Executive Summary

This report presents the results of a read-only API Security Risk Analysis conducted on a public demo API (JSONPlaceholder). The assessment focused on identifying common API security weaknesses related to authentication, authorization, data exposure, and rate limiting.

Multiple high-risk issues were identified, including unauthenticated write and delete operations, exposure of sensitive user data, and insufficient access controls. While the tested API is a demo environment, these findings represent **critical risks in real-world SaaS systems** and could lead to data breaches, data manipulation, service abuse, and regulatory impact if left unmitigated.

Methodology

The assessment was conducted using ethical, read-only testing techniques. The following approach was used:

- Reviewed public API documentation
- Tested endpoints using Postman
- Inspected request headers and responses
- Identified risks based on OWASP API Security Top 10
- Assessed severity based on impact and likelihood
- Proposed remediation aligned with security best practices

Table 1: Key Findings

Main API Security Findings						
Endpoint	**Method**	**Auth Required**	**Identified Risks**	**Severity**	**Business Impact**	**Remediation**
/posts	GET	No	Open endpoint, excessive data exposure	Medium	Data scraping and abuse if real data exists	Require authentication, limit fields, enforce rate limiting
/posts/1	GET	No	Unauthenticated access to individual records	Medium	Unauthorized access to user content	Require authentication, validate access
/posts/1/ comments	GET	No	Exposes user email addresses	High	Email harvesting and phishing	Mask/remove emails, require authentication
/posts	POST	No	Unauthenticated write operation	High	Spam, data pollution	Enforce auth, RBAC, input validation
/posts/1	DELETE	No	Unauthenticated delete operation	High	Data loss, service disruption	Enforce auth, logging, monitoring

Table 2: Technical Observations (Appendix A)

Headers & Response Analysis					
Endpoint	**Method**	**Auth Required**	**Headers Observed**	**Response Fields**	**Notes**
/posts/1/ comments	GET	No	Content-Type, X-RateLimit	postId, id, name, email, body	Email exposed via unauthenticated access
/posts	POST	No	Content-Type, Location	id	Write operation without authentication

OWASP API Security Top 10 Mapping

- API1: Broken Object Level Authorization
- API2: Broken Authentication
- API3: Excessive Data Exposure
- API4: Lack of Resources & Rate Limiting
- API8: Injection (risk due to lack of input validation)