BÁO CÁO ĐỒ ÁN

**Môn học: BẢO MẬT WEB VÀ ỨNG DỤNG**

**Tên chủ đề:**

**SSRF (Server-side Request Forgegy)**

*GVHD: ThS. Nguyễn Công Danh*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.P12.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hồ Vỉ Khánh | 22520633 | 22520633@gm.uit.edu.vn |
| 2 | Lê Công Danh | 22520199 | 22520199@gm.uit.edu.vn |
| 3 | Nguyễn Hữu Bình | 22520132 | 22520132@gm.uit.edu.vn |
| 4 | Phạm Trường Thiên Ân | 22520028 | 22520028@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 |  | 100% |
| 2 |  | 100% |
| 3 |  | 100% |
| 4 |  | 90% |
| 5 |  | 60% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## THÔNG TIN DỰ ÁN

Lỗ hổng bảo mật: SSRF (Server-side Request Forgegy).

## BÁO CÁO TỔNG QUÁT

**Server-side Request Forgery (SSRF)** – giả mạo yêu cầu phía máy chủ là một lỗ hổng bảo mật mà nó cho phép kẻ tấn công sửa đổi tham số trong yêu cầu gửi đi để khiến máy chủ thực hiện truy xuất đến một miền tùy ý mà đó có thể là các dịch vụ nằm trong nộ bộ như là cơ sở dữ liệu,...

Tấn công Server-Side Request Forgery (SSRF) liên quan đến việc kẻ tấn công lợi dụng chức năng máy chủ để truy cập hoặc sửa đổi tài nguyên. Kẻ tấn công nhắm mục tiêu vào ứng dụng hỗ trợ nhập dữ liệu từ URL hoặc cho phép chúng đọc dữ liệu từ URL. URL có thể bị thao túng, bằng cách thay thế chúng bằng URL mới hoặc bằng cách can thiệp vào quá trình duyệt đường dẫn URL.

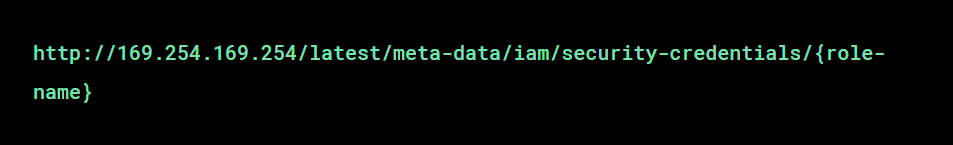
Thông thường, kẻ tấn công cung cấp một URL (hoặc sửa đổi URL hiện có) và mã chạy trên máy chủ sẽ đọc hoặc gửi dữ liệu đến URL đó. Kẻ tấn công có thể tận dụng URL để truy cập vào dữ liệu và dịch vụ nội bộ không được phép tiết lộ – bao gồm cơ sở dữ liệu hỗ trợ HTTP và dữ liệu cấu hình máy chủ.

Khi kẻ tấn công đã can thiệp vào yêu cầu, máy chủ sẽ nhận được yêu cầu đó và cố gắng đọc dữ liệu vào URL đã thay đổi. Ngay cả đối với các dịch vụ không được hiển thị trực tiếp trên internet công cộng, kẻ tấn công vẫn có thể chọn một URL mục tiêu, cho phép chúng đọc dữ liệu.

**Rủi ro về SSRF:** Hậu quả mà SSRF gây ra có thể gây ra hoàn toàn phụ thuộc vào cấu hình của hệ thống và sự sáng tạo của kẻ tấn công. Sau đây sẽ là một số rủi ro phổ biến ở SSRF:

* **Data Exposure:**

Một trong những ví dụ phổ biến nhất về cuộc tấn công SSRF là truy cập vào thông tin xác thực của phiên bản Amazon EC2. Nếu vai trò IAM được gán cho phiên bản EC2, thông tin xác thực tạm thời có thể được truy cập bằng cách hoàn tất yêu cầu tới:



Mức độ thiệt hại mà kẻ tấn công có thể gây ra phụ thuộc vào mức độ truy cập được cấp cho vai trò IAM. Quyền của vai trò càng cao thì mức độ vi phạm càng lớn.

Đối với máy chủ ứng dụng, điều này có xu hướng chỉ ra rằng, ít nhất, tội phạm mạng sẽ có khả năng truy xuất thông tin khách hàng. Nếu cấp quá nhiều quyền cho vai trò IAM, kẻ tấn công có thể thực thi mã từ xa trên các phiên bản EC2 trong tài khoản AWS của mục tiêu.

* Reconnaissance:

Một biện pháp bảo mật phổ biến được sử dụng để giảm thiểu bề mặt tấn công từ các mạng bên ngoài là hạn chế sử dụng các máy chủ công khai. Các máy chủ còn lại được dành riêng cho giao tiếp nội bộ. SSRF cho phép kẻ tấn công thực hiện quét và thu thập thông tin về các mạng nội bộ. Khi kẻ tấn công đã có quyền truy cập vào máy chủ, chúng có thể sử dụng thông tin này để xâm phạm các máy chủ khác trong mạng.

* Port Scans or Cross Site Port Attack (XSPA):

Các cuộc tấn công SSRF không phải lúc nào cũng trả lại dữ liệu cho kẻ tấn công. Tuy nhiên, thời gian phản hồi hoặc siêu dữ liệu khác có thể cho phép kẻ tấn công xác định xem yêu cầu có thành công hay không. Nếu có thể xác định được cổng và máy chủ, kẻ tấn công có thể quét cổng mạng của máy chủ ứng dụng bằng cách tận dụng siêu dữ liệu này trong Tấn công cổng chéo trang web (XSPA).

Thời gian chờ cho kết nối mạng thường không thay đổi, bất kể máy chủ hay cổng. Do đó, kẻ tấn công có thể thử một yêu cầu mà chúng biết sẽ được lưu trữ và sử dụng điều này làm cơ sở cho thời gian phản hồi trong tương lai. Các yêu cầu thành công có xu hướng ngắn hơn đáng kể so với cơ sở này và đôi khi dài hơn nếu kết nối được thiết lập không được bảo mật bởi một trong các bên.

Bằng cách này, kẻ tấn công có thể lấy dấu vân tay các dịch vụ đang được thực hiện trên mạng, cho phép chúng bắt đầu các cuộc tấn công buôn lậu giao thức.

* Denial of Service (DoS):

Lượng yêu cầu mà máy chủ nội bộ nhận được thường thấp hơn lưu lượng truy cập đến máy chủ công cộng. Do đó, chúng được cấu hình để sử dụng băng thông thấp hơn. Tội phạm mạng có thể sử dụng SSRF để làm ngập máy chủ nội bộ bằng lượng truy cập lớn nhằm chiếm dụng băng thông của chúng, dẫn đến tấn công DoS nội bộ .

Ngoài các cuộc tấn công phổ biến này, tội phạm mạng có thể sử dụng SSRF để thực hiện các hành động độc hại hoặc trái phép hoặc nhúng phần mềm độc hại . Các tổ chức càng có nhiều kiến ​​thức về những rủi ro này thì chúng càng trở nên đáng báo động. Tuy nhiên, có những biện pháp bạn có thể thực hiện để ngăn chặn các cuộc tấn công này.

* Remote Code Excution (RCE):

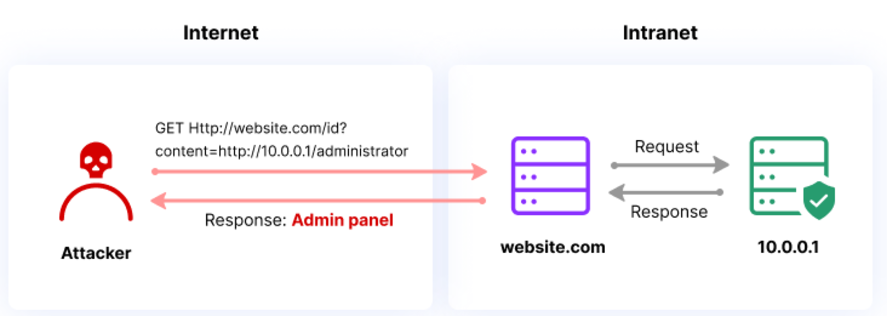
Một số dịch vụ hiện đại được thiết kế để giao tiếp hoàn toàn thông qua các truy vấn HTTP. Do đó, việc kiểm soát không giới hạn URL có thể cho phép tội phạm mạng khai thác một số dịch vụ nhất định, có thể dẫn đến bất kỳ điều gì—thậm chí là thực thi mã từ xa trên máy chủ cốt lõi (một ví dụ nổi tiếng là Redis).

Nguyên nhân: do một số tài nguyên trong một ứng dụng web cần được lấy từ bên ngoài, các yêu cầu phái máy chủ được sử dụng để tìm nạp tài nguyên và đưa nó vào ứng dụng web nhưng lại không kiểm soát chặt chẽ yêu cầu tìm nạp tài nguyên đó, cho phép kẻ tấn công có thể hoàn toàn kiểm soát yêu cầu tìm nạp tìa nguyên đến bất kì đâu ngay cả những nơi có chứa dữ liệu nhạy cảm. Trong một vài trường hợp khác, máy chủ cho phép người dùng gửi đến 1 đường dẫn url với mục đích lấy dữ liệu đầu vào do người dùng cung cấp, nhưng do không kiểm soát chặt chẽ đầu vào đó của người dùng dẫn đến những hậu quả như máy chủ bị cài backdoor, RCE,...

Các loại tấn công SSRF: Các cuộc tấn công SSRF thường khai thác mối quan hệ tin cậy trong chính máy chủ (được gọi là cuộc tấn công SSRF của máy chủ) hoặc giữa máy chủ và các hệ thống phụ trợ khác (được gọi là cuộc tấn công SSRF của máy chủ).

* Server SSRF Attacks: SSRF có thể giả mạo yêu cầu để truy xuất đến các miền khác nhau trong nội bộ hệ thống và nó bao gồm luôn cả chính máy chủ của nó.

Trong một cuộc tấn công SSRF máy chủ, kẻ tấn công khai thác một quy trình trong đó trình duyệt hoặc hệ thống máy khách khác truy cập trực tiếp vào URL trên máy chủ. Kẻ tấn công sẽ thay thế URL gốc bằng một URL khác, thường sử dụng IP 127.0.0.1 hoặc tên máy chủ "localhost", trỏ đến hệ thống tệp cục bộ trên máy chủ. Dưới tên máy chủ này, kẻ tấn công tìm thấy một đường dẫn tệp dẫn đến dữ liệu nhạy cảm .



Ví dụ, trên một trang web thời tiết, ứng dụng web sẽ truy vấn máy chủ của mình để hiển thị dự báo thời tiết hiện tại. Nó có thể thực hiện việc này bằng cách sử dụng REST API, truyền URL có yêu cầu API từ trình duyệt của người dùng đến máy chủ. Yêu cầu có thể trông như thế này:

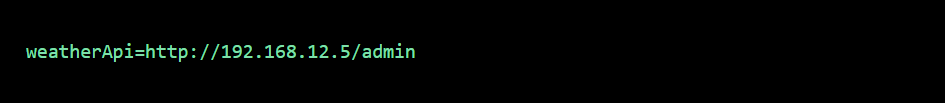


Điều này sẽ khiến máy chủ hiển thị nội dung của thư mục /admin cho kẻ tấn công. Vì yêu cầu được thực hiện trong hệ thống tệp của máy chủ nên nó bỏ qua các biện pháp kiểm soát truy cập thông thường và tiết lộ thông tin ngay cả khi kẻ tấn công không được ủy quyền.

* Back-End SSRF attacks: tương tự như trên nhưng lần này hacker tấn công vào một miền nằm trong sự kiểm soát của máy chủ, khó khăn hơn với việc cần phải tìm chính xác được địa chỉ của miền mà muốn tấn công vào.

Một biến thể khác của SSRF là khi máy chủ có mối quan hệ đáng tin cậy với một thành phần phụ trợ. Nếu khi máy chủ kết nối với thành phần đó, nó có toàn quyền truy cập, kẻ tấn công có thể tạo yêu cầu giả mạo và truy cập vào dữ liệu nhạy cảm hoặc thực hiện các hoạt động trái phép. Các thành phần phụ trợ thường có bảo mật yếu vì chúng được coi là được bảo vệ bên trong chu vi mạng.

Tiếp tục ví dụ trước, kẻ tấn công có thể thay thế lệnh gọi API bằng:



Nếu máy chủ kết nối với một thành phần phụ trợ trên địa chỉ IP 192.168.12.5 và được phép truy cập vào thư mục /admin trên hệ thống tệp của thành phần đó, kẻ tấn công cũng có thể truy cập và xem nội dung của thư mục đó.

* SSRF Blind: tương tự, kẻ tấn công gửi yêu cầu giả mạo và phía máy chủ thực thi nó nhưng thay vì trả lại kết quả như bình thường thì nó lại không trả về bất cứ thứ gì. Để nhận biết được một lỗ hổng SSRF Blind, thông thường chúng ta sẽ thêm vào những payload độc hại một cách “may rủi”, nếu gặp may thì kẻ tấn công sẽ thắng.

**Giảm thiểu việc làm giả yêu cầu phía máy chủ:**

* Người ta thường áp dụng các biểu thức chính quy và danh sách đen đơn giản cho dữ liệu đầu vào của người dùng để giảm thiểu SSRF và các cuộc tấn công tương tự. Tuy nhiên, nói chung, danh sách đen là một phương pháp kiểm soát bảo mật không hiệu quả. Kẻ tấn công có thể dễ dàng tìm ra cách để vượt qua chúng. Ví dụ, tội phạm mạng có thể sử dụng dịch vụ DNS ký tự đại diện, chuyển hướng HTTP hoặc mã hóa IP thay thế.

Cách ngăn chặn:

* Lọc kĩ đầu vào của mỗi yêu cầu bằng cách sử dụng Whitelist (danh sách hợp lệ) thay vì Blacklist (danh sách không hợp lệ).
* Whitelist là những gì được phép truy cập còn Blacklist là những gì không được phép. Dễ thấy kiến thức hay những câu lệnh là bao la vì vậy chúng ta không thể nào chặn được hết các trường hợp, do đó chúng ta nên sử dụng Whitelist hơn.

## BÁO CÁO CHI TIẾT

## DEMO

## PHẦN MỞ RỘNG A: THÔNG TIN ĐÁNH GIÁ

## PHẦN MỞ RỘNG B: PHÂN LOẠI RỦI RO

Các bước thực hiện/ Phương pháp thực hiện/Nội dung tìm hiểu (Ảnh chụp màn hình, có giải thích)

---

**HẾT**

1. Ghi nội dung công việc [↑](#footnote-ref-1)