



Broken Access Control Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



ACCESS CONTROL – Levels

- Applications have different roles
- Typical examples:
- Non-authenticated
- Guest
- Regular user
- Manager
- Admin



ACCESS CONTROL - Basics

- Privilege escalation
- 2 types (horizontal and vertical)
- IDOR is a type of broken access control
- No authorization checks on object
- Test all levels (user, guest, manager, admin etc.) against each other
- Try all endpoints as unauthenticated



ACCESS CONTROL – Horizontal

- Examples of **HORIZONTAL** privilege escalation:
- User A can view, modify or delete User B data
- User A reads the last orders on a shopping site from user B



ACCESS CONTROL – Vertical

- Examples of **VERTICAL** privilege escalation:
- Regular user can view, modify or delete things only Admins should be able to
- Un-authenticated user can query info only auth users should be able to



ACCESS CONTROL - Tests

- Try accessing admin only endpoints as low privilege or unauthenticated user
- Try different CRUD methods (GET / POST / PUT / DELETE etc.)
- Look for IDORs (Insecure Direct Object Reference)
- Understand the application in detail



ACCESS CONTROL - IDOR

- IDOR example:
- <https://shop.com/user/1201>
- If you change **1201** to **1200** and it shows other information than your own, you have an IDOR
- Full section on IDORs later



ACCESS CONTROL - IDOR

- IDOR example:
Sometimes IDs are GUIDs
- <https://shop.com/user/46dhsdha-f546-sdhdhah-1378-er>
- Still try integers because the backend may process them!
- Or look for leaks of the GUIDs!



Thank You!

Become a Successful
Bug Bounty Hunter