Báo cáo lỗi bảo mật ứng dụng di động myFAP

Thiếu sử dụng giao thức HTTPS và mối đe doạ bị tấn công Man-in-The-Middle (MiTM)

Họ và tên	Huỳnh Ngọc Quang
Mã số sinh viên	SE181838
Trường	Đại học FPT

nquangit

Mục lục

I. Giới thiệu

a. Tổng quan:

Báo cáo này nhằm đánh giá lỗ hổng bảo mật của ứng dụng di động myFAP và tập trung vào hai vấn đề chính: việc sử dụng giao thức HTTP thay vì HTTPS và khả năng bị tấn công Man-in-the-Middle (MiTM). Ứng dụng myFAP, một ứng dụng di động đang được sử dụng rộng rãi bởi các sinh viên trường đại học FPT, đang gặp phải những rủi ro và mối đe dọa đáng lo ngại liên quan đến bảo mật thông tin người dùng.

b. Mục tiêu của báo cáo

Mục tiêu của báo cáo này là phân tích và đề xuất các biện pháp khắc phục để tăng cường bảo mật của ứng dụng myFAP. Bằng cách tìm hiểu về lỗ hổng bảo mật hiện tại, chúng tôi hy vọng đưa ra những khuyến nghị cụ thể và thiết thực để cải thiện sự bảo mật của ứng dụng này và bảo vệ thông tin cá nhân của người dùng.

c. Phạm vi của báo cáo

Báo cáo tập trung vào hai vấn đề chính là việc sử dụng giao thức HTTP thay vì HTTPS và khả năng bị tấn công Man-in-the-Middle (MiTM). Chúng tôi sẽ mô tả chi tiết về các lỗ hổng này, nhấn mạnh tác động tiềm tàng của chúng và đưa ra các giải pháp để khắc phục vấn đề an ninh này. Tuy nhiên, báo cáo không bao gồm kiểm tra các lỗ hổng khác có thể tồn tại trong ứng dụng myFAP.

d. Phương pháp nghiên cứu

Để thực hiện báo cáo này, chúng tôi đã tiến hành một quá trình nghiên cứu kỹ lưỡng, bao gồm kiểm tra ứng dụng myFAP, phân tích luồng dữ liệu và mô phỏng các cuộc tấn công MiTM. Chúng tôi đã sử dụng các công cụ và phương pháp phù hợp để xác định và đánh giá lỗ hổng bảo mật trong ứng dụng.

e. Cấu trúc báo cáo

Báo cáo này được chia thành các phần chính để giúp người đọc hiểu rõ vấn đề. Các phần bao gồm: giới thiệu, miêu tả ứng dụng myFAP, miêu tả lỗi không sử dụng HTTPS, miêu tả lỗ hổng MiTM, bước tái hiện lỗi, hậu quả, giải pháp và kết luận. Mỗi phần sẽ cung cấp thông tin chi tiết và các khuyến nghị tương ứng để giải quyết các vấn đề an ninh trong ứng dụng di động myFAP.

II. Mô tả ứng dụng myFAP

a. Tên ứng dụng

myFAP

b. Mô tả chức năng chính

myFAP là một ứng dụng di động nhằm hỗ trợ sinh viên trường đại học FPT trong việc quản lý, giám sát, cập nhật những thông tin học tập của cá nhân mới nhất từ trường.

c. Người dùng

Sinh viên thuộc trường đại học FPT.

d. Phiên bản

1.2.4

e. Mô tả chức năng liên quan đến bảo mật

Trường đại học sẽ cấp cho mỗi sinh viên một tài khoản mail @fpt.edu.vn và sinh viên dùng chính tài khoản này để đăng nhập vào ứng dụng myFAP. Chức năng của ứng dụng là truy xuất những thông tin của sinh viên như thông tin cá nhân, lịch học, lịch thi, …

f. Kiến trúc ứng dụng

myFAP được phát triển dựa trên mô hình kiến trúc khách-máy chủ (client-server), trong đó ứng dụng di động hoạt động như một máy khách và kết nối với máy chủ để lưu trữ và truy xuất dữ liệu.

III. Mô tả mối đe doạ khi không sử dụng giao thức HTTPS

a. Mô tả lỗi

Trong ứng dụng myFAP, đã xác định rằng việc truyền dữ liệu giữa ứng dụng di động và máy chủ không sử dụng giao thức HTTPS. Thay vào đó, ứng dụng đang sử dụng giao thức HTTP không được mã hóa để truyền tải thông tin giữa các bên.

b. Hậu quả của lỗi

Việc sử dụng giao thức HTTP không bảo mật khi truyền tải dữ liệu gây ra nhiều vấn đề bảo mật nghiêm trọng. Dữ liệu nhạy cảm của người dùng, bao gồm thông tin tài khoản, mật khẩu và các giao dịch tài chính, có thể bị đánh cắp hoặc thay đổi bởi kẻ tấn công trung gian. Những dữ liệu này có thể bị lộ ra công chúng hoặc được sử dụng sai mục đích, gây hậu quả nghiêm trọng cho người dùng.

c. Nguy cơ bảo mật

Việc không sử dụng HTTPS tạo điều kiện cho các cuộc tấn công như Man-in-the-Middle (MiTM). Kẻ tấn công có thể giả mạo máy chủ hoặc xâm nhập vào kết nối mạng giữa ứng dụng di động và máy chủ, theo dõi và can thiệp vào dữ liệu truyền tải. Điều này cho phép kẻ tấn công đọc thông tin nhạy cảm hoặc thậm chí thay đổi nội dung của các giao dịch và thông tin được truyền đi, mà người dùng không hề hay biết.

d. Ảnh hưởng đến uy tín và lòng tin của người dùng

Việc không sử dụng HTTPS trong ứng dụng gây mất lòng tin của người dùng. Người dùng có thể không tin tưởng vào tính bảo mật và sự bảo vệ của ứng dụng, dẫn đến việc giảm sự sử dụng và tiềm ẩn rủi ro về mất mát người dùng và thương hiệu.

e. Yêu cầu khắc phục

Để khắc phục lỗi này, cần triển khai giao thức HTTPS để bảo mật dữ liệu truyền tải giữa ứng dụng di động và máy chủ. Việc sử dụng chứng chỉ SSL/TLS, xác thực máy chủ và mã hóa dữ liệu sẽ giúp tăng cường tính bảo mật và ngăn chặn các cuộc tấn công MiTM.

IV. Mô tả cuộc tấn công Man-in-The-Middle (MiTM)

a. Mô tả lỗ hổng

Trong quá trình phân tích ứng dụng myFAP, đã phát hiện một lỗ hổng bảo mật nghiêm trọng là khả năng bị tấn công Man-in-the-Middle (MiTM). Lỗ hổng này cho phép một kẻ tấn công can thiệp vào kết nối mạng giữa ứng dụng di động và máy chủ, giả mạo máy chủ hoặc theo dõi và can thiệp vào dữ liệu truyền tải. Sau đây là một số phương pháp tấn công MiTM:

1. ARP Poisoning: Đây là một kỹ thuật tấn công MiTM phổ biến nhắm vào giao thức ARP (Address Resolution Protocol). Kẻ tấn công gửi các gói tin giả mạo có địa chỉ MAC sai lẫn vào mạng, khiến cho các thiết bị trong mạng tin tưởng rằng địa chỉ MAC của máy chủ hoặc thiết bị mạng khác đã bị thay đổi. Như vậy, dữ liệu từ các thiết bị trong mạng sẽ được chuyển đến máy kẻ tấn công trước khi đến đích.
2. DNS Spoofing: Kỹ thuật này nhằm làm giả một máy chủ DNS (Domain Name System) để chuyển hướng các yêu cầu DNS của người dùng đến máy chủ DNS giả mạo. Khi kẻ tấn công chiếm quyền kiểm soát DNS, họ có thể chuyển hướng người dùng đến các trang web giả mạo hoặc lừa đảo.
3. IP Spoofing: Kỹ thuật này liên quan đến làm giả địa chỉ IP nguồn trong các gói tin mạng. Kẻ tấn công tạo ra các gói tin với địa chỉ IP nguồn giả mạo nhằm mất danh tính và làm người nhận tin tưởng rằng gói tin đến từ một nguồn hợp lệ.
4. Wi-Fi Eavesdropping: Đây là kỹ thuật tấn công MiTM thường xuyên xảy ra trong môi trường Wi-Fi công cộng. Kẻ tấn công sử dụng phần mềm độc hại để nghe trộm hoặc bắt gói tin trên mạng Wi-Fi, từ đó có thể lấy được thông tin nhạy cảm như tên người dùng, mật khẩu và dữ liệu cá nhân.
5. Session Hijacking: Kỹ thuật này nhằm chiếm quyền điều khiển một phiên làm việc hợp pháp giữa hai bên giao tiếp. Kẻ tấn công sử dụng các phương pháp như cookie hijacking hoặc sử dụng kỹ thuật sniffing để chặn, chuyển hướng hoặc thay đổi thông tin trong phiên làm việc.

b. Cơ chế hoạt động của tấn công MiTM

Kẻ tấn công sẽ tạo một điểm truy cập giả mạo, thường được gọi là "proxy" hoặc "cầu nối", để trung gian trong quá trình giao tiếp giữa ứng dụng di động và máy chủ thực. Khi người dùng kết nối với ứng dụng myFAP, dữ liệu sẽ được chuyển tiếp thông qua proxy giả mạo này. Kẻ tấn công có thể đọc, thay đổi hoặc thậm chí lấy cả dữ liệu truyền qua để thực hiện các hành vi xâm nhập, ăn cắp thông tin cá nhân hoặc thực hiện yêu cầu giả mạo.

c. Hậu quả của lỗ hổng MiTM

Tấn công Man-in-the-Middle (MiTM) có thể gây ra những hậu quả nghiêm trọng. Kẻ tấn công có khả năng thu thập thông tin nhạy cảm của người dùng như tên người dùng, phiên đăng nhập và thông tin tài chính. Hơn nữa, kẻ tấn công có thể thực hiện các yêu cầu đến máy chủ với quyền truy cập tương đương với nạn nhân.

d. Nguy cơ bảo mật và ảnh hưởng đến người dùng

Tấn công MiTM đe dọa tính bảo mật và sự riêng tư của người dùng trong quá trình sử dụng ứng dụng. Người dùng có thể không nhận ra sự hiện diện của kẻ tấn công và tin tưởng vào

tính bảo mật của ứng dụng, dẫn đến việc rơi vào tình trạng lộ thông tin cá nhân và tài chính quan trọng.

e. Yêu cầu khắc phục

Để khắc phục lỗ hổng MiTM, cần triển khai các biện pháp bảo mật như sử dụng giao thức HTTPS để mã hóa dữ liệu truyền tải và đảm bảo xác thực máy chủ. Thêm vào đó, kiểm tra tích hợp các biện pháp kiểm tra và phát hiện các cuộc tấn công MiTM, như xác thực chứng chỉ SSL/TLS, sử dụng giao thức bảo mật mạng (VPN) để tạo kênh kết nối an toàn.

V. Tái hiện lỗi

a. Mô tả bước tái hiện lỗi

Để đảm bảo xác thực lỗi không sử dụng HTTPS và lỗ hổng bị tấn công MiTM trong ứng dụng myFAP, chúng tôi đã tiến hành một số bước tái hiện lỗi để chứng minh tính khả thi và mức độ nguy hiểm của chúng. Các bước tái hiện lỗi được thực hiện như bên dưới.

b. Xác định môi trường tái hiện

Đầu tiên, chúng tôi đã tạo ra một môi trường tái hiện gồm một môi trường mạng không dây có kết nối đến server của ứng dụng myFAP với một router, máy tính của hacker (chạy hệ điều hành Kali Linux) đã được cài đặt sẵn những công cụ cần thiết và một thiết bị di động để dùng ứng dụng myFAP.

c. Thiết lập kết nối

Tiếp theo, chúng tôi đã cấu hình để máy tính của hacker và di động kết nối đến cùng mạng không dây đã thiết lập từ trước. Đăng nhập tài khoản myFAP vào thiết bị di động và đảm bảo rằng ứng dụng có khả năng giao tiếp với server thông qua mạng đã cấu hình.

d. Thiết lập kịch bản tấn công MiTM

Chúng tôi đã triển khai một kịch bản tấn công MiTM bằng phương pháp ARP Poisoning trong môi trường tái hiện. Bằng cách sử dụng công cụ tấn công phổ biến như dnsniff, ettercap và Wireshark, chúng tôi đã can thiệp vào quá trình truyền tải dữ liệu giữa ứng dụng di động và máy chủ.

e. Thu thập thông tin và kiểm tra ảnh hưởng

Trong quá trình chạy kịch bản tấn công MiTM, chúng tôi đã thu thập dữ liệu truyền qua proxy giả mạo và kiểm tra xem liệu kẻ tấn công có thể đọc, thay đổi hoặc lấy cả dữ liệu nhạy cảm của người dùng. Chúng tôi cũng đã đánh giá mức độ ảnh hưởng của tấn công MiTM đối với tính bảo mật và uy tín của ứng dụng myFAP.

f. Ghi lại kết quả và chứng minh lỗi

Cuối cùng, chúng tôi đã ghi lại các kết quả của quá trình tái hiện lỗi, bao gồm thông tin về các dữ liệu bị đánh cắp, thay đổi hoặc lấy cắp, cũng như mức độ ảnh hưởng của lỗ hổng MiTM đối với người dùng và ứng dụng FAP. Tất cả những thông tin này sẽ được bao gồm trong mục báo cáo chi tiết về lỗi bên dưới.

g. Báo cáo chi tiết về lỗi

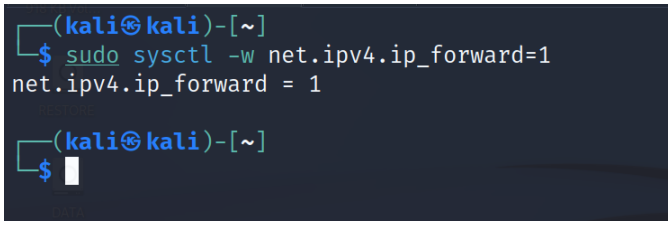
Lỗi trong ứng dụng FAP được phát hiện là sử dụng giao thức HTTP thay vì HTTPS, đây là một lỗ hổng bảo mật nghiêm trọng. Giao thức HTTP không mã hóa dữ liệu truyền tải, làm cho thông tin nhạy cảm của người dùng dễ bị đánh cắp và bị tấn công Man-in-the-Middle (MiTM). Điều này đặt người dùng và dữ liệu của họ trong tình trạng nguy hiểm, gây nguy cơ mất danh tính, rò rỉ thông tin cá nhân và tiềm năng cho việc tấn công vào tài khoản và gian lận.

Lỗi không sử dụng HTTPS trong ứng dụng FAP cho phép kẻ tấn công nắm bắt và xem trộm dữ liệu truyền tải giữa thiết bị di động của người dùng và máy chủ. Kẻ tấn công có thể sử dụng các công cụ đơn giản để giành được quyền truy cập vào thông tin cá nhân, giao dịch tài chính và dữ liệu quan trọng khác. Điều này tạo ra một môi trường không an toàn và mở ra cánh cửa cho các cuộc tấn công MiTM, mà kẻ tấn công có thể can thiệp, thay đổi và thậm chí lừa đảo người dùng.

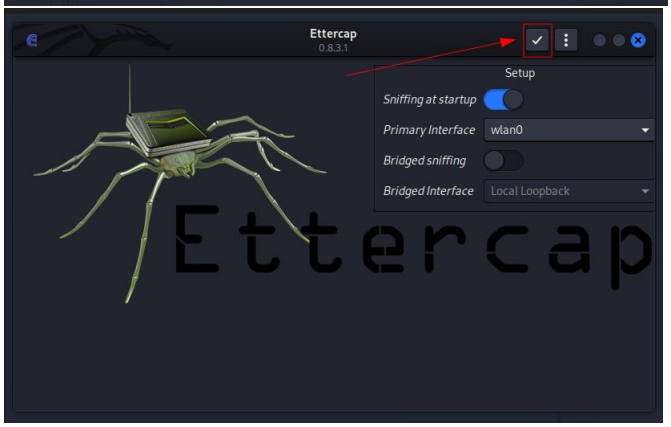
Để đảm bảo tính bảo mật và bảo vệ thông tin cá nhân của người dùng, việc triển khai giao thức HTTPS là cần thiết. HTTPS cung cấp mã hóa dữ liệu truyền tải, đảm bảo tính toàn vẹn và bảo mật của thông tin. Bằng cách sử dụng chứng chỉ SSL/TLS hợp lệ, kiểm tra tính toàn vẹn dữ liệu và triển khai các biện pháp bảo mật mạng, những lỗ hổng bảo mật trong ứng dụng FAP có thể được khắc phục và tăng cường niềm tin của người dùng vào tính bảo mật của ứng dụng.

Sau đây là mô tả chi tiết quá trình tấn công Man-in-The-Middle (MiTM) dùng phương pháp ARP Poisoning khai thác lỗ hổng thiếu sử dụng giao thức mã hoá HTTPS:

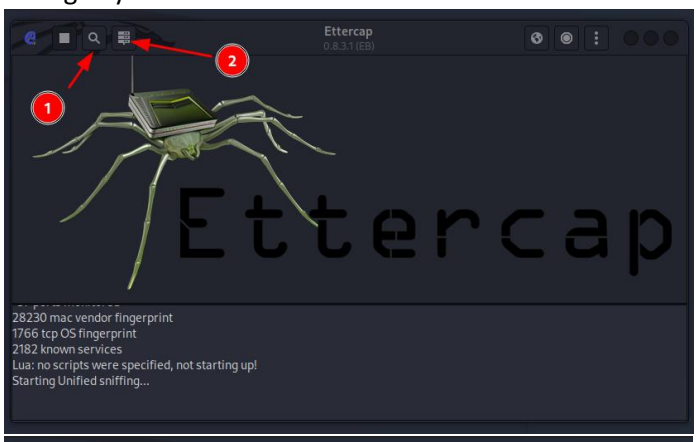
- Đầu tiên chúng tôi sẽ cấu hình máy tính của hacker cho phép chuyển tiếp gói tin, điều này cho phép chuyển tiếp gói tin từ một interface này đến một interface khác có nghĩa rằng hệ thống có thể hoạt động như một router.

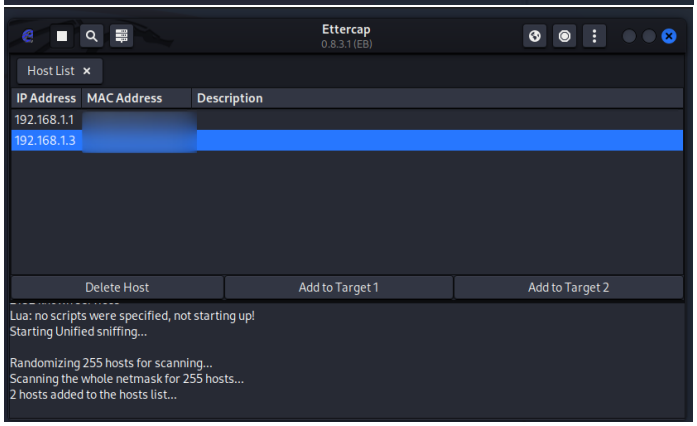


- Tiếp theo chúng tôi khởi chạy công cụ Ettercap, có thể sử dụng command line hoặc giao diện đồ hoạ (GUI). Ở đây chúng tôi sẽ sử dụng giao diện đồ hoạ (GUI) để có một cái nhìn trực quan hơn.

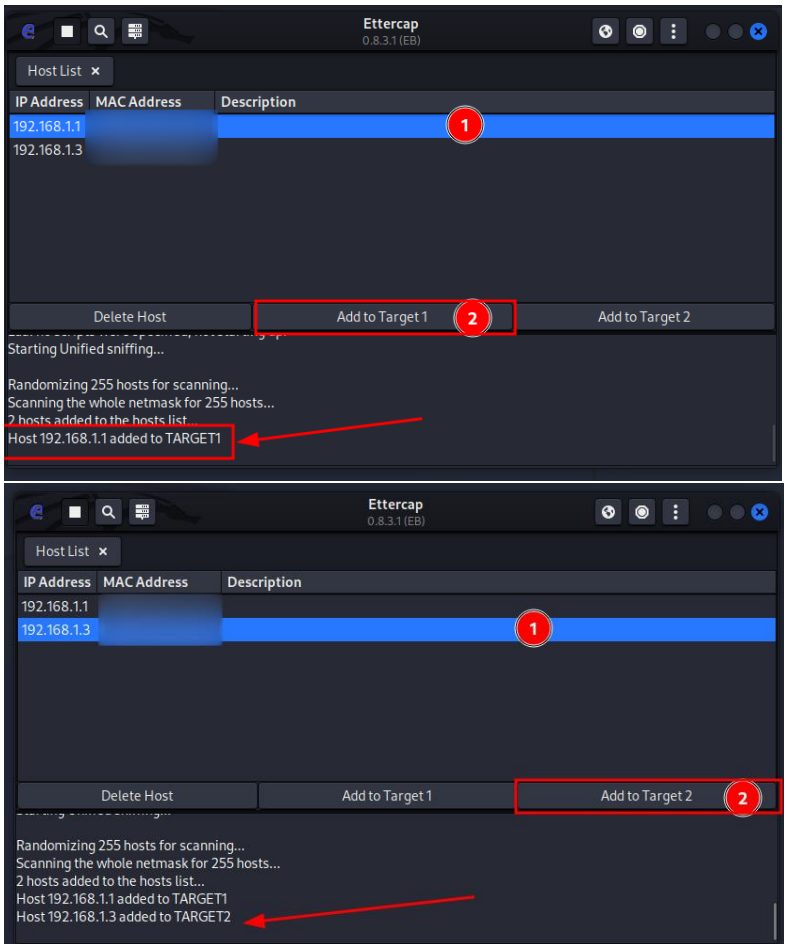


- Sau khi khởi chạy Ettercap chúng tôi bắt đầu quét các thiết bị có trong mạng không dây.

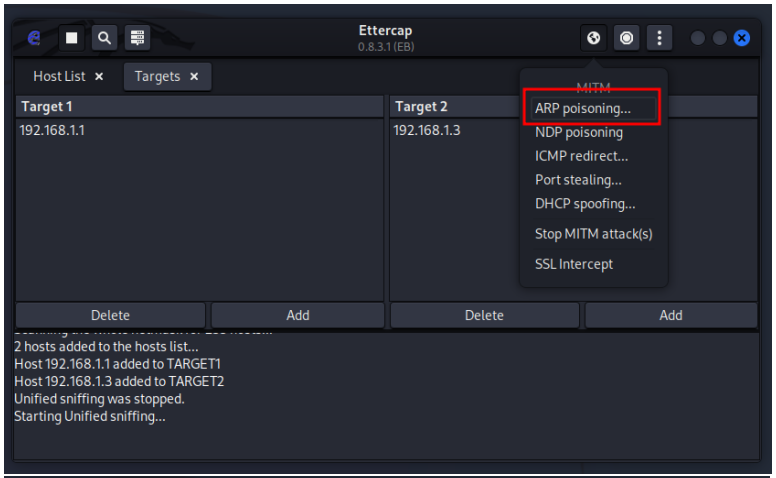


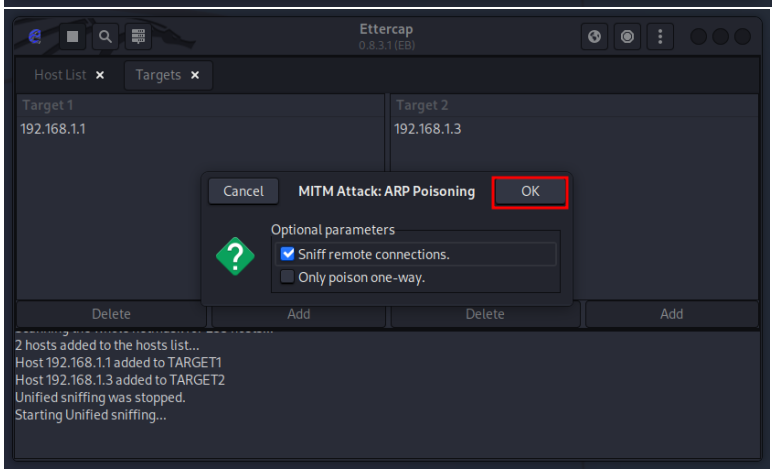


- Sau khi quét các thiết bị có trong mạng xong, chúng tôi có thể thấy rằng có 2 thiết bị: IP 192.168.1.1 là địa chỉ của router và IP 192.168.1.3 chính là địa chỉ của thiết bị di động (target). Tiếp theo chúng tôi thêm những thiết bị này vào tầm ngắm (scope) để tiến hành giả mạo để đánh cắp gói tin.



- Sau khi thêm các thiết bị đối tượng vào tầm ngắm (scope) chúng tôi bắt đầu cuộc tấn công ARP Poisoning.

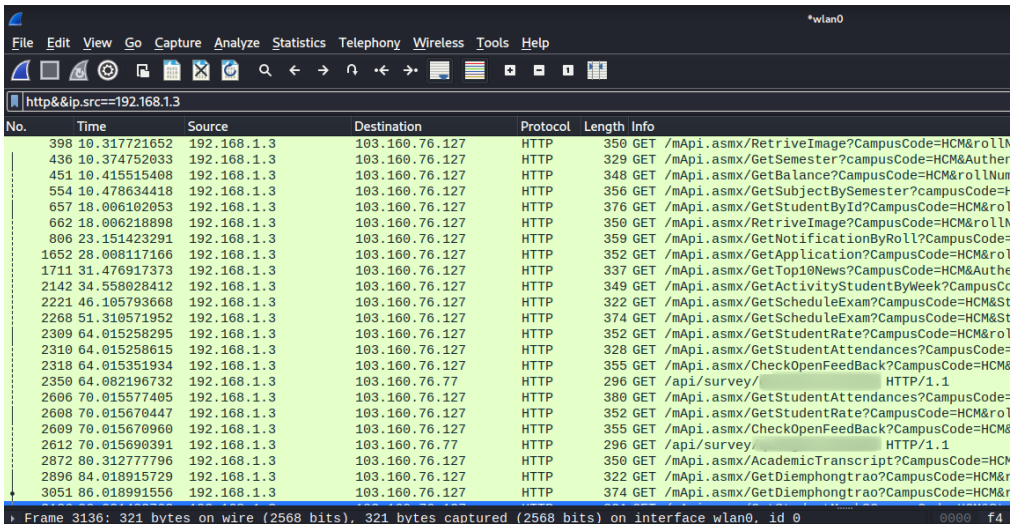




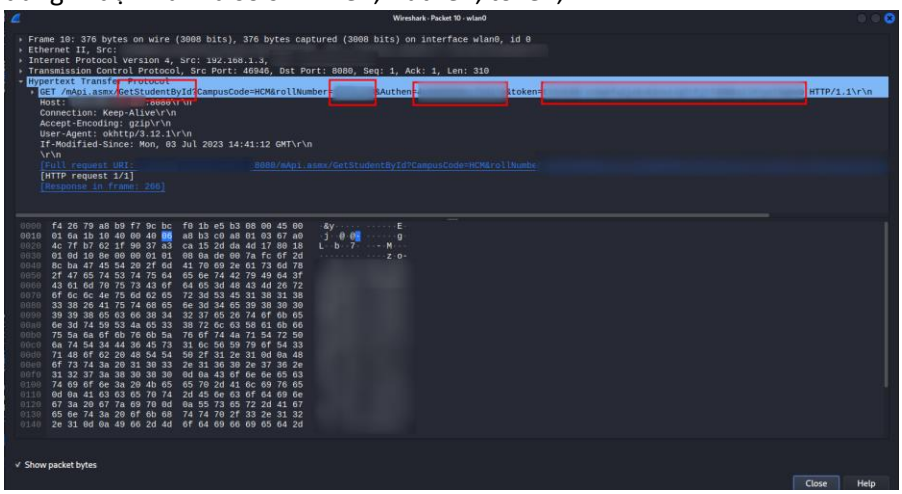
- Đây là cách sử dụng công cụ arpspoof từ gói dnsniff cũng cho kết quả tương tự với Ettercap nhưng câu lệnh đơn giản hơn.

- Sau khi bắt đầu quá trình tấn công ARP Poisoning các gói tin từ thiết bị di động gửi đến router và ngược lại sẽ không được gửi trực tiếp đến điểm cuối mà sẽ thông qua máy tính của hacker. Và chúng tôi khởi chạy Wireshark để xem các gói tin giữa thiết bị di động và router. Sau khi khởi động Wireshark chúng tôi sẽ chọn lắng nghe ở interface wlan0 (Wi-fi).
- Khi phân tích ứng dụng myFAP, các yêu cầu gửi lên server là các yêu cầu HTTP (HTTP request) vì thế chúng tôi đặt các filter để lọc các gói tin mà chúng tôi

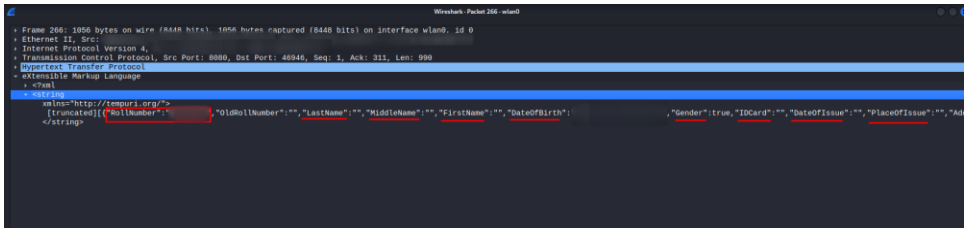
nhắm đến.



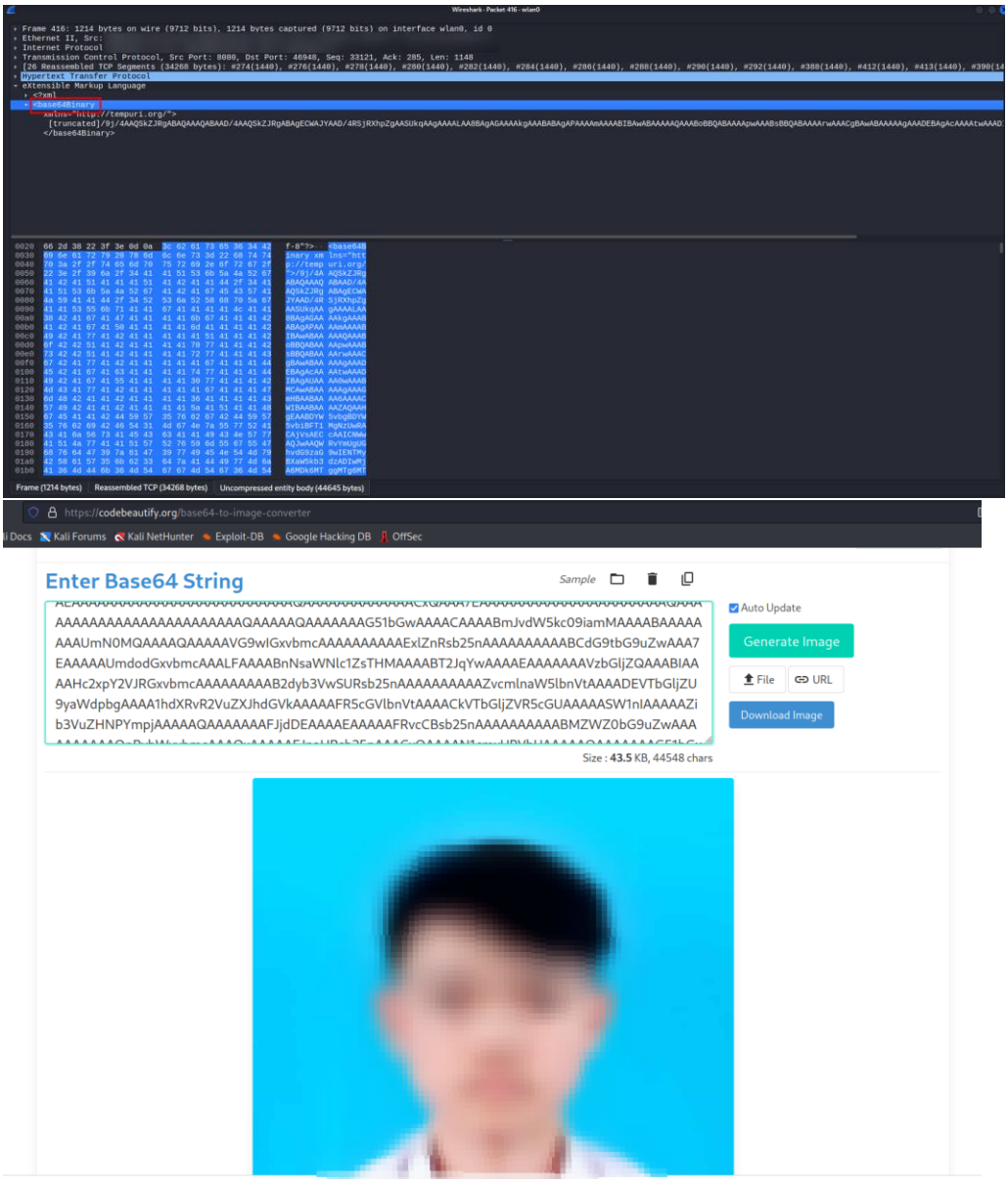
- Ở đây chúng tôi có thể thấy rằng có rất nhiều điểm cuối (endpoint) có thể truy xuất đến những thông tin cá nhân của người dùng. Khi mở một gói tin để quan sát, chúng tôi nhận thấy rằng có đầy đủ thông tin về phiên đăng nhập của người dùng ví dụ như mã số sinh viên, Authen, token,…



- Một số điểm cuối có thể truy cập đến những thông tin cá nhân của người dùng, tuy nhiên server đã khắc phục trước đó bằng cách chỉ trả về một số trường cơ bản.

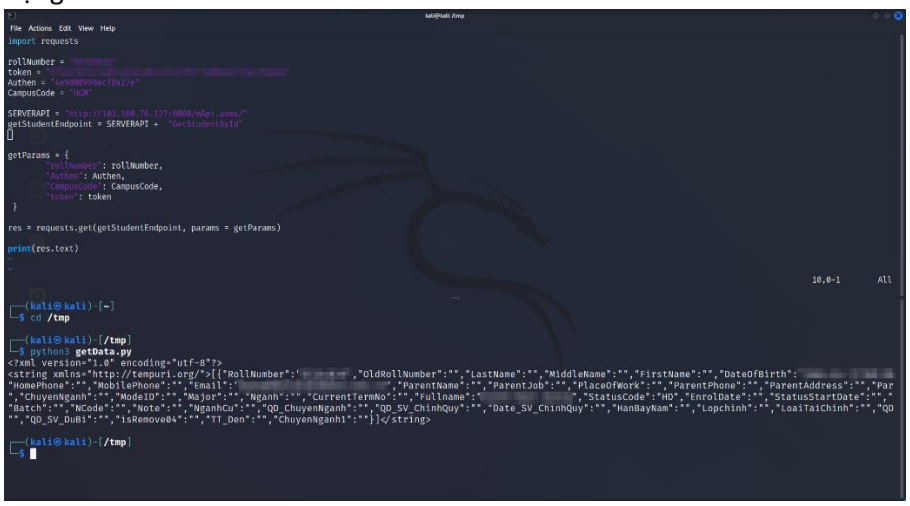


- Nhưng thông tin cơ bản có thể truy xuất như Họ và tên, ngày tháng năm sinh, mã số sinh viên, email và đặc biệt là base-64 ảnh của sinh viên. Tôi có thể dễ dàng xem được bức ảnh này bằng cách chuyển đổi base64 thành định dạng ảnh sử dụng các công cụ online có sẵn như bên dưới



- Ngoài ra từ các điểm cuối (endpoint) cùng các thông tin về phiên đăng nhập từ phía trên, chúng tôi hoàn toàn có thể viết một đoạn mã để lấy cả thông tin khả

dụng của sinh viên từ server.



Kết luận: Từ mô tả chi tiết quá trình tấn công MiTM trong ứng dụng FAP, chúng tôi nhận thấy rằng đây là một lỗ hổng bảo mật nghiêm trọng với cách khai thác không quá phức tạp. Qua việc tận dụng việc sử dụng giao thức HTTP thay vì HTTPS, kẻ tấn công có thể tiếp cận và xem trộm thông tin người dùng một cách trực tiếp và hiệu quả.

VI. Hậu quả

Lỗi không sử dụng HTTPS và lỗ hổng MiTM trong ứng dụng FAP có thể gây ra những hậu quả nghiêm trọng như sau:

- Đánh cắp thông tin nhạy cảm: Với giao thức HTTP, dữ liệu truyền tải không được mã hóa, dễ dàng bị kẻ tấn công đánh cắp. Thông tin cá nhân, tài khoản người dùng và các dữ liệu nhạy cảm khác có thể bị lộ ra ngoài.
- Thay đổi và xâm nhập dữ liệu: Kẻ tấn công có thể can thiệp vào quá trình truyền tải dữ liệu và thực hiện các hành động như thay đổi nội dung dữ liệu, chèn mã độc hoặc thực hiện các hành vi xâm nhập vào hệ thống.
- Mất uy tín và tin tưởng: Sự thiếu an toàn của ứng dụng FAP do không sử dụng HTTPS và lỗ hổng MiTM có thể gây mất uy tín và tin tưởng của người dùng. Người dùng có thể mất lòng tin vào tính bảo mật của ứng dụng và từ chối sử dụng nó.

VII. Giải pháp

Để khắc phục lỗi không sử dụng HTTPS và mỗi đe doạ tấn công MiTM, chúng tôi đề xuất các giải pháp sau đây:

- Triển khai giao thức HTTPS: Chuyển đổi từ giao thức HTTP sang HTTPS để đảm bảo rằng dữ liệu truyền tải được mã hóa và bảo mật. Điều này đảm bảo tính toàn vẹn và bảo mật của dữ liệu trong quá trình truyền.
- Sử dụng chứng chỉ SSL/TLS hợp lệ: Đảm bảo rằng máy chủ sử dụng chứng chỉ SSL/TLS hợp lệ từ tổ chức uy tín. Kiểm tra và xác thực chứng chỉ SSL/TLS để đảm bảo tính toàn vẹn của kết nối và ngăn chặn các cuộc tấn công MiTM.

- Yêu cầu người dùng sử dụng giao thức bảo mật mạng (VPN): Sử dụng một kênh kết nối an toàn thông qua giao thức bảo mật mạng (VPN) để tạo ra một môi trường truyền tải dữ liệu an toàn giữa thiết bị di động và máy chủ.

VIII. Kết luận

Lỗi không sử dụng HTTPS và lỗ hổng MiTM trong ứng dụng FAP có thể gây ra hậu quả nghiêm trọng cho người dùng và ứng dụng. Để đảm bảo tính bảo mật và bảo vệ thông tin cá nhân của người dùng, việc triển khai giao thức HTTPS, sử dụng chứng chỉ SSL/TLS hợp lệ, sử dụng VPN và kiểm tra tính toàn vẹn dữ liệu là thực sự cần thiết. Bằng cách áp dụng những giải pháp này, chúng ta có thể nâng cao tính bảo mật và đáng tin cậy của ứng dụng FAP, đồng thời tăng cường niềm tin và sự hài lòng của người dùng