rate Limits
- **25 mins: Hands-on API Security**
  - Hands-on: Configuring API Security Tests
  - Hands-on: Executing API Security Tests
- 20 mins: : .....{Exercise}
- **50 mins: API Security Program**
  - Preventing API Attacks
  - Role of API Gateways
  - Continuous API Monitoring
- **30 mins: Summary and Conclusions**
  - Take Home Exercises
  - Questions and Answers

Brief History of APIs



Web Based APIs



An API is light-weight software that connects applications & systems throug the Internet, e.g., Google Maps

Examples include making a purchase on Amazon using PayPal, or booking a flight on Delta using Priceline.

Most large companies have built APIs either for customers, for internal use or for independent vendors.

Importance of APIs in Today's Digital Economy

Why care about API Forensics ?

API Security Incidents - Some Real Examples

1+ Billions
Users affected

2021: Facebook postings (unauthorized) via API

3+ Thousands
Student affected

2020: Aura COVID tracing app compromised via API

2+ Millions
Customers affected

2018: T-Mobile was attacked through a leaky API on their website

1+ Millions
Customers affected

2021: VMWare - vRealize API compromised to steal administrative credentials

7+ Millions
Customers affected

2019: Venmo had millions of transactions scraped through an API

2+ Millions
Patients affected

2018: Atrium Health Care Personal data exploited through an API

Atrium Health GATEHUB T-Mobile venmo Uber Instagram

API Security Incidents - Some Real Examples

30+ Millions
Vehicles affected

2024: Kia APIs exploited to access remote features

1+ Thousand
Employees affected

2023: OpenAI' messaging system hacked via APIs

2+ Millions
Customers affected

2021: Peloton API exposed user details: age, gender, etc.

3+ Millions
Expense loss (Q2)

2024: Advance Auto Parts API leaked employee/user details

10+ Millions
Customers affected

2022: Optus customer data exposed via unauthorized API

5+ Millions
Users affected

2022: Twitter API exposed user data: name, email, phone

KIA OpenAI PELOTON Advance Auto Parts OPTUS X

API Incidents – Deepseek (Jan 2025)

Company: DeepSeek (AI startup based in China)

Incident: A publicly accessible database exposed over a million log lines containing sensitive user data, chat histories, API authentication keys, and system logs.

Impact: Unauthorized access led to privilege escalation, data leak, and system breache.

Consequences: The issue was promptly addressed after being reported by security firm Wiz, but it remains unclear if data was accessed before remediation.

Reference: https://www.theverge.com/news/603163/deepseek-breach-ai-security-database-exposed

API Incidents – U.S. Treasury Department (Dec 2024)

Company: U.S. Treasury Department

Incident: A state-sponsored attacker from China exploited a compromised API key from BeyondTrust's remote support software, gaining unauthorized access to workstations and unclassified documents

Impact: The breach posed a severe threat to national security and data integrity

Consequences: The Treasury, in collaboration with CISA and the FBI, revoked the compromised API key and shut down the affected service

Reference: https://www.theverge.com/2024/12/30/24332429/us-treasury-department-beyondtrust-hack-security-breach

API Incidents – Kia's Web Portal Vulnerability (Sep 2024)

Company: Kia Motors

Incident: A flaw in Kia’s web portal allowed unauthorized access to internet-connected vehicle features, enabling attackers to track vehicle locations, unlock doors, honk horns, and start ignitions using only a license plate number

Impact: Millions of vehicles were potentially vulnerable to remote exploitation

Consequences: Kia patched the vulnerability after being notified in June. Similar issues were found in other car manufacturers' systems, highlighting a widespread industry concern

Reference: https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track

API Incidents – Optus Data Breach (Nov 2024)

Company: Optus (Australian telecommunications provider)

Incident: An exposed API endpoint allowed unauthorized access to personal information of over 10 million customers, including names, addresses, and passport details

Impact: Major privacy violation affecting millions of users

Consequences: The Australian government and regulators launched investigations, and Optus faced significant reputational damage and legal scrutiny

Reference: https://www.upguard.com/blog/how-did-the-optus-data-breach-happen

API Incidents – Twitter Exploit (April 2024)

Company: Twitter (X)

Incident: Attackers exploited a vulnerability in Twitter's API to scrape data of 200 million users, including email addresses and phone numbers

Impact: Risk of phishing attacks and identity theft

Consequences: Twitter faced backlash over weak API security and had to implement stricter rate limits and security measures

Reference: https://purplesec.us/breach-report/twitter-data-leak-200-million-users/?utm

API Incidents – Smart Car API Exploit (2024)

Company: Mercedes Benz Group

Incident: Identified a valid Subaru employee email address. Guessed with a simple LinkedIn search. API access was possible through an auth API endpoint that returned an error message with an invalid address. This behavior enabled attackers to systematically guess email addresses until a valid account was found (account enumeration vulnerability).

Impact: The affected parties were the employees and customers.

Consequences: Unauthenticated users remotely controlled vehicles in the United States, Japan, and Canada.

Reference: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#authentication-and-error-messages

API Incidents – Kronos API Attack (2023)

Company: Kronos Research (Fintech and Cryptocurrency firm)

Incident: Attackers gained unauthorized access through compromised API keys

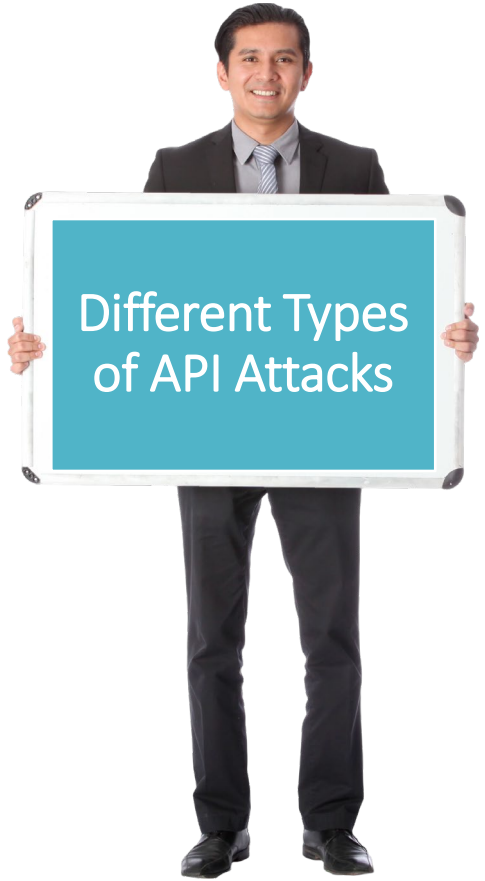
Impact: The company suffered financial losses estimated at $25 million

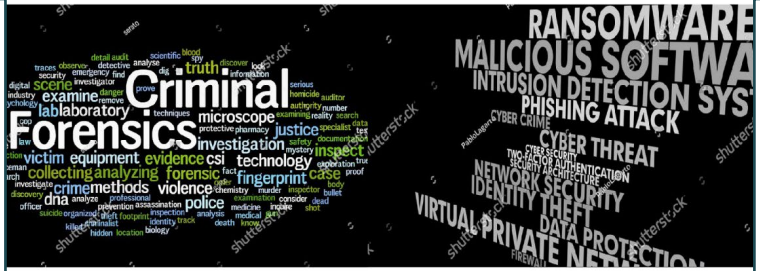
Consequences: This incident reinforced the necessity of strong API key security policies to prevent unauthorized access and financial damage

Reference: https://apisecurity.io/issues-235-25m-loss-at-kronos-due-to-api-key-loss-and-three-other-api-vulnerabilities

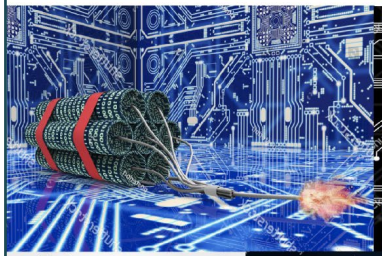
Question 1

Are there different types of API Attacks ?





API Security Blueprint



- **30 mins: Introductions and Overview**
  - Brief History of APIs
  - Importance of APIs in Digital Ecosystem
  - Motivations for Securing APIs
- **30 mins: Basics of API Security**
  - Examples of API Breaches/Impacts
  - Understanding API Attacks/Patterns
- 15 mins: ..... {Case Study}
- **25 mins: Advanced API Security**
  - OWASP Top 10: Authentication and Authorization
  - OWASP Top 10: Injections and Rate Limits
- **25 mins: Hands-on API Security**
  - Hands-on: Configuring API Security Tests
  - Hands-on: Executing API Security Tests
- 20 mins: : .....{Exercise}
- **50 mins: API Security Program**
  - Preventing API Attacks
  - Role of API Gateways
  - Continuous API Monitoring
- **30 mins: Summary and Conclusions**
  - Take Home Exercises
  - Questions and Answers

Understanding API Attacks - Overview

Types of Attacks (7)	Description
API Spoofing	Attackers create fake APIs that imitate legitimate ones. When users connect to these fake APIs, attackers can steal user credentials or inject malware into the user's system.
API Injection	Malicious code is inserted into valid API calls to execute it on the targeted system. This can be achieved by exploiting API input flaws or intercepting and modifying API calls using man-in- the-middle attacks.
API Fuzzing	Attackers modify parameters in API calls to gain unauthorized access or manipulate data. This can be done by intercepting and modifying API calls or using automated tools to manipulate API inputs.
API Poisoning	API poisoning refers to the process of manipulating the data used by an API to corrupt its functionality, disrupt services, or degrade the quality of responses. This attack targets the data that the API processes, often aiming to corrupt the underlying systems or machine learning models that the API might rely on.
API DoS	Deniel of Service (DoS). APIs are overwhelmed with excessive requests, causing them to crash or become unresponsive. This can be achieved by flooding the API with requests using automated tools or exploiting vulnerabilities in the API's design or implementation.
API Phishing	Users are deceived into connecting to fake APIs that appear legitimate. When users enter their credentials into these fake APIs, attackers steal them for future use.
API RCE	Remote Code Execution (RCE). API RCE attacks leverage weaknesses in APIs to execute arbitrary code on the targeted machine. This can be accomplished by using a malicious payload in an API call or exploiting vulnerabilities in the API's input validation or authentication mechanisms.

API Attack - Spoofing

API Spoofing

Create fake APIs

Connect to these APIs

Steal credentials

Inject malware

API Attack - Injection

API Injection

Intercept/modify API call

Exploit API input flaws

Insert code via valid API call

Execute code on the target

API Attack - Remote Code Execution (RCE)

API RCE

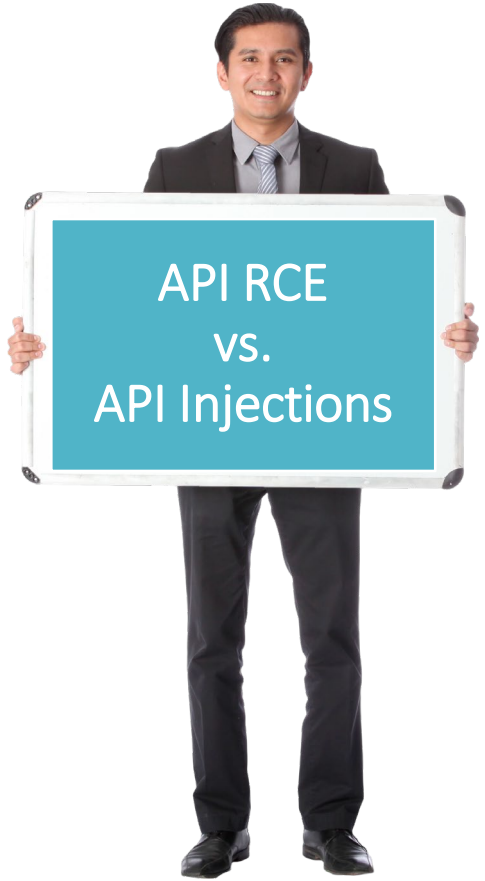
Design malicious payloads

Exploit vulnerabilities in the API's input validation or authentication mechanisms

Execute arbitrary code on the targeted

Question 2

What is the difference between API Remote Code Execution and API Injection Problems ?



API RCE vs API Injections

Attack Features	API RCEs	API Injections
Method	Exploits insecure deserialization, command injection, or code execution flaws in endpoints.	Injecting malicious payloads into API requests to manipulate or access unauthorized data.
Impact	Allows to run arbitrary commands, gain system control, exfiltrate data, or deploy malware.	Unauthorized access, data leaks, or application manipulation without direct system compromise.
Examples	- Exploit deserialization via untrusted JSON input to execute arbitrary code. - Using an API endpoint to execute system commands (e.g., os.system()).	- SQL Injection via API query parameters. - Injecting malicious XML payloads in SOAP APIs. - Cross-Site Scripting (XSS) via JSON responses.
Prevention	- Avoid unsafe deserialization. - Use input validation & parameterized queries. - Restrict API permissions. - Implement Web Application Firewalls (WAFs).	- Implement strong input validation. - Use parameterized queries and prepared statements. - Enforce Content Security Policies (CSP).

API Attack - Fuzzing

API Fuzzing

Manipulate API inputs

Intercept/modify API call

Modify parameters in API call

Gain unauthorized access

Manipulate data

API Attack - Phishing

API Phishing

Deceive with fake APIs

Steal credentials when users enter details

Use credentials for APTs

API Attack – Denial of Service (DoS)

API DoS

Overwhelm system with excessive API requests

Use automated tools to flood systems with API requests

Exploit design/implementation vulnerabilities

API Attack - Poisoning

API Poisoning

Manipulate data used by an API

Corrupt its functionality

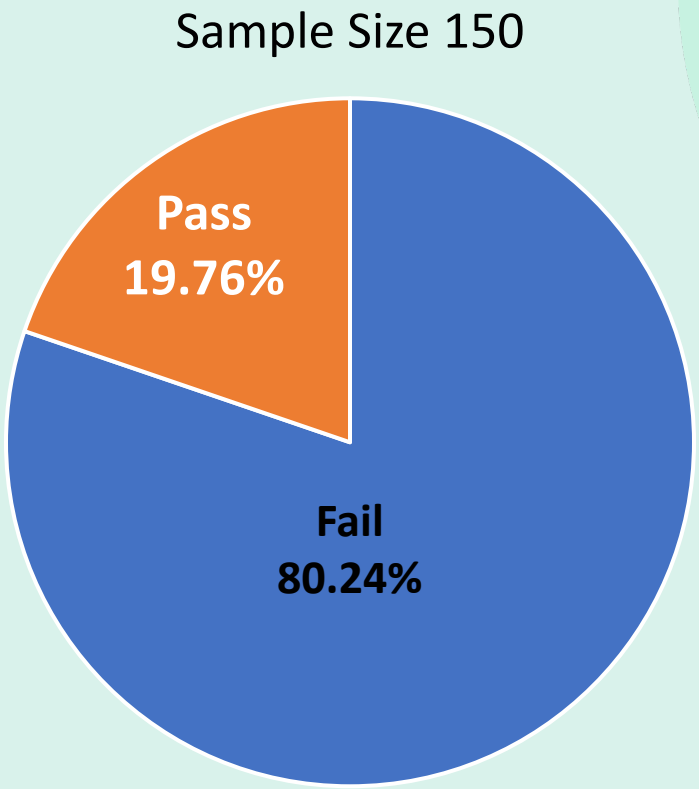
Disrupt services/degrade quality

Aimed at corrupting underlying systems or ML models

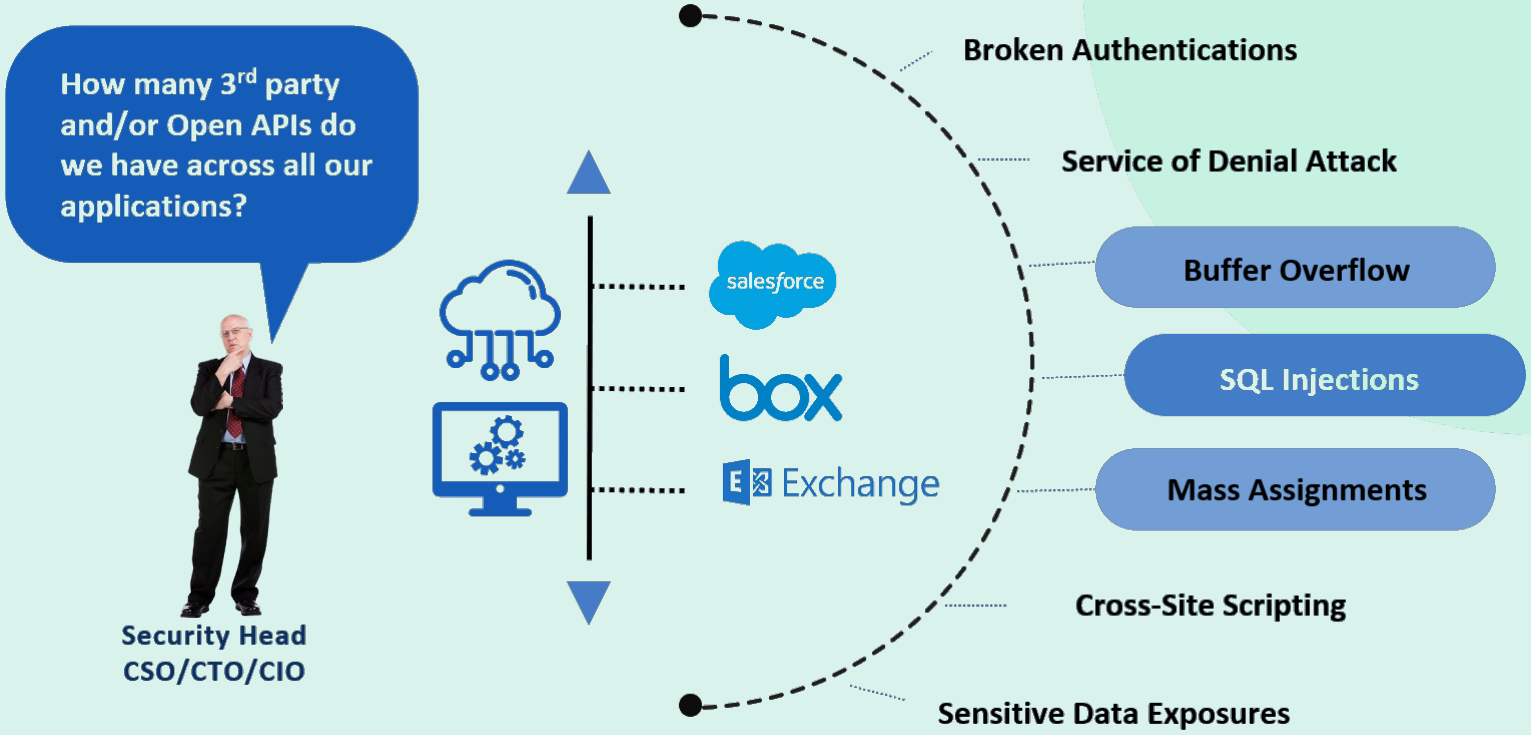
API Attack Cases

API	Category	Function	Vulnerability 1	Vulnerability 2	Possible Attack
API 1	Event Management	Create, cancel, and delete events.	Server leaks version information via 'server' HTTP response header	No Strict-Transport-Security Header Setting	API DoS API Injections
API 2	Public Sector	Provides approximate location of litter bins.	Server leaks version information via 'server' HTTP response header		API DoS
API 3	Finance Banking	EUR/USD conversion	Cookie without secure flag	Cookie without same site attribute	API DoS
API 4	Space Exploration	Launched Spacecrafts & Rockets data	Cross-domain misconfiguration	x-Content-Type-Options Header Missing	API DoS API Phishing

API Vulnerability Tests - Summary of Results

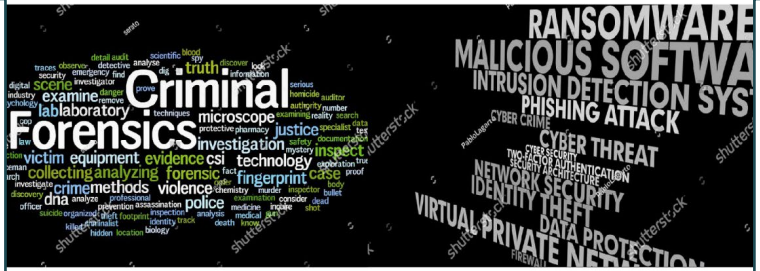


Open and 3rd Party APIs

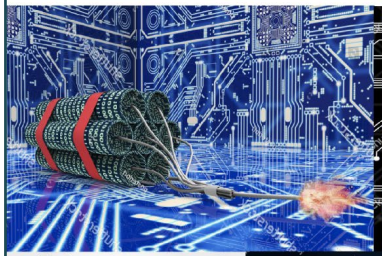


Question 3

Are you familiar with API Security Frameworks ?



API Security Blueprint



- **30 mins: Introductions and Overview**
  - Brief History of APIs
  - Importance of APIs in Digital Ecosystem
  - Motivations for Securing APIs
- **30 mins: Basics of API Security**
  - Examples of API Breaches/Impacts
  - Understanding API Attacks/Patterns
- 15 mins: …… {Case Study}
- **25 mins: Advanced API Security**
  - OWASP Top 10: Authentication and Authorization
  - OWASP Top 10: Injections and Rate Limits
- **25 mins: Hands-on API Security**
  - Hands-on: Configuring API Security Tests
  - Hands-on: Executing API Security Tests
- 20 mins: : ……{Exercise}
- **50 mins: API Security Program**
  - Preventing API Attacks
  - Role of API Gateways
  - Continuous API Monitoring
- **30 mins: Summary and Conclusions**
  - Take Home Exercises
  - Questions and Answers

OWASP Top 10

- Broken Object Level Authorization
- Broken Authentication
- Broken Object Property Level Authorization
- Unrestricted Resource Consumption
- Broken Function Level Authorization
- Unrestricted Access to Sensitive Business Workflow
- Server-Side Request Forgery
- Security Misconfiguration
- Improper Inventory Management
- Unsafe Composition of APIs

Top 1 - Broken Object Level Authorization

Broken Object Level Authorization (BOLA)

API call parameters use the ID of the resource accessed through the API /api/shop1/financial_info.

Attackers replace the IDs of their resources with a different one which they guessed through /api/shop2/financial_info.

The API does not check permissions and lets the call through.

Problem is aggravated if IDs can be enumerated /api/123/financial_info.

Top 2 - Broken Authentication

Broken Authentication

- Unprotected APIs that are considered “internal”
- Weak authentication that does not follow industry best practices
- Weak API keys that are not rotated
- Passwords that are weak, plain text, encrypted, poorly hashed, shared, or default passwords
- Authentication susceptible to brute force attacks and credential stuffing
- Credentials and keys included in URLs
- Lack of access token validation (including JWT validation)
- Unsigned or weakly signed non-expiring JWTs

Top 3 - Broken Object Level Authorization

Broken Object Property Level Authorization (BOPLA)

- The API returns full data objects as they are stored in the backend database.
- The client application filters the responses and only shows the data that the users really need to see.
- Attackers call the API directly and retrieve sensitive data that the UI would filter out.
- The API works with the data structures without proper filtering.
- Received payload is blindly transformed into an object and stored.
- Attackers can guess the fields by looking at the GET request data.

Top 4 – Unrestricted Resource Consumption

Unrestricted Resource Consumption

Attackers overload the API by sending more requests than they can handle.

Attackers send requests at a rate exceeding the API's processing speed, clogging it up.

The size of the requests or some fields in them exceeds what the API can process.

An attacker submits requests with excessively large payloads or complex queries causing the API to hit a bottleneck and drop requests.

Top 5 – Broken Function Level Autherization

Broken Function Level Autherization

Some administrative functions are exposed as APIs.

Sensitive operations should only be available internally (for example deleting a resource)

Non-privileged users can access these functions without authorization if they know how.

Can be a matter of knowing the URL, or using a different verb or a parameter:

/api/users/v1/user/myinfo

/api/admins/v1/users/all

Top 6 – Unrestricted Access to Sensitive Business Flow

Unrestricted Access to Business Flow

An attacker discovers an API to buy a product online and uses automation to bulk purchase all items of a newly released product which they later re-sell.

Real-estate website's price information can be scraped over time to predict house price trends in an area.

Attackers can use automation to perform actions faster than a human user and gain an unfair advantage on auction sites, or similar.

Top 7 – Server-Side Request Forgery

Server-Side Request Forgery

An API accepts a URL as a parameter for a redirection, and an attacker finds that they can use this to redirect the response to a rogue site which is able to steal sensitive API data.

An attacker can force an API to load resources from a server under their control; this is the basis of a key injection attack in JWTs.

An API allows access to the local host allowing an attacker to use malform requests to access local resources.

Top 8 – Security Misconfiguration

Security Misconfiguration

- Unpatched systems
- Unprotected files and directories
- Unhardened images
- Missing, outdated, or misconfigured TLS
- Exposed storage or server management panels
- Missing CORS policy or security headers
- Error messages with stack traces
- Unnecessary features enabled

Top 9 – Improper Inventory Management

Improper Inventory Management

DevOps, the cloud, containers, and Kubernetes make having multiple deployments easy (for example, dev, test, branches, staging, and old versions).

Desire to maintain backward compatibility forces to leave old APIs running.

Old or non-production versions are not properly maintained, but these endpoints still have access to production data.

Once authenticated with one endpoint, attackers may switch to the other, production one.

Top 10 – Unsafe Consumption of APIs

Unsafe Consumption of APIs

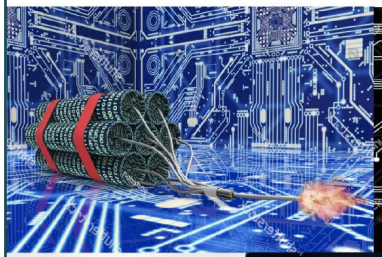
An upstream API may inadvertently store data provided to it by a consumer, thereby violating the data governance regulations of the consumer.

An upstream API provider may be attacked and compromised and then pass malicious data to its consumers due to insufficient internal controls. A typical example is an SQL injection attack.

Question 4

How do we know APIs are under attack ?

API Security Blueprint



- **30 mins: Introductions and Overview**
  - Brief History of APIs
  - Importance of APIs in Digital Ecosystem
  - Motivations for Securing APIs
- **30 mins: Basics of API Security**
  - Examples of API Breaches/Impacts
  - Understanding API Attacks/Patterns
- 15 mins: ..... {Case Study}
- **25 mins: Advanced API Security**
  - OWASP Top 10: Authentication and Authorization
  - OWASP Top 10: Injections and Rate Limits
- **25 mins: Hands-on API Security**
  - Hands-on: Configuring API Security Tests
  - Hands-on: Executing API Security Tests
- 20 mins: : .....{Exercise}
- **50 mins: API Security Program**
  - Preventing API Attacks
  - Role of API Gateways
  - Continuous API Monitoring
- **30 mins: Summary and Conclusions**
  - Take Home Exercises
  - Questions and Answers

Understanding API Attacks for Prevention

API Indicators of Compromise

IC1
Unusual or Suspicious API calls

IC2
Failed AuthC and AuthZ Calls

IC3
Anomalous User Behavior

IC4
Unusual Traffic Patterns/Volume

IC5
Deprecated or Outdated Versions

IC6
API Rate-Limiting Violations

IC7
Cross-Site Scripting or Injections

IC8
Misuse of API Tokens or Oauth

IC9
Changes to API Configurations

IC10
Evidence of Command/Control

IC1 – Unusual or Suspicious API Calls

Unfamiliar API Endpoints

Unusual access to API endpoints that are not part of typical business processes or that deal with sensitive data, such as administrative endpoints.

IC1 – Unusual or Suspicious API Calls

Unfamiliar Request Methods

Abnormal use of HTTP request methods (e.g., PUT, DELETE) where only GET or POST is expected. For example, DELETE requests targeting critical resources may indicate an attempt to remove data or disrupt services.

IC1 – Unusual or Suspicious API Calls

Excessive Request to Single Endpoint

Repeated access attempts to a specific API endpoint could indicate a brute-force attack or a bot attempting to exploit a vulnerability.

IC2 – Failed Authentication and Authorization API Calls

Multiple Failed Logins

Repeated failed login attempts, particularly from the same IP address or user, often suggest credential stuffing or brute-force attacks.

IC2 – Failed Authentication and Authorization API Calls

Invalid API Keys or Tokens

The use of expired or invalid API keys or tokens could indicate that an attacker is attempting to gain unauthorized access through stolen or compromised credentials.

IC2 – Failed Authentication and Authorization API Calls

Excessive Token Refresh Requests

A high volume of token refresh requests could suggest that attackers are attempting to maintain persistent access to the API by continuously renewing expired tokens or circumventing token expiration limits.

IC3 – Anomalous User Behavior

Unusual IP Addresses

Logins or API calls originating from IP addresses that are not typical for the user's location or known region can suggest that credentials have been compromised.

IC3 – Anomalous User Behavior

Unusual Time of Activity

API requests made outside of regular business hours, especially if the user typically operates within a specific time frame, may signal unauthorized access.

IC3 – Anomalous User Behavior

Abnormal Data Requests

A legitimate user suddenly accessing large amounts of data or requesting sensitive information they do not usually access could indicate credential misuse or a compromised account.

IC4 – Anomalous Traffic Pattern

Traffic Spikes

Sudden, unexplained increases in traffic, particularly targeting specific API endpoints, may indicate a DoS attack, where the goal is to overwhelm the system and make it unavailable.

IC4 – Anomalous Traffic Pattern

High Data Volume Exfiltration

Large amounts of data being transferred through the API, particularly in short bursts or outside typical patterns, could indicate that attackers are trying to extract sensitive information.

IC4 – Anomalous Traffic Pattern

Repeated Requests from a Single Source

Multiple requests originating from the same IP address within a short period may be an indication of automated attacks, such as API scraping or credential stuffing.

IC5 – Use of Deprecated or Outdated APIs

Deprecated or Outdated APIs

- Access to Deprecated Endpoints: API logs that show access to endpoints associated with older versions of the API suggest attackers are probing for known vulnerabilities that may not exist in the current version.
- Usage of Outdated Protocols: API requests using outdated or insecure protocols (e.g., HTTP instead of HTTPS) could indicate an attempt to exploit older security flaws.

IC6 – Rate Limiting Violations

Rate-Limit Violations and Bypassing

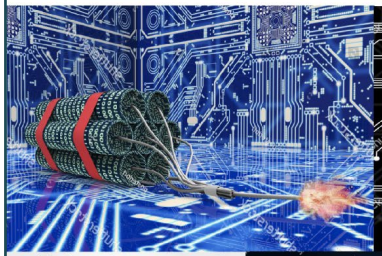
- Frequent Rate-Limit Warnings: Logs showing repeated rate-limit violations, particularly by the same user or IP address, indicate that the attacker is likely trying to flood the API or perform brute-force attacks.
- Attempts to Bypass Rate Limiting: If logs show multiple requests sent from different IP addresses in an attempt to circumvent rate limiting, this could signal the use of botnets or other distributed attack methods.

IC7 – Injection Attempts

Injection Attempts

- Unusual or Malformed Input: API requests containing special characters (e.g., SQL queries, shell commands, or script tags) may indicate an attempt to inject code or manipulate the system.
- Error Messages Indicating Injection Attempts: Logs that show database or server error messages specific to requests may suggest that the API failed to properly sanitize inputs, allowing an attacker to execute an injection attack.

API Security Blueprint



- **30 mins: Introductions and Overview**
  - Brief History of APIs
  - Importance of APIs in Digital Ecosystem
  - Motivations for Securing APIs
- **30 mins: Basics of API Security**
  - Examples of API Breaches/Impacts
  - Understanding API Attacks/Patterns
- 15 mins: …… {Case Study}
- **25 mins: Advanced API Security**
  - OWASP Top 10: Authentication and Authorization
  - OWASP Top 10: Injections and Rate Limits
- **25 mins: Hands-on API Security**
  - Hands-on: Configuring API Security Tests
  - Hands-on: Executing API Security Tests
- 20 mins: : ……{Exercise}
- **50 mins: API Security Program**
  - Preventing API Attacks
  - Role of API Gateways
  - Continuous API Monitoring
- **30 mins: Summary and Conclusions**
  - Take Home Exercises
  - Questions and Answers

Role of API Gateway

Traffic Management and Load Balancing	**AuthC, AuthZ and Security**	**Request & Response Transportation**	**Logging, Monitoring and Analytics**
Cashing & Performance Optimization	**Service Discovery and Management**	**Rate Limiting and Quota Management**	**Cross Origin Resource Sharing (CORS)**

API Gateway Role – Traffic Control and Load Balancing

Traffic Control and Load Balancing

- Routes requests to the appropriate backend service.
- Prevents bottlenecks and ensures high availability.
- Performs round-robin, weighted, or least-connection load balancing to optimize performance.

API Gateway Role – Cross Origin Resource Sharing (CORS)

Cross Origin Resource Sharing (CORS)

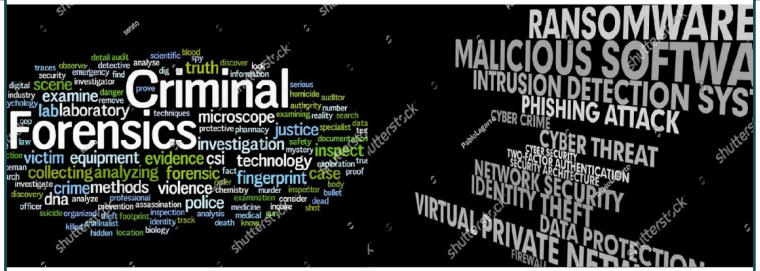
- Controls which domains can access APIs via CORS policies.
- Prevents unauthorized cross-domain requests.

Question 5

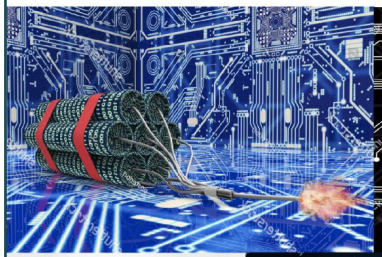
What should be in our checklist for API Due Diligence ?

API Security Checklist

- API Discovery & Inventory Management
- Authentication & Access Control
- Encryption & Data Protection
- API Rate Limiting & Throttling
- Logging & Monitoring
- Continuous API Security Testing
- API Gateway & Security Controls
- API Lifecycle & Secure Development Practices
- API Breach Response & Business Continuity



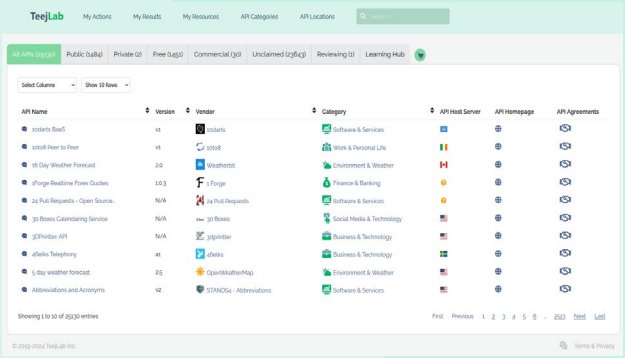
API Security Blueprint



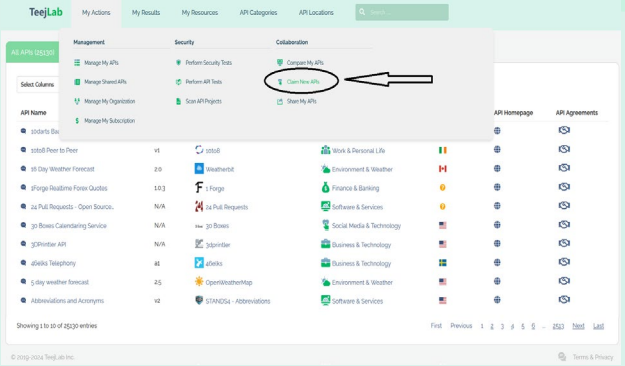
- **30 mins: Introductions and Overview**
  - Brief History of APIs
  - Importance of APIs in Digital Ecosystem
  - Motivations for Securing APIs
- **30 mins: Basics of API Security**
  - Examples of API Breaches/Impacts
  - Understanding API Attacks/Patterns
- 15 mins: …… {Case Study}
- **25 mins: Advanced API Security**
  - OWASP Top 10: Authentication and Authorization
  - OWASP Top 10: Injections and Rate Limits
- **25 mins: Hands-on API Security**
  - Hands-on: Configuring API Security Tests
  - Hands-on: Executing API Security Tests
- 20 mins: : ……{Exercise}
- **50 mins: API Security Program**
  - Preventing API Attacks
  - Role of API Gateways
  - Continuous API Monitoring
- **30 mins: Summary and Conclusions**
  - Take Home Exercises
  - Questions and Answers

Take Home Exercise

Step 1: Go to your API Discovery account



Step 2: Claim an API from Marketplace



Step 3: Conduct your analysis