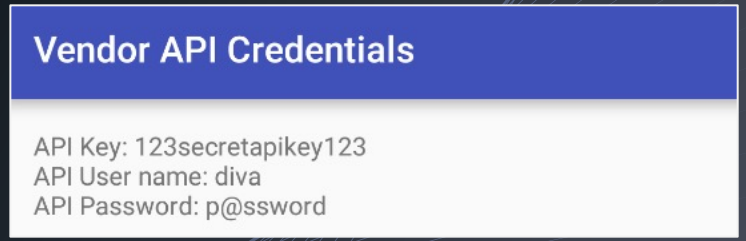
M4 - Insecure Authentication.

M4 - Insecure Authentication

Dapat dieksploitasi dengan cara menjalankan fungsionalitas dalam aplikasi seluler atau di backend. Ini sering dapat dilakukan melalui serangan otomatis dan *tools* yang mengirimkan beberapa permintaan untuk memeriksa apa yang bisa membypass skema dan mekanisme dari otentikasi yang diterapkan.

Kegagalan untuk mengidentifikasi pengguna dan menerapkan manajemen sesi yang aman adalah penyebab umum. Namun demikian, melakukan permintaan otentikasi di sisi server dan bukan secara lokal dapat membantu untuk menghindari serangan yang bergantung pada perangkat seluler. Akan tetapi, enkripsi data pada sisi klien adalah lapisan keamanan tambahan jika perangkat seluler diperoleh secara fisik.



M5 - Insufficient Cryptography.

M2 - Insufficient Cryptography

Memungkinkan penyerang untuk berpotensi mengembalikan data sensitif ke keadaan semula sehingga menghasilkan akses tidak sah ke data pengguna. Secara umum, *attacker* dengan akses fisik ke perangkat seluler yang tidak menerapkan algoritma enkripsi yang kuat dapat mengeksploitasi kelemahan ini dengan cukup mudah.

Untuk mencegah serangan yang memanfaatkan kerentanan ini, pengembang harus yakin untuk menangani data sensitif dengan hati-hati dengan menghindari penyimpanan data sensitif lokal pada perangkat seluler dan menerapkan standar kriptografi yang kuat yang sesuai dengan algoritma yang disarankan dan dalam praktiknya pada dunia industri.

M6 - Insecure Authorization.

M6 - Insecure Authorization

Dapat memungkinkan musuh untuk mendapatkan hak istimewa yang dapat mengakibatkan akses ke informasi sensitif dan yang dapat menyebabkan kerusakan reputasi. Ini dapat dilakukan dengan memanfaatkan API yang rentan untuk melakukan tindakan administratif yang dapat dilakukan dan ditemukan secara manual atau melalui *BURP* Suite..

Memverifikasi roles dan *permissions* secara ketat di backend dan memastikan bahwa permintaan diajukan hanya oleh user yang memiliki otorisasi untuk melakukannya dapat membantu mencegah otorisasi tidak aman.

TERIMA KASIH