

Implementasi Zero Trust Access Control pada Aplikasi Sederhana

kelompok 4

Luthfi Kurniawan (2201020013)

M. Afief Anugrah (2201020015)

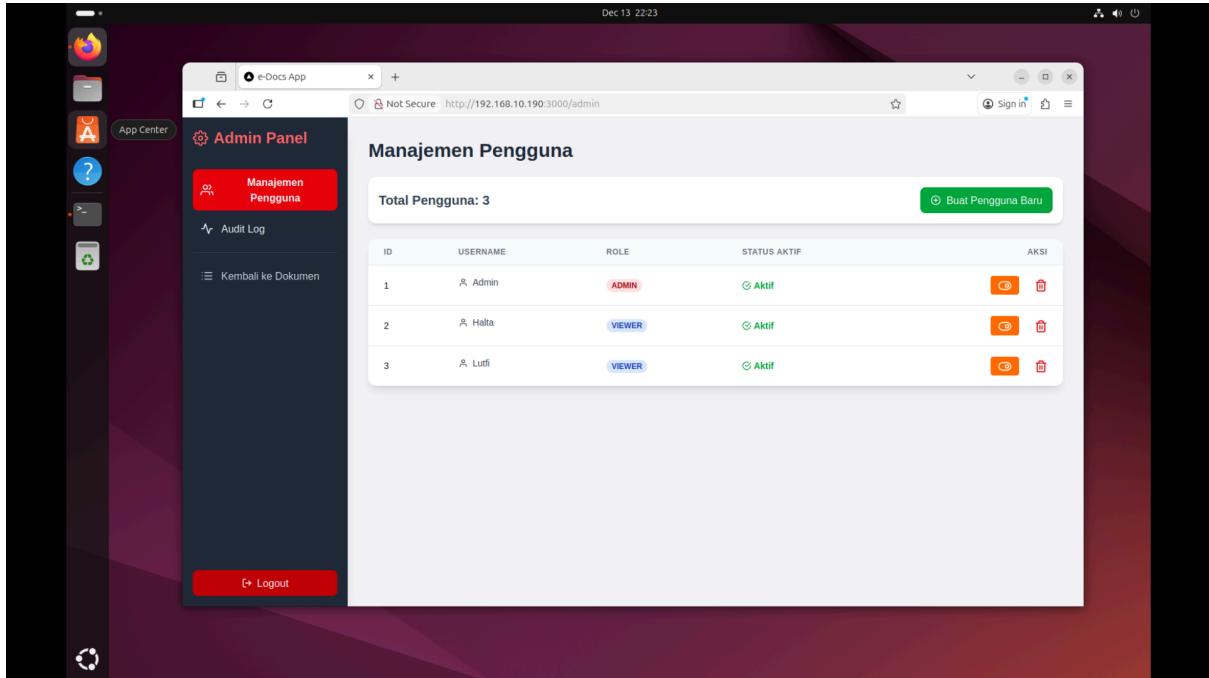
Aditya Firmansyah (2201020018)

Halta Putra Ash Sidiq (2201020092)

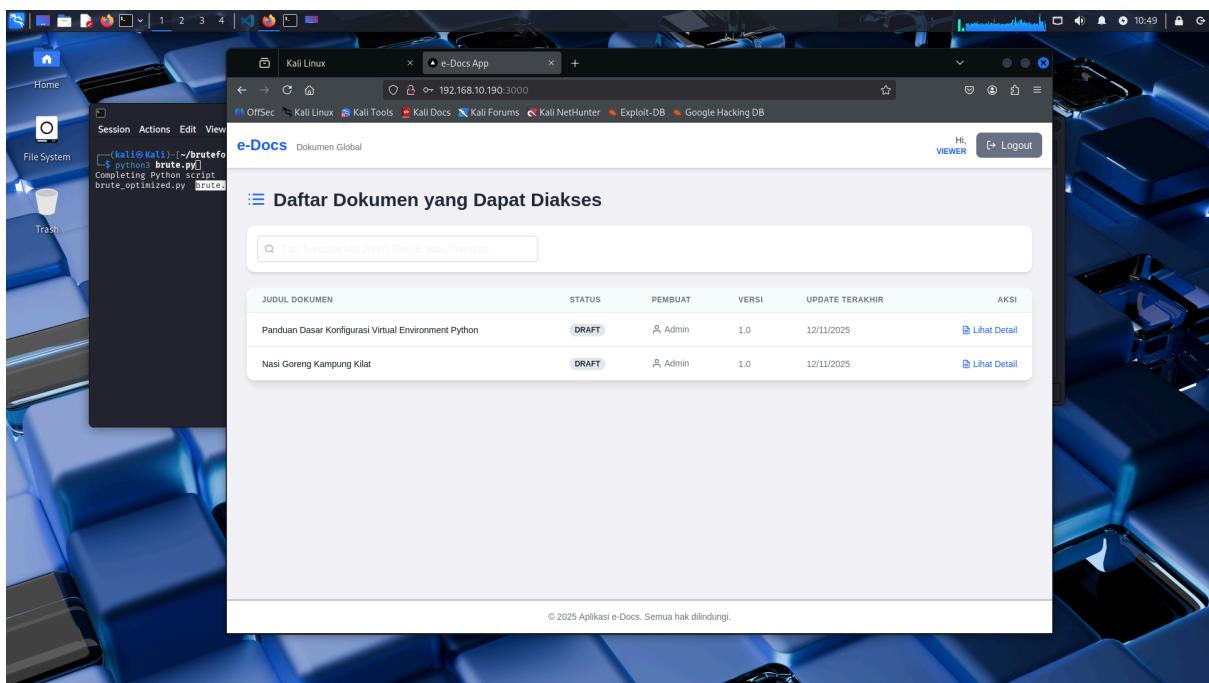
Minggu 5 : Pengujian brute-force / bypass

1. PENGUJIAN KETAHANAN SERANGAN (BRUTE-FORCE)

A.Persiapan Data Serangan dan tampilan login yang akan diserang



Halaman Admin Melihat Semua User



Tampilan User Lutfi mencoba login dan berhasil

A screenshot of a Kali Linux desktop environment. In the center is a terminal window titled '(kali㉿Kali)-[~/bruteforce]'. The terminal displays the command 'cat passwords.txt' followed by a list of 20 password entries. The desktop background is a blue metallic keyboard texture. Icons for Home, File System, and Trash are visible on the left.

```
(kali㉿Kali)-[~/bruteforce]
cat passwords.txt
123456
123123
Lutfi123!@
AHU6
Lutfi
lutfi
Lutfii
lutfi12
Lutfi123
Lutfi123!@#
Lutfi1238
Lutfi1230
Lutfi1231
Lutfi123!@#
Lutfi12
Lutfi123!@#
Lutfi1232
Lutfi12323
Lutfi12323
Lutfi12367
```

Penjelasan Percobaan *brute-force* dilakukan menggunakan skrip yang mengambil daftar *password* dari *data sheet* yang telah disiapkan (passwords.txt) untuk menyerang *username* Lutfi. Daftar tersebut berisi kombinasi *password* yang bervariasi.

B. Pelaksanaan dan Hasil Brute-Force

A screenshot of a Kali Linux desktop environment. In the center is a terminal window titled '(kali㉿Kali)-[~/bruteforce]'. The terminal displays the command '\$ python3 brute.py' followed by a detailed log of the brute-force attack results. It shows numerous successful findings ('BERHASIL') for various password combinations. At the bottom, it indicates 20 valid passwords found. The desktop background is a blue metallic keyboard texture. Icons for Home, File System, and Trash are visible on the left.

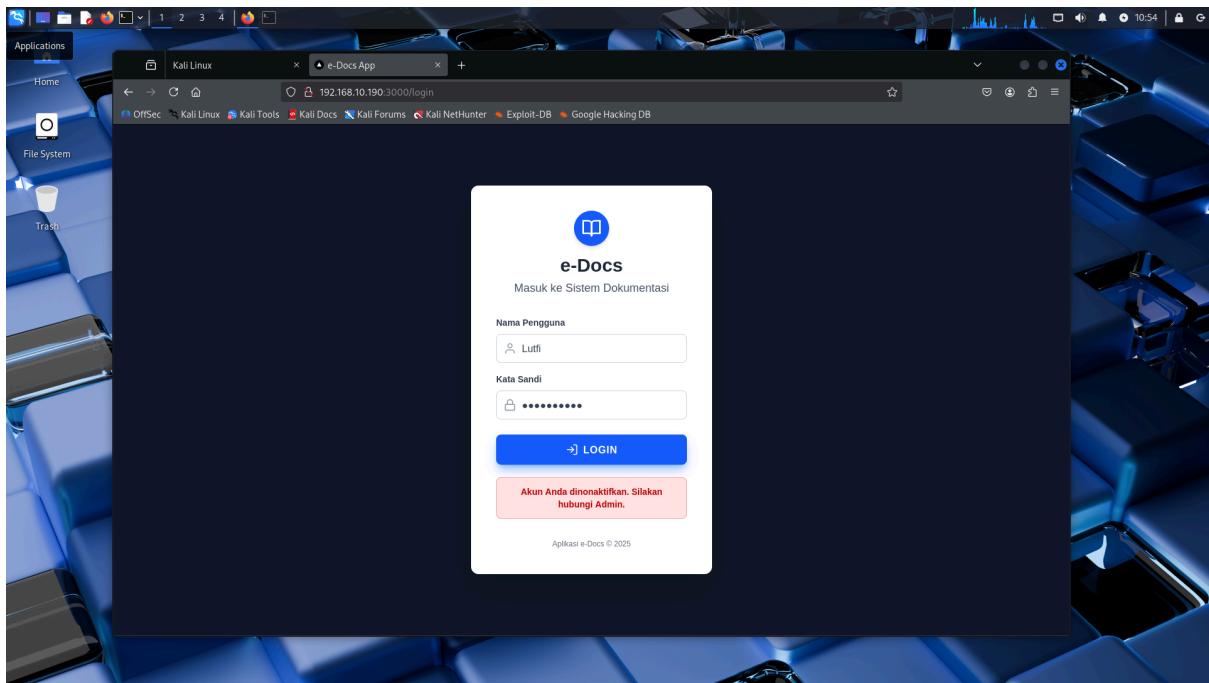
```
(kali㉿Kali)-[~/bruteforce]
$ python3 brute.py
[*] Mulai pengujian Brute Force (JSON) pada http://192.168.10.190:3200/api/auth/login
[+] BERHASIL DITEMUKAN: Lutfi:1234456 (Status: 401)
[+] BERHASIL DITEMUKAN: Lutfi:123123 (Status: 401)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi123!@ (Status: 200)
[+] BERHASIL DITEMUKAN: Lutfi:AHU6 (Status: 401)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi (Status: 401)
[+] BERHASIL DITEMUKAN: Lutfi:lutfi (Status: 401)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfii (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi12 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi123 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi123!@# (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi1238 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi1230 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi1231 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi123!@# (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi12 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi123!@# (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi1232 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi12323 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi123233 (Status: 403)
[+] BERHASIL DITEMUKAN: Lutfi:Lutfi12367 (Status: 403)

— Ringkasan Hasil —
[*] Ditemukan 20 Password Valid!
→ 1234456
```

Dibuat Dengan menggunakan python dengan library **RequestS**, Penjelasan Meskipun skrip *brute-force* berhasil menemukan beberapa *password* yang valid (ditunjukkan oleh status **200 OK**), sistem tidak menghentikan serangan secara langsung. Karena *lockout* (penguncian akun) diatur setelah **3 kali kegagalan login**, dan skrip terus mencoba kombinasi *password*.

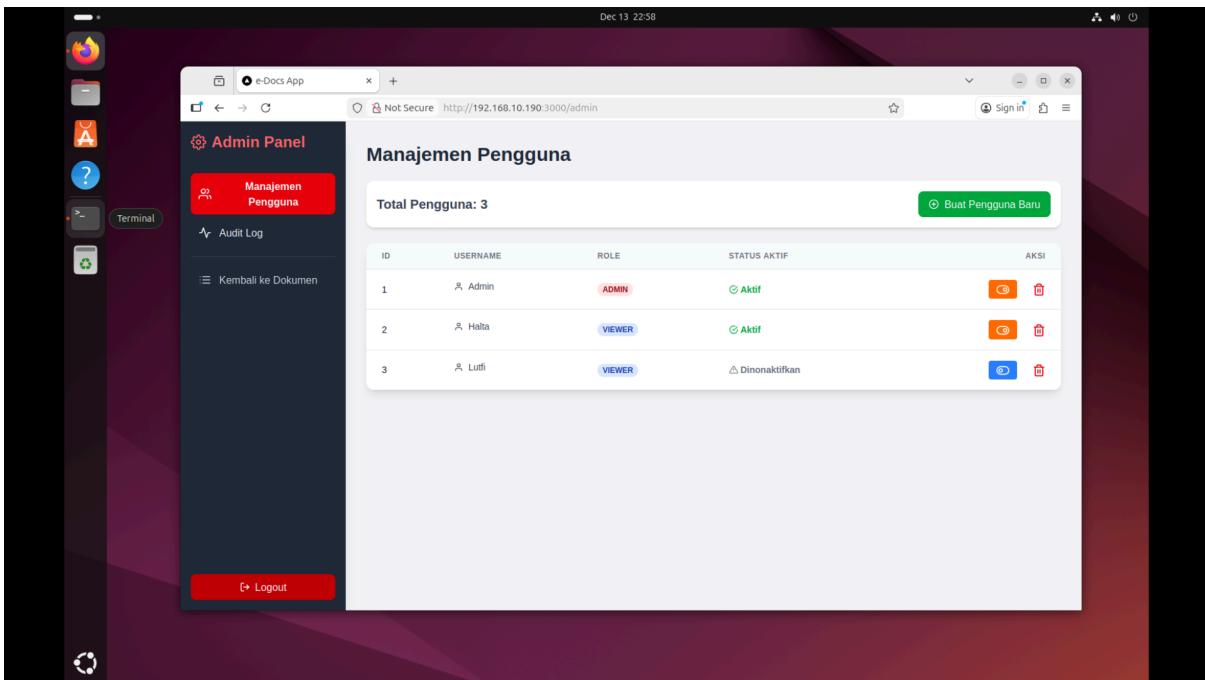
yang salah setelah menemukan yang benar, *limit* kegagalan terlampaui. Akibatnya, akun *user* tersebut dikunci. Mnggunkan sistem ketika 3 kali sati salah akan di blok, di porses brute force yang di buat tadi kan gak di stop langsung ketika password nya dapat jadi akan mencobah lagi sampai habis jadi akun ddeng Lutfi akan ke blok

C. Verifikasi Account Lockout



Penjelasan Ketika *user* Lutfi mencoba *login* kembali menggunakan *password* yang benar, sistem menolak aksesnya dengan pesan *error* **Akun Anda dikunci**, karena ambang batas percobaan gagal telah melampaui limit yang diizinkan oleh sistem.

D. Konfirmasi Lockout dari Admin Panel



Penjelasan Verifikasi status *lockout* dikonfirmasi melalui *Admin Panel* (Manajemen Pengguna). *Admin* dapat melihat status pengguna Lutfi telah berubah menjadi [Blokir / Non-Aktif] (`isActive: false`), membuktikan bahwa mekanisme *Account Lockout* berfungsi dan Admin dapat memantau insiden serangan.

E. Bukti Forensik (Audit Log)

Aksi	Tujuan	Tanggal	User	IP Address
LOGIN_BLOCKED_INACTIVE	Pada Tabel: Users	12/13/2025, 10:51:14 PM	Lutfi (3)	::ffff:192.168.10.167
LOGIN_BLOCKED_INACTIVE	Pada Tabel: Users	12/13/2025, 10:51:13 PM	Lutfi (3)	::ffff:192.168.10.167
ACCOUNT_LOCKED	Pada Tabel: Users	12/13/2025, 10:51:13 PM	Lutfi (3)	::ffff:192.168.10.167
LOGIN_FAILED	Pada Tabel: Users	12/13/2025, 10:51:12 PM	Lutfi (3)	::ffff:192.168.10.167
LOGIN_FAILED	Pada Tabel: Users	12/13/2025, 10:51:11 PM	Lutfi (3)	::ffff:192.168.10.167
USER_LOGIN	Pada Tabel: Users	12/13/2025, 10:51:11 PM	Lutfi (3)	::ffff:192.168.10.167
LOGIN_FAILED	Pada Tabel: Users	12/13/2025, 10:51:10 PM	Lutfi (3)	::ffff:192.168.10.167
LOGIN_FAILED	Pada Tabel: Users	12/13/2025, 10:51:09 PM	Lutfi (3)	::ffff:192.168.10.167
READ_ALL_DOCUMENTS	Pada Tabel: Documents	12/13/2025, 10:49:29 PM	Lutfi (3)	::ffff:192.168.10.167
SESSION_CHECK	Pada Tabel: Users	12/13/2025, 10:49:29 PM	Lutfi (3)	::ffff:192.168.10.167

Penjelasan Semua aktivitas *brute-force*, baik upaya sukses maupun kegagalan yang menyebabkan *lockout*, direkam oleh **Audit Log** (Prinsip *Assume Breach*). Log ini mencakup detail **User ID**, **IP Address**, dan **Timestamp**, yang krusial untuk analisis keamanan pasca-insiden.