IDOR
Vulnerability

Sharing Session Backend

Insecure Direct Object Reference

Apa sih artinya?

IDOR adalah salah satu kerentanan pada akses kontrol yang muncul ketika attacker bisa mengakses atau memodifikasi objek dengan memanipulasi ID pada form input, url atau parameter sebuah aplikasi web.

IDOR mulai populer saat masuk dalam Top 10 OWASP 2007, dan muncul lagi pada Top 10 OWASP 2021 namun masuk dalam kategori Broken Access Control.

Kerentanan ini erat kaitannya dengan Horizonal Privilege Escalation. Namun pada kasus tertentu juga dikaitkan dengan Vertical Privilege Escalation.

Privilege Escalation

Teknik penyerangan dimana seorang penyerang mencoba untuk menaikkan level hak akses pada sebuah sistem dengan memanfaatkan celah keamanan, ekspoitasi sistem, atau dengan memanipulasi konfigurasi sistem.

Horizontal Privilege Escalation

Terjadi ketika pengguna atau aplikasi mencoba mendapatkan akses atau hak yang seharusnya dimiliki oleh pengguna lain pada tingkat yang sama. Contoh ketika pengguna mencoba mengakses sumber daya pengguna lain dengan memanfaatkan identitas dari pengguna lain tersebut.

Vertical Privilege Escalation

Terjadi ketika pengguna atau aplikasi mencoba untuk mendapatkan akses atau hak istimewa yang lebih tinggi dari yang mereka miliki dalam suatu sistem. Contoh ketika seorang pengguna mencoba untuk mendapatkan akses sebagai administrator atau superuser.

Di mana IDOR bisa terjadi?

Akses data ke Database

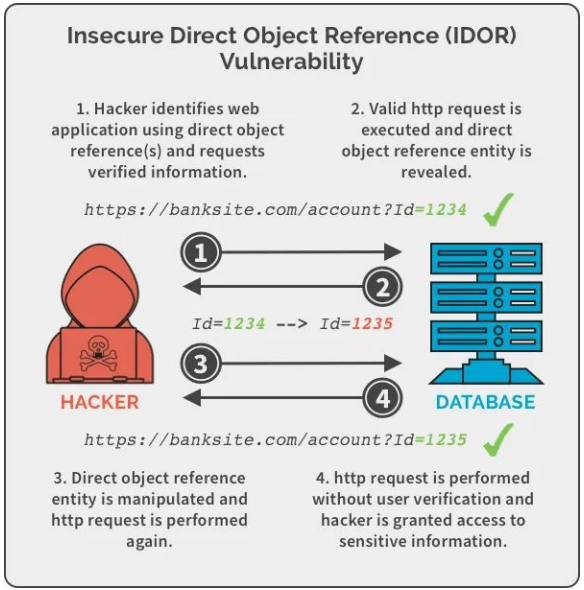
Celah IDOR bisa terjadi ketika mengakses suatu objek dari database. Misalnya untuk mengakses sebuah data invoice milik pengguna pada aplikasi web dibutuhkan ID dari invoice tersebut.

```
https://example.com/invoice?id=1234
```

Attacker bisa memanfaatkan parameter id untuk mengakses data milik user yang lain dengan mengganti nilai id tersebut, contoh

```
https://example.com/invoice?id=1342
```

Karena ID invoice tersebut bersifat auto increment menjadikan attacker dengan mudah menebak ID invoice yang lain. Selain itu tidak adanya validasi hak akses menyebabkan attacker bisa mengakses invoice yang bukan miliknya.



Mengubah data ke Database

Selain bisa terjadi pada saat mengakses data, IDOR juga bisa terjadi pada saat proses mengubah data pada database. Misalnya pada sebuah form mengandung ID dari data yang akan disimpan.

```
1 <form action="/update-profile" method="POST">
2     <input type="hidden" name="user_id"
3 value=":1243">
4 </form
```

Ketika form tersebut dikirim dan tidak ada pengecekan apakah pengguna memiliki hak akses ke ID tersebut atau tidak, maka pengguna tersebut bisa bebas memanipulasi data milik pengguna lain.

Akses ke File Statis

IDOR juga bisa terjadi pada saat menyimpan file statis user yang bersifat sensitif pada server. Sebagai contoh ketika sebuah aplikasi menyimpan file data diri dari penggunanya dengan format nama file menggunakan ID pengguna tersebut.

```
https://example.com/storage/static/ktp-1.jpg
```

Dengan format seperti di atas, attacker bisa dengan mudah mendapatkan file sensitif milik pengguna lain.

Dan masih banyak tempat yang bisa disusupi IDOR

Mitigasi

1. Validasi Hak Akses
2. ID yang sulit ditebak
3. Logging dan monitoring pengguna
4. Server side validation
5. Uji keamanan aplikasi
6. Least Privilege

Demo

https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references

Terima Kasih

https://crashtest-security.com/insecure-direct-object-reference-idor/

https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

https://portswigger.net/web-security/access-control