TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO
ĐỒ ÁN TỐT NGHIỆP

Đề tài:

NGHIÊN CỨU VÀ XÂY DỰNG MÃ KHAI THÁC LỖ HỔNG PROTOTYPE POLLUTION

Giảng viên hướng dẫn: VŨ VIỆT DŨNG
Sinh viên thực hiện: CAO XUÂN SANG
MSSV: DTC175524802990008
Chuyên ngành: An Toàn Thông Tin
Môn học: Đồ Án Tốt Nghiệp

Thái Nguyên, tháng 1 năm 2022

NHIỆM VỤ ĐỒ ÁN TỐT NGHIỆP

Họ và tên**:** **Cao Xuân Sang** MSSV: **DTC175524802990008**

Chuyên ngành: **AN TOÀN THÔNG TIN** Lớp: **ATTT-K16A**

Emai: **sang999hb@gmail.com** SĐT: **0334760905**

Tên đề tài: **Nghiên cứu và xây dựng mã khai thác lỗ hổng Prototype pollution**

Giảng viên hướng dẫn: **Vũ Việt Dũng**

Thời gian thực hiện: ***25/10/2021*** *đến ngày:* ***21/01/2022***

Nhiệm vụ/nội dung:

Chương I: Tổng quan về an ninh mạng, giới thiệu về JavaScript và Node.js

Chương II: Lỗ hổng Prototype pollution

Chương III: Thực nghiệm khai thác lỗ hổng Prototype pollution

TRƯỞNG BỘ MÔN
(Ký và ghi rõ họ tên)

GIÁO VIÊN HƯỚNG DẪN
(Ký và ghi rõ họ tên)

LỜI CẢM ƠN

Lời đầu tiên em xin cảm ơn thầy Vũ Việt Dũng đã giúp đỡ và hướng dẫn nhiệt tình cho em trong suốt thời gian em làm báo cáo này.

Tiếp theo em xin cảm ơn quý thầy cô trong trường ĐH CNTT&TT Thái Nguyên đã giảng dạy và truyền cảm hứng đến tất cả những sinh viên như em, để chúng em có thêm nhiều kiến thức, mở mang thêm cách tư duy, sáng tạo trong cuộc sống.

Với những kiến thức còn thiếu sót, những kỹ năng còn hạn hẹp, em không thể tránh được những sai lầm, em mong thầy cô có thể thông cảm và bỏ qua cho em.

Xin cảm ơn bạn bè, những người đã cùng em sánh bước, đã đóng góp, động viên em những lúc gặp khó khăn, tạo điều kiện giúp em hoàn thành tốt đề tài này.

Lời cuối cùng em xin gửi lời cảm ơn sâu sắc nhất và chúc thầy cô luôn dồi dào sức khỏe, tiếp tục giảng dạy hết tâm huyết của mình cho những lứa học trò sau này để đất nước ta ngày càng có nhiều nhân tài, những người giỏi trong các doanh nghiệp, xây dựng đất nước phát triển hơn nữa.

Thái Nguyên, Tháng 01 năm 2022

Sinh viên

Cao Xuân Sang

MỤC LỤC

DANH MỤC HÌNH ẢNH

LỜI MỞ ĐẦU

Cùng với sự phát triển của công nghệ thông tin, công nghệ mạng máy tính và sự phát triển của mạng Internet ngày càng đa dạng và phong phú. Các dịch vụ, ứng dụng Web đã thâm nhập vào hầu hết các lĩnh vực trong đời sống xã hội. Các thông tin trên Internet cũng đa dạng về nội dung và hình thức, trong đó có rất nhiều thông tin cần được bảo mật cao hơn bởi tính kinh tế, tính chính xác và tính tin cậy của nó.

Bên cạnh đó, các hình thức phá hoại ứng dụng Web cũng trở nên tinh vi và phức tạp hơn. Do đó đối với mỗi hệ thống, nhiệm vụ bảo mật được đặt ra cho người quản trị mạng là hết sức quan trọng và cần thiết. Xuất phát từ những thực tế đó, bài viết sẽ đi tìm hiểu về kỹ thuật tấn công Prototype pollution và các cách phòng chống loại tấn công này.

Việc nghiên cứu kỹ thuật tấn công Prototype pollution, cách bảo mật loại tấn công này với mong muốn góp một phần sức nhỏ vào việc nghiên cứu và tìm hiểu về các vấn đề an ninh mạng giúp cho việc học tập và nghiên cứu.

Lý do chọn đề tài

Trong những năm gần đây, Việt Nam ngày càng phát triển về mặt công nghệ thông tin, đặc biệt là về ứng dụng Web. Hầu hết mọi người ai cũng từng nghe và làm việc trên ứng dụng Web. Website trở nên phổ biến và trở thành một phần quan trọng của mọi người và nhất là các doanh nghiệp, công ty. Bên cạnh lý do an toàn, bảo mật cho ứng dụng Web luôn là vấn đề nan giải cho người quản trị Website, một trong những lỗ hổng nguy hiểm và phổ biến gần đây là lỗ hổng Prototype pollution, luôn tạo ra các khó khăn đối với các lập trình viên website. Chính vì lẽ đó, bài đồ án tốt nghiệp đã đi vào tìm hiểu một kỹ thuật tấn công Prototype pollution và xây dựng mã khai thác nhằm mục đích tìm hiểu sâu hơn về kỹ thuật tấn công, phòng thủ trước loại tấn công này, và sau đó là chia sẻ kiến thức với mọi người.

Mục tiêu

Hiểu cách thức tấn công và phòng chống tấn công lỗ hổng Prototype pollution, xây dựng thành công mã khai thác lỗ hổng Prototype pollution

Phạm vi

Tìm hiểu các kỹ thuật tấn công, cách bảo mật, phòng thủ của kỹ thuật tấn công Prototype pollution một cách tổng quan nhất.

Bố cục của đồ án tốt nghiệp

Nội dung của báo cáo bao gồm các phần sau:

- Chương I: Tổng quan về an ninh mạng, giới thiệu về JavaScript và Node.js
- Chương II: Lỗ hổng Prototype pollution
- Chương III: Thực nghiệm khai thác lỗ hổng Prototype pollution
- KẾT LUẬN: Trình bày các kết quả đạt được.