LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB	: KERENTANAN DAN ANCAMAN
NAMA	: DANI ADRIAN
NIM	: 225150201111009
TANGGAL	: 14/03/2024
ASISTEN	: Bernas Cakra Sakti Harisna
	Mohammad Seto Aji Pamungkas

Langkah Praktikum

Instalasi Persiapan Lingkungan Praktikum

1. Langkah 1
    a. Buka terminal pada sistem operasi Linux
    b. Pada terminal, lakukan instalasi git:

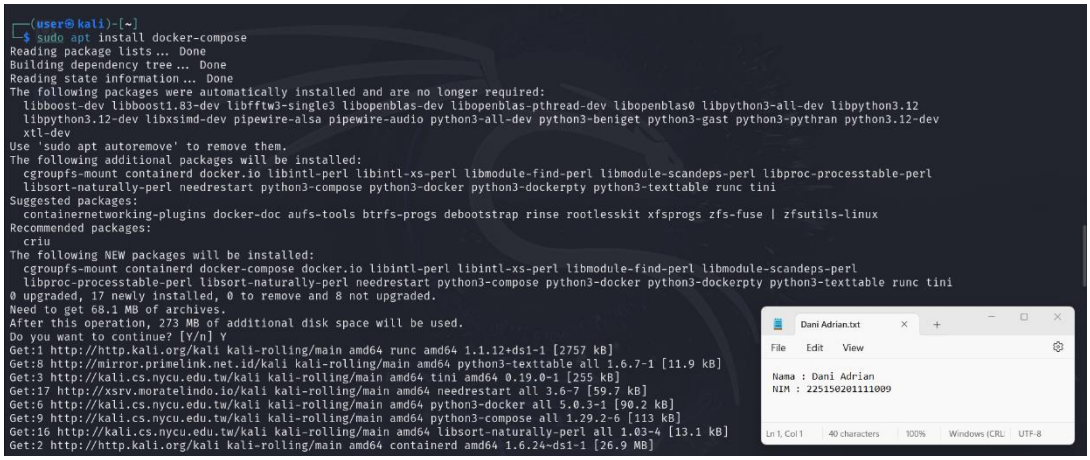
```
sudo apt install git
```

Git adalah sistem kontrol versi yang digunakan untuk melacak perubahan dalam kode sumber selama pengembangan perangkat lunak. Untuk menginstal Git di sistem operasi Linux, gunakan perintah sudo apt install git pada terminal. Perintah ini akan mengunduh dan menginstal Git serta dependensinya dari repositori paket sistem. Setelah proses instalasi selesai, gunakan Git untuk mengelola proyek secara efisien.

2. Langkah 2
    c. Lakukan instalasi docker-compose dengan perintah:

```
sudo apt install docker-compose
```

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Docker-Compose adalah alat yang memungkinkan pengguna untuk mendefinisikan dan menjalankan aplikasi Docker yang terdiri dari beberapa wadah. Untuk menginstal Docker-Compose di sistem operasi Linux, gunakan perintah `'sudo apt install docker-compose'` pada terminal. Perintah ini akan mengunduh dan menginstal Docker-Compose serta dependensinya dari repositori paket sistem. Setelah proses instalasi selesai, maka dapat menggunakan Docker-Compose untuk mengelola aplikasi yang terdiri dari beberapa wadah Docker dengan mudah.

3. Langkah 3
   d. Kemudian lakukan cloning github repository untuk lab percobaan bagian 1:

```
git clone https://github.com/adhiyaksactf/sqli-part1.git
```

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Cloning adalah proses membuat salinan lokal dari repositori Git yang ada. Untuk melakukannya, gunakan perintah git clone di terminal, diikuti dengan URL repositori yang ingin diklon. Perintah 'git clone https://github.com/adhiyaksactf/sqli-part1.git' akan membuat salinan lokal dari repositori sqli-part1.git di direktori saat ini di terminal. Setelah proses cloning selesai, kita akan memiliki salinan lengkap dari repositori tersebut di komputer lokal untuk digunakan dalam praktikum.

4. Langkah 4
   e. Lakukan cloning github repository untuk lab percobaan bagian 2:

```
git clone https://github.com/adhiyaksactf/sqli-part2.git
```

Dengan menjalankan perintah di atas pada terminal, kita akan membuat salinan lokal dari repositori sqli-part2.git di direktori saat ini di terminal. Setelah proses cloning selesai, kita akan memiliki salinan lengkap dari repositori tersebut di komputer lokal untuk digunakan dalam praktikum.

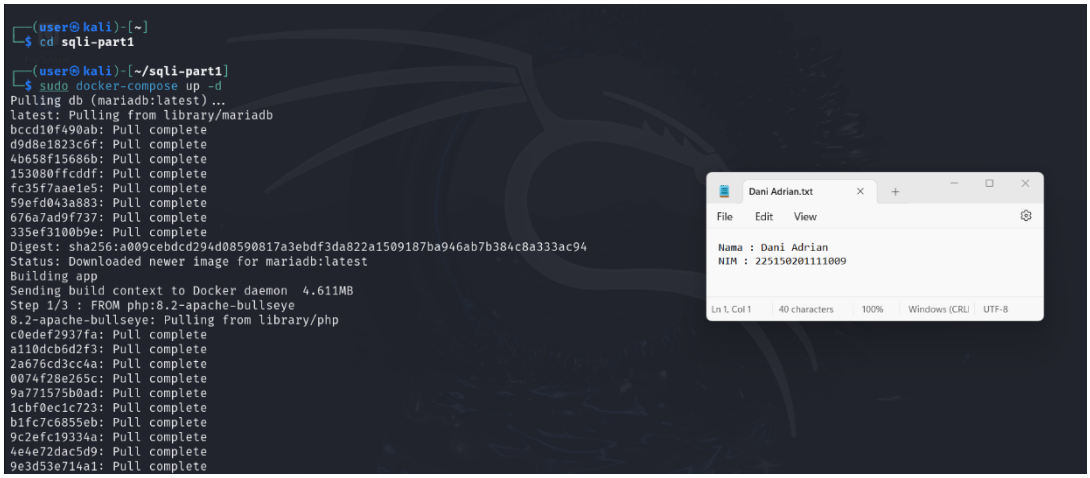
5. Langkah 5
   f. Masuk ke dalam direktori sqli-part1 dengan perintah:

```
cd sqli-part1
```

   g. Melakukan build docker untuk sqli-part1 dengan perintah:

```
sudo docker-compose up -d
```

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



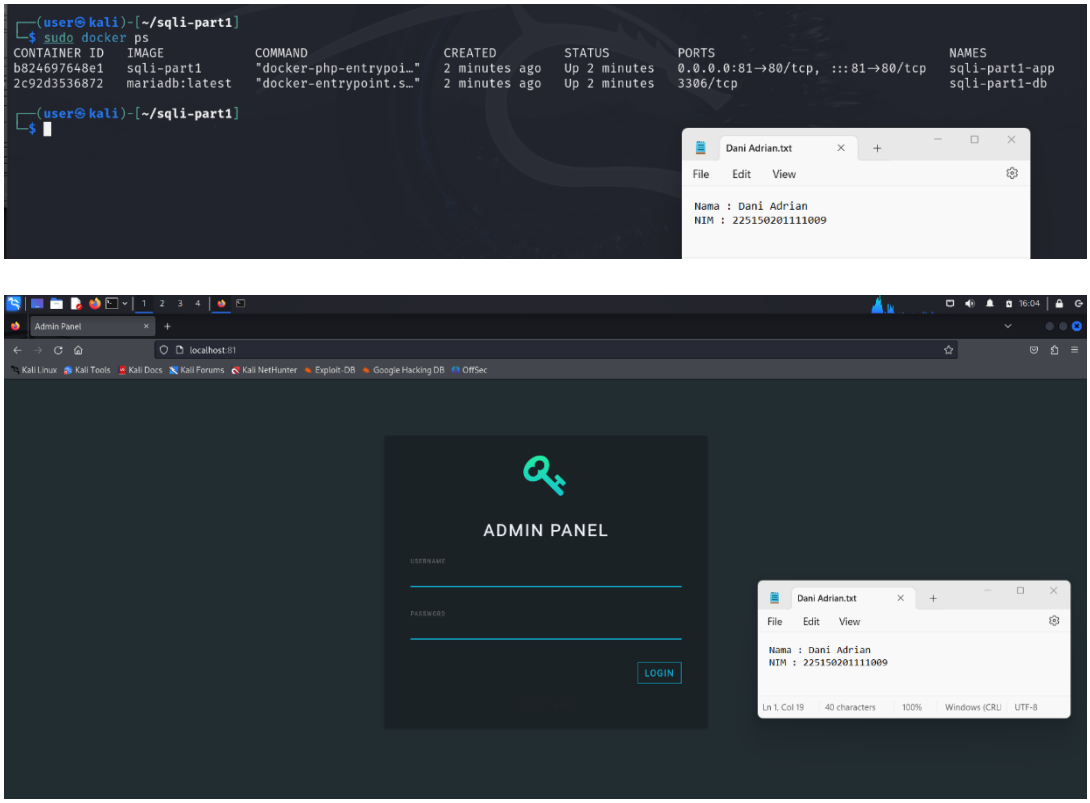
Dengan menjalankan perintah tersebut, Docker akan membangun dan menjalankan kontainer Docker yang didefinisikan dalam file `docker-compose.yml` di mode detasemen (-d), yang berarti kontainer akan berjalan di latar belakang. Setelah selesai, kita dapat mengakses aplikasi yang berjalan di kontainer Docker tersebut.

6. Langkah 6
    h. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:

```
sudo docker ps
```

    i. Apabila berhasil maka service akan berjalan pada port 81, sehingga dapat mengakses pada browser dengan alamat localhost:81

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Dengan mengakses alamat tersebut di browser, kita dapat melihat layanan yang berjalan dengan baik pada port 81.

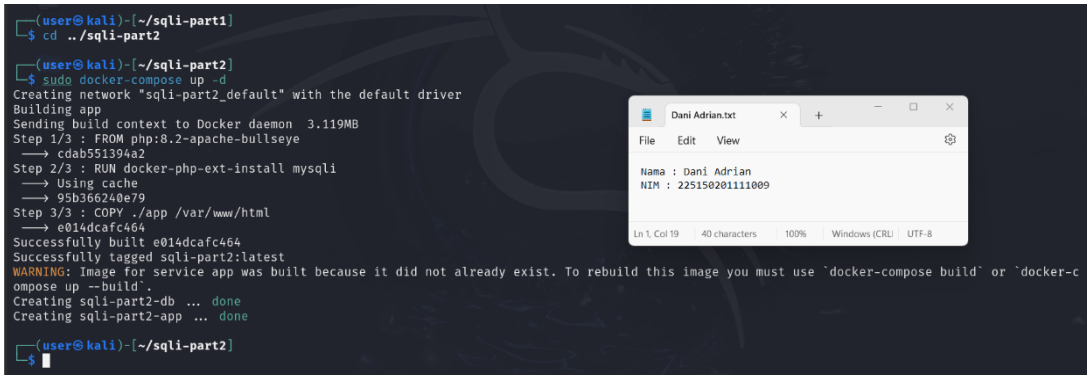
7. Langkah 7
   j. Kembali pada terminal Anda lakukan perintah untuk masuk ke direktori sqli-part2:

```
cd ../sqli-part2
```

   k. Melakukan build docker untuk sqli-part2 dengan perintah:

```
sudo docker-compose up -d
```

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

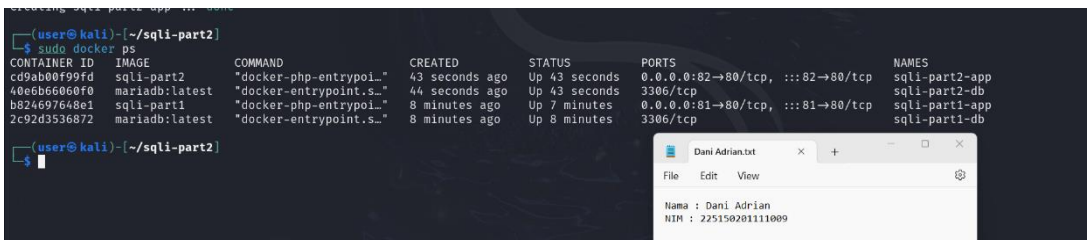


Dengan menjalankan perintah tersebut, Docker akan membangun dan menjalankan kontainer Docker yang didefinisikan dalam file `docker-compose.yml` di mode detasemen (-d), yang berarti kontainer akan berjalan di latar belakang. Setelah selesai, kita dapat mengakses aplikasi yang berjalan di kontainer Docker tersebut.

8. Langkah 8
   l. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:

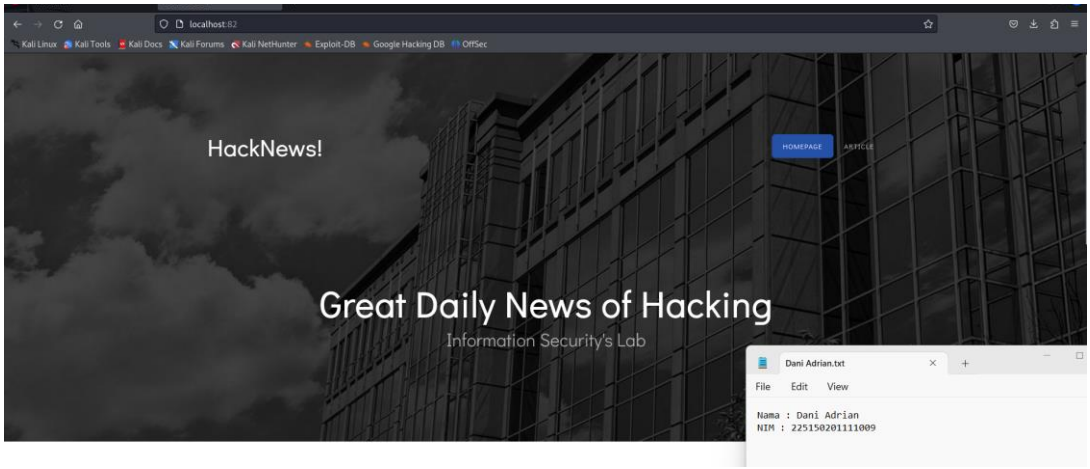
      `sudo docker ps`

   m. Apabila berhasil maka service akan berjalan pada port 82, sehingga dapat mengakses pada browser dengan alamat localhost:82



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Dengan mengakses alamat tersebut di browser, kita dapat melihat layanan yang berjalan dengan baik pada port 82.

SQL Injection Basic

1. Langkah 1
    a. Masuk pada bagian lab pertama (localhost:81).
    b. Lakukan percobaan serangan SQL Injection untuk mem-bypass halaman login milik admin dengan menggunakan query berikut:

```
' OR 1=1#
```

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Serangan SQL Injection: Pada kolom yang dimaksudkan untuk username atau email, masukkan query SQL Injection `' OR 1=1#`. Dengan memasukkan ini, kita mencoba untuk memanipulasi kueri SQL yang dijalankan oleh halaman login.

2. Langkah 2
    c. Apabila Anda berhasil, Jelaskan bagaimana query yang Anda gunakan dapat mem-bypass laman tersebut, tanpa perlu mengetahui username dan password milik admin.

Pada langkah tersebut, query yang digunakan adalah `' OR 1=1#`.

`'`: Ini adalah tanda kutip satu (single quote) yang menandakan awal dari string pada query SQL.

`OR`: Ini adalah operator logika yang digunakan untuk menggabungkan kondisi-kondisi dalam sebuah pernyataan SQL. Dalam kasus ini, digunakan untuk menyisipkan kondisi tambahan ke dalam pernyataan WHERE yang ada.

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

`1=1` : Ini adalah kondisi logika yang selalu bernilai benar (true) dalam SQL. Dengan demikian, menggunakannya akan memastikan bahwa kondisi ini selalu terpenuhi, yang berarti baris data yang diperiksa akan selalu dipilih.

`#` : Ini adalah tanda pagar (hash) yang digunakan untuk menandakan komentar dalam SQL. Dengan meletakkan tanda pagar setelah query, kita dapat "menutup" query yang ada sehingga bagian lain dari query yang mungkin ada setelahnya akan diabaikan.

Dengan menggabungkan semua elemen ini, query `' OR 1=1#` digunakan untuk menyisipkan kondisi tambahan `(OR 1=1)` ke dalam pernyataan SQL yang sedang dieksekusi, yang menyebabkan pernyataan tersebut selalu bernilai benar. Akibatnya, halaman login akan melewatkan verifikasi username dan password karena kueri yang dieksekusi secara efektif menjadi "temukan pengguna mana pun yang memiliki nama pengguna apa pun dan kata sandi apa pun" karena `1=1` selalu benar. Sehingga, halaman akan membiarkan akses tanpa memerlukan kredensial yang valid.

SQL Union Injection Basic

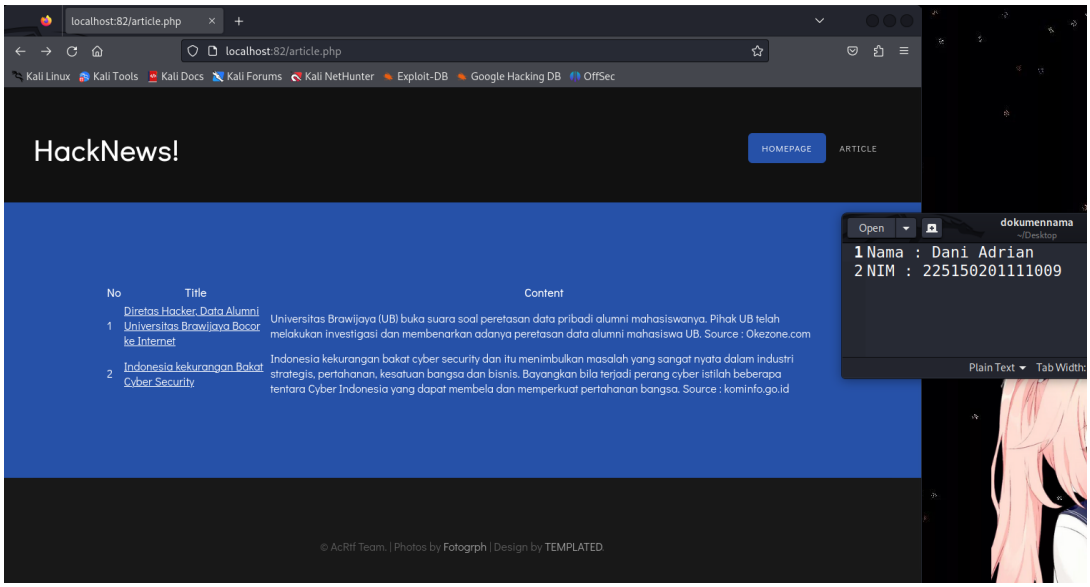
Berikut ini langkah-langkah yang perlu dilakukan dalam menyelesaikan lab praktikum:

1. Langkah 1
    a. Masuk pada bagian lab kedua (localhost:82).
    b. Setelah berhasil masuk ke dalam web, pelajarilah bagaimana web tersebut bekerja, dan temukan letak celah dari website tersebut. (Celah atau titik injeksi berada di parameter url article)
    c. Apabila Anda berhasil menemukan letak celah atau titik injeksi dari website tersebut, berikanlah tanda ' (single-quote) pada parameter tersebut. Jelaskan bagaimana dapat menyebabkan website tersebut menampilkan error.

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

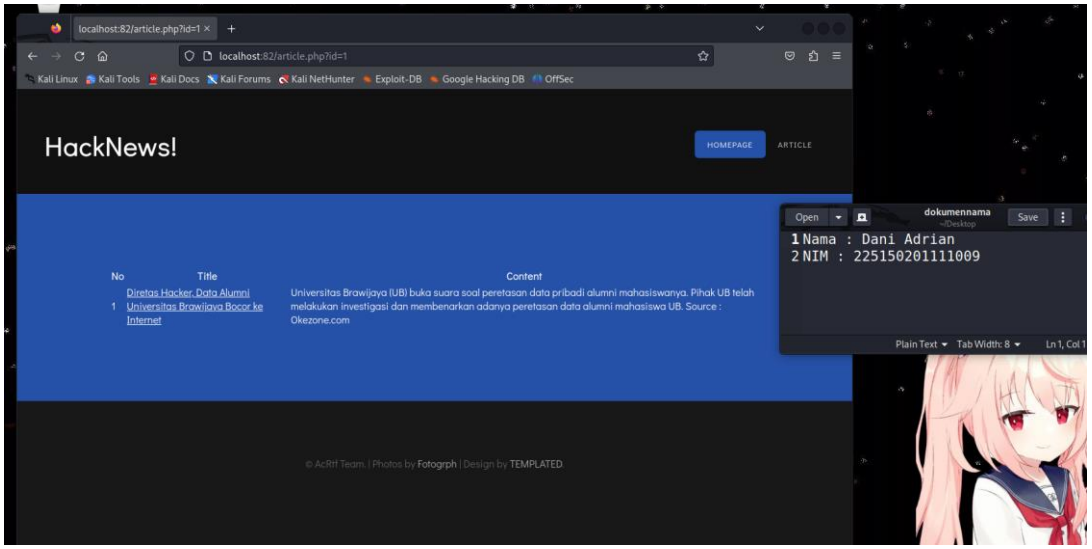
Perhatikan parameter URL, khususnya **artikel**.



Pilih salah satu Artikel

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

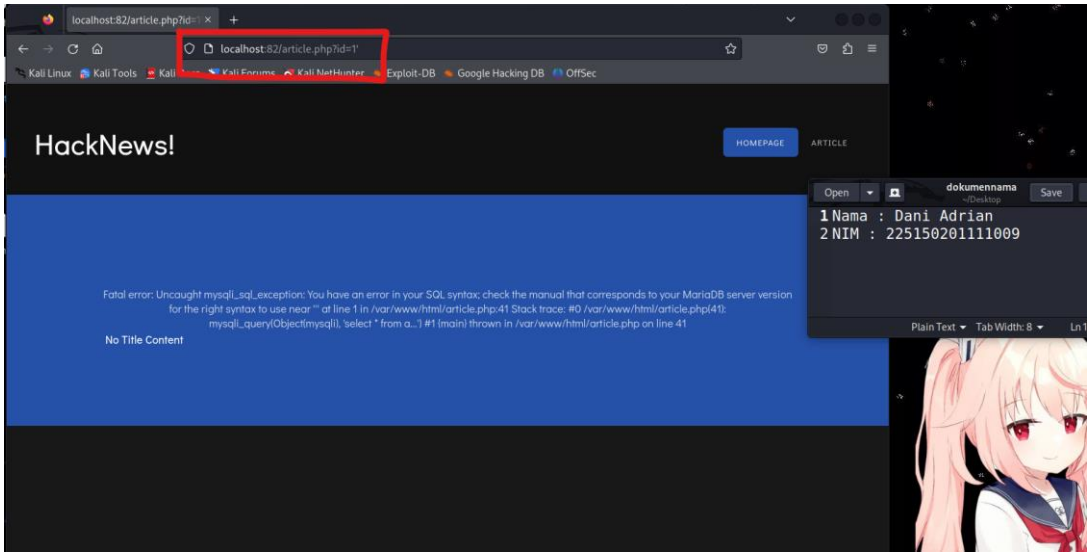


Tambahkan Tanda Single-Quote: Pada parameter `http://localhost:82/article.php?id=1`, tambahkan tanda single-quote (') sebagai input. Ini akan mengakibatkan sebuah kueri SQL yang salah saat dijalankan oleh server.

Sesudah ditambahkan single-quote :

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Website menampilkan pesan error atau perilaku yang tidak semestinya, ini menunjukkan bahwa ada celah SQL Injection yang dapat dieksploitasi.

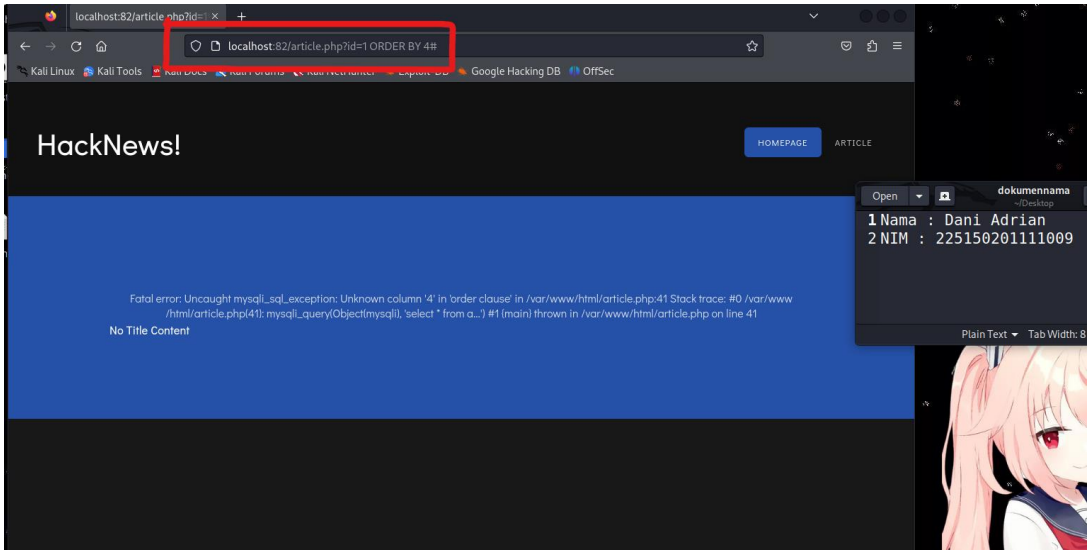
2. Langkah 2
    d. Lakukan serangan berikutnya untuk mengetahui berapa jumlah kolom yang dimiliki database pada website tersebut dengan menggunakan query:

```
1 ORDER BY 4#
```

    e. Lalu coba kurangi nilai ORDER BY menjadi 3, lalu apa yang terjadi pada laman web tersebut?

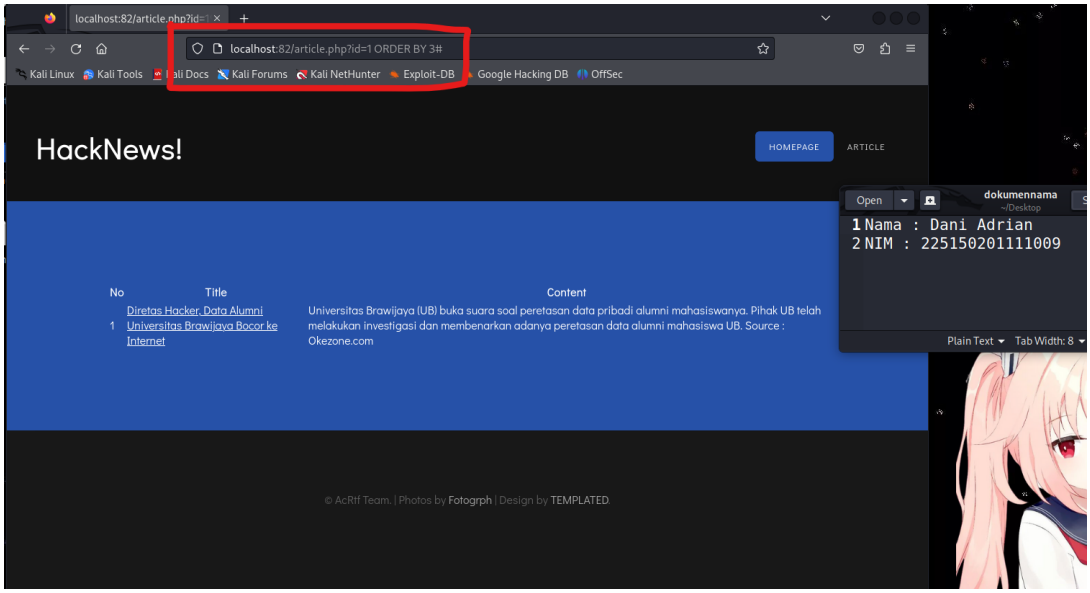
LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Jumlah kolom pada tabel database kurang dari 4, sistem database menghasilkan kesalahan karena mencoba mengurutkan hasil berdasarkan kolom yang tidak ada. Respons dari halaman web berupa pesan error.

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

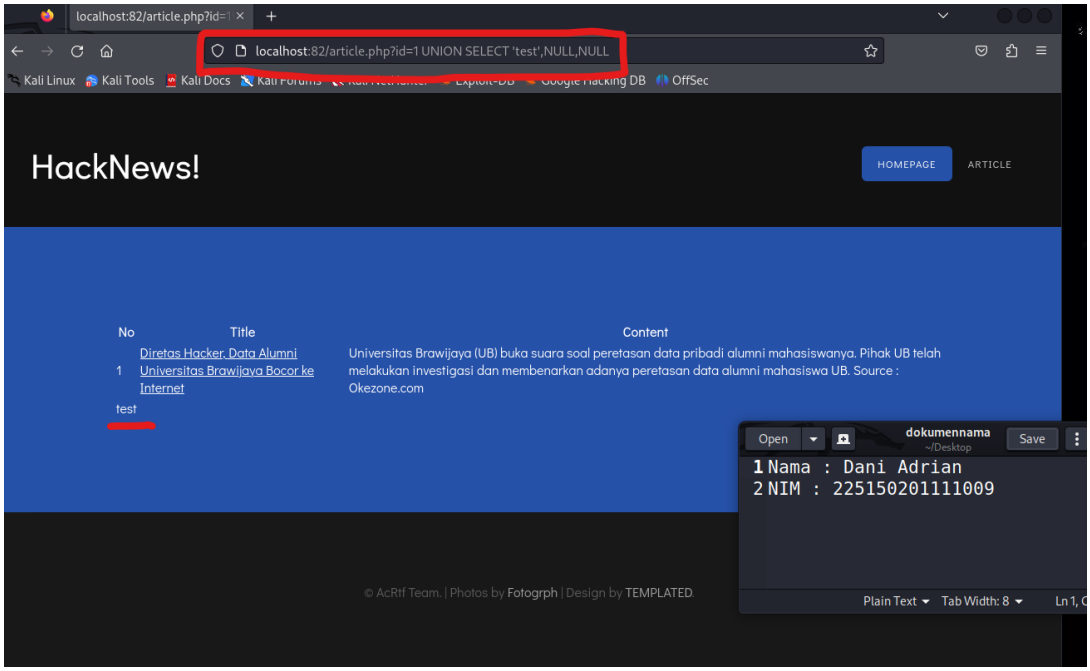


Melalui serangan SQL Injection yang kedua, dengan mengurangi nilai `ORDER BY` menjadi 3, kita mencoba mengkonfirmasi apakah jumlah kolom yang dimiliki oleh tabel database kurang dari 3. Hasilnya tidak akan terjadi kesalahan, dan halaman web kemungkinan akan berperilaku seperti biasa menunjukkan jumlah kolom yang dimiliki oleh tabel database lebih dari atau sama dengan 3.

3. Langkah 3
    f. Selanjutnya kita bisa mencari column yang dapat kita injeksi. dengan menggunakan query statement berikut:

```
1 UNION SELECT 'test',NULL,NULL
```

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Query diatas mencoba untuk menyisipkan data string `'test'` ke dalam hasil kueri bersama dengan dua nilai `NULL`. Kita mencoba untuk menemukan kolom yang dapat diinjeksi dengan menambahkan hasil `UNION SELECT` ke dalam kueri asli.

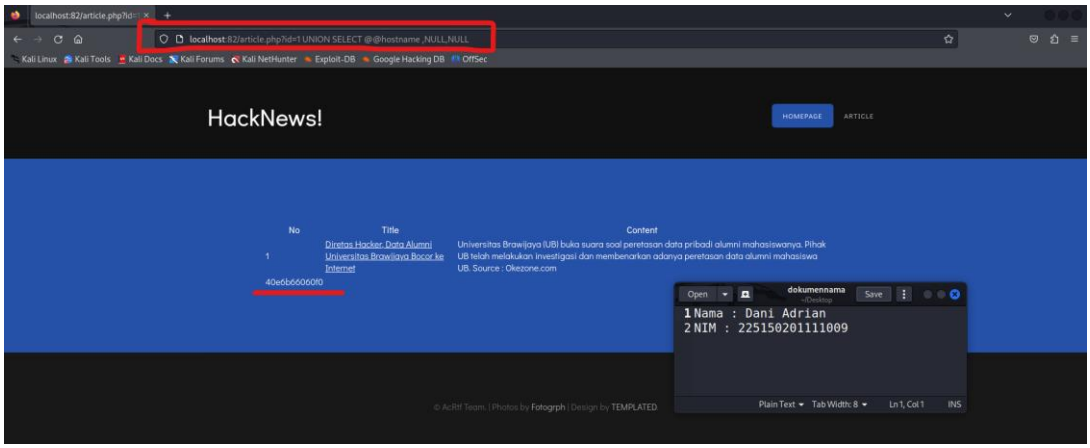
Query berhasil dieksekusi, kita melihat nilai `'test'` ditampilkan di dalam salah satu bagian dari halaman web, menandakan bahwa kolom tersebut dapat diinjeksi.

4. Langkah 4
    g. Kita bisa menampilkan informasi terkait database, dengan mengganti 'test' menjadi @@hostname untuk menampilkan nama host dari DB, database() untuk nama database, @@version untuk menampilkan versi dari DB.

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

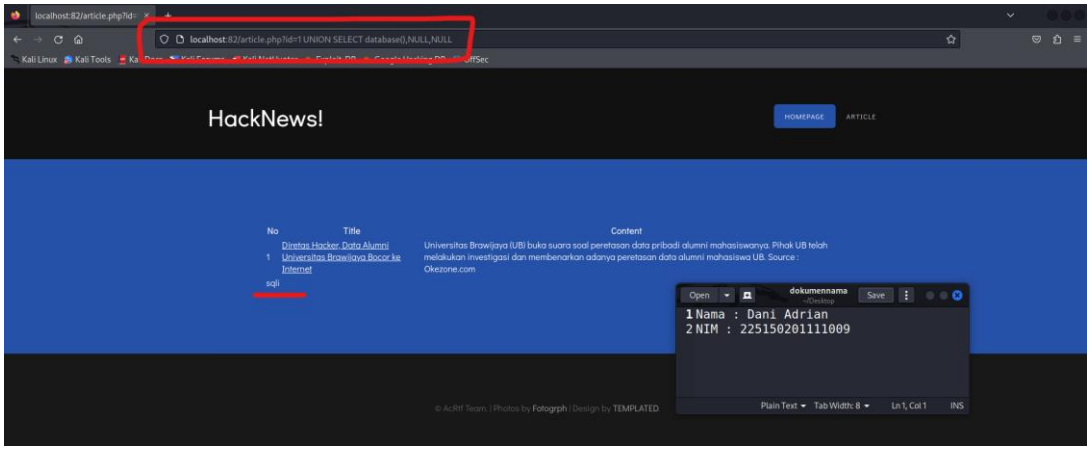
BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Hostname :



Query diatas untuk menampilkan nama host dari database

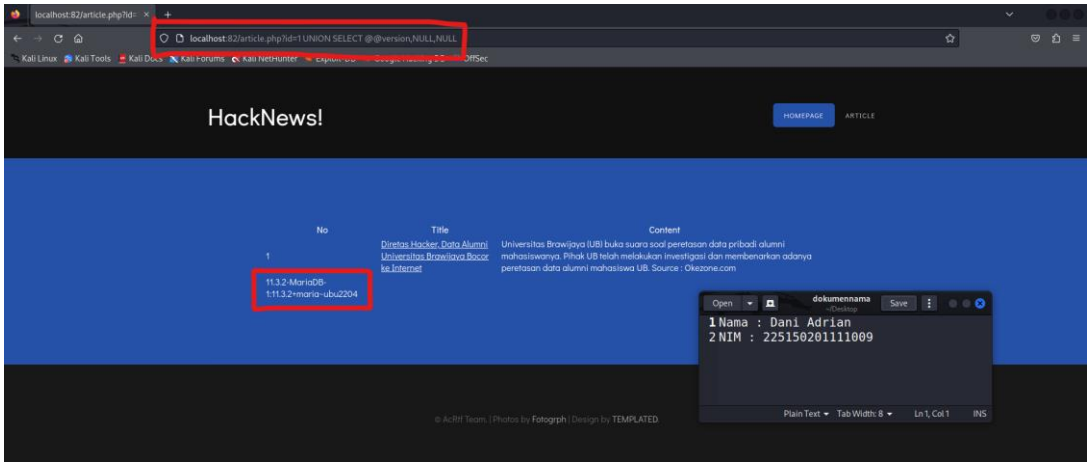
Database :



Query diatas untuk menampilkan nama database

Versi :

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Query diatas untuk menampilkan versi dari database

Hostname : `1 UNION SELECT @@hostname,NULL,NULL`

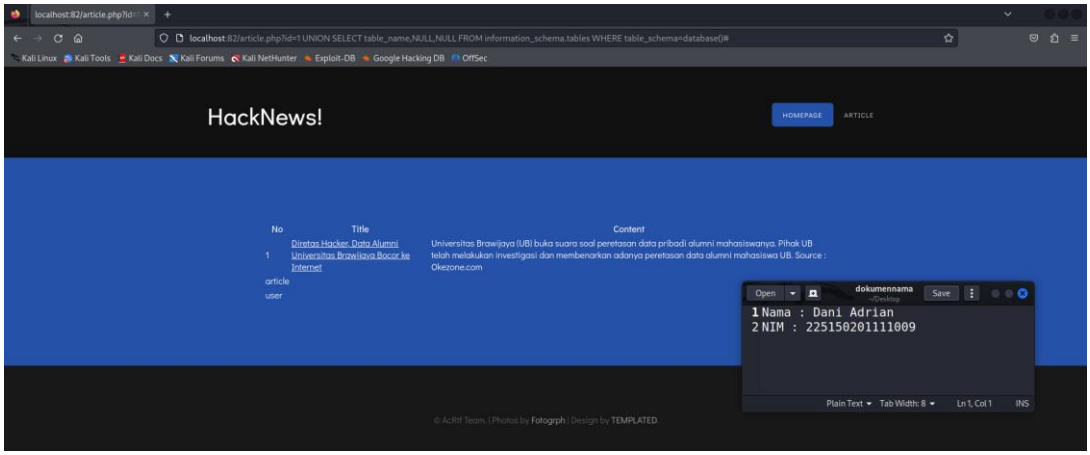
Database : `1 UNION SELECT database(),NULL,NULL`

Versi : `1 UNION SELECT @@version,NULL,NULL`

5. Langkah 5
    h. Berikutnya tampilkan table yang dimiliki database dengan menggunakan query berikut:

```
1 UNION SELECT table_name,NULL,NULL FROM
    information_schema.tables WHERE
        table_schema=database()#
```

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



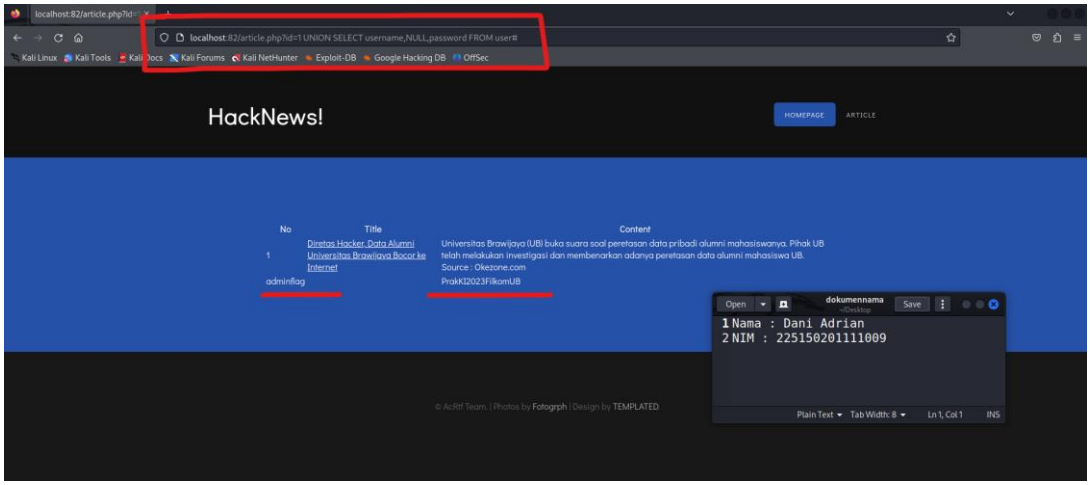
Dalam query, kita menggunakan `UNION SELECT` untuk menyisipkan query ke dalam hasil yang ada. Kita memilih kolom `table_name` dari tabel `information_schema.tables` di mana `table_schema` sama dengan database yang sedang digunakan.

Kemudian kita memilih `user`.

6. Langkah 6
    i. Setelah Anda mengetahui nama kolom dari sebuah table, tampilkan value dari kolom tersebut. Dengan menggunakan query berikut, dan ganti kolom1 dan kolom2 sesuai dengan column yang telah Anda temukan:
    `1 UNION SELECT kolom1,NULL,kolom2 FROM nama_table#`

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas




```
1 UNION SELECT username,NULL,password FROM user#
```

Query diatas bertujuan untuk mengganti `kolom1` dan `kolom2` dengan `username` dan `password`, dan ganti `nama_table` dengan `user`.

Kemudian kita akan mendapatkan username dan password nya, yaitu :

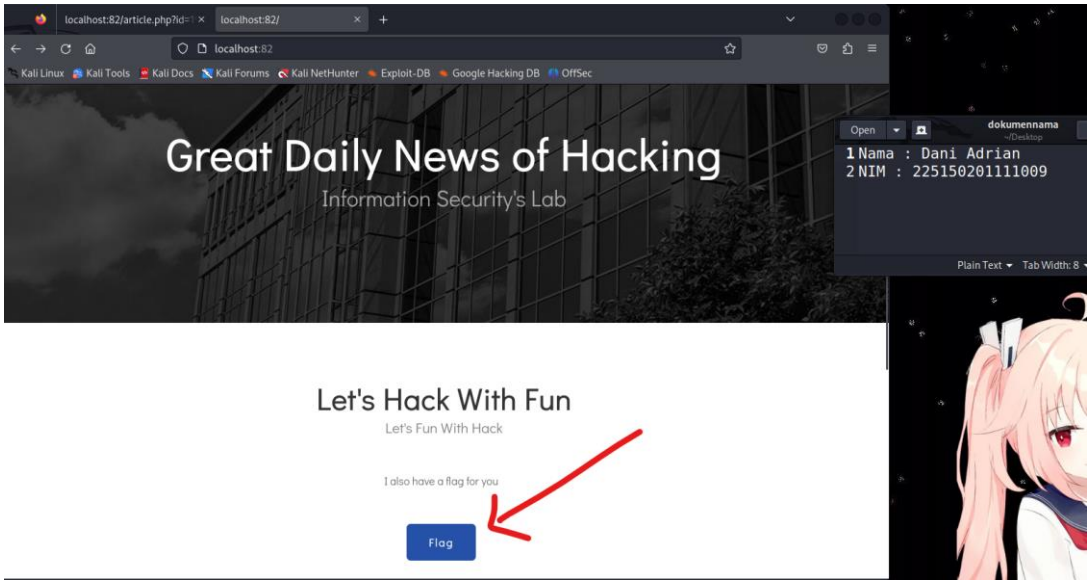
Username : adminflag

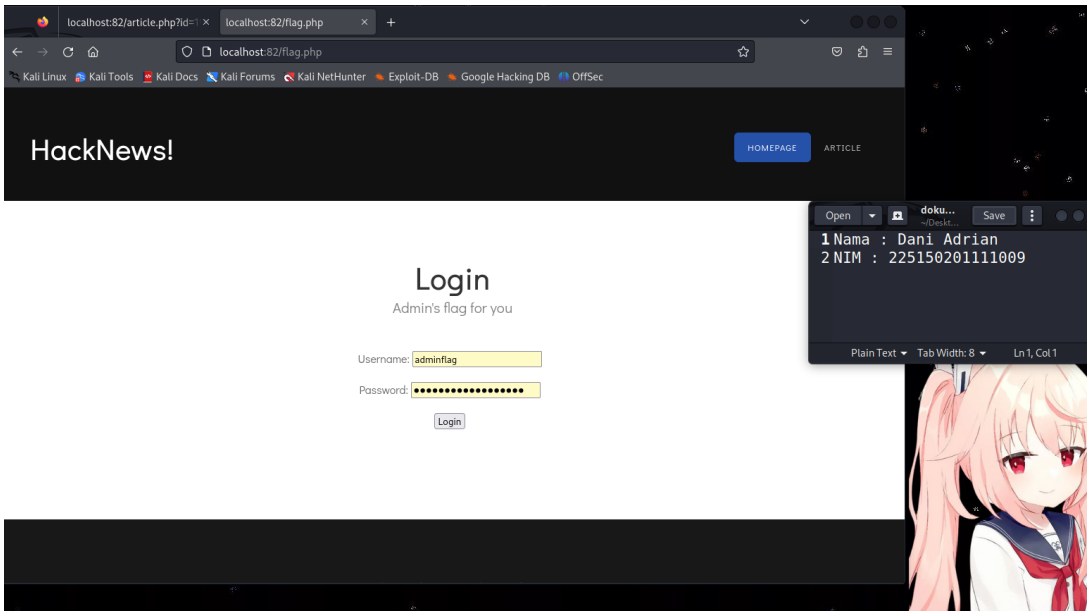
Password : PrakKI2023FilkomUB

7. Langkah 7
    j. Setelah Anda berhasil menemukan kredensial dari admin lakukan login pada laman flag, untuk mendapatkan flagnya.

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

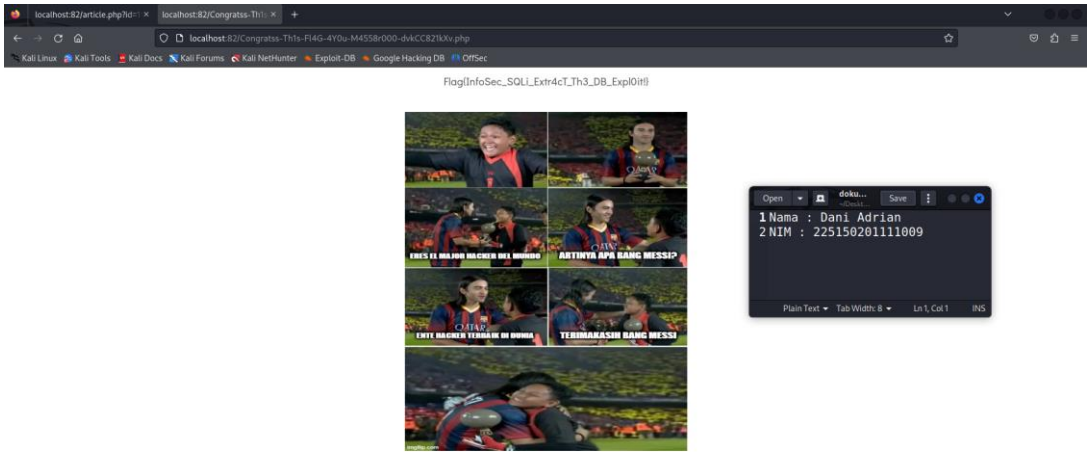




Akses halaman login untuk laman flag.

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

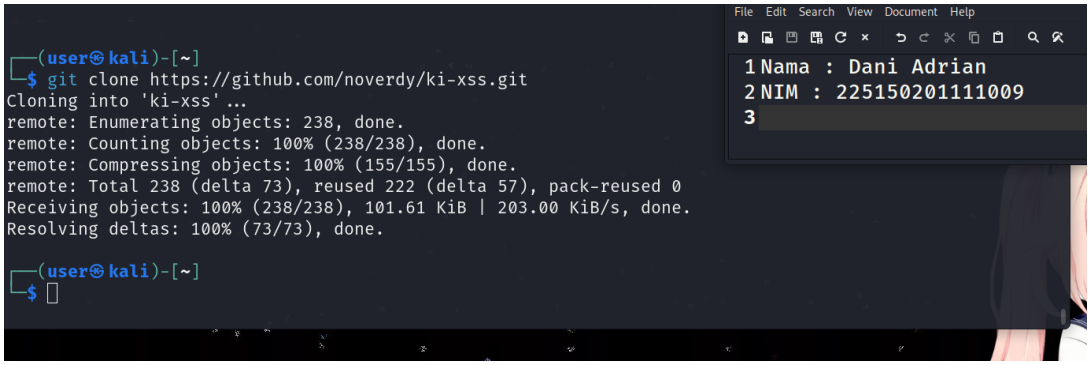
Gunakan kredensial admin (username & password) yang telah ditemukan untuk login ke laman flag Masukkan username dan password pada formulir login, dan tekan tombol login. Dapatkan Flag
Flag : 

Stored XSS (Cross-site Scripting)

1. Langkah 1
    a. Buka terminal pada sistem operasi Linux.
    b. Kemudian lakukan cloning github repository untuk lab praktikum XSS:
    `git clone https://github.com/noverdy/ki-xss.git`

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



c. Masuk ke dalam direktori ki-xss dengan perintah:

```
cd ki-xss
```

d. Melakukan build docker untuk sqli-part1 dengan perintah:

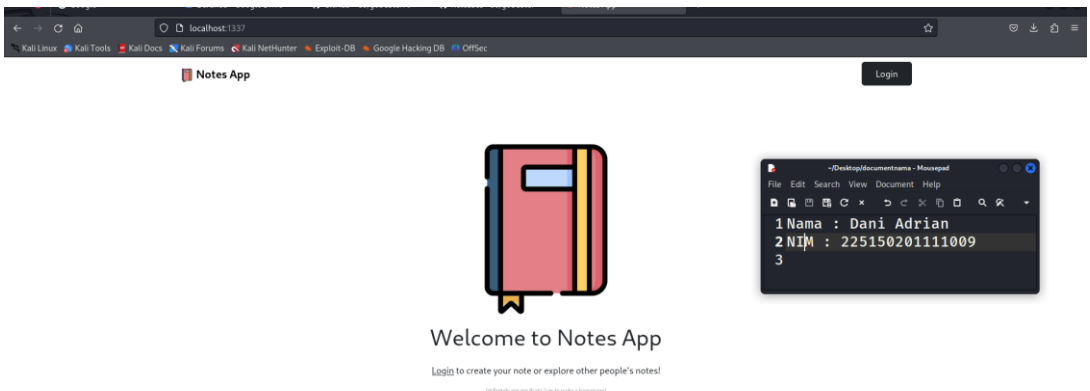
```
sudo docker-compose up -d
```

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

e. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:

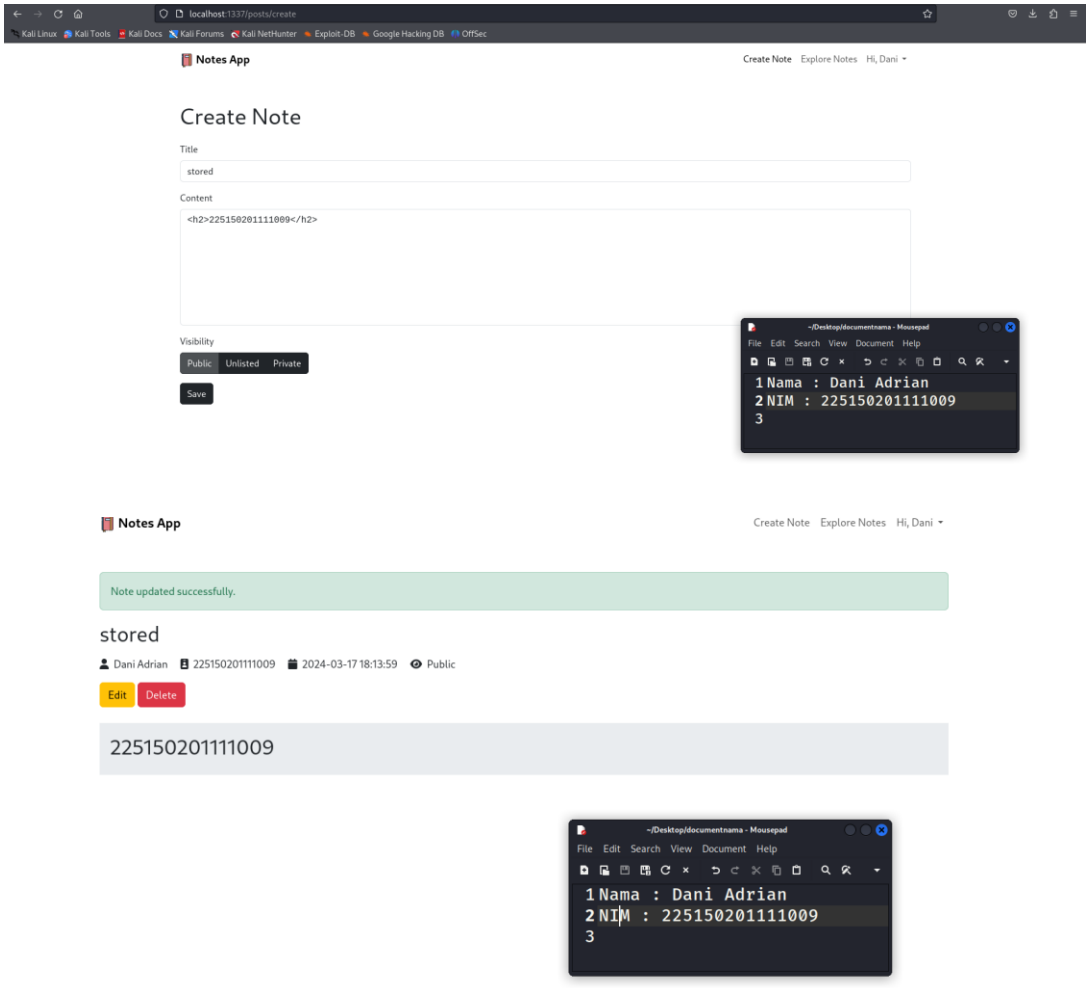
```
sudo docker ps
```

f. Apabila berhasil maka service akan berjalan pada port 1337, sehingga dapat mengakses pada browser dengan alamat localhost:1337



BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

2. Langkah 2
    a. Pertama lakukan pengujian HTML Injection pada bagian form Create Notes, berikan teks dengan ukuran h2 bertuliskan NIM Anda.



Dengan menyisipkan tag HTML seperti `<h2>NIM Anda</h2>` pada form Create Notes, kita dapat menguji apakah aplikasi membiarkan tag HTML tersebut dieksekusi dan ditampilkan sebagai HTML yang sebenarnya di halaman web.

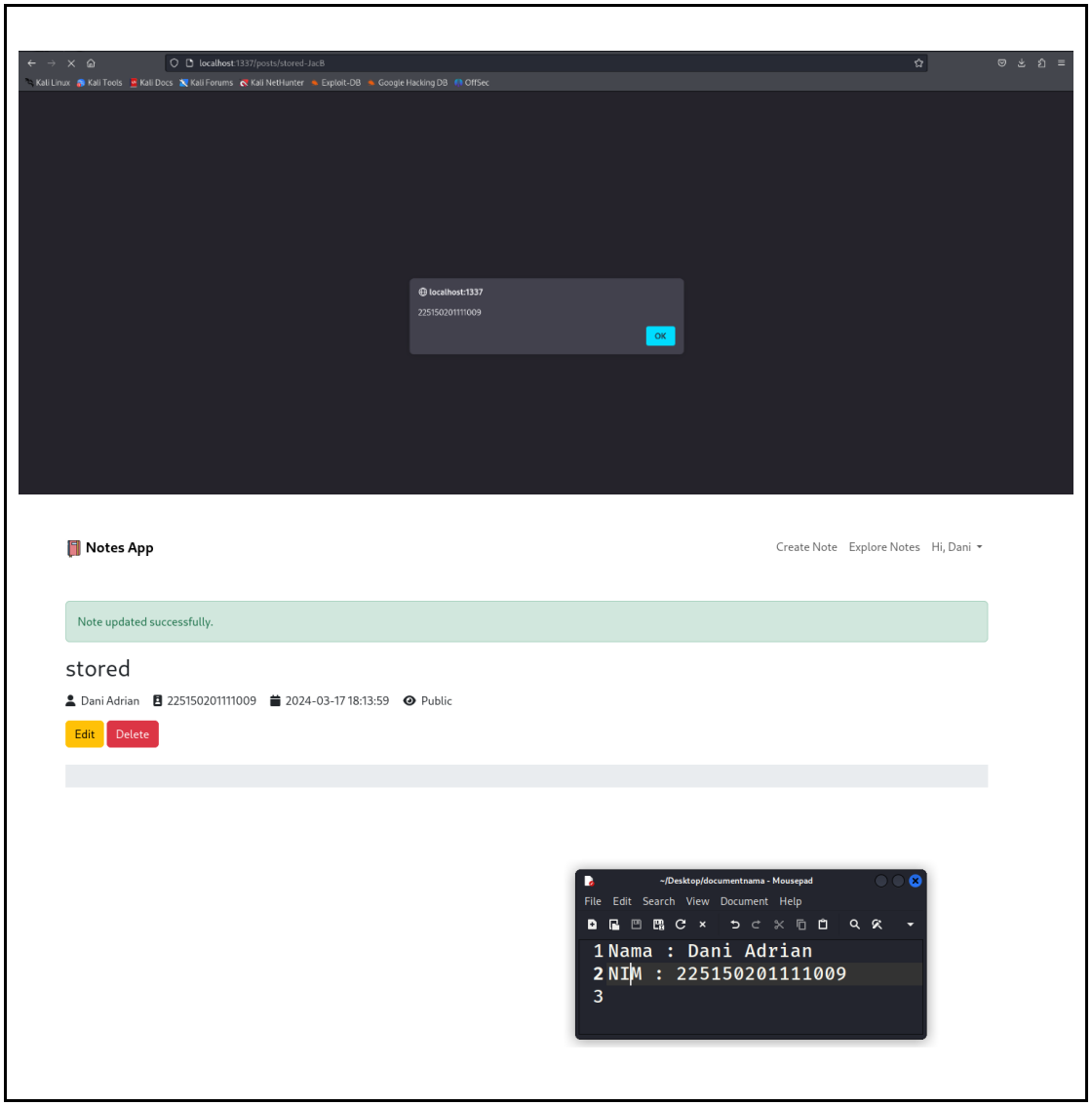
LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

b. Berikutnya, Masukkan komentar dengan potongan kode berikut:

```
<script>alert("NIM ANDA")</script>
```

Mengapa hal tersebut dapat terjadi?



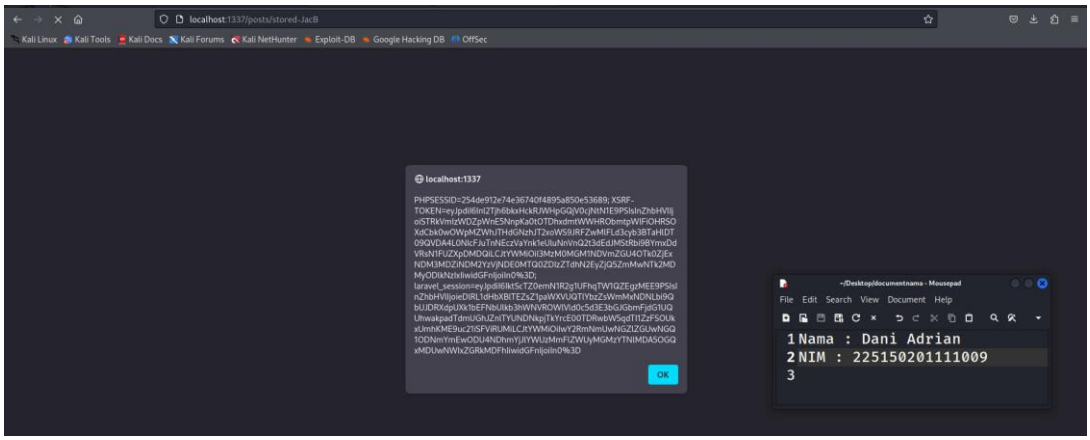
LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Tujuan dari langkah ini adalah untuk melihat apakah aplikasi rentan terhadap serangan Cross-Site Scripting (XSS), di mana kode JavaScript yang tidak aman dieksekusi oleh browser pengguna.

c. Berikutnya, kita akan menampilkan session cookie milik kita dengan kode berikut:

```
<script>alert(document.cookie)</script>
```



Browser secara otomatis mengirimkan session cookie ketika memuat halaman web yang diminta. Kode JavaScript yang dieksekusi di dalam halaman web memiliki akses ke session cookie tersebut karena cookie merupakan bagian dari informasi yang tersedia dalam lingkungan klien (browser). Dengan menggunakan document.cookie, kode JavaScript dapat mengakses dan menampilkan session cookie yang terkait dengan situs web yang sedang diakses.

Kesimpulan

LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KERENTANAN DAN ANCAMAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 14/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Praktikum ini menegaskan pentingnya memahami dan menguji kerentanan keamanan dalam aplikasi web. Dengan memahami cara kerja serangan seperti SQL Injection, kita dapat mengidentifikasi, mencegah, dan memperbaiki celah keamanan yang mungkin ada. Penggunaan alat-alat seperti Docker dan teknik-teknik khusus seperti SQL Injection membantu dalam menguji dan mengevaluasi keamanan aplikasi web. Melalui praktikum ini, kita diajarkan untuk memikirkan keamanan sejak awal dalam pengembangan perangkat lunak. Dengan mengidentifikasi dan memperbaiki celah keamanan sejak dini, kita dapat mencegah serangan potensial dan melindungi data sensitif dari akses yang tidak sah. Praktikum ini juga menjadi indikator untuk mengukur pemahaman peserta tentang konsep keamanan informasi secara umum. Kemampuan mereka dalam mengidentifikasi dan memperbaiki celah keamanan akan mencerminkan tingkat pemahaman mereka tentang konsep tersebut. Dengan demikian, praktikum ini memberikan wawasan yang berharga tentang celah keamanan yang mungkin ada dalam aplikasi web dan pentingnya mengimplementasikan langkah-langkah perlindungan yang tepat untuk melindungi data dan privasi pengguna.

Evaluasi

Kesuksesan praktikum kali ini bergantung pada kesiapan dan keterampilan peserta dalam mengikuti instruksi dan menerapkan teknik-teknik yang diajarkan ketika praktikum dengan benar. Selain itu, penggunaan teknologi seperti Docker dan metode-metode khusus seperti SQL Injection juga perlu dievaluasi. Kemampuan peserta dalam menggunakan alat dan teknik ini dengan benar akan menghasilkan keberhasilan praktikum yang baik dan tepat. Evaluasi juga mencakup pemahaman peserta tentang konsep keamanan informasi secara umum. Kemampuan mereka dalam mengidentifikasi dan memperbaiki celah keamanan akan mencerminkan tingkat pemahaman mereka tentang konsep tersebut.