Slides Web Security - Access Control

Access Control Vulnerability

Access Control

Mengatur hak akses, siapa boleh melakukan apa. Contoh:

- Nasabah boleh melakukan transfer uang ke rekening lain.
- Seller boleh menampilkan barang pada market place.
- Admin boleh mengetahui seluruh informasi milik user.

Cara Membuat Access Control

- Authentication: Mengidentifikasi user dengan konfirmasi (contoh login)
- Session management: Mengidentifikasi user dari request (contoh cookie)

Broken Access Control

Privilege Escalation: Mengubah hak akses secara ilegal

- Horizontal PE: User mengubah hak aksesnya menjadi user lainnya.
  Contoh: mengubah hak akses menjadi nasabah lain dan mengambil saldo bank.

- Vertical PE: User mengubah hak aksesnya menjadi user yang lebih tinggi secara hirarki teknis.
  Contoh: mengubah hak akses user biasa menjadi admin.

IDOR

IDOR

Insecure Direct Object References (IDOR)

Celah pada access control yang disebabkan ketika aplikasi mengambil input milik user untuk mengakses objek secara langsung.

Isi Database

www.infoom.com

id	username	nama	kota	pekerjaan
1	andi123	Andi Mantap	Jakarta	PNS
2	joko_l	Joko Langsing	Makassar	Dokter
3	riakhar	Ria Kharisma	Medan	PNS
4	apis	Aprilia Susanti	Denpasar	Dosen
5	chris222	Chris	Surabaya	Guru
6	budar	Budi Sudarmo	Semarang	Guru

Object Reference

www.infoom.com/user/1

id	username	nama	kota	pekerjaan
1	andi123	Andi Mantap	Jakarta	PNS

www.infoom.com/user/2

id	username	nama	kota	pekerjaan
2	joko_l	Joko Langsing	Makassar	Dokter

IDOR

www.infoom.com/user/1

id	username	nama	kota	pekerjaan
1	andi123	Andi Mantap	Jakarta	PNS

id	username	nama	kota	pekerjaan
1	andi123	Hacked	Bekasi	Ngaret