

WRITEUP PROOF OF CONCEPT



Leaking Sensitive Merchant Project Data via IDOR in DUITKU.com

Bug: IDOR (Insecure Direct Object Reference)

Url: <https://sandbox.duitku.com/merchant/Project/Edit?code={CODEPROJECT}>

Reporter/Credit To: Aldhy Prakoso (Sulawesi I.T Security)

Severity Level: High Risk Bug

DESCRIPTION BUG

IDOR adalah Celah yang bisa dimanfaatkan penyerang untuk dapat mengakses, mengedit, atau menghapus objek/value user lain

dengan mengubah nilai variabel seperti "id", "pid", "uid" dan lain-lain. dalam kasus ini saya menemukan bug Idor di web **SANDBOX DUITKU** yang bisa **MENGAkses** Data Informasi PROJECT semua user berdasarkan **CODE PROJECT** yang di temukan di web **SANDBOX DUITKU**, Dan yang lebih parah lagi saya dapat meng-take over project user lain/alias mengambil alih project tersebut, Dan setelah saya analisis ternyata website/api key data project itu dipakai untuk payment gateway di duitku.com. Tentu ini sangat berbahaya, dimana bisa **mengakses/mengubah data informasi akun user** di duitku dan impact nya bisa melakukan take over project user lain. **Tentu ini juga bertentangan** dengan kebijakan keamanan dari duitku yang berkomitmen bahwa informasi data user/client aman.

****METHOD****

Setelah login ke web sandbox di <https://sandbox.duitku.com/>, saya melakukan **Intercepting Request/Response** di semua menu/fitur web merchant duitku untuk mendapatkan request-request yang ada di web, saya memulai dari menu **My Project** dan di fitur **Add Project** dimana disitu kita dapat menambah project untuk payment gateway merchant kita.

Sandbox

Balance: Rp 0.000testerx

My Projects

Add Project

FILTER DATA

MERCHANT CODEContoh : D9999PROJECT NAMEContoh : Toko Ba

DAFTAR PROJECT

Merchant Code	Project Name	Project Website	Project Callback Url	Project API Key	
D4449	a	www.aaa.com	www.aaa.com/callback	39d88fe5e36c89aee90d81c1d39fe51e	<div><div></div><div></div><div></div></div>

Desc: Disitu saya sudah add project saya dengan merchant code: D4449.

Kemudian saya mencoba untuk mengedit project tersebut dan mendapatkan tampilan sebagai berikut:

 Sandbox ▾

Edit Project

PROJECT DETAIL

Nama Project

WebSite Project

Callback Url Project

Logo Website (Size 150x40)

Logo Website (Size 150x40)

No file chosen

Gambar Background (Size
1920x1080)

Gambar Background (Size 1920x1080)

No file chosen

Desc:

Linkweb: <https://sandbox.duitku.com/merchant/Project/Edit?code=D4449>

Dari hasil analisa saya bahwa form buat edit tersebut mengirim post data ke url diatas, jadi kalau mengubah project tersebut harus sesuai dengan code merchant nya. Code merchant saya: D4449

Kemudian saya mencoba mengganti code tersebut sebagai berikut:


<https://sandbox.duitku.com/merchant/Project/Edit?code=D4448>

Sandbox ▾

Edit Project

PROJECT DETAIL

Nama Project	<input type="text" value="IDBRIX"/>
WebSite Project	<input type="text" value="https://www.idbrix.com"/>
Callback Url Project	<input type="text" value="https://www.idbrix.com/thank-you"/>
Logo Website (Size 150x40)	<div>Logo Website (Size 150x40) <input type="button" value="Choose File"/> No file chosen</div>



Desc: Saya mencoba mengubah code merchant saya dari D4449 menjadi D4448 dan didapatkan hasil seperti di foto tersebut, dapat dilihat saya mendapatkan data informasi dari project tersebut, dengan nama project: IDBRIX yang tentunya ini bukan project saya. Disini juga saya dapat mengedit data tersebut. Namun disini saya hanya mendapatkan nama, website, callback url, logo website project. saya tidak mendapatkan Project API Key nya yang dimana itu sangat penting di project. Saya mencari cara untuk mendapatkan api key tersebut, mencoba mengedit data form nya tetap saja tidak

mendapatkan api key nya dan juga mencoba mengedit dan menambah parameter apikey untuk mencoba mengubah api key namun tetap saja gagal.

Kemudian saya mencoba membuat akun kedua saya untuk mencoba mendapatkan api key project nya hanya dengan menggunakan code merchant tersebut (KARENA TIDAK DIBOLEHKAN MENGEDIT DATA USER LAIN JADI SAYA MENCOBA MEMBUAT AKUN LAGI UNTUK PERCOBAAN). Berikut akun & project di akun kedua saya;

DAFTAR PROJECT				
Merchant Code	Project Name	Project Website	Project Callback Url	Project API Key
D4452	project akunkedua	www.projectkedua.com	www.projectkedua.com/callback/	d724321e3e07bf419fddc5fb04d4931d


Showing 20 to 1 of 1 record(s)

Desc: ini adalah akun kedua saya dan project akun kedua saya dengan merchant code: D4452.

Dan api key project akun kedua

saya: d724321e3e07bf419fddc5fb04d4931d

Kemudian saya mencoba mengakses code merchant akun kedua saya di akun pertama saya.

 Sandbox ▾

Edit Project

PROJECT DETAIL

Nama Project	<input type="text" value="project akunkedua"/>
WebSite Project	<input type="text" value="www.projectkedua.com"/>
Callback Url Project	<input type="text" value="www.projectkeduaXXX.com/callback/"/>
Logo Website (Size 150x40)	Logo Website (Size 150x40) <input type="button" value="Choose File"/> No file chosen
Gambar Background (Size 1920x1080)	Gambar Background (Size 1920x1080) <input type="button" value="Choose File"/> No file chosen

Desc: Saya mencoba mengedit data informasi project akun kedua saya di akun pertama saya hanya menggunakan merchant code tersebut.

Disitu saya hanya mengganti callback url project.

Setelah klik save saya mendapatkan tampilan sebagai berikut:

Project project akunkedua berhasil diperbarui.

FILTER DATA







MERCHANT CODE

Contoh : D9999

PROJECT NAME

Contoh : Toko Ba

DAFTAR PROJECT

Merchant Code	Project Name	Project Website	Project Callback Url	Project API Key			
D4449	aXXX	www.aaa.com	www.aaa.com/callback	39d88fe5e36c89aee90d81c1d39fe51e			
D4452	project akunkedua	www.projectkedua.com	www.projectkeduaXXX.com/callback/	d724321e3e07bf419fddc5fb04d4931d			

Desc: Saya berhasil mendapatkan project & api key akun kedua saya tersebut hanya menggunakan code merchant nya. Dan yang lebih penting lagi saya mendapatkan Project API KEY nya yang sama dengan api key sebelumnya (TIDAK TERGANTI) ini berarti project tersebut sudah menjadi milik saya.

Kenapa saya mencoba mengganti data project tersebut di parameter 'url callback' ? karena sebelumnya saya sudah mencoba mengedit semua data-data di parameter2 tersebut dan tidak mendapatkan apa-apa, setelah itu saya mencoba mengedit url callback nya dengan cara mengedit url nya dan mendapatkan api key/project tersebut.

Ini menandakan bahwa form tersebut tidak diberi otentikasi untuk mengakses code merchant lain, ini juga sangat parah dimana saya dapat mengedit data tersebut tanpa otentikasi juga.

Hasil analisa saya bahwa code merchant tersebut terbentuk terurut, jadi akun pertama saya membuat project dengan code merchant: 8, kemudian saya membuat project di akun kedua maka code merchant saya adalah: 9.

Saya menyarankan untuk membuat code merchant yang acak/random untuk mencegah ini, dan juga membuat otentikasi jika mengakses/mengubah code merchant tersebut.

Impact dari bug ini adalah pengguna yang diautentikasi akun lain dapat melakukan grabbing dan leak informasi data yang sensitif dan juga mengubah data- data sensitif dari pengguna lain.

Tentu ini juga bertentangan dengan kebijakan keamanan dari duitku yang berkomitmen bahwa informasi data user/client aman.

TIMELINE REPORT

17/12/2018 – Sending Initial Report

17/12/2018 – Sending Detail Report

18/12/2018 – Verifying and confirm the Report as valid

18/12/2018 – Duitku fixed the bug and retest

18/12/2018 – Duitku asking my data, and assign this issue as High Risk

18/12/2018 – Sending data to Duitku

19/12/2018 – Duitku sent reward

Stay Awesome,
Aldhy Prakoso
Sulawesi I.T Security