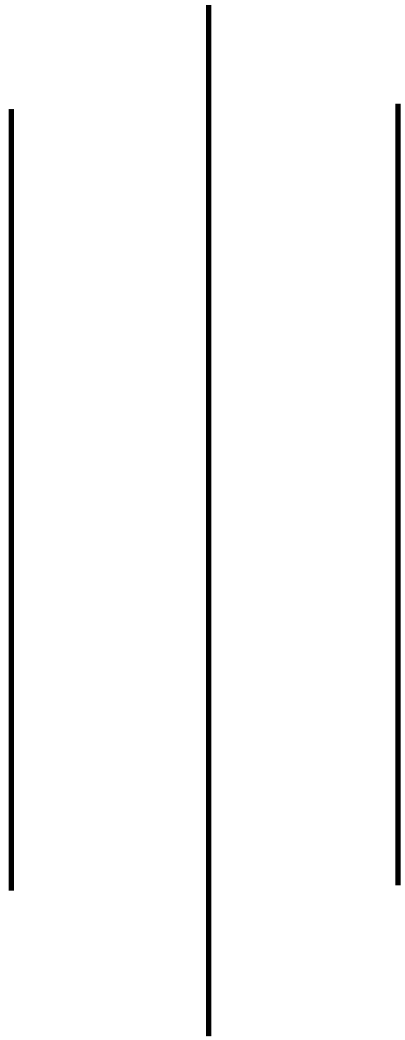
Bug Report



Oleh: Indra Budiman

Bug Report | 2

Title	Unrestricted File Upload (UFU) pada fitur register
Description	Terdapat kerentanan yang memungkinkan penyerang mengeksekusi kode jarak jauh melalui celah yang terdapat pada fitur registrasi dimana dengan cara menyisipkan file berbahaya ke target. Hal ini dikarenakan tidak adanya validasi terhadap file yang terdapat pada form registrasi
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N - MEDIUM 5.3
Steps to Reproduce	1. Mengkases http://157.245.194.94/ 2. Beralih ke menu login 3. Menekan 'Create an Account' untuk ke menu register 4. Menyisipkan file/payload yang memungkinkan kerentanan UFU, seperti file berekstensi php
OS and Browser	OS: Windows 10 Browser: Chrome versi 105.0.5195.127
Proof of Concept	https://drive.google.com/file/d/1jK0vZUDQKLmGGr3F_Q8i8sR3fQrWi2NI/view?usp=sharing
Impact	Bisa menyisipkan dan menjalankan kode berbahaya
Remediation	1. Memberikan filter/validasi pada file yang terdapat pada form
References	1. https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload 2. https://elib.unikom.ac.id/files/disk1/664/jbptunikompp-gdl-jamiekaris-33168-12-unikom_j-a.pdf

Bug Report | 3

Title	SQLI pada fitur edit data
Description	Terdapat kerentanan yang memungkinkan penyerang dapat mengetahui data data yang tersimpan pada database sistem. Hal ini dikarenakan tidak adanya filter terhaadp metakarakter yang digunakan dalam sintaks sql sehingga penyerang dapat menginputkan metakarakter yang diinginkan.
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - HIGH 7.5
Steps to Reproduce	1. Mengkases http://157.245.194.94/ 2. Register dan login ke sistem 3. Mengaktifkan burpsuite, ke modul proxy dan menekan intercept on 4. Edit salah satu data yang ada di dashboard 5. Menyimpan request tersebut ke file txt 6. Menjalankan sqlmap dan memasukkan payload yang dibuat pada step sebelumnya ex: sqlmap -r nama_file --dump
OS and Browser	OS: Linux (Kali) Browser: Firefox versi 91.11.0esr (64-bit)
Proof of Concept	https://drive.google.com/file/d/1kQe1BTe6bQiRIUeall4Wc72_bzWx_PMd/view?usp=sharing
Impact	Bisa mendapatkan data data rahasia yang ada di DB sistem
Remediation	1. Memberikan filter metakarakter pada form-form yang ada pada sistem
References	1. https://owasp.org/www-community/attacks/SQL_Injection 2. https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

Bug Report | 4

Title	CSRF pada fitur add data
Description	Terdapat kerentanan yang memungkinkan penyerang dapat melakukan HTTP request POST yang tidak asah atas nama korban/user untuk menambah data baru. Hal ini dikarenakan tidak adanya validasi terhadap token rahasia milik user.
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N - MEDIUM 5.7

Steps to Reproduce	1. Mengkases http://157.245.194.94/
	2. Login ke sistem
	3. Mengaktifkan burpsuite, ke modul proxy dan menekan intercept on
	4. Menambahkan satu data baru, masukkan nama dan kuantitas barang
	5. Mengamati request yang terbuat pada burp suite
	6. Membuat file html dengan isian seperti berikut
	`<form action="http://157.245.194.94/user/cek-tambah-data" method="POST">`
	`<input type="hidden" name="nama_barang" value="CSRF">`
	`<input type="hidden" name="kuantitas" value="99">`
	`<input type="submit" value="sikat gan!">`
	`</form>`
	7. Menjalankan file html yang dibuat dan mengklik tombol sikat gan!

OS and Browser	OS: Linux (Kali) Browser: Firefox versi 91.11.0esr (64-bit)
Proof of Concept	https://drive.google.com/file/d/1KErTFiiRgGGImXkYimLt1sGB28yJVtvo/view?usp=sharing
Impact	Bisa mendapatkan data data rahasia yang ada di DB sistem
Remediation	1. Membuat validasi token unik user pada proses request add new data
References	1. https://owasp.org/www-community/attacks/csrf 2. https://gudangssl.id/blog/csrf-adalah/

Title	SQLI pada plugin BadgeOS yang digunakan pada CMS yang terinstall di http://157.245.194.94/wp/
Description	Plugin BadgeOS yang digunakan tidak mensanitasi parameter yang digunakan sehingga memungkinkan
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - HIGH 7.5
Steps to Reproduce	1. http://157.245.194.94/wp/wp-admin/admin-ajax.php?action=get-achievements&total_only=true&user_id=11%20AND%20(SELECT%209628%20FROM%20(SELECT(SLEEP(5)))WOrh)--%20KUsb
OS and Browser	OS: Windows 10 Browser: Chrome versi 105.0.5195.127
Proof of Concept	https://drive.google.com/file/d/1GoE5eiftdFBe6AcBdAR2K1FIdxXKc-FK/view?usp=sharing
Impact	Mendapatkan data data rahasia yang tersimpan dalam DB
Remediation	1. Memperbarui plugin BadgeOS yang digunakan ke versi minimal 3.7.1.3
References	1. https://owasp.org/www-community/attacks/SQL_Injection 2. https://wpscan.com/vulnerability/8743534f-8ebd-496a-99bc-5052a8bac86a

Bug Report | 6

Title	Local File Inclusion (LFI) pada fitur manage list tabel
Description	Terdapat kerentanan yang memungkinkan penyerang mengakses file file yang terdapat pada direktori target. Hal ini dikarenakan tidak adanya filter pada input terdapat pada halaman manage list table
CVSS Vector and Score	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - HIGH 7.5
Steps to Reproduce	1. Mengakses http://157.245.194.94/administrator/ 2. Login dengan memasukkan username: administrator; password: administrator 3. Mengakses list table yang terdapat pada menu tables 4. Mengganti value dari parameter file yang terdapat pada url link http://157.245.194.94/administrator/tables.php?file=list-news.php menjadi etc/passwd
OS and Browser	OS: Windows 10 Browser: Chrome versi 105.0.5195.127
Proof of Concept	https://drive.google.com/file/d/1dn-nSZJd7h3Pm2va_Z2tlR5j7W6SYu6G/view?usp=sharing
Impact	Mendapatkan data-data rahasia yang tersimpan dalam direktori target
Remediation	1. Filter input dari user 2. Tidak menggunakan fungsi include file
References	1. https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion