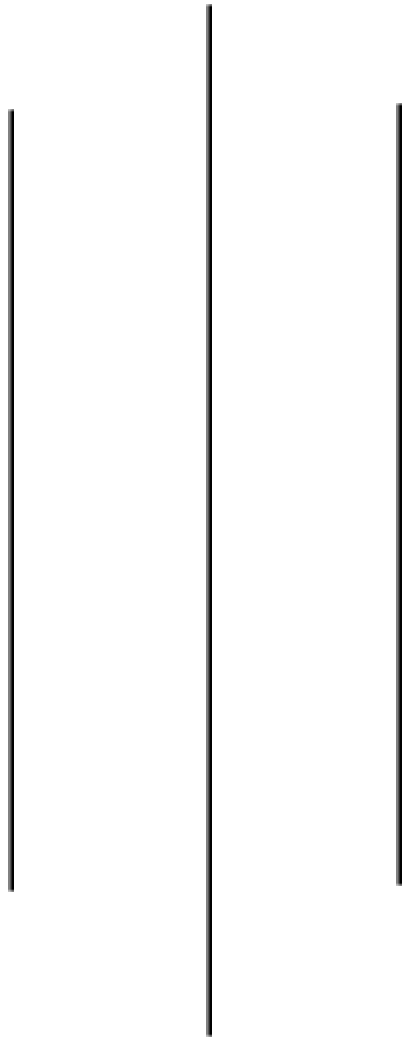
Bug Report



Oleh: Made Doddy Adi Pranatha

Bug Report | 2

Title	IDOR pada edit data barang
Description	Terdapat kelemahan IDOR paa halaman edit data barang sehingga user dapat melihat data barang yang dibuat oleh user lain
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L 6.7 Medium
Steps to Reproduce	1. Login user ke halaman dashboard user 2. Masuk ke halaman data barang 3. Edit data barang 4. Ganti id barang pada query string id barang
OS and Browser	OS: Windows 11 Browser: Chrome Version 105.0.5195.127
Proof of Concept	https://youtu.be/L-_MQH479YM
Impact	Dapat melihat data dari user lain
Remediation	1. Filter data barang berdasarkan user yang login
References	1. https://www.bugcrowd.com/blog/how-to-find-idor-insecure-direct-object-reference-vulnerabilities-for-large-bounty-rewards/

Bug Report | 2

Title	**IDOR Pada Delete Data Barang**
Description	Terdapat kelemahan IDOR paa halaman delete data barang sehingga user dapat mendelete data barang yang dibuat oleh user lain
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L 6.7 Medium
Steps to Reproduce	2. Login pada halaman dashboard user 3. Pergi ke halaman data barang 4. Buka burp suite dan aktifkan intercept 5. Klik tombol delete 6. Ganti id barang waktu delete produk 7. Maka data yang terdelete adalah data pada user lain
OS and Browser	OS: Windows 11 Browser: Firefox version 104.02
Proof of Concept	https://youtu.be/SVw7XXyI3ZY
Impact	Bisa mendelete data barang milik user lain
Remediation	1.Filter data barang berdasarkan user yang login
References	8. https://www.bugcrowd.com/blog/how-to-find-idor-insecure-direct-object-reference-vulnerabilities-for-large-bounty-rewards/

Bug Report | 2

Title	**CSRF Pada halaman data barang**
Description	Terdapat kelemahan CSRF pada halaman data barang sehingga penyerang dapat menambah data barang yang dibuat oleh non user
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L 5.5 Medium
Steps to Reproduce	1. Login pada halaman dashboard user 2. Pergi ke halaman data barang 3. Buat sebuah file form tambah data barang pada html 4. Jalankan file form tambah data barang 5. Submit 6. Maka data barang di tambahkan
OS and Browser	OS: Windows 11 Browser: Firefox version 104.02
Proof of Concept	https://youtu.be/wHlPwGsdYns
Impact	Bisa menambahkan data barang tanpa login
Remediation	1.Tambahkan autentikasi user yang dapat menambahkan data barang
References	1. https://owasp.org/www-community/attacks/csrf

Bug Report | 2

Title	**CSRF Pada halaman edit data barang**
Description	Terdapat kelemahan CSRF pada halaman edit barang sehingga penyerang dapat edit data barang yang dibuat oleh non user
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L 5.5 Medium
Steps to Reproduce	1. Login pada halaman dashboard user 2. Pergi ke halaman edit data barang 3. Buat sebuah file form edit data barang pada html 4. Jalankan file form tambah data barang 5. Submit 6. Maka data barang di edit
OS and Browser	OS: Windows 11 Browser: Firefox version 104.02
Proof of Concept	https://youtu.be/Nt-okyYQ7gQ
Impact	Bisa mengedit data barang tanpa login
Remediation	1.Tambahkan autentikasi user yang dapat mengedit data barang
References	1. https://owasp.org/www-community/attacks/csrf

Bug Report | 2

Title	**CSRF Pada halaman delete data barang**
Description	Terdapat kelemahan CSRF pada halaman delete barang sehingga penyerang dapat delete data barang yang dibuat oleh non user
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L 5.5 Medium
Steps to Reproduce	1. Login pada halaman dashboard user 2. Buat sebuah file form delete data barang pada html 3. Jalankan file form delete data barang 4. Submit 5. Maka data barang di delete
OS and Browser	OS: Windows 11 Browser: Firefox version 104.02
Proof of Concept	https://youtu.be/6E-wo3aj2yE
Impact	Bisa mengedit data barang tanpa login
Remediation	1.Tambahkan autentikasi user yang dapat men-delete data barang
References	1. https://owasp.org/www-community/attacks/csrf

Bug Report | 2

Title	**Host Header Pada halaman Forgot Password**
Description	Terdapat kelemahan Host Header pada halaman forget password sehingga penyerang dapat menyisipkan sembarang url sehingga penyerang dapat mengambil token user.
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L 4.7 Medium
Steps to Reproduce	1. Masuk ke halaman forgot password 2. Buka burp suite 3. Masukkan email address 4. Ganti pada bagian host dengan menggunakan sembarang url 5. Maka di kirimkan email dengan url sembarang tersebut
OS and Browser	OS: Windows 11 Browser: Firefox version 104.02
Proof of Concept	https://youtu.be/LqeNyPN3EJ4
Impact	Penyerang bisa mengambil informasi token pada forget password
Remediation	1.Memfilter host header agar sesuai dengan current url
References	1. https://portswigger.net/web-security/host-header

Bug Report | 2

Title	**Arbitary File Upload Pada halaman Register User**
Description	Terdapat kelemahan Arbitary File Upload pada halaman register user sehingga penyerang dapat mengupload file berbahaya.
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L 4.7 Medium
Steps to Reproduce	1. Buat sebuah file php yang dapat mendapatkan informasi php info 2. Masuk ke halaman registrasi 3. Input field - field user 4. Upload file phpinfo yang telah dibuat tadi 5. Ketika user berhasil dibuat login sebagai user tersebut 6. Masuk ke halamn profile 7. Klik kanan dan tampilkan gambar maka didapatkan informasi tentang bahasa yang digunakan
OS and Browser	OS: Windows 11 Browser: Firefox version 104.02
Proof of Concept	https://youtu.be/0nn9nORNmYo
Impact	1. Penyerang bisa mengambil informasi penting 2. Penyerang bisa mengupload file berbahaya
Remediation	1.Memfilter file yang diupload oleh user
References	1. https://portswigger.net/web-security/host-header