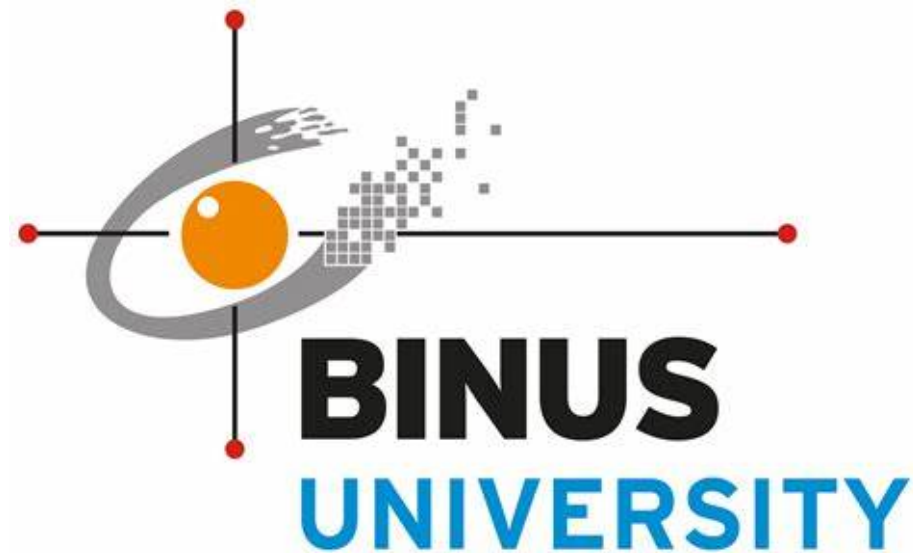


ASSURANCE OF LEARNING (AOL)

SOFTWARE SECURITY



Simulation of Broken Access Control (BAC) Attack on "Plus One" Website

Group 7:

- Dinanti Nabilah Ardelia (2702313615)
 - Jovan Rivaldo (2702303500)
- Michelle Aurelia Anggriawan (2702247645)
 - Rachelle Celina Salim (2702326800)

JUNE 2025

TABLE OF CONTENTS

TABLE OF CONTENTS..... 1

SIMULATION ROLES.....2

TARGET OBJECT..... 3

BACKGROUND WEBSITE “Plus One”..... 4

ATTACK SIMULATION.....5

STRIDE ATTACK ANALYSIS.....9

SECURITY (MITIGATION).....12

SOURCES..... 14

SIMULATION ROLES

Nama	Role	Jobdesk	Kontribusi
Dinanti Nabilah Ardelia	CEO	<ul style="list-style-type: none"> - Menyusun skenario dan dampak serangan. - Memberi arahan ke tim security. - Ambil keputusan setelah serangan. 	<ul style="list-style-type: none"> - Membuat background - Menyusun mitigation strategy
Rachelle Celina Salim	Attacker	<ul style="list-style-type: none"> - Mencari celah keamanan. - Melakukan simulasi serangan dan mendokumentasikan langkah teknis 	<ul style="list-style-type: none"> - Menyusun alur dari attack simulations dan STRIDE attack analysis
Michelle Aurelia Anggriawan	Security Manager	<ul style="list-style-type: none"> - Melakukan analisis attack dan mitigasi STRIDE - Menyusun mitigasi dan saran perbaikan sistem 	<ul style="list-style-type: none"> - Menyusun background - Menyusun mitigation strategy
Jovan Rivaldo	Security Team Member	<ul style="list-style-type: none"> - Melakukan analisis attack dan mitigasi STRIDE - Melaksanakn mitigasi dan saran perbaikan sistem 	<ul style="list-style-type: none"> - Menyusun mitigation strategy

TARGET OBJECT



Website Name:

Plus One

Release Date:

On Progress

Developer:

Software Engineering AOL Group 6 (LB07)

Description:

Website pendukung produktivitas tim dengan fitur catatan, todo list, dan group. Dilengkapi juga dengan *streak feature* yang bertambah setiap ada *productivity action* dilakukan user.

BACKGROUND WEBSITE “Plus One”

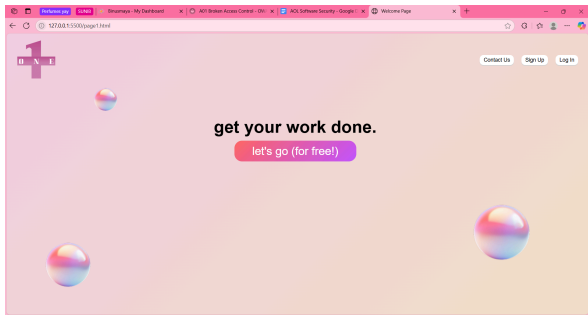
Website Plus One adalah sebuah website yang memiliki tujuan untuk meningkatkan produktivitas siswa/mahasiswa maupun para pekerja lainnya. Di dalam website Plus One ini, terdapat fitur untuk bergabung ke dalam group, membuat to-do list dan catatan. Untuk serangan pada website ini, kami menggunakan teknik Broken Access Control yang di mana kami masuk sebagai anggota dari group berdasarkan link yang dikirim host untuk meng-invite membernya. Ketika kami sudah berhasil masuk ke dalam group tersebut, kami bisa mengakses data di dalam group tersebut, selain itu kami pun bisa mengedit maupun mengetahui isi dari data dalam group tersebut.

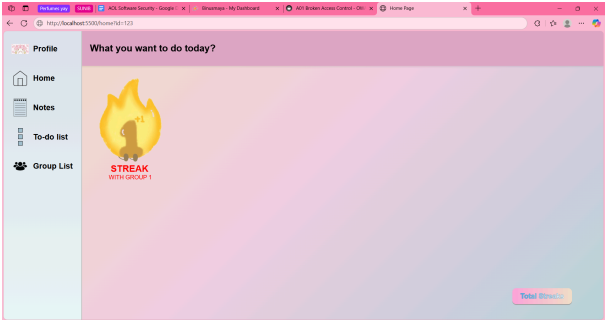
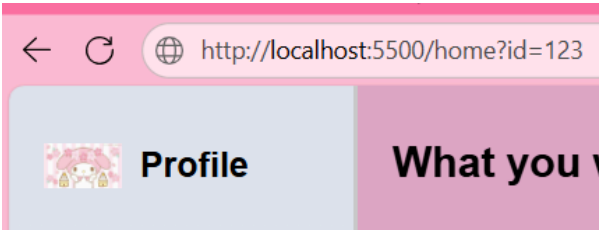
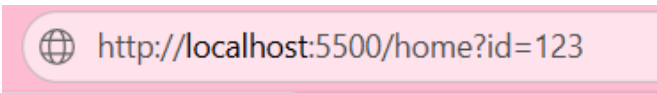
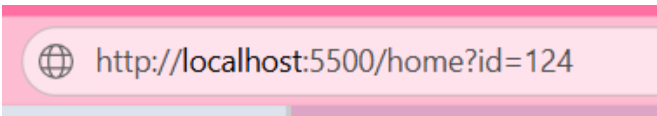
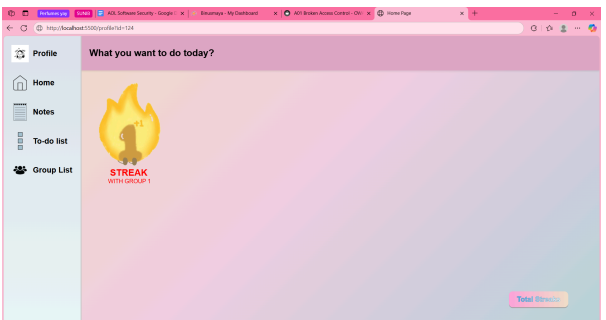
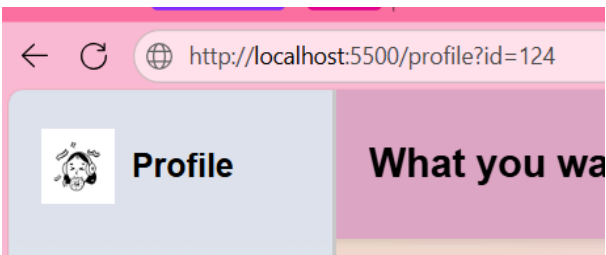
Serangan yang menggunakan Broken Access Control ini kami bisa menyerang dengan melewati celah dari Insecure Direct Object Reference (IDOR) yang di mana pada teknik ini kami memanfaatkan kelemahan pada access control. Maka dari itu kami dapat mengakses data yang terdapat di dalam group tersebut karena tidak adanya sistem yang melakukan pengecekan atau verifikasi terhadap hak akses yang di mana apakah memang user tersebut merupakan pengguna yang benar-benar bergabung dengan group tersebut atau bukan.

Selain itu, website ini juga merupakan website buatan tugas kami yang di mana tentunya masih terdapat banyak vulnerability.

ATTACK SIMULATION

(Note: Kami mensimulasikan attack ini menggunakan static local web kami sendiri dikarenakan belum terhubung dengan backend. Tapi bayangkan saja website ini sudah di launch secara sempurna.)

IDOR Exploitation Between User		
Description: Serangan ini merupakan jenis serangan Broken Access Control (BAC), tepatnya Insecure Direct Object Reference (IDOR). Dalam konteks ini kami mensimulasikan IDOR atas dasar ketidaktersediaan fitur validasi hak akses dalam website Plus One sehingga kami bisa memodifikasi parameter ID user pada URL. Jika sistem tidak memvalidasi kepemilikan data secara benar, maka pengguna bisa menelusuri ID lain secara manual maupun otomatis, sehingga membuka potensi pencurian data pribadi, manipulasi informasi, atau akses ke group sensitif. Selain itu, alasannya juga karena sistem hanya mengandalkan parameter client side tanpa pengamanan atau pembatasan dari sisi server.		
Risk: <ul style="list-style-type: none">- Privacy Breach- Broken System Integrity- Lost of User Trust		
Steps	Action	Screenshoots
1.	Open website page Plus One lalu click log in dan lakukan log in sebagai user biasa atau sign in jika belum memiliki account.	

		 
2.	Setelah log in, akan muncul URL sejenis berikut. Misalkan userID nya adalah 123	
3.	Coba mengganti ID nya dengan nomor lain yang mengindikasikan ID user lain. Misalkan 124. Lalu click enter.	
4.	Disini bisa terlihat bahwa kita sudah masuk ke account user lain hanya dengan mengganti ID pada URL.	 

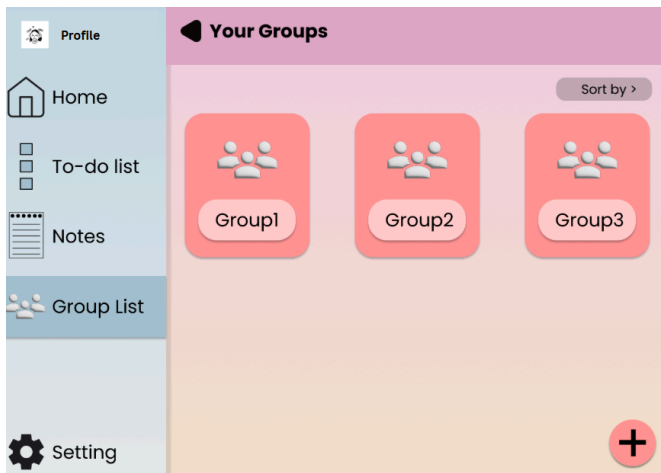
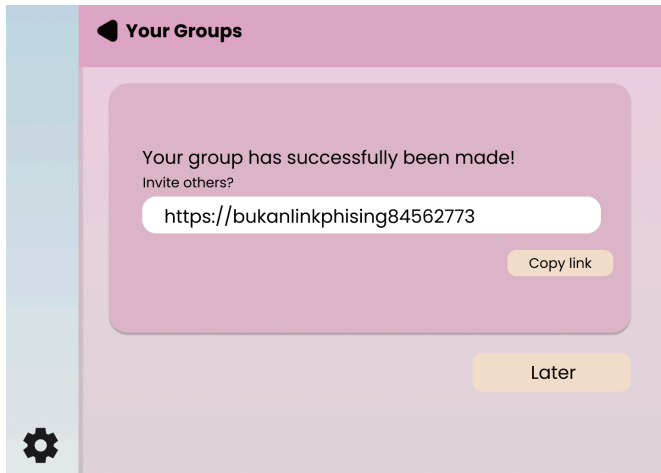
BAC Attack with Group Link Invitation

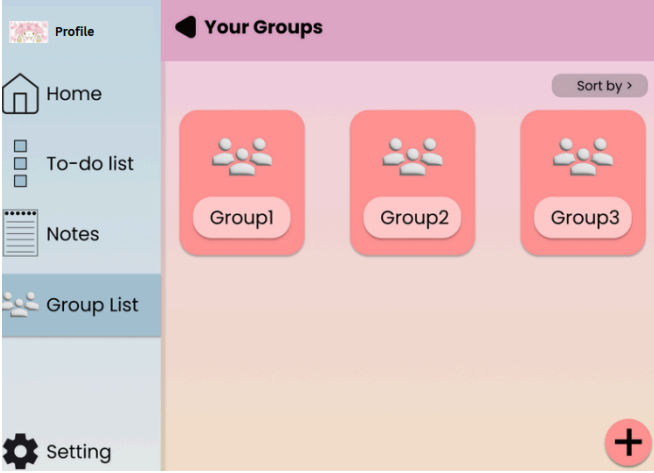
Description:

Serangan ini menggunakan teknik Broken Access Control (BAC), di mana attacker bisa masuk ke dalam sebuah group hanya dengan menggunakan link undangan yang dibagikan oleh host. Website Plus One tidak memiliki sistem pengecekan hak akses yang kuat, sehingga siapa pun yang memiliki link bisa langsung bergabung ke group.

Risk:

- Attacker bisa melihat seluruh isi grup
- Attacker mengetahui data pribadi anggota lain
- Attacker dapat mengubah atau menghapus isi dari group.

Steps	Action	Screenshots
1.	Setelah masuk sebagai user lain, kami dapat mengakses group list dari user tersebut.	
2.	Untuk menginvite user lain join dalam group yang sama, tersedia link yang dapat diakses oleh admin group tersebut.	

<p>3.</p>	<p>Copy link tersebut dan send ke user lain. User lain dapat masuk ke group melalui direct link tersebut tanpa validasi apa-apa dan dapat mengedit isi notes, to do list, dan lain-lain.</p>	 <p>The screenshot displays a mobile application interface. On the left is a sidebar menu with options: Profile (with a person icon), Home (with a house icon), To-do list (with a checklist icon), Notes (with a notepad icon), Group List (with a group of people icon), and Setting (with a gear icon). The main area on the right is titled 'Your Groups' and features a 'Sort by >' button. Below this, there are three red rounded rectangular buttons labeled 'Group1', 'Group2', and 'Group3', each with a group of people icon above the text. A red circular button with a white plus sign is located at the bottom right corner of the main area.</p>
-----------	--	---

STRIDE ATTACK ANALYSIS

STRIDE ATTACK ANALYSIS: IDOR Exploitation Between User			
STRIDE	Yes/ No	Description	Risk
Spoofing: Impersonating another user or entity.	Yes	Penyamaran sebagai user lain hanya dengan mengganti ID di URL, karena sistem tidak cek apakah ID itu benar-benar milik dia.	Penipuan atau penyalahgunaan account
Tampering: Altering data or system integrity.	Yes	Mengubah data user lain jika sistem tidak cek hak aksesnya, misalnya mengganti profile atau data penting.	Data user lain bisa diubah dan dapat bersifat merugikan.
Repudiation: Denying actions or transactions without accountability.	Yes	Tidak ada log atau catatan aktivitas, attacker bisa menyangkal bahwa dia pernah masuk ke akun user lain.	Kesulitan mencari tau pelakunya
Information Disclosure: Exposing sensitive data to unauthorized parties.	Yes	Attacker bisa melihat data pribadi pengguna lain hanya dengan mengganti angka ID di URL.	Kebocoran data pribadi user seperti email, password, notes.
Denial of Service: Disrupting system	No	IDOR tidak secara langsung membuat sistem down, kecuali dipakai secara otomatis dan berulang-ulang.	-

availability or performance.			
Elevation of Privilege: Gaining unauthorized access to higher system privileges.	Yes	Attacker mencoba masuk sebagai admin atau pengguna dengan akses tinggi hanya dengan ganti ID.	Punya akses kendali terhadap fitur - fitur yang terdapat dalam website Plus One.

STRIDE ATTACK ANALYSIS: BAC Attack with Group Link Invitation			
STRIDE	Yes/ No	Description	Risk
Spoofing: Impersonating another user or entity.	No	Attacker tidak menyamar sebagai user lain secara langsung, hanya memanfaatkan link grup.	-
Tampering: Altering data or system integrity.	Yes	Setelah masuk ke grup lewat link, attacker bisa mengubah isi group seperti notes, to do list, atau komentar.	Pemanipulasian dan deletion isi group
Repudiation: Denying actions or transactions without accountability.	Yes	Tidak ada sistem log aktivitas yang mencatat siapa yang membuka atau mengedit data, jadi attacker bisa menyangkal	Kesulitan mencari tau pelakunya
Information Disclosure:	Yes	Attacker bisa melihat semua isi grup yang seharusnya hanya bisa diakses	Informasi tugas, strategi, atau data

Exposing sensitive data to unauthorized parties.		oleh member user resmi.	internal bocor ke pihak luar
Denial of Service: Disrupting system availability or performance.	No	Attack ini tidak ditujukan untuk membuat sistem down atau tidak bisa digunakan.	-
Elevation of Privilege: Gaining unauthorized access to higher system privileges.	Yes	Attacker yang rolenya sekedar user biasa bisa mengakses grup yang seharusnya terbatas (private) hanya dengan invite link.	Potensi kontrol atas data atau anggota grup yang bukan haknya.

SECURITY (MITIGATION)

Sebagai tim security, kami menerima laporan bahwasanya terdapat beberapa celah keamanan yang rentan terhadap serangan dan laporan dimana attacker berhasil mencoba melakukan serangan.

Langkah utama yang harus kami lakukan adalah memitigasi serangan IDOR (Insecure Direct Object Reference). Seperti pada kasus awal, mitigasi yang bisa dilakukan oleh tim security yaitu dengan menerapkan kontrol akses yang ketat baik pada sisi client maupun sisi server (server side authorization). Endpoint - endpoint yang berisis data sensitif harus divalidasi berdasarkan identitas pengguna yang sedang login bukan berdasarkan parameter ID yang dikirim dari sisi client. Serta parameter yang dapat dimanipulasi seperti user_id harus dihindari.

Langkah selanjutnya untuk memitigasi serangan Broken Access Control, yaitu dengan cara memberikan kepada anggotanya hak akses yang sesuai dengan role mereka masing-masing dan sesuai dengan tanggung jawab yang sebenarnya, maka dari itu kita bisa menerapkan Role-Based Access Control (RBAC). Data di dalam group juga bisa dipisahkan sesuai dengan fungsinya supaya terhindar dari pencemaran suatu data. Selain itu, kita juga harus memastikan bahwa implementasi access control sudah diterapkan dengan baik, benar dan sesuai. Serta dilakukannya pengujian secara berkala untuk menguji apakah web sudah secure dan mendeteksi celah security yang memungkinkan hacker masuk ke dalam sistem.

STRIDE MITIGATIONS : IDOR Exploitation Between User & BAC Attack with Group Link Invitation	
STRIDE	MITIGATION
Spoofing	<ul style="list-style-type: none">- Jangan izinkan pengguna memilih/mengganti ID yang dikirim ke server tanpa validasi- Gunakan sistem autentikasi yang ketat
Tampering	<ul style="list-style-type: none">- Terapkan kontrol akses berbasis otorisasi yang ketat di sisi server- Gunakan protokol komunikasi yang aman seperti HTTPS

Repudiation	<ul style="list-style-type: none"> - Simpan log di tempat terpisah dengan akses yang terbatas - Catat setiap user ID, waktu, IP address dan aksi yang dilakukan
Information Disclosure	<ul style="list-style-type: none"> - Enkripsi setiap data sensitif dalam database - Terapkan kontrol akses berbasis role (RABC) - Token link harus memiliki expiry time & scope
Denial Of Service	<ul style="list-style-type: none"> - Terapkan rate-limiting dan load balancing - Lakukan audit setiap saat untuk menghindari DoS - Batasi jumlah undangan aktif per user/grup
Elevation Of Privilage	<ul style="list-style-type: none"> - Update dan patch sistem secara berkala - Validasi role setelah join grup via link

SOURCES

[A01 Broken Access Control - OWASP Top 10:2021](#)

[Understanding the STRIDE Threat Model: A Beginner's Guide | by Selvakumar Subramanian | Medium](#)

<https://ridhomarhaban2000.medium.com/memahami-idor-insecure-direct-object-references-ab176af79cb1>

[Broken Access Control: Risiko Keamanan & Cara Menghindarinya](#)

https://owasp.org/www-community/Threat_Modeling_Process

<https://medium.com/@selvakumarsubramanian/understanding-the-stride-threat-model-a-beginners-guide-a555a7bbb62c>

https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

Chat GPT