HTTP REQUEST SMUGGLING ATTACKS

Team Members:
Taha Adeel Mohammed CS20BTECH11052
Shambhu Prasad Kavir
CS20BTECH11045

T.A. Mentor(s):
Harinder Kaur

Problem Statement

- HTTP request smuggling allows attackers to modify HTTP requests and responses between client and server and gain access to sensitive data.
- Over the years, this problem has become increasingly common and poses a significant threat to organizations relying on web applications.
- Explore, implement and analyze existing HRS attacks.
- Explore, implement and analyze existing mitigation techniques.
- Analyze varying vulnerability levels among different HTTP versions.
- Attempt to implement new mitigation techniques based on the existing techniques.

MOTIVATION

- While the problem of HRS attacks and their mitigation strategies have been known for sometime, there is still a wide scope for improvement.
- As technology advances, attackers keep coming up with newer and more innovative methods to perform such attacks.
- With the levels of internet traffic in today's time, the vulnerabilities have only gotten more severe.
- While many mitigation techniques persist, a lot of them have their own inadvertent consequences, such as hampering performance and preventing authorised traffic, so they can be improved upon by exploring better techniques.

Approach (1/2)

- Go through relevant articles and papers on HRS attacks.
- Set up a sandbox environment to perform experiments.
- Gain better understanding of HRS attacks by performing simulated attacks
- Analyze the impact of the attacks and varying vulnerabilities of different HTTP versions.
- Report findings for the same.

Approach (2/2)

- Implement existing mitigation strategies and analyze their results.
- Report findings for the same.
- Attempt to implement new mitigation techniques based on existing strategies.
- Attempt to perform attacks and analyze the results of the same on HTTP/3.

TIMELINES AND WORK DISTRIBUTION

Timeline	Student 1	student 2
Week i (March 27-)	Go through relevant articles and papers on HRS attacks. Prepare a project proposal.	Go through relevant articles and papers on HRS attacks. Set up a sandbox environment to perform HRS attacks.
Week i+1 (April 3-)	Gain better understanding. Performing HRS attacks in prepared sandbox environment. Prepare weekly report.	Gain better understanding. Perform HRS attacks in prepared sandbox environment. Prepare weekly report.
Week i+2 (April 10-)	Understand, perform and analyze existing detection and mitigation techniques of HRS. Prepare weekly report.	Understand perform and analyze existing detection and mitigation techniques of HRS. Prepare weekly report.
Week i+3 (April 17-, FINAL)	Attempt to implement new techniques based on existing techniques of mitigating HRS. Prepare final report.	Attempt to implement new techniques based on existing techniques of mitigating HRS. Prepare final report.
***Please note respective TA will evaluate your project on the basis of this timeline only.		

DELIVERABLES

- Links to github repositories considering codes and scripts used to simulate HRS.
- Reports containing methodology and analysis of the performed attacks.
- Links to repositories of detection and implementation of existing mitigation techniques.
- Reports with the methodology, observations, results and analysis of existing techniques.
- Links to repositories of attempted HRS techniques on HTTP/3 and why it did/did not work.
- Report containing the analysis of the impact of HRS on HTTP/3 and why it does/does not work.

Summary of Work Done (so far…) 1/2

Taha Adeel Mohammed:

- Went through relevant articles and papers on HRS attacks and their mitigation techniques.
- Explored existing implementations of HRS attacks and techniques of mitigating them.
- Set up a sandbox environment to perform HRS attacks.

Summary of Work Done (so far…) 2/2

Shambhu Prasad Kavir:

- Went through articles and papers on HRS attacks and their mitigation techniques.
- Narrowed down articles useful for the project.
- Prepared a project proposal.

REFERENCES

[1] Qi-Xian Huang, Min-Yi Chiu, Ying-Feng Chen, Hung-Min Sun, "Attacking Websites: Detecting and Preventing HTTP Request Smuggling Attacks", Security and Communication Networks, vol. 2022, Article ID 3121177, 14 pages, 2022. https://doi.org/10.1155/2022/3121177

[2] Mattias Grenfeldt, Asta Olofsson, Viktor Engstrom, and Robert Lagerström. “Attacking Websites Using HTTP Request Smuggling: Empirical Testing of Servers and Proxies”, 2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)

[3] Amit Klein, “HTTP Request Smuggling in 2020 – New Variants, New Defenses and New Challenges”, SafeBreach Labs

[4] PortSwigger’s HTTP Request Smuggling Article: https://portswigger.net/web-security/request-smuggling