MAJOR PROJECT

BUG HUNTING ON ANY TARGET 0F OPEN BUGBOUNTY

* TEAM ONE
* SHAN PRADEEP
* S CHANDAN KADAM
* RAJU C
* HAZIM KAMAL
* SHIVPRIYA MISHRA
* PAVAN VP
* ELANGOVAN
* MITHUN MENON

ISSUE DESCRIPTION

* *Target website we got*

<https://www.openbugbounty.org/> <https://hackerone.com/aeromexico_vdp?type=team>

* ***SQL injection is a technique used to extract user data by injecting web page inputs as statements through SQL commands. Basically, malicious users can use these instructions to manipulate the application.***

ISSUE IDENTIFIED

***SQL injection****is a****web security vulnerability****that allows attackers to manipulate the queries executed by a web application against its database. By injecting malicious SQL statements into input fields (such as search boxes or login forms), attackers can gain unauthorized access to sensitive data. This includes user credentials, personal information, and financial details. Additionally, SQL injection can alter data within the database, compromise application behavior, and even escalate to server compromise.*

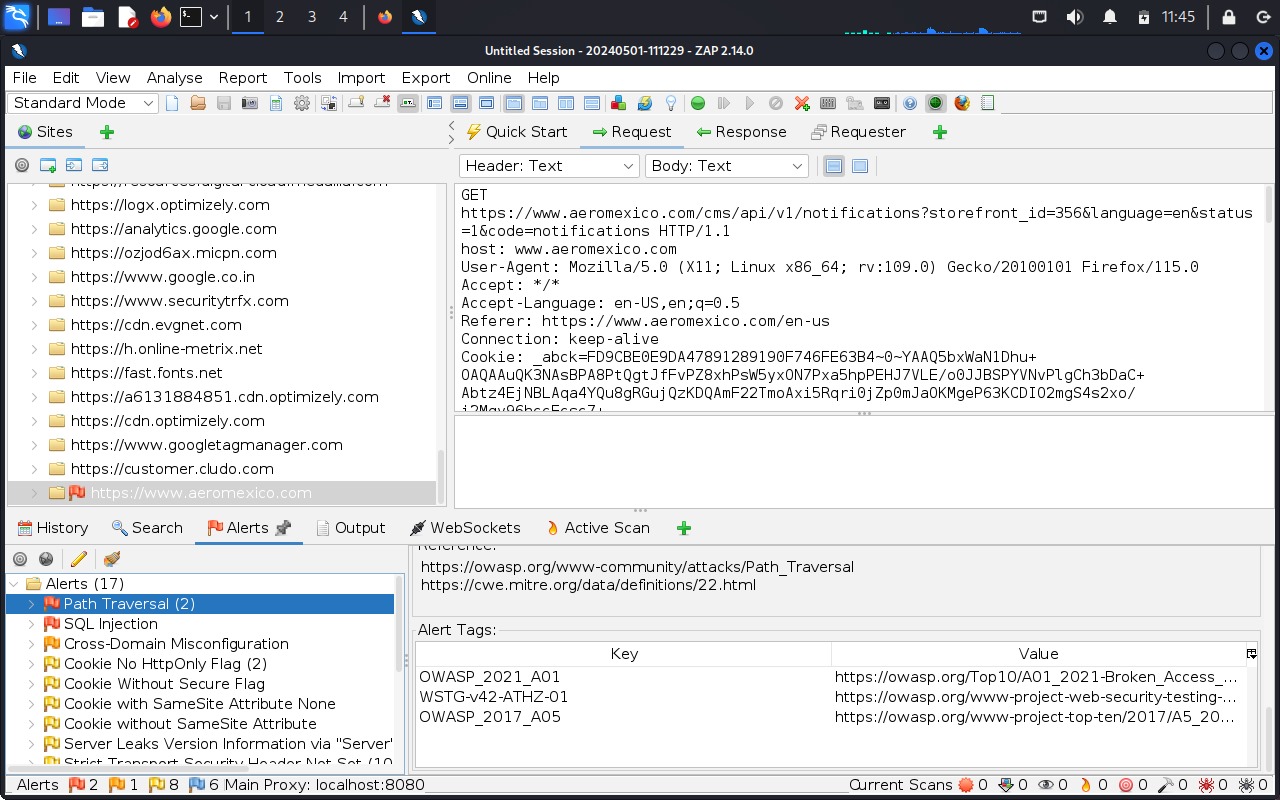
*RISK BREAKDOWN*

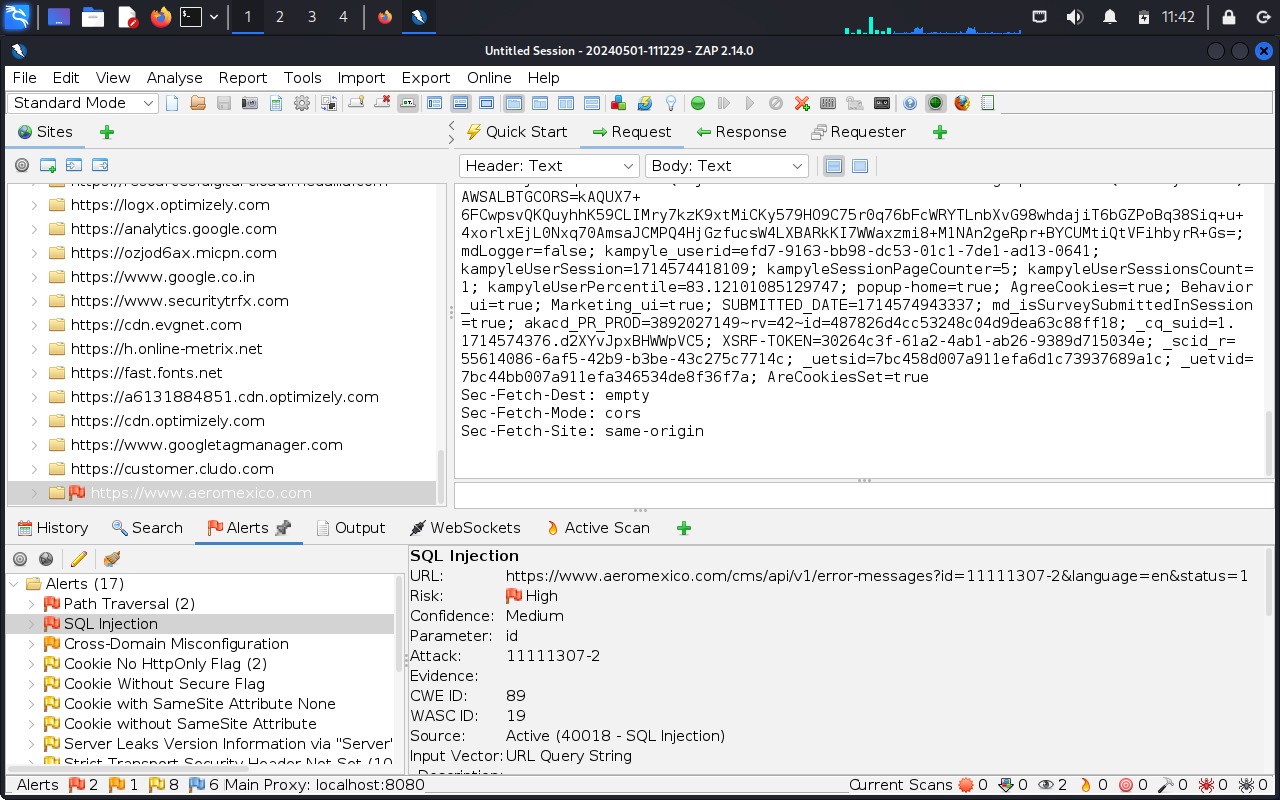
*RISK : HIGH*

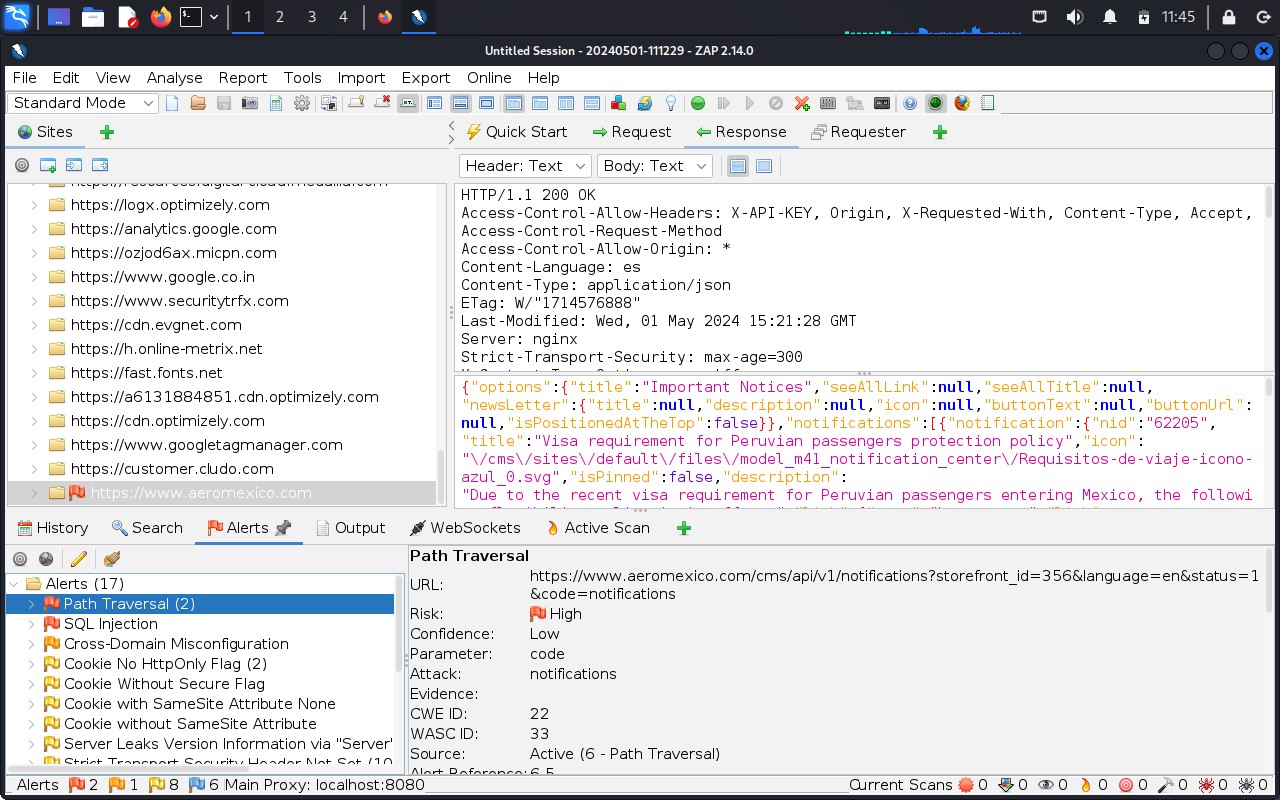
*DIFFICULTY TO EXPLOIT: MEDIUM*

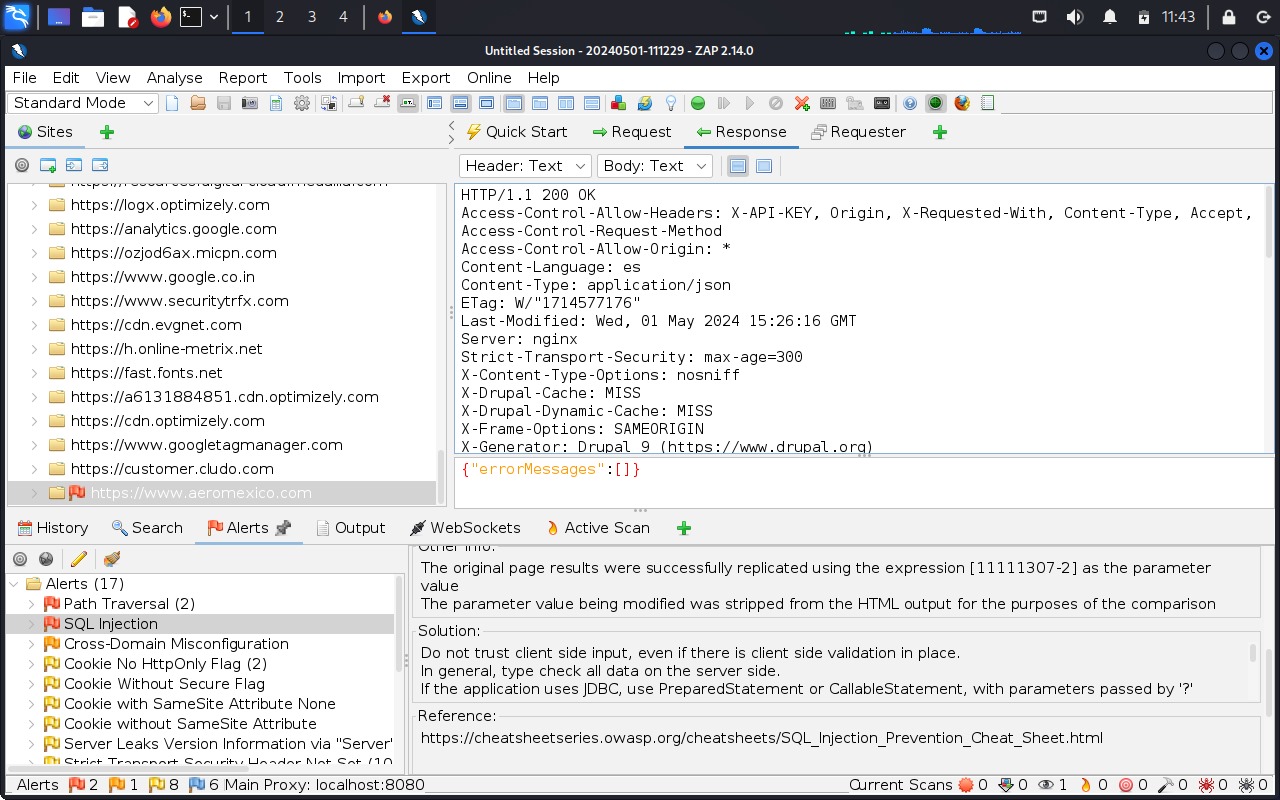
*CVSS2 SCORE: 7.7*

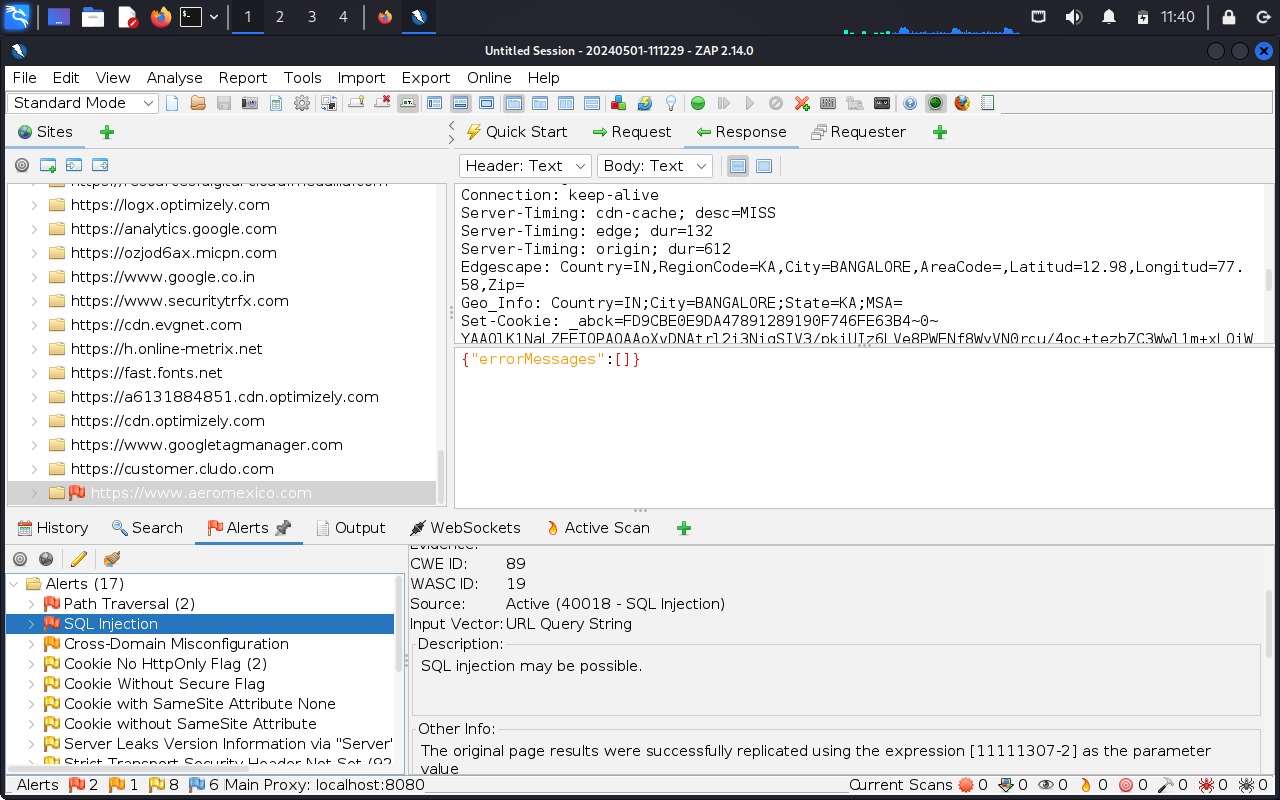
STEPS TO CHECK

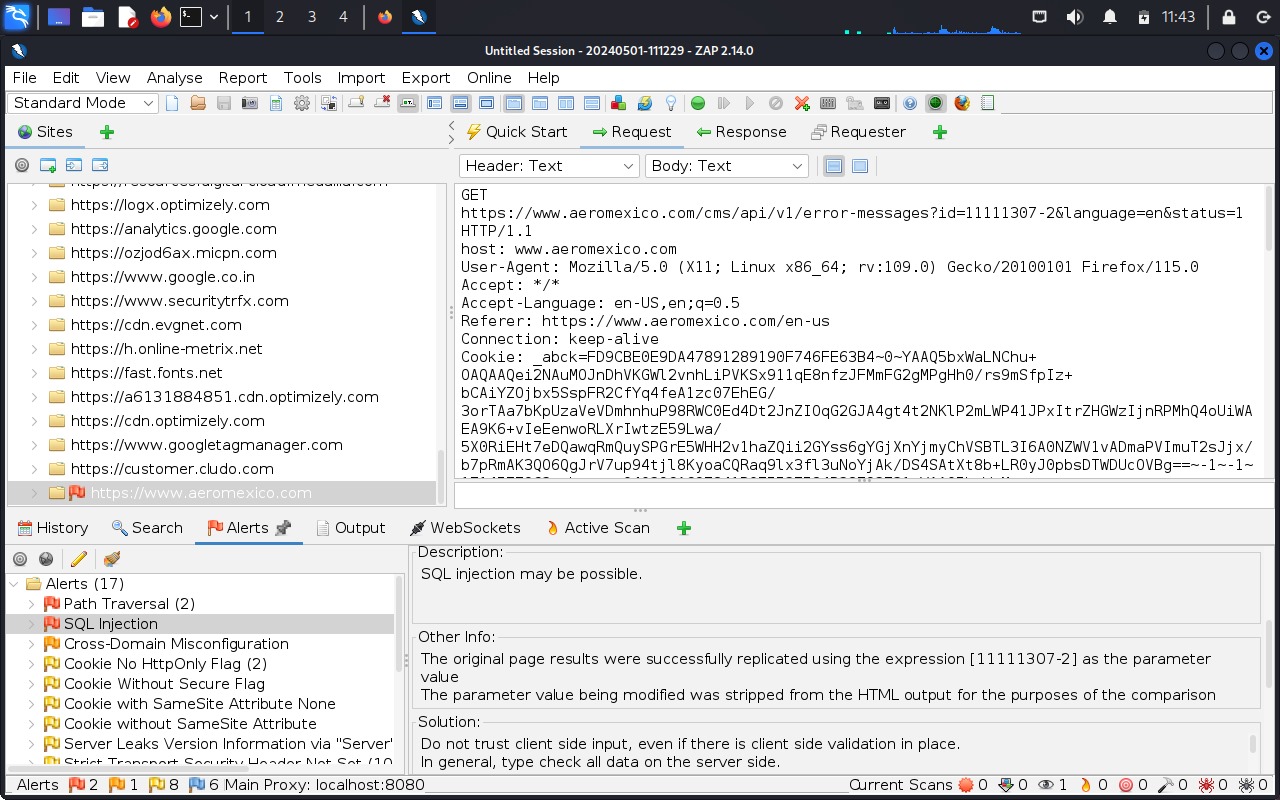












AFFECTED AREAS

*This issue will affect all users on the site who click the link of the attacker, when the url is rendered the payload is executed instead of a legitimate website. Additionally when the malicious user posts anything on the forums the payload will execute.*

REFRENCES

**

**

**

[SQL Injection | OWASP Foundation](https://owasp.org/www-community/attacks/SQL_Injection)

[SQL Injection Prevention - OWASP Cheat Sheet Series](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)