Cybersecurity Seminar

Home Content

Introduction to

BROKEN ACCESS CONTROL

WHAT ATTACKERS DO & WHAT DEVELOPERS SHOULD PAY ATTENTION TO

Start

Who am i?

Home **Content**

M Hasyim A

CAP; CMPen; CAPen; eJPT; CVE-2024-35191; CVE-2023-47636;

Satpam at Punggawa CyberSecurity
Ketak ketik - medium.com/@kresec
& Tegalsec Blog

linkedin/mhasyim
yt/@kresec

To do list

Home **Content**

1. Pengantar Cyber Security
2. CIA Triad
3. Overview OWASP Top Ten
    - *Definition; Use Case;*
4. Broken Access Control
    - *Definition; Factors; Exploitation; Impact; Mitigation; etc.*
    - *+Demo;*
5. FAQ / Q&A
6. Closing

What is Cyber Security?

Home **Content**

Keamanan siber adalah praktik untuk melindungi komputer, server, perangkat mobile, sistem elektronik, jaringan, dan data dari serangan digital berbahaya atau akses yang tidak sah. Tujuannya adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi dalam dunia digital.

Where is Cyber Security Applied?

Home **Content**

- Di perusahaan dan organisasi.
- Pada perangkat pribadi seperti ponsel dan laptop dari malware dan pencurian data (human).
- Di infrastruktur penting .

Ex: Sistem perbankan online yang memakai cyber security untuk mencegah akses ilegal ke rekening nasabah.

Why is Cyber Security Important?

Home **Content**

- Untuk melindungi informasi pribadi dan rahasia dari pencurian atau penyalahgunaan.
- Mencegah kerugian finansial dan reputasi yang disebabkan oleh serangan siber.
- Menjamin kelangsungan layanan penting yang bergantung pada teknologi.
- Memelihara kepatuhan terhadap peraturan seperti GDPR; PCI DSS.

Ex: Serangan ransomware; data breach; account takeover.

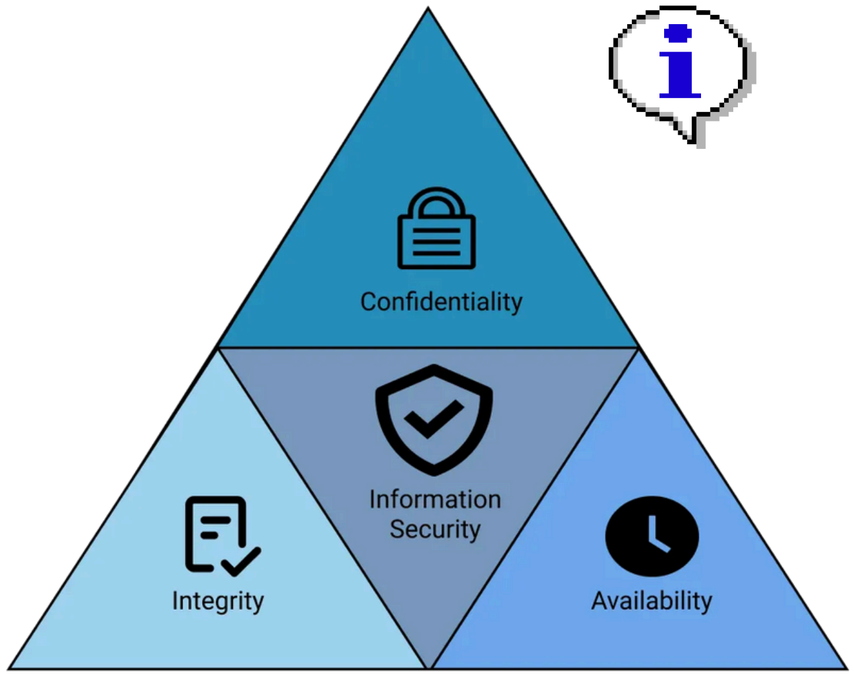
CIA Triad

Home **Content**

CONFIDENTIALITY
Memastikan informasi hanya dapat diakses oleh pihak yang berwenang.

INTEGRITY
Memastikan data tetap akurat, konsisten, dan tidak diubah tanpa izin.

AVAILABILITY
Memastikan sistem dan data selalu dapat diakses saat dibutuhkan.



Common Security Vulnerabilities

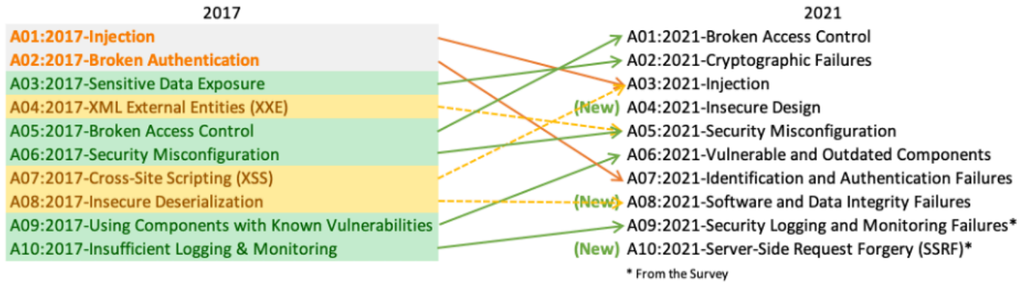
Home **Content**

OWASP
Open Web Application Security Project

;Adalah org nirlaba global yang fokus pada peningkatan keamanan perangkat lunak dan aplikasi web.
;provide (paduan, tools, dan standar keamanan)

OWASP TOP 10 - 2021

;OWASP Top Ten adalah daftar 10 risiko keamanan aplikasi web paling kritis.
;Digunakan sebagai standar global untuk meningkatkan kesadaran dan praktik keamanan.

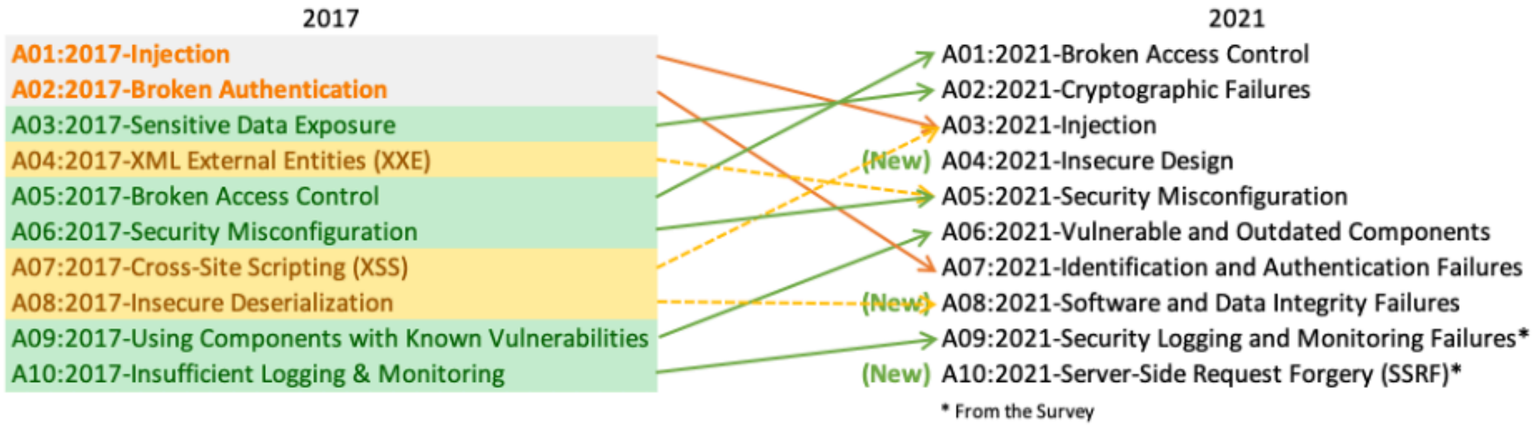


Common Security Vulnerabilities

Home **Content**

OWASP TOP 10 - 2021

why 2021? (history: 1-every-3y)
next owasp top ten? Nov 2025



Owasp Top 10 - Use Case sample

Home **Content**

- *Developer* menggunakan daftar OWASP Top Ten sebagai panduan untuk menghindari kesalahan dalam menulis kode yang dapat menyebabkan celah keamanan.
- *Security tester* menggunakan OWASP sebagai referensi untuk merencanakan dan menjalankan pengujian keamanan, termasuk penetration testing dan vulnerability assessment.

Use Case	OWASP Top 10 2021	OWASP Application Security Verification Standard
Awareness	Yes	
Training	Entry level	Comprehensive
Design and architecture	Occasionally	Yes
Coding standard	Bare minimum	Yes
Secure Code review	Bare minimum	Yes
Peer review checklist	Bare minimum	Yes
Unit testing	Occasionally	Yes
Integration testing	Occasionally	Yes
Penetration testing	Bare minimum	Yes
Tool support	Bare minimum	Yes
Secure Supply Chain	Occasionally	Yes

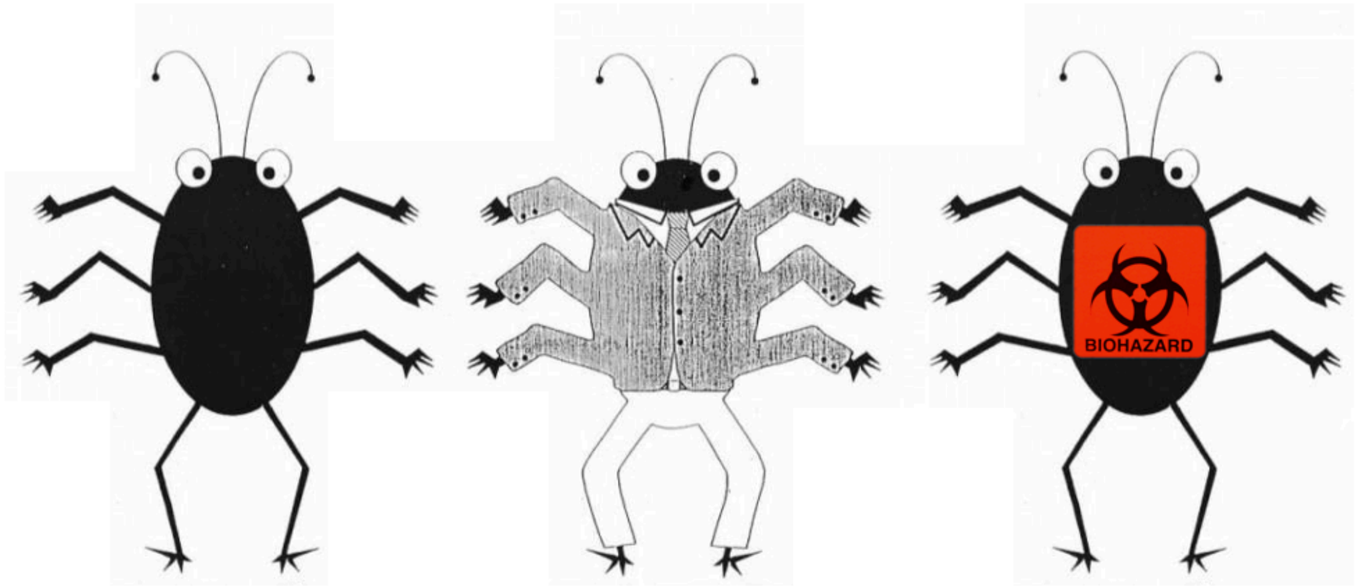
Examples in the Application Development Life Cycle (SDLC)

Home **Content**

- Dalam fase perencanaan dan analisis, tim menggunakan OWASP untuk melakukan threat assessment dan menetapkan security requirements yang jelas sejak awal pengembangan.
- Saat desain aplikasi, prinsip secure architecture diadopsi dengan memperhatikan pedoman OWASP, mengantisipasi ancaman dan mengatur kontrol akses yang tepat.
- Di fase implementasi, developer mengacu pada OWASP untuk praktik pengkodean aman agar menghindari kerentanan seperti injection atau broken access control.
- **Pada fase pengujian, tester melakukan pemeriksaan berdasarkan OWASP Top Ten untuk mengidentifikasi kelemahan sebelum aplikasi dirilis.**
- Selama deployment dan maintenance, OWASP membantu memastikan patch keamanan diterapkan tepat waktu dan monitoring terhadap potensi celah tetap dilakukan.

????

Home **Content**

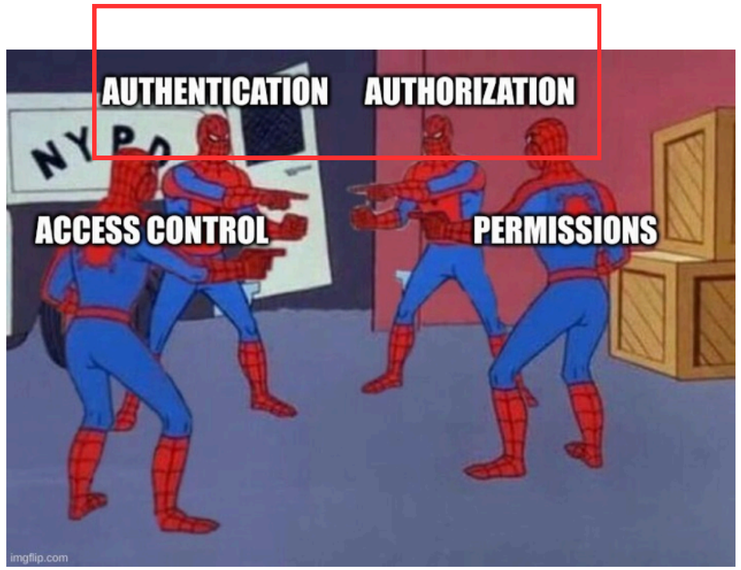


Bug Feature Vulnerability

Access Control

Home **Content**

Access Control adalah mekanisme keamanan yang mengatur siapa saja yang diperbolehkan mengakses sumber daya, data, atau sistem tertentu. Tujuannya adalah agar hanya orang yang berwenang yang dapat memperoleh akses, sehingga mencegah akses yang tidak sah dan menjaga keamanan informasi.



Authentication & Authorization

Home **Content**

Authentication (Autentikasi)

Verifikasi identitas pengguna, misalnya melalui password, biometrik, atau token.

Authorization (Otorisasi)

Menentukan hak akses pengguna setelah autentikasi, seperti melihat atau mengedit data / **CRUD**.

Broken Access Control

Home **Content**

Kerentanan *broken access control* terjadi ketika seorang pengguna dapat mengakses sumber daya atau melakukan tindakan yang seharusnya tidak dapat mereka lakukan.

Causes of Broken Access Control

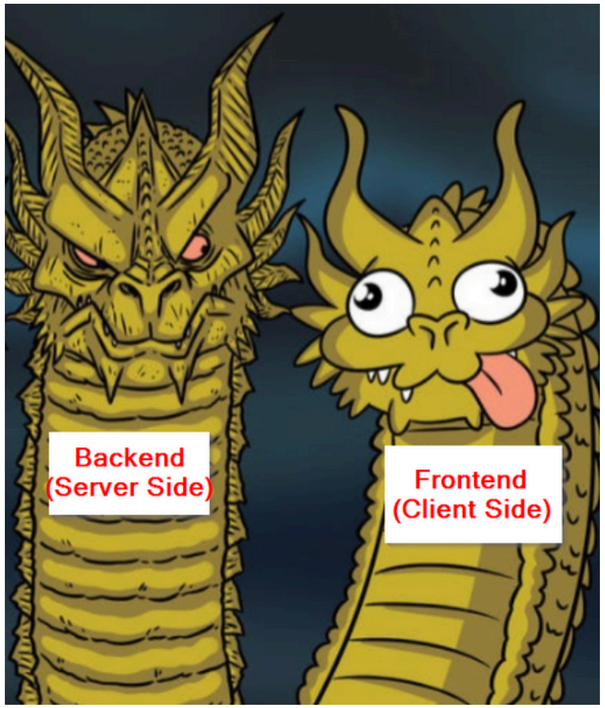
Home **Content**

No authentication & authorization;
CVE on dependency (ex: CVE-2024-51479);
Weak Permission Check;
Etc.

Permission Checks

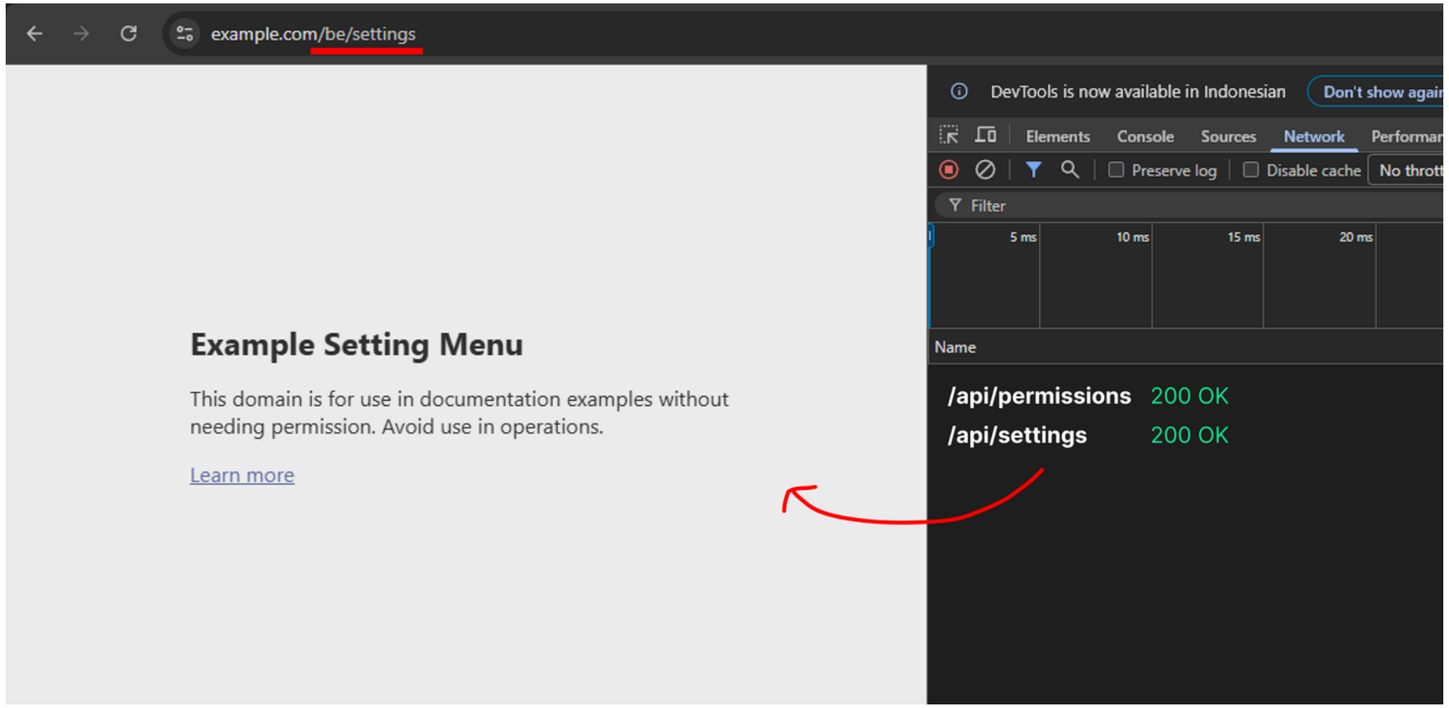
Home **Content**

SSR Vs CSR



(C/S)SR - Example

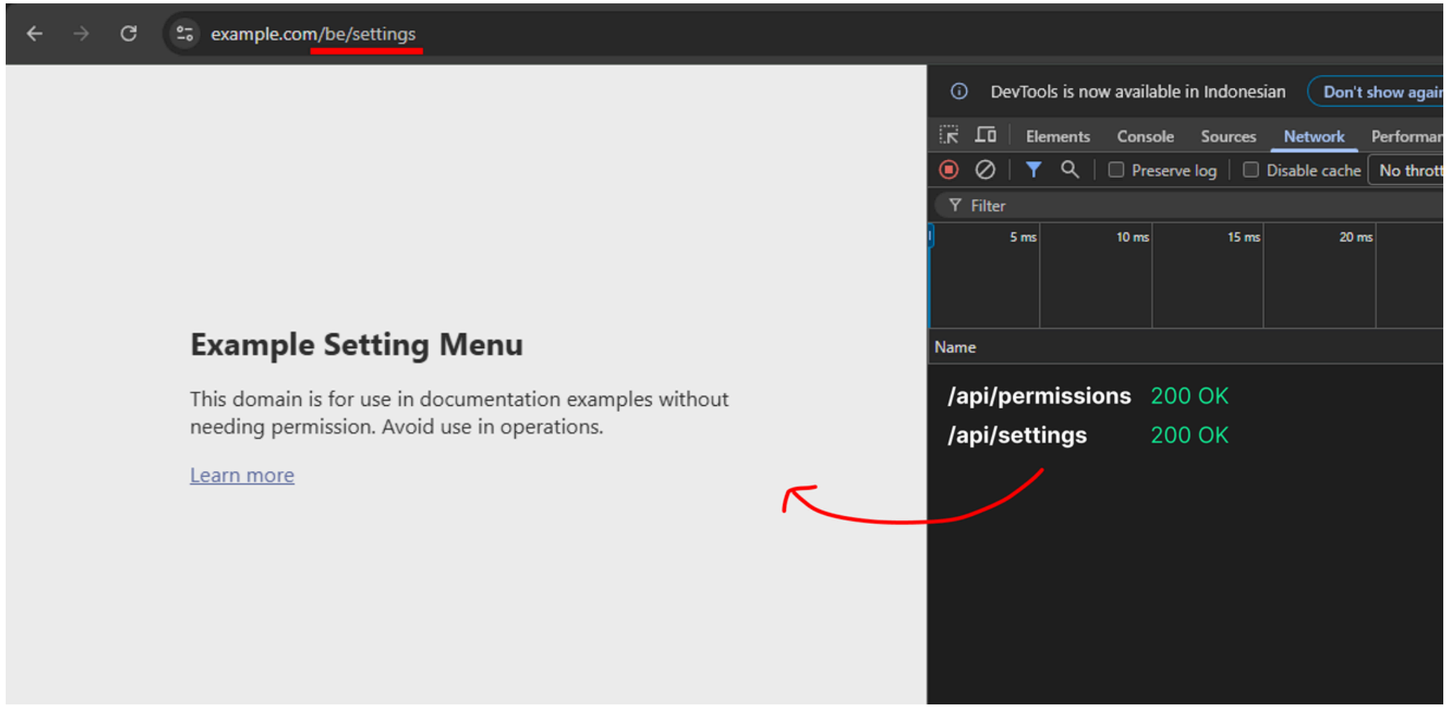
Home **Content**



Data/Resource diproses & ditampilkan (render) oleh client (js-umum nya)

(C/S)SR - Example

Home **Content**

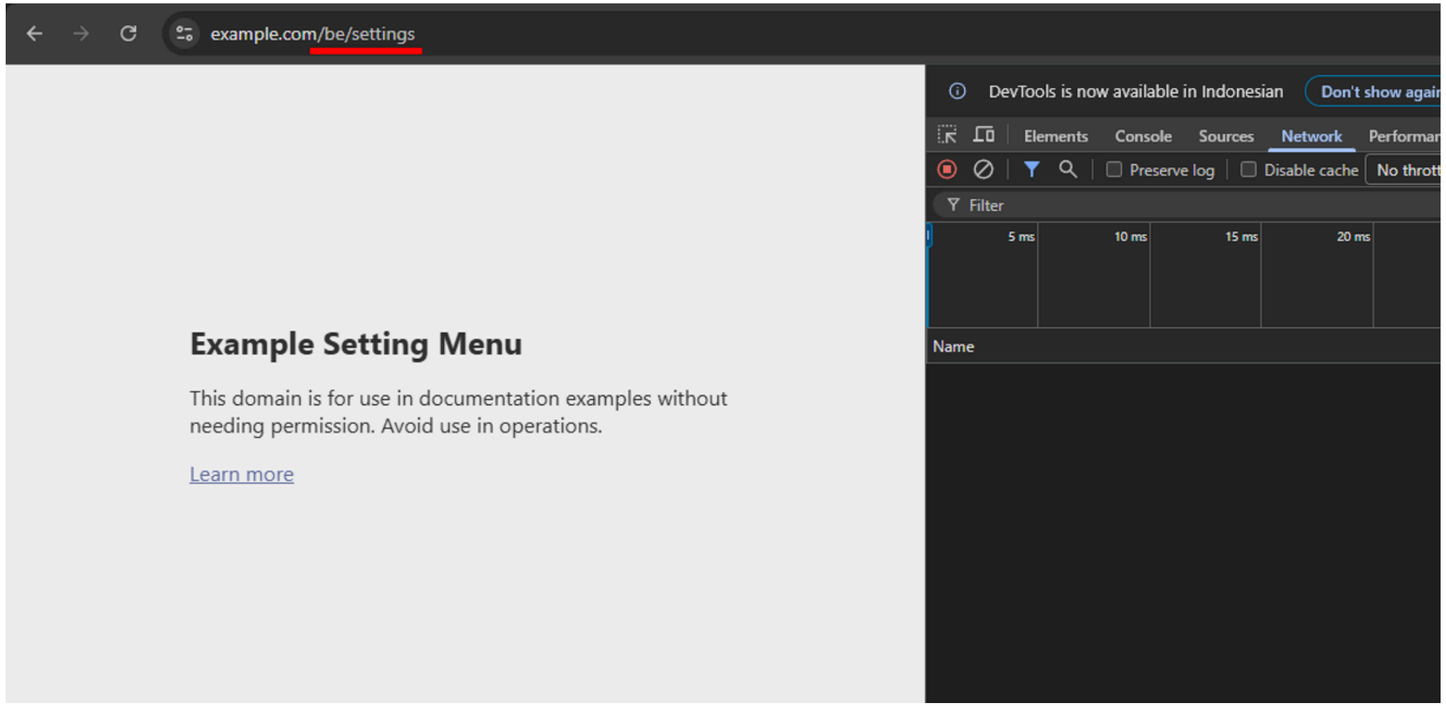



```
role === "admin" ? showSettingPage() : error();
```

```
{
  "user_id": 12345,
  "permissions": [
    "read:settings",
    "write:settings",
    "delete:settings"
  ],
  "roles": [
    "admin"
  ],
  "access_level": "full"
}
```

(C/S)SR - Example

Home **Content**



Data/Resource diproses oleh server.

validasi server side.

Common Broken Access Control vulnerabilities

Home **Content**

- CWE-862 Missing Authorization
- CWE-425 Direct Request ('Forced Browsing')
- IDOR (Insecure Direct Object Reference)
- Privilege Escalation (Vertical & Horizontal)
- etc.

List of Mapped CWEs

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-23 Relative Path Traversal

CWE-35 Path Traversal: '.../...//'

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CWE-201 Exposure of Sensitive Information Through Sent Data

CWE-219 Storage of File with Sensitive Data Under Web Root

CWE-264 Permissions, Privileges, and Access Controls (should no longer be used)

CWE-275 Permission Issues

CWE-276 Incorrect Default Permissions

CWE-284 Improper Access Control

Common Broken Access Control vulnerabilities

Home **Content**

CWE-862 Missing Authorization

Terjadi ketika sistem tidak memeriksa apakah pengguna memiliki izin sebelum mengakses fungsi atau data tertentu.

```
GET /api/v1/user/admin HTTP/1.1
Host: target-website.com
User-Agent: Mozilla/5.0
Accept: application/json
Connection: close


HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 153

{
  "user_id": 1029,
  "username": "admin",
  "email": "admin@target-website.com",
  "role": "administrator"
}
```

Common Broken Access Control vulnerabilities

Home **Content**

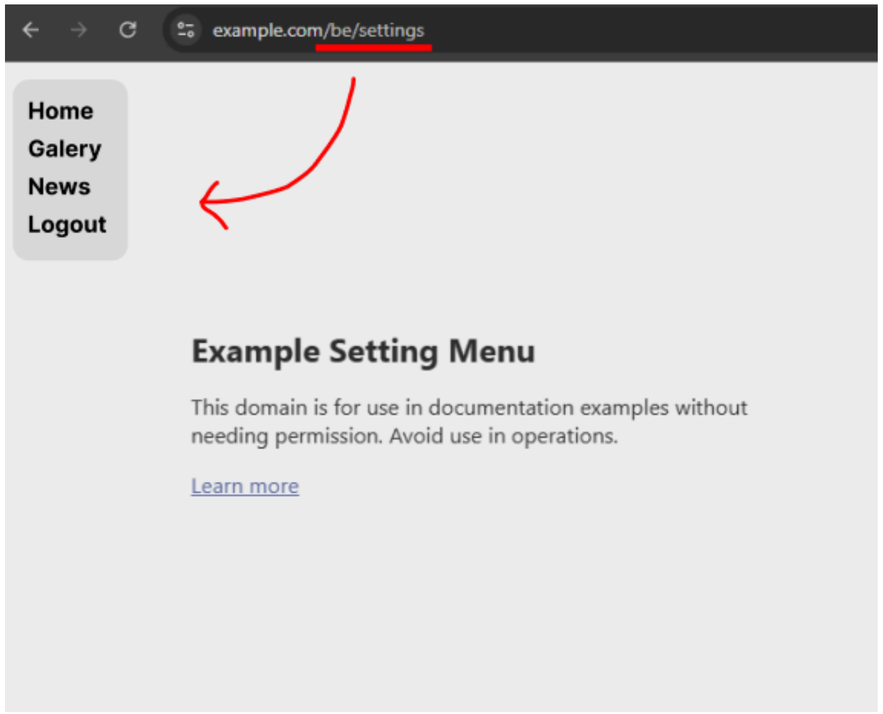

```
GET /api/v1/user/admin HTTP/1.1
Host: target-website.com
User-Agent: Mozilla/5.0
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6...
Accept: application/json
Connection: close


HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 153

{
  "user_id": 1029,
  "username": "admin",
  "email": "admin@target-website.com",
  "role": "administrator"
}
```

Common Broken Access Control vulnerabilities

Home **Content**

CWE-425 Direct Request ('Forced Browsing')

Terjadi saat pengguna dapat mengakses resource tersembunyi atau terbatas secara langsung tanpa otorisasi, misalnya dengan membuka URL yang tidak terlindungi.



Common Broken Access Control vulnerabilities

Home **Content**

IDOR (Insecure Direct Object Reference)

Terjadi saat pengguna dapat mengakses data atau resource milik orang lain hanya dengan mengubah ID di URL atau parameter, tanpa validasi otorisasi.

```
GET /api/user/profile?user_id=101 HTTP/1.1
Host: example.com
Cookie: session=abcd1234

-
HTTP/1.1 200 OK
Content-Type: application/json

{
  "user_id": 101,
  "username": "johndoe",
  "email": "john@example.com",
  "role": "user"
}
```

Common Broken Access Control vulnerabilities

Home **Content**

IDOR (Insecure Direct Object Reference)

Terjadi saat pengguna dapat mengakses data atau resource milik orang lain hanya dengan mengubah ID di URL atau parameter, tanpa validasi otorisasi.

```
GET /api/user/profile?user_id=102 HTTP/1.1
Host: example.com
Cookie: session=abcd1234

-
HTTP/1.1 200 OK
Content-Type: application/json

{
  "user_id": 102,
  "username": "pwt-dev",
  "email": "pwt-dev@example.com",
  "role": "user"
}
```

Common Broken Access Control vulnerabilities

Home **Content**

IDOR (Insecure Direct Object Reference)

Terjadi saat pengguna dapat mengakses data atau resource milik orang lain hanya dengan mengubah ID di URL atau parameter, tanpa validasi otorisasi.

```
GET /api/user/profile?user_id=102 HTTP/1.1
Host: example.com
Cookie: session=abcd1234

-
HTTP/1.1 200 OK
Content-Type: application/json

{
  "user_id": 102,
  "username": "pwt-dev",
  "email": "pwt-dev@example.com",
  "role": "user"
}
```

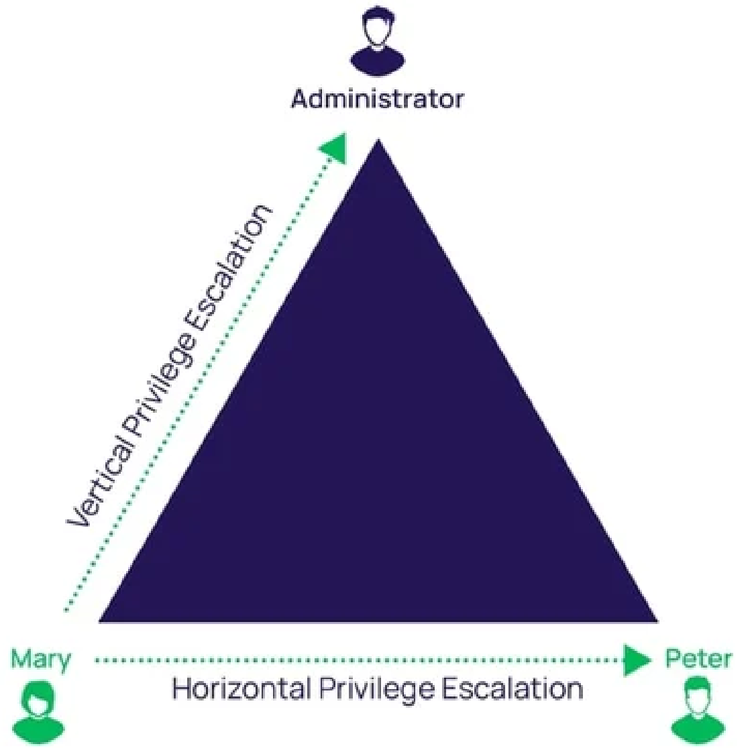
Common Broken Access Control vulnerabilities

Home **Content**

Privilege Escalation (Vertical & Horizontal)

Peningkatan hak akses pengguna melebihi yang seharusnya.

- Vertical: Pengguna biasa mendapat akses admin.
- Horizontal: Pengguna mengakses data atau fungsi milik pengguna lain dengan level akses yang sama.



Mitigation of Broken Access Control

Home **Content**

No authentication & authorization;
CVE on dependency (CVE-2024-51479);
Weak Permission Check;
Etc.

Mitigation of Broken Access Control

Home **Content**

Implementation of strong authentication and authorization;
use the latest dependencies
Good permission/validation checks;
etc.

Demo of Broken Access Control

Home **Content**


```
root@root$ cat /etc/hosts

127.0.0.1       demo0.bac
127.0.0.1       demo1.bac
127.0.0.1       demo2.bac
127.0.0.1       demo3.bac
127.0.0.1       demo5.bac
```

FAQ - QNA

Home **Content**

root@root$ cat /tmp/oot/faq.txt

Info berkarir di cysec?
Mulai dari mana ya?
Perlu bisa ngoding ga?

root@root$ cat /tmp/qna.txt

???????
??????????
??????????????

Thank you all.

Home **Content**

Reference

Home **Content**

1. https://aws.amazon.com/what-is/cybersecurity/
2. https://medium.com/@hendprw/photo-by-flyd-on-unsplash-3742b25843d8
3. https://muh-hidayat7799.medium.com/owasp-top-10-series-a1-broken-access-control-indonesia-1fce2a892a04