7. Real Time Streaming Protocol (RTSP). RFC 2326 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2326 – Дата звернення: 21.10.2025.

УДК 004.056.5:004.738.5

В. Ю. Кащин, Т.А. Лечаченко доктор філософії
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ ВРАЗЛИВОСТЕЙ HTTP REQUEST SMUGGLING ЗАСОБАМИ ДИФЕРЕНЦІАЛЬНОГО ФАЗЗИНГУ HTTP-ЗАПИТІВ

V. Kashchyn, T. Lechachenko Ph.D.

ANALYSIS OF HTTP REQUEST SMUGGLING VULNERABILITIES USING DIFFERENTIAL FUZZING OF HTTP REQUESTS

Вразливості типу HTTP Request Smuggling (HRS) залишаються однією з найнебезпечніших загроз для багаторівневих вебінфраструктур, у яких трафік послідовно проходить через балансувальники навантаження, проксі-сервери, брандмауери та бекенд-сервери [1]. Їхня природа полягає не у помилці окремого вебсервера, а в неузгодженості трактування структур HTTP/1.1-запитів різними компонентами ланцюга обробки. Конфлікт між заголовками Content-Length і Transfer-Encoding: chunked, а також неоднозначна обробка CRLF/LF-роздільників створюють умови, за яких один вузол вважає запит завершеним, тоді як інший продовжує читати потік як частину того самого або нового повідомлення. Це відкриває можливість інжекції прихованих запитів, обходу контролю доступу, отруєння кешу та реалізації DoS-сценаріїв.

Метою дослідження є експериментальне виявлення та класифікація уразливостей HTTP Request Smuggling шляхом застосування диференціального фазингу HTTP/1.1-запитів з використанням утиліти HTTP Request Smuggler у складі Burp Suite [2]. Для цього побудовано ізольований тестовий стенд типу Client → Nginx (reverse proxy) [3] → Apache HTTP Server (backend) [4], розгорнутий на віртуальних машинах під керуванням гіпервізора KVM [5] у середовищі Ubuntu Linux. Nginx налаштовано як зворотний проксі з акцентом на обробці конфліктних заголовків Content-Length і Transfer-Encoding, Apache виступає бекендом із власною логікою визначення меж тіла HTTP-повідомлень. У дослідженні сформовано репрезентативний набір HTTP/1.1-запитів із варіативними заголовками та роздільниками рядків: класичні CL- та TE-запити, конфліктні вектори CL.TE та TE.CL, дубльовані Content-Length із різними значеннями, подвійні Transfer-Encoding, некоректні або неповні заголовки, а також змішані варіанти CRLF/LF. Диференціальний фазинг реалізовано як багаторазове відтворення цих шаблонів через Burp Suite з HTTP Request Smuggler у напрямку Nginx → Apache з паралельною фіксацією артефактів. Для реєстрації результатів використано розширене логування access/error на обох серверах і перехоплення трафіку інструментом tshark у форматі pcap, що забезпечило повну картину обробки кожного запиту на мережевому й прикладному рівнях.

Отримані результати демонструють, що для ряду конфігурацій виникають стійкі парсингові розбіжності між Nginx і Apache. Для векторів CL.TE та TE.CL показано сценарії, за яких проксі орієнтується на Content-Length, а бекенд - на Transfer-Encoding: chunked, або навпаки, унаслідок чого в межах одного TCP-з’єднання з’являється «прихований» GET-запит, що фактично минає первинний рівень контролю. У випадку

дубльованих Content-Length виявлено ситуації, коли один компонент бере перше значення, інший - останнє, що призводить до розділення потоку на валідний та некоректний запити. Для змішаних CRLF/LF-варіантів зафіксовано випадки, коли Nginx приймає LF як допустимий роздільник, тоді як Apache повертає 400 Bad Request через некоректне завершення секції заголовків, що також відображає критичну асиметрію трактувань.

Диференціальний фазинг у поєднанні з HTTP Request Smuggler є ефективним підходом до систематичного виявлення HRS-вразливостей у багаторівневих вебінфраструктурах. Запропонована методика дозволяє не лише виявляти конкретні експлуатаційні сценарії CL.TE, TE.CL і CRLF-інжекцій у типових зв'язках Nginx–Apache, але й формалізувати критерії парсингових розбіжностей для подальшого впровадження превентивних заходів, зокрема жорсткішої валідації заголовків, уніфікації політики обробки Content-Length/Transfer-Encoding та суворого дотримання стандартів HTTP/1.1 у проміжних вузлах.

Література

1. Exploiting and Preventing HTTP Request Smuggling. VAADATA - Ethical Hacking Services. URL: https://www.vaadata.com/blog/what-is-http-request-smuggling-exploitations-and-security-best-practices/ (date of access: 30.11.2025).

2. What is HTTP request smuggling? Tutorial & Examples | Web Security Academy. Web Application Security, Testing, & Scanning - PortSwigger. URL: https://portswigger.net/web-security/request-smuggling (date of access: 30.11.2025).

3. NGINX Reverse Proxy | NGINX Documentation. NGINX Documentation. URL: https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/ (date of access: 30.11.2025).

4. Documentation: Apache HTTP Server - The Apache HTTP Server Project. Welcome! - The Apache HTTP Server Project. URL: https://httpd.apache.org/docs/ (date of access: 30.11.2025).

5. Interactive cybersecurity training system based on simulation environments / D. Tymoshchuk et al. Measuring and computing devices in technological processes. 2024. No. 4. P. 215–220. URL: https://doi.org/10.31891/2219-9365-2024-80-26 (date of access: 30.11.2025).

УДК 004.7:681.518:004.89

С.Б. Кіт, В.Р. Перун, С.І. Перун, Г.В. Шимчук
(Тернопільський національний технічний університет імені Івана Пулюя)

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНТРОЛЮ ПАРАМЕТРІВ МІКРОКЛІМАТУ В ЖИТЛОВОМУ ПРИМІЩЕННІ З ВИКОРИСТАННЯМ БСМ

S.B. Kit, V.R. Perun, S.I. Perun, G.V. Shymchuk

INTELLIGENT SYSTEM FOR CONTROLLING MICROCLIMATE PARAMETERS IN A RESIDENTIAL PREMISES USING BSM

Мікроклімат житлового приміщення безпосередньо впливає на самопочуття людини, працездатність і ризики респіраторних захворювань. У квартирах типові проблеми пов'язані з нерівномірним прогрівом кімнат, локальними зонами підвищеної вологості (кухня/ванна), накопиченням CO_2 у спальнях та появою летких органічних сполук (VOC) від меблів і побутової хімії. Тому актуальним є створення інформаційної