jamk

A01:2021 – Broken Access Control

Issue Report

Daniil Lebedev, AD1375, TTV22S2

Assignment report
Web Application Security TTC6500 / Daniil Lebedev
26.01.2025
School of Technology / Information and Communication Technology

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

1 Wasdat – Order History Is Vulnerable to Indirect Object Reference

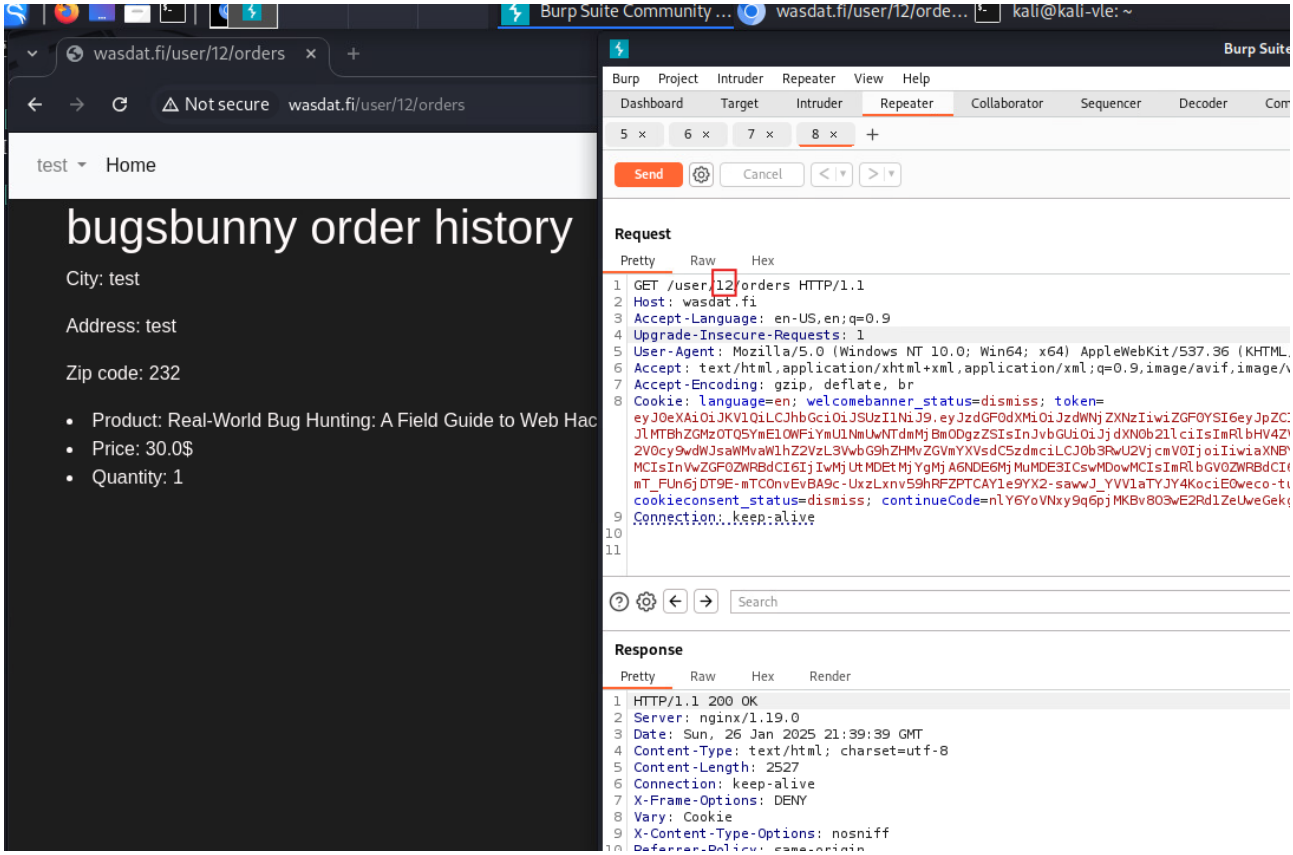
Title: User can access others order history

Description:

Anonymous user can access and view other users order history by changing unique numerical user ID in HTTP GET request.

Steps to reproduce:

- Open the wasdat.fi site
- Add - ”/users/*numerical ID (starting from 1)*/orders” for the request
- Enter crafted request to access other users order history (see Picture 1)



Picture 1

Impact estimation:

- Low to medium severity: In the worst-case scenario, this vulnerability allows anonymous users to access and view other users order histories, potentially exposing sensitive business information. This could lead to reputational damage, loss of customer trust, and unauthorized enumeration of user data.

Mitigation:

- Replace predictable numerical user IDs with UUIDs or random identifiers. These identifiers are harder to guess and cannot be enumerated easily.
- See https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

2 Time management

Date	Used hours	Description
Tuesday 21.01.2025	2h	Reading required chapters
Sunday 26.01.2025	1h	Exploiting the target weakness
Sunday 26.01.2025	1h	Writing report