Webshell là một loại phần mềm độc hại được sử dụng để kiểm soát máy tính của nạn nhân thông qua các lệnh, thường được viết bằng các ngôn ngữ như PHP, ASP, JSP, Perl, Python và Ruby. Webshell cho phép kẻ tấn công thực hiện các hành động như thêm, xóa, chỉnh sửa tệp tin, chạy mã độc, thu thập thông tin và kiểm soát máy tính của nạn nhân.

Khi máy chủ bị nhiễm webshell, kẻ tấn công có thể truy cập từ xa vào hệ thống thông qua trình duyệt web hoặc các công cụ quản lý tệp.

**Các loại webshell**

1. **Cmd shell**: Đây là loại webshell có khả năng thực thi các lệnh thông qua giao diện dòng lệnh của hệ điều hành, thường sử dụng hàm shell\_exec.
2. **HTTP Tunnel**: Loại webshell này sử dụng giao thức HTTP để truyền lệnh từ kẻ tấn công đến máy chủ và nhận phản hồi qua các yêu cầu HTTP. Nó có thể vượt qua các biện pháp bảo vệ như tường lửa hoặc cơ chế an ninh ngăn chặn kết nối bất thường.
3. **Chooper**: Là một loại webshell cho phép thực hiện các hành vi độc hại và kiểm soát từ xa các hệ thống đã bị xâm nhập. Với kích thước nhỏ, nó rất khó bị phát hiện.
4. **Upload shell**: Đây là kỹ thuật mà kẻ tấn công tải lên một đoạn mã độc (webshell) thông qua tính năng tải tệp của ứng dụng web. Khi webshell được tải lên thành công và kích hoạt, kẻ tấn công có thể kiểm soát máy chủ từ xa, thực thi các lệnh hệ thống, truy cập tệp tin hoặc cài đặt phần mềm độc hại.