

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

Phân tích các kỹ thuật tấn công bộ nhớ đệm trên môi trường Web và biện pháp phòng ngừa

Nguyễn Đức Chung

chung.nd204817@sis.hust.edu.vn

Ngành: Kỹ thuật Máy tính

Giảng viên hướng dẫn: TS. Lê Xuân Thành

Chữ kí GVHD

Khoa:

Kỹ thuật Máy tính

Trường:

Công nghệ Thông tin và Truyền thông

HÀ NỘI, 06/2024

LỜI CAM KẾT

Họ và tên sinh viên: Nguyễn Đức Chung

Điện thoại liên lạc: 0387682103

Email: chung.nd204817@sis.hust.edu.vn

Lớp: Kỹ Thuật Máy Tính 02 - K65

Hệ đào tạo: Cử nhân

Tôi – *Nguyễn Đức Chung* – cam kết Đồ án Tốt nghiệp (ĐATN) là công trình nghiên cứu của bản thân tôi dưới sự hướng dẫn của *TS. Lê Xuân Thành*. Các kết quả nêu trong ĐATN là trung thực, là thành quả của riêng tôi, không sao chép theo bất kỳ công trình nào khác. Tất cả những tham khảo trong ĐATN – bao gồm hình ảnh, bảng biểu, số liệu, và các câu từ trích dẫn – đều được ghi rõ ràng và đầy đủ nguồn gốc trong danh mục tài liệu tham khảo. Tôi xin hoàn toàn chịu trách nhiệm với dù chỉ một sao chép vi phạm quy chế của nhà trường.

Hà Nội, ngày tháng năm

Tác giả ĐATN

Nguyễn Đức Chung

LỜI CẢM ƠN

Tôi xin cảm ơn chân thành tới gia đình đã luôn đồng hành, ủng hộ và giúp đỡ tôi trong quá trình học tập cho tới khi hoàn thành đồ án tốt nghiệp tại trường.

Tôi gửi lời cảm ơn sâu sắc đến thầy TS. Lê Xuân Thành đã dành thời gian và công sức hướng dẫn và giúp đỡ tôi trong quá trình làm đồ án này.

Cảm ơn bạn bè đã cùng đồng hành, giúp đỡ và chia kiến thức với tôi, giúp tôi tiến bộ hơn trong học tập, đồng thời thu nhận được nhiều kiến thức có ích cho tương lai.

Cuối cùng, tôi xin gửi lời cảm ơn tới Trường Công nghệ Thông tin và Truyền thông - Đại học Bách khoa Hà Nội đã tạo điều kiện thuận lợi và cung cấp kiến thức chất lượng để tôi phát triển và hoàn thành đồ án tốt nghiệp.

Chân thành cảm ơn mọi người.

TÓM TẮT NỘI DUNG ĐỒ ÁN

Cuộc cách mạng công nghiệp 4.0 đang diễn ra với sự phát triển mạnh mẽ của công nghệ thông tin trong đó máy tính và mạng máy tính đóng vai trò quan trọng không thể thiếu trong thế giới hiện đại. Ngày nay khi có đến 67,1% [1] người sử dụng Internet trên toàn cầu. Điều này đặt ra thách thức không nhỏ tới sự an toàn và bảo mật khi tham gia vào môi trường này khi ngày càng nhiều các cuộc tấn công từ tội phạm mạng nhắm vào người dùng. Để hạn chế và ngăn chặn những hành vi phạm pháp trên không gian mạng, các chuyên gia an ninh mạng trên thế giới đang nỗ lực nghiên cứu các phương pháp tấn công và các giải pháp bảo vệ sự an toàn của trường mạng. Trong đồ án này, tôi tập trung vào việc phân tích các kỹ thuật tấn công bộ nhớ đệm trên môi trường Web và đưa ra biện pháp giải quyết. Đóng góp chính của đồ án là cung cấp một cái nhìn tổng quan về các kỹ thuật tấn công bộ nhớ đệm trên môi trường Web và đề xuất các biện pháp phòng ngừa cụ thể. Kết quả đạt được là một số giải pháp hiệu quả giúp bảo vệ các ứng dụng Web khỏi các cuộc tấn công bộ nhớ đệm. Đồng thời, thông qua đồ án, hy vọng có thể đóng góp vào việc nâng cao nhận thức về an ninh mạng và tạo ra một môi trường trực tuyến an toàn hơn cho mọi người.

Sinh viên thực hiện
(Ký và ghi rõ họ tên)

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....	1
1.1 Đặt vấn đề.....	1
1.2 Đóng góp của đề án	1
1.3 Bố cục đề án	2
CHƯƠNG 2. NỀN TẢNG LÝ THUYẾT	3
2.1 Các kiến thức tổng quan về cache server	3
2.1.1 Khái niệm cache server.....	3
2.1.2 Cơ chế hoạt động của cache server.....	4
2.1.3 Dấu hiệu nhận biết	4
2.1.4 Cache rule	5
2.2 Các kiến thức tổng quan về cache browser.....	7
2.2.1 Khái niệm cache browser	7
2.2.2 Service worker.....	7
2.2.3 Tương tác giữa service worker và cache của trình duyệt.....	8
2.2.4 Quy trình hoạt động của service worker	8
2.3 Các kiến thức liên quan khác	11
2.3.1 Kỹ thuật tấn công XSS.....	11
2.3.2 Dịch vụ lưu trữ đám mây	12
CHƯƠNG 3. KỸ THUẬT TẤN CÔNG	13
3.1 Tấn công vào cache server	13
3.1.1 Tấn công lừa đảo bộ đệm	13
3.1.2 Tấn công ngộ độc bộ đệm	19
3.2 Tấn công vào cache browser.....	20

CHƯƠNG 4. BIỆN PHÁP PHÒNG NGỪA.....	29
4.1 Biện pháp phòng ngừa cuộc tấn công vào cache server.....	29
4.2 Biện pháp phòng ngừa cuộc tấn công vào cache browser	30
CHƯƠNG 5. KẾT LUẬN	33
5.1 Kết luận.....	33
5.2 Hướng phát triển trong tương lai	33
TÀI LIỆU THAM KHẢO.....	34

DANH MỤC HÌNH VẼ

Hình 2.1	Mô hình hoạt động của cache server [2]	3
Hình 2.2	Cơ chế hoạt động [3]	4
Hình 2.3	Dấu hiệu nhận biết khi dữ liệu được lưu trữ	5
Hình 2.4	Tùy chọn cache keys của cloud flare	6
Hình 2.5	Ví dụ về cache rule	6
Hình 2.6	Tệp tin khi chưa được lưu trữ	7
Hình 2.7	Tệp tin khi đã được lưu trữ	7
Hình 2.8	Đăng ký service worker	8
Hình 2.9	Lưu trữ dữ liệu vào bộ đệm trình duyệt	9
Hình 2.10	Xử lý dữ liệu trả về	9
Hình 2.11	kiểm tra cài đặt	10
Hình 2.12	Kiểm tra vận hành	10
Hình 2.13	Ví dụ minh họa XSS [4]	11
Hình 2.14	Minh họa về đường dẫn trong Amazon S3 [5]	12
Hình 2.15	Minh họa về Presigned URL	12
Hình 3.1	Mô hình tấn công lừa đảo bộ đệm	13
Hình 3.2	Lưu trữ thành công dữ liệu bằng tệp tin tĩnh	14
Hình 3.3	Lưu trữ thất bại dữ liệu bằng tệp tin tĩnh	15
Hình 3.4	Cấu trúc URL	15
Hình 3.5	Luồng xử lý URL	16
Hình 3.6	Thông tin cá nhân người dùng	17
Hình 3.7	Kiểm tra cache rule (i)	17
Hình 3.8	Kiểm tra cache rule (ii)	18
Hình 3.9	Kiểm tra dữ liệu đã lưu trữ	18
Hình 3.10	Mô hình tấn công ngộ độc bộ đệm [6]	19
Hình 3.11	Self-XSS trên User-Agent	20
Hình 3.12	Lưu trữ XSS trên cache server	20
Hình 3.13	Môi trường giả định	21
Hình 3.14	Giao diện nhấn tin	21
Hình 3.15	Giao diện nội dung tin nhắn	22
Hình 3.16	Tệp tin trên Cloud Storage truy cập thông qua đường dẫn	22
Hình 3.17	Mã nguồn chuyển tiếp đường dẫn tới máy chủ kẻ tấn công	23
Hình 3.18	Luồng hoạt động chuyển tiếp dữ liệu	23
Hình 3.19	Mã nguồn khai báo lưu trữ dữ liệu	24

Hình 3.20	Mã nguồn đăng ký service worker và tạo cookie	24
Hình 3.21	Luồng hoạt động khi người dùng mở dữ liệu của kẻ tấn công .	25
Hình 3.22	Luồng hoạt động khi người dùng mở dữ liệu cá nhân	25
Hình 3.23	Tải lên tệp tin điều hướng tới máy chủ kẻ tấn công	26
Hình 3.24	Tải lên tệp tin khai báo service worker	26
Hình 3.25	Tải lên tệp tin SVG độc hại	27
Hình 3.26	Giao diện gửi tệp tin độc hại cho người dùng	27
Hình 3.27	Tệp tin trước khi bấm vào được dẫn độc hại	27
Hình 3.28	Tệp tin sau khi bấm vào đường dẫn độc hại	28
Hình 3.29	Presigned URL được gửi về máy chủ của kẻ tấn công	28
Hình 4.1	Mô hình website	29
Hình 4.2	Tạo cache rule bỏ qua lưu trữ	30
Hình 4.3	Thứ tự sắp xếp cache rule	30
Hình 4.4	Mô tả định dạng dữ liệu chỉ cho phép tải về	31
Hình 4.5	Đoạn mã minh họa ngăn chặn phần mở rộng trong danh sách cấm	31

DANH MỤC THUẬT NGỮ VÀ TỪ VIẾT TẮT

Thuật ngữ	Ý nghĩa
API	Giao diện lập trình ứng dụng (Application Programming Interface)
CDN	Mạng phân phối nội dung (Content Delivery Network)
CSS	Cascading Style Sheets
DOM	Mô hình Đối tượng Tài liệu (Document Object Model)
HTML	Ngôn ngữ đánh dấu siêu văn bản (HyperText Markup Language)
HTTP	Giao thức truyền tải siêu văn bản (Hypertext Transfer Protocol)
ID	Nhận dạng (Identification)
JSON	JavaScript Object Notation
URI	Uniform Resource Identifier
XML	Ngôn ngữ đánh dấu mở rộng (Extensible Markup Language)
XSS	Cross Site Scripting