Дата/період тестування	27.04.2026 - 28.04.2026
Оператор МІС	ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ДОКДРІМ"
Назва МІС	DocDream
ЄДРПОУ	42313028
Модуль безпекових вимог на який протестована МІС	2
Версія ПЗ МІС	1.8.X.X
Тестувальник(и)	Сидоров О.В.
ПЗ, що використовувалося при тестуванні (у разі застосування)	BurpSuite, SQLmap , Dalfox , nmap, dirsearch, gobuster, nuclei
Підсумковий результат тестування	**Відповідає вимогам**

Підпис, прізвище та ініціали тестувальника: Сидоров О.В.

№ п/п	Вимога до безпеки	МІС відповідає вимогам (Так/Ні)	Примітки
2 Загальні вимоги до безпеки			
1	МІС повинна використовувати чинний SSL/TLS сертифікат, який відповідає таким криптографічним стандартам: ECC (ECDSA P-256, P-384) або RSA (з довжиною ключа не менше 2048 біт);	Так	
2	МІС повинна бути захищена від SQL-ін'єкцій. Дані, що передаються до МІС не повинні призводити до виконання непередбачених SQL-запитів, модифікації існуючих запитів або виконання додаткових запитів, ініційованих користувачем;	Так	
3	МІС повинна бути захищена від XSS-ін'єкцій. Дані, що передаються до МІС або обробляються на клієнтській стороні не повинні призводити до виконання неавторизованого чи шкідливого коду у	Так	

	контексті веб браузера кінцевого користувача;		
4	МІС повинна бути захищена від SSRF-атак. Дані що передаються до МІС не повинні призводити до формування запитів з боку сервера до внутрішніх або зовнішніх ресурсів, доступ до яких не передбачено бізнес-логікою системи;	Так	
5	МІС повинна бути захищена від атак LFI та RFI. Дані що передаються до МІС не повинні призводити до завантаження, читання, виконання або іншим чином обробки локальних чи віддалених файлів, доступ до яких не передбачено;	Так	
6	МІС повинна бути захищена від атак, що призводять до виконання довільного коду або системних команд ("Command Execution"). Дані що передаються до МІС не повинні дозволяти запуск системних команд, а також виконання скриптів або програм на стороні сервера;	Так	
7	МІС повинна бути захищена від атак типу IDOR. Дані, що передаються до МІС, зокрема параметри запитів (URL, body, headers, cookies, тощо), не повинні дозволяти користувачам отримувати доступ до інформації, ресурсів чи виконувати дії від імені інших користувачів. МІС повинна обов’язково здійснювати перевірку прав доступу до	Так	

	кожного об’єкта незалежно від того, чи змінив користувач ідентифікатор ресурсу вручну.		
8	МІС повинна використовувати тільки безпечні способи передачі даних, а саме: між МІС та користувачем МІС - протокол TLS версії не нижче 1.2;	Так	
9	МІС повинна реалізовувати власний механізм автентифікації, авторизації та керування сесіями користувачів, який застосовується до будь-якої взаємодії користувача із МІС (окрім первинної реєстрації НМП). Ініціювання автентифікації та/або авторизації користувача в Системі допускається виключно в межах активної сесії користувача, створеної та керованої МІС.	Так	
10	МІС повинна бути захищена від атак типу brute-force. МІС повинна реалізовувати механізми протидії автоматизованому підбору облікових даних, зокрема: 1. обмеження кількості невдалих спроб автентифікації в МІС до 5 протягом 15 хвилин для одного облікового запису 2. автоматичне блокування облікового запису на 5 хвилин після 5 невдалих спроб автентифікації в МІС;	Так	

11	МІС повинна підтримувати та обов'язково застосовувати механізм 2FA для всіх користувачів. Автентифікація в МІС повинна здійснюватися із використанням щонайменше двох незалежних факторів: одного фактора знання та одного фактора володіння.	Так	
12	МІС повинна дозволяти лише одну активну сесію на одного користувача в будь-який момент часу. У разі повторної автентифікації користувача в МІС усі раніше активні сесії цього користувача повинні бути автоматично завершені. Після цього доступ користувача до МІС можливий лише після проходження повторної авторизації в МІС.	Так	
13	МІС повинна автоматично завершувати сесію користувача у разі бездіяльності протягом 60 хвилин. Бездіяльністю вважається відсутність будь-яких дій з інтерфейсом системи, включаючи введення з клавіатури, рух миші, навігацію між сторінками. Після досягнення порогу бездіяльності МІС повинна заборонити будь-які дії (зокрема, завершити поточну сесію) Користувача до повторної авторизації.	Так	
14	МІС повинна забезпечити, що значення "mis_client_secret" не є доступним кінцевому користувачу, у тому числі через клієнтські застосунки, незалежно від платформи їх реалізації	Так	

	(web, desktop), включаючи, але не обмежуючись: 1. вихідним кодом або бінарними файлами клієнтської частини; 2. frontend-компонентами (HTML, JavaScript); 3. локальними сховищами клієнтського середовища; 4. cookies, URL-параметрами, HTTP-заголовками або тілом відповіді;		

Зауваження та рекомендації Адміністратора до модулю:

Додаткові рекомендації для розробників та адміністраторів:

1. **Використання простих ідентифікаторів наприкладі доступу до даних пацієнтів.**

В результаті аналізу HTTP запитів веб застосунку виявлено що застосунок напряму звертається до внутрішніх об’єктів за допомогою послідовних ідентифікаторів (ID).

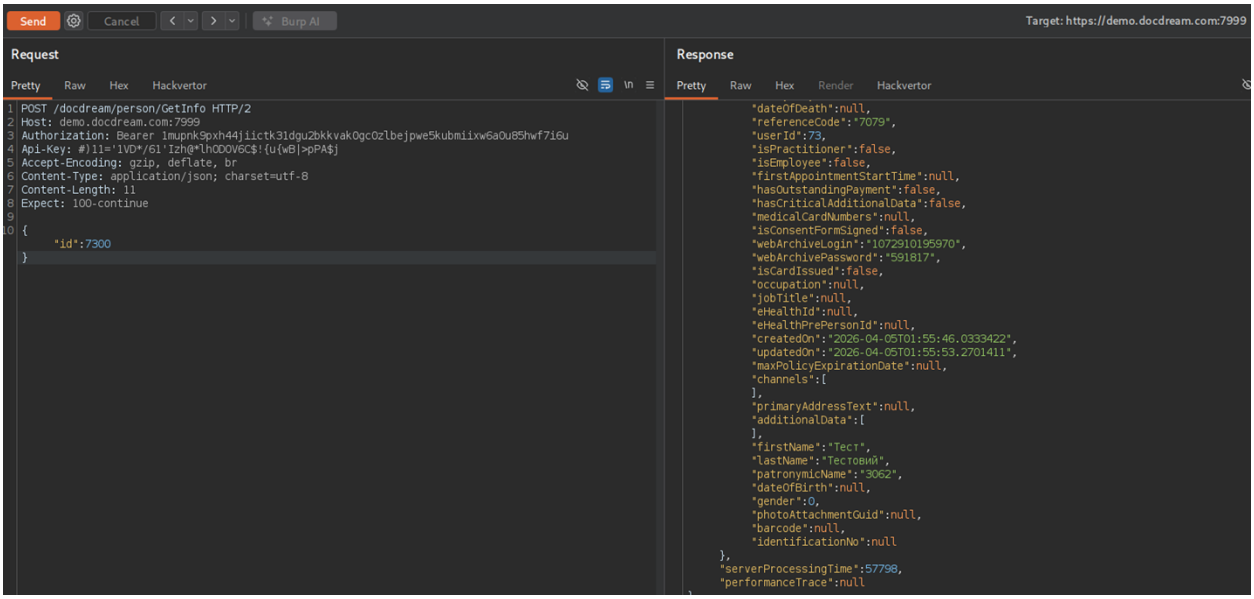
Виконуючи запит наведений нижче та замінюючи параметр “id” на числа від 1 до 7300.

```
POST /docdream/person/GetInfo HTTP/2
Host: demo.docdream.com:7999
Authorization: Bearer 1mupnk9pxh44jiictk31dgu2bkkvak0gc0zlbejpwe5kubmiixw6a0u85hwf7i6u
Api-Key: #)11='1VD*/61'Izh@*lhODOV6C$!{u{wB|>pPA$j
Accept-Encoding: gzip, deflate, br
Content-Type: application/json; charset=utf-8
Content-Length: 11
Expect: 100-continue

{"id":7300}

```

Отримуємо всі дані про пацієнта:



Це може призвести до масового витоку персональних даних, що використовуватимуться для фішингу, соціальної інженерії. Використання отриманих даних для доступу до веб застосунку.

Рекомендації:

- Замініть послідовні ID на UUID v4 або salted hashes для складності перебору.

Даний аналіз базується на технологіях та відомих вразливостях на момент тестування MIC. Ми радимо дотримуватись рекомендацій зазначених у цьому звіті у порядку критичності вразливостей.

Також ми рекомендуємо провести повторне тестування ресурсу після проведення зазначених вище заходів. Тим самим ви можете переконатися, що ваш ресурс більше не схильний до подібних ризиків та заходи виконані правильно.

Коментарі та заперечення оператора MIC до протоколу: