CWL
CyberWarFare Labs

Exploring Damn Vulnerable API

About CyberWarFare Labs:

- CyberWarFare Labs is an UK-based Ed-tech company
- Specializes in cybersecurity cyber range labs.
- Offers on-demand Cyber Security upskilling courses.
- Emphasizes the importance of adapting to evolving threats and client needs.
- Operates with two primary divisions:
  - Cyber Range Labs
  - Up-Skilling Platform

About Speaker:

Rohith Sai Krishna (Security Researcher)

With one year of experience as a cybersecurity intern, he have gained valuable experience in the field of pentesting, specializing in identifying vulnerabilities and testing the security of various systems. His areas of interest lie in Red/Blue team operations, which encompasses API security, web application security, and enterprise network.

Disclaimer

- This webinar is intended solely for educational purposes, focusing on API security awareness and mitigation techniques.
- Live demonstrations of vulnerabilities are conducted within the provided environment.
- Participants are advised not to replicate these actions on real-world systems without proper authorization.
- The organizers, presenters, and hosts of this webinar disclaim any liability for actions taken outside ethical and legal boundaries.
- Knowledge gained should be used responsibly and legally.

Topics:

- API Security Overview
- Introduction of Damn Vulnerable API
- Common API Vulnerabilities
- API Testing Tools
- Hands-On Demo

API Security Overview

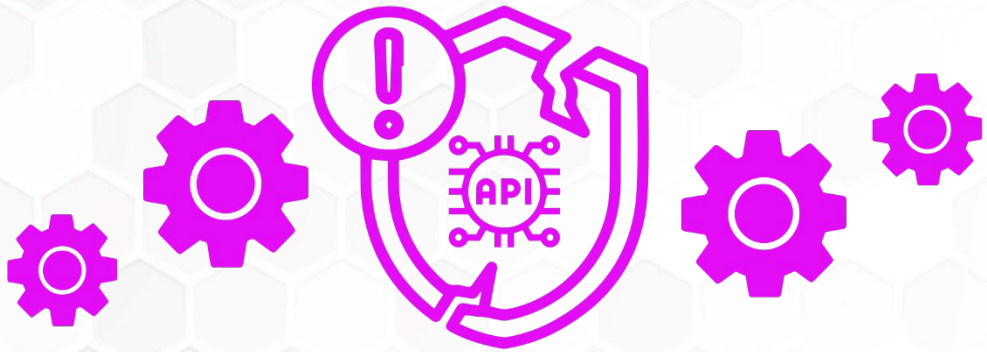
- API security is essential for modern software development.
- It ensures data and service confidentiality, integrity, and availability.
- Authentication and authorization are crucial for verifying user or application identity and access.
- Input validation and sanitization prevent injection attacks.

- Content security policies control resource loading on client web pages.
- Token management involves securely handling API keys and access tokens.
- Data encryption is essential for data at rest and in transit.
- Audit trails and logging provide visibility into API activities.

Damn vulnerable API

- Damn Vulnerable API is a valuable resource for learning for about API vulnerabilities

- It provides a safe environment for exploring and understanding common security flaws.



- Users can experiment with realistic scenarios to enhance their API security knowledge.

- A variety of challenges are available, covering different aspects of API security.

Common API Vulnerabilities

1. Authentication and Authorization Flaws
2. Injection Attacks
3. Insecure Deserialization
4. XML and JSON Parsing Vulnerabilities
5. Sensitive Data Exposure
6. Security Misconfiguration

Authentication and Authorization Flaws

Authentication and authorization are crucial components of API security, as they determine who can access your API and what actions they can perform. When these mechanisms are flawed, it can lead to significant security vulnerabilities that can be exploited by malicious actors.

- Insufficiently strong authentication mechanisms.
- Exploitable flaws in authentication.
- Failure to enforce proper access controls.
- Granting more access than necessary.

Common attack Vectors

- **API Token Theft**

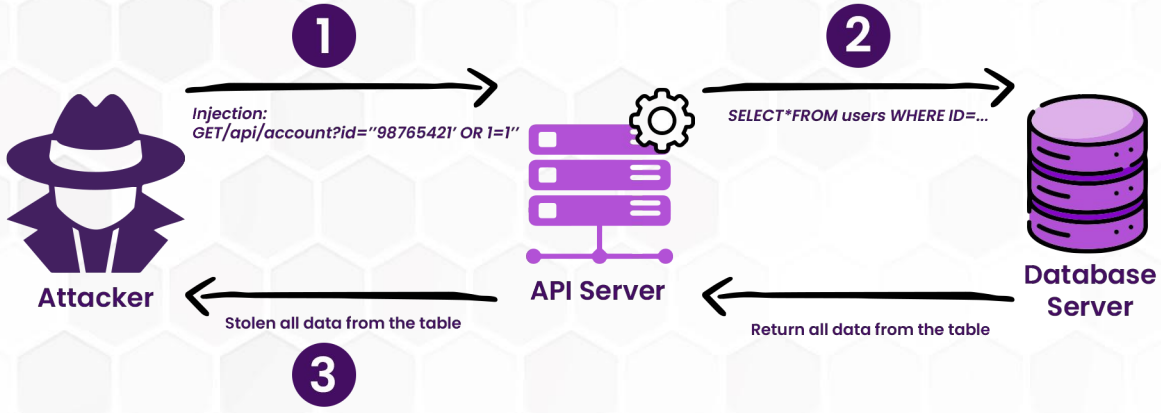
  Stealing authentication tokens
- **Session Fixation**

  Fixing a user's session ID
- **CSRF (Cross-Site Request Forgery)**

  Forging requests on behalf of a user.

Injection Attacks

Injection attacks are one of the most common and critical security threats that APIs face. These attacks occur when an attacker manipulates input data in a way that can execute unintended commands or access sensitive data



- Injection attacks involve maliciously injecting untrusted data or code into an application or system to exploit vulnerabilities.

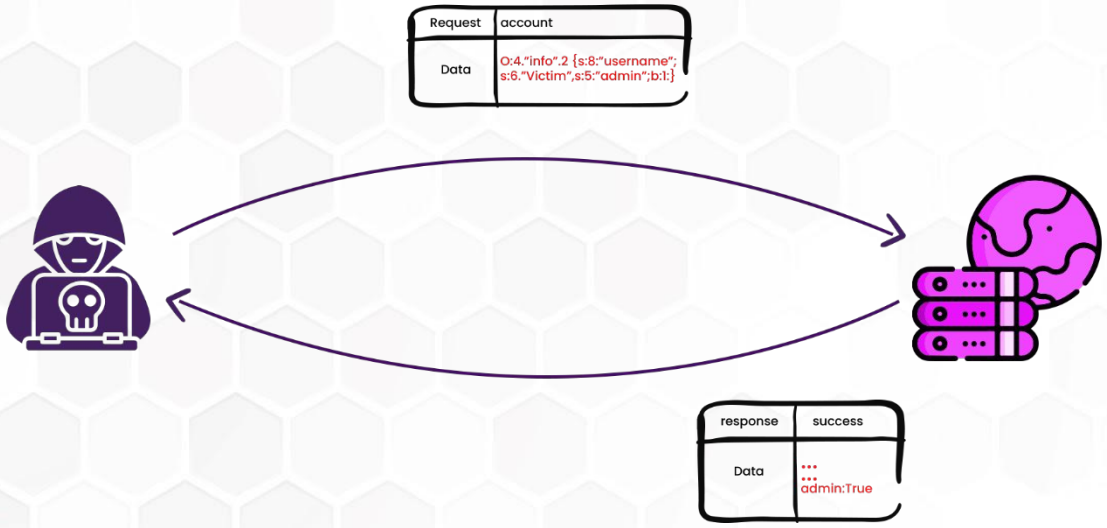
- Attackers use input fields or parameters to insert malicious content, potentially compromising the application's security.

Injection Attacks Types

- **SQL Injection**
  Exploiting SQL queries to manipulate the database.
- **Cross-Site Scripting (XSS)**
- Injecting malicious scripts into API viewed by other users.
- **Command Injection**
- Executing arbitrary commands on the server.

Insecure Deserialization

Insecure deserialization is a critical security vulnerability that can expose APIs to a range of threats, including remote code execution, data tampering, and denial of service attacks.



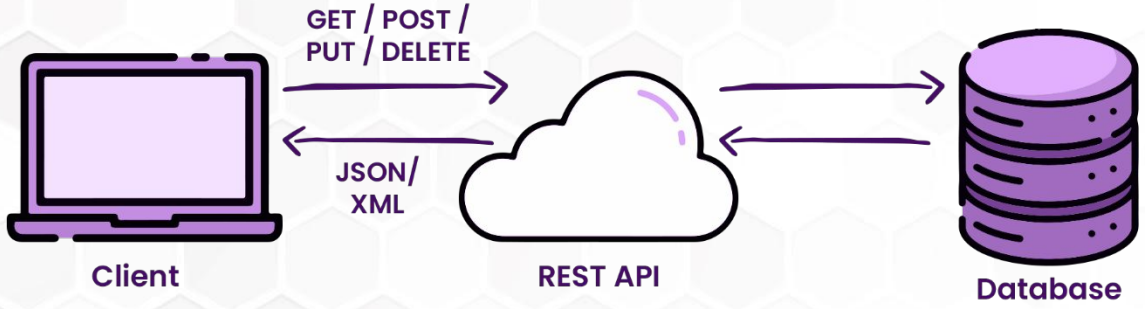
- Attackers exploit deserialization processes to execute malicious code.

- Attacker modifies serialized data to execute arbitrary code on the server.

- Attackers modify serialized data to alter the application's behaviour.

XML and JSON Parsing Vulnerabilities

XML and JSON are widely used formats for data interchange in APIs. While they offer versatility and ease of use, they also present security risks when parsed improperly.



- JSON parsing vulnerabilities can expose APIs to risks.
- Types:
    - JSON Injection.
    - Insecure JSON Deserialization.
- XML parsing vulnerabilities can lead to security issues.
- Types:
    - XML External Entity Injection (XXE)
    - Billion Laughs Attacks

Sensitive Data Exposure

Sensitive data exposure is a critical security issue that can have severe consequences for both organizations and their users. APIs, which often handle sensitive data such as user information, financial records, and personal details, are prime targets for attackers seeking to exploit this vulnerability.

- Mishandling sensitive data can lead to exposure.
- Lack of encryption can expose data in transit.

Security Misconfiguration

Security misconfigurations are among the most prevalent and dangerous vulnerabilities affecting APIs today. These misconfigurations can expose sensitive data, provide unauthorized access, and lead to data breaches

Types of security misconfigurations

Exposed Debugging Information:
APIs may expose detailed error messages or debugging information in their responses.

Default Credentials:
Default usernames and passwords for API components or services are not changed.

Unrestricted Access:

APIs lack proper access controls, allowing unauthorized users to access sensitive resources.

Unnecessary Services:

Unused or unnecessary API endpoints or services remain active.

Misconfigured Security Headers:

API responses lack essential security headers or contain incorrect settings.

API Security Tools

- APIs have unique security challenges that demand specialized tools tailored to address their vulnerabilities effectively.

- These tools play a pivotal role in safeguarding APIs from various threats.

Types of API security tools

- API Security Posture Tools:
  1.Provide visibility into the security state of APIs.
  examples: **Swagger, API Gateway Management Tools**
- API Runtime Security Tools:
  1. Detect and prevent malicious requests in real-time.
  examples: **Web Application Firewalls, API Rate Limiting Tools**
- API Security Testing Tools:
  1. Identify vulnerabilities and misconfigurations
  examples: **Postman, Burpsuite, Zed Attack Proxy**

Its Demo time

Resources

- **Explore these essential resources for further learning:**

  "API Security: How to Properly Secure APIs" by John Doe

  "The OWASP API Security Top Ten" from OWASP

  "API Security: A Comprehensive Overview" by Jane Smith

- **Links**
- https://owasp.org/API-Security/
- https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html

THANK YOU :)

For any queries

Mail : support@cyberwarfare.live