

## Question

What are the top 10 API security risks listed in the OWASP API Security Top 10?

What is the first OWASP 2023 Top 10 API vulnerability?

What is the second OWASP 2023 Top 10 API vulnerability?

What is the third OWASP 2023 Top 10 API vulnerability?

What is the fourth OWASP 2023 Top 10 API vulnerability?

What is the fifth OWASP 2023 Top 10 API vulnerability?

What is the sixth OWASP 2023 Top 10 API vulnerability?

What is the seventh OWASP 2023 Top 10 API vulnerability?

What is the eighth OWASP 2023 Top 10 API vulnerability?

What is the ninth OWASP 2023 Top 10 API vulnerability?

What is the tenth OWASP 2023 Top 10 API vulnerability?

In the OWASP 2023 Top 10 list, what does the notation "A" stand for?

What is OWASP and what does it stand for?

What types of resources does OWASP provide?

Are OWASP's resources accessible to everyone?

What is OWASP's approach to application security?

Is OWASP affiliated with any commercial technology company?

What is the OWASP Foundation?

Who contributes to OWASP?

How does OWASP support security research?

What kind of events and community involvement does OWASP have?

What is the primary focus of the OWASP API Security Top 10?

How does API security differ from broader web application security?

Is there an example of a common API vulnerability?

Where can one contribute to the OWASP API Security Top 10?

What should new readers of the OWASP Top 10 series do?

What is the OWASP API Security Top 10 - 2023?

When was the first edition of the OWASP API Security Top 10 published?

Why are APIs considered crucial in modern application architecture?

Can you provide a code example that shows a common API vulnerability?

What are some related OWASP top 10 projects recommended for reading?

What is the OWASP API Security Top 10 2023 and how is it structured?

Why was there a combination of "Excessive Data Exposure" and "Broken Object Level Authorization" in the 2023 list?

What is the new category "Unrestricted Access to Sensitive Data" and why was it added?

What does the "Unsafe Consumption of APIs" category encompass?

How was the OWASP API Security Top 10 2023 list compiled?

What methodology does OWASP use for risk analysis in the Top 10?

How does the OWASP Risk Rating Methodology categorize vulnerabilities?

What factors are considered in the OWASP Risk Rating Methodology?

Does the OWASP Risk Rating Methodology for API security differ from other categories?

Is the OWASP API Security Top 10 risk analysis data-driven?

What is the purpose of the OWASP API Security Top 10?

What are the levels of Weakness Prevalence in the OWASP API Security Top 10?

How is Weakness Detectability classified in the OWASP Ri

What does Technical Impact mean in the context of the C

How are Business Impacts evaluated in the OWASP Risk R

What is the significance of categorizing Exploitability in th

What is Broken Object Level Authorization (BOLA) in APIs

How does Broken Object Level Authorization impact an a

What are some example attack scenarios for BOLA?

How can Broken Object Level Authorization be prevented

What are the threat agents and attack vectors for Broken

What is the security weakness associated with BOLA?

What are the impacts of Broken Object Level Authorizatio

Can you provide an attack scenario for BOLA involving an

How would BOLA manifest in an automobile manufacture

What is an example of BOLA in an online document stora

Discuss the exploitability, prevalence, and technical impac

What is API2:2023 Broken Authentication in the OWASP 1

How easy is it to exploit the broken authentication vulner

Why is broken authentication a common security weakne

What is the technical and business impact of broken auth

Can you provide an example of a broken authentication v

What are the signs that an API might be vulnerable to brc

How can broken authentication be prevented in APIs?

What is an example attack scenario involving broken auth

How can GraphQL batching be used as an attack vector in

What makes broken authentication a significant threat in

Can you explain the security weakness in broken authent

What are the long-term impacts of broken authentication

What is API3:2023 Broken Object Property Level Authoriz

How can the exploitability of API3:2023 be described?

What is the prevalence and detectability of API3:2023?

What are the technical and business impacts of API3:2023

Can you give an example of an attack scenario exploiting

What is a code example of an API request that could lead

How can API3:2023 be prevented in API design?

What are some related references for understanding API3

What is API4:2023 Unrestricted Resource Consumption in

How can unrestricted resource consumption be exploited

Can you provide a code example of an API vulnerable to u

What are some examples of attack scenarios for unrestrict

How can API4:2023 Unrestricted Resource Consumption I

What are some reference materials to understand API4:2

What are the threat agents and attack vectors associated

What is the security weakness in APIs that leads to Unres

What are the impacts of API4:2023 Unrestricted Resource

How easy is it to exploit the Unrestricted Resource Consu

How widespread is the issue of Unrestricted Resource Consumption?

What is the technical severity of the Unrestricted Resource Consumption vulnerability?

What is Broken Function Level Authorization in API security?

How can attackers exploit Broken Function Level Authorization?

Can you provide an example of an attack exploiting Broken Function Level Authorization?

What are the best practices to prevent Broken Function Level Authorization?

What are some external resources for understanding and preventing Broken Function Level Authorization?

Who are the typical threat agents in Broken Function Level Authorization attacks?

What is the common security weakness in Broken Function Level Authorization?

What is the impact of Broken Function Level Authorization?

How easy is it to exploit Broken Function Level Authorization?

How common are Broken Function Level Authorization vulnerabilities?

What is the technical severity of Broken Function Level Authorization?

What is API6:2023 Unrestricted Access to Sensitive Business Data?

How can attackers exploit Unrestricted Access to Sensitive Business Data?

What are some example attack scenarios for this vulnerability?

How can businesses prevent Unrestricted Access to Sensitive Business Data?

Can you provide a code example of how to detect non-human traffic?

Are there any references for further information on API security?

What is the exploitability level of the API6:2023 vulnerability?

What does the prevalence metric indicate for API6:2023?

How would you describe the security weakness in API6:2023?

What is the detectability level for API6:2023?

Can you discuss the technical impact of API6:2023?

What are the business-specific impacts of API6:2023?

What is API7:2023 Server-Side Request Forgery (SSRF) in APIs?

How exploitable is the SSRF vulnerability, and what are the impacts?

Can you provide an example of an SSRF vulnerability in an API?

What's another scenario where SSRF can be exploited?

How can SSRF vulnerabilities be prevented?

Are there any additional references for understanding SSRF?

What does "Threat Agents/Attack Vectors" mean in the context of SSRF?

What are the security weaknesses associated with SSRF?

What impacts can SSRF have on a system or business?

How easy is it to exploit SSRF vulnerabilities?

How common are SSRF vulnerabilities?

What is the technical impact of SSRF vulnerabilities?

What is API8:2023 Security Misconfiguration in the OWASP API Security Top 10?

What are the common indicators that an API might be vulnerable to Security Misconfiguration?

Can you provide an example attack scenario demonstrating Security Misconfiguration?

How can API Security Misconfiguration be prevented?

What are the reference materials for understanding and preventing Security Misconfiguration?

What is the exploitability level of API8:2023 Security Misconfiguration?

How prevalent is Security Misconfiguration in APIs as per OWASP?

What is the detectability level of Security Misconfiguration?

What kind of security weakness does API8:2023 Security Misconfiguration represent?

What are the technical impacts of Security Misconfiguration?

How does Security Misconfiguration impact businesses?

What is API9:2023 in the OWASP Top 10 2023?

How can attackers exploit Improper Inventory Management?

What are some real-world attack scenarios for API9:2023?

How can organizations prevent the API9:2023 vulnerability?

Can you provide an example of how to document an API threat?

What are the threat agents associated with API9:2023?

What is the security weakness in API9:2023?

What impacts can result from exploiting API9:2023 vulnerability?

How easy is it to exploit the API9:2023 vulnerability?

How prevalent is the API9:2023 vulnerability?

What is the technical impact of the API9:2023 vulnerability?

What is API10:2023 in the OWASP Top 10 2023 list?

How can attackers exploit Unsafe Consumption of APIs vulnerability?

What are the common security weaknesses in Unsafe Consumption of APIs?

Can you provide an example of how an attacker might exploit Unsafe Consumption of APIs?

What is another attack scenario for Unsafe Consumption of APIs?

What is a preventive measure for Unsafe Consumption of APIs?

Can you list some relevant OWASP Cheat Sheets for preventing Unsafe Consumption of APIs?

What are the Threat Agents in the context of API10:2023?

What are the Attack Vectors for Unsafe Consumption of APIs?

How does the Security Weakness manifest in Unsafe Consumption of APIs?

What is the Impact of Unsafe Consumption of APIs on technical systems?

How would you rate the Exploitability of Unsafe Consumption of APIs?

What is the Prevalence of Unsafe Consumption of APIs in the wild?

What makes the Detectability of Unsafe Consumption of APIs difficult?

Can you discuss the Technical Severity of Unsafe Consumption of APIs?

## Answer

The OWASP Top 10 API Security Risks for 2023 are as follows:

The first OWASP 2023 Top 10 API vulnerability is "Broken

The second OWASP 2023 Top 10 API vulnerability is "Broken

The third OWASP 2023 Top 10 API vulnerability is "Broken

The fourth OWASP 2023 Top 10 API vulnerability is "Unres

The fifth OWASP 2023 Top 10 API vulnerability is "Broken

The sixth OWASP 2023 Top 10 API vulnerability is "Unrest

The seventh OWASP 2023 Top 10 API vulnerability is "Ser

The eighth OWASP 2023 Top 10 API vulnerability is "Secur

The ninth OWASP 2023 Top 10 API vulnerability is "Improp

The tenth OWASP 2023 Top 10 API vulnerability is "Unsafe

In the OWASP 2023 Top 10 list, the notation "API1:2023" i

OWASP stands for the Open Web Application Security Pro

OWASP offers a variety of resources that are free and ope

Yes, all OWASP tools, documents, videos, presentations, a

OWASP advocates for a comprehensive approach to appli

No, OWASP is not affiliated with any technology company

The OWASP Foundation is the non-profit entity responsib

OWASP is primarily a volunteer-driven organization. This i

OWASP supports security research by providing grants an

OWASP hosts and participates in extensive conferences w

The primary focus of the OWASP API Security Top 10 is to **Foreword**

API security differs from broader web application security

A common API vulnerability is "Broken Object Level Authc

Contributions to the OWASP API Security Top 10 can be m

New readers of the OWASP Top 10 series are recommend

The OWASP API Security Top 10 - 2023 is the second editi **Introduction**

The first edition of the OWASP API Security Top 10 was pu

APIs are crucial in modern application architecture becaus

Certainly. One common API vulnerability is improper input

Some related OWASP Top 10 projects include OWASP Clo

The OWASP API Security Top 10 2023 is an updated list of

In the OWASP API Security Top 10 2023, "Excessive Data E

"Unrestricted Access to Sensitive Business Flows" is a new

The "Unsafe Consumption of APIs" category highlights the

Despite a public call for data yielding no contributions, the

OWASP utilizes the OWASP Risk Rating Methodology for a **API Security Risks**

The OWASP Risk Rating Methodology categorizes the exp

The OWASP Risk Rating Methodology for API security con

No, the OWASP Risk Rating Methodology for API security

No, the OWASP API Security Top 10 risk analysis is not dat

The purpose of the OWASP API Security Top 10 is to ident

In the OWASP Risk Rating Methodology for API security, v

Weakness Detectability in the OWASP Risk Rating Methodology  
Technical Impact in the OWASP Risk Rating Methodology  
Business Impacts in the OWASP Risk Rating Methodology  
Categorizing Exploitability in the OWASP Risk Rating Methodology

Broken Object Level Authorization, featured as API1:2023 **API1:2023 Broken Object Level Authorization**

The impacts of BOLA can be significant, ranging from unauthorized access to sensitive data. One scenario involves an e-commerce platform where an attacker can bypass authentication and authorization controls. To prevent BOLA:1. Implement robust authorization mechanisms. The threat agents for BOLA typically include attackers who exploit weaknesses in the authorization logic. The primary security weakness in BOLA lies in the failure to properly validate and enforce access controls. The technical impact of BOLA is generally moderate but can be severe depending on the context. Yes, in an e-commerce platform scenario, an attacker could potentially access sensitive user data or perform unauthorized transactions. In this scenario, the automobile manufacturer's API allows unauthorized access to sensitive data. In an online document storage service, users can perform unauthorized actions. BOLA is considered to have high exploitability due to its status as a common vulnerability.

API2:2023 Broken Authentication refers to security issues **API2:2023 Broken Authentication**

The exploitability of broken authentication in APIs is considered high. Broken authentication is common due to misconceptions about its severity. The technical impact is 'Severe', as attackers can gain unauthorized access. Yes, consider a GraphQL API where login attempts are subverted. An API could be vulnerable if it allows:1. Credential stuffing. To prevent broken authentication:1. Understand all authentication flows. In one scenario, attackers exploit the absence of a re-authentication step. Attackers can leverage GraphQL query batching to bypass rate limits. The threat agents in broken authentication scenarios are typically automated scripts or malicious actors. The security weakness often stems from misconceptions about the severity of the issue. The long-term impacts are severe for both the technical integrity and business operations.

API3:2023 Broken Object Property Level Authorization is a **API3:2023 Broken Object Property Level Authorization**

The exploitability of API3:2023 is considered "Easy." Attackers can exploit this vulnerability. API3:2023 is common in prevalence, indicating it's a frequent finding. The technical impact is rated as "Moderate," which means it can lead to unauthorized access. Scenario #1: In a dating app, an API endpoint allows a user to access sensitive data. Json Code:``POST /graphql{ "operationName":"reportUserActivity"}`` To prevent this vulnerability:1. Validate user access to specific data. Relevant references include:1. OWASP API Security Top 10. API4:2023 Unrestricted Resource Consumption is a vulnerability.

API4:2023 Unrestricted Resource Consumption is a vulnerability **API4:2023 Unrestricted Resource Consumption**

Exploitation typically involves sending multiple or crafted requests to exhaust resources. Certainly. Consider an API endpoint that generates reports. One scenario involves a social network's "forgot password" endpoint. Prevention strategies include:1. Using solutions like Content DDoS Protection. Reference materials include OWASP's own documentation. The threat agents in this context are individuals or systems that can send a high volume of requests. The primary security weakness is the lack of effective rate limiting or request throttling. Technically, this vulnerability can lead to Denial of Service. The exploitability of this vulnerability is considered average.

The prevalence of this vulnerability is widespread. Many /

The technical severity of this vulnerability is considered se

Broken Function Level Authorization occurs when an API € **API5:2023 Broken Function Level Authoriz**

Attackers can exploit these vulnerabilities by sending legit

Certainly. Consider a registration process for an invite-onl

To prevent these issues, your application should have a cc

Useful external resources include the OWASP website, pai

Threat agents in the context of Broken Function Level Aut

The common security weakness in Broken Function Level

The business impact of Broken Function Level Authorizati

Broken Function Level Authorization vulnerabilities are ge

Broken Function Level Authorization vulnerabilities are qu

The technical severity of Broken Function Level Authoriza

API6:2023 refers to a vulnerability where sensitive busine **API6:2023 Unrestricted Access to Sensitive**

Attackers typically exploit this vulnerability by understand

1. Scalping High-Demand Products: An attacker automate:

Prevention should be approached on two fronts: business

Sure, here's a simple JavaScript example that might be use

Yes, for more information, you can refer to the OWASP Au

The exploitability of the API6:2023 vulnerability is conside

The prevalence of the API6:2023 vulnerability is described

The security weakness in API6:2023 is primarily due to a la

The detectability of the API6:2023 vulnerability is conside

The technical impact of exploiting API6:2023 is generally r

The business-specific impacts of API6:2023 can vary signif

API7:2023 Server-Side Request Forgery (SSRF) is a security **API7:2023 Server Side Request Forgery**

The exploitability of SSRF is considered easy, especially in

Sure, consider a social networking API that allows users to

In a scenario involving webhooks, consider a security proc

To prevent SSRF vulnerabilities:1. Isolate resource fetching

Yes, for further understanding of SSRF, you can refer to:1.

In the context of SSRF (API7:2023), "Threat Agents/Attack

The primary security weakness in SSRF lies in the applicati

The impacts of SSRF can be significant, both technically ar

Exploiting SSRF vulnerabilities is generally considered eas

SSRF vulnerabilities are quite common. This prevalence is

The technical impact of SSRF vulnerabilities can range for

API8:2023 Security Misconfiguration refers to a vulnerabil **API8:2023 Security Misconfiguration**

An API might be vulnerable to Security Misconfiguration if

Scenario #1: An API server uses a logging utility with JNDI

To prevent API Security Misconfiguration:1. Implement a i

Key references include:1. OWASP Secure Headers Project.

The exploitability of API8:2023 Security Misconfiguration i

Security Misconfiguration is considered "Widespread" in t

The detectability of Security Misconfiguration in APIs is al

API8:2023 Security Misconfiguration represents a security

The technical impact of Security Misconfiguration in APIs is

The impact of Security Misconfiguration on businesses can be

API9:2023 refers to "Improper Inventory Management" in **API9:2023 Improper Inventory Management**

Attackers can exploit this vulnerability by accessing old API

Two real-world scenarios include:1. An attacker finds a bug

To prevent this vulnerability, organizations should:1. Inver

To mitigate the risk of this vulnerability, API documentatio

The threat agents in API9:2023 mainly include external at

The core security weakness in API9:2023 stems from inad

The exploitation of API9:2023 can lead to several impacts,

The exploitability of API9:2023 is generally considered eas

The prevalence of API9:2023 is widespread. Many organiz

The technical impact of API9:2023 can be moderate to sev

API10:2023, in the OWASP Top 10 2023 list, refers to "Unsafe **API10:2023 Unsafe Consumption of APIs**

Attackers can exploit this vulnerability by identifying and i

The common security weaknesses in Unsafe Consumption

Sure, here's an example related to SQL injection:Scenario:

Another scenario involves redirect vulnerabilities:Scenario

A key preventive measure is to always validate and sanitiz

Yes, relevant OWASP Cheat Sheets include:1. Web Service

The threat agents for API10:2023 primarily include attacke

Attack vectors for Unsafe Consumption of APIs include int

The primary security weakness in Unsafe Consumption of

Technically, Unsafe Consumption of APIs can lead to seve

The exploitability of Unsafe Consumption of APIs is consid

The prevalence of Unsafe Consumption of APIs is commo

Detectability is rated as average because while some inst

The technical severity of Unsafe Consumption of APIs is c



tion

authorization

ption

ation

: Business Flows

nt