Raj Sheth

rajsheth.cs28@gmail.com | +49 157 5829 9434
github.com/Raptor2807 | linkedin.com/in/raj-sheth-860136176
Saarbrücken, Germany

Profile

Master's student in **Cybersecurity** with hands-on experience analyzing HTTP traffic, understanding web attack vectors, and experimenting with WAF behaviour using tools like **WAFW00F**. Practical exposure to **OWASP Top 10**, request/response structure, header inspection, pattern-based detection, and simple **regex** matching in lab environments. Strong interest in web application security, WAF signature logic, and structured documentation of research findings.

Education

Saarland University, Saarbrücken, Germany **Oct 2022 – Present**

M.Sc. in Cybersecurity
Relevant Coursework: Web Security, Network Security, Secure AI, Cryptography, Statistical Learning Theory, Human–Computer Interaction

Gujarat Technological University, Ahmedabad, India **2018 – 2022**

B.E. in Information Technology
Bachelor project: simple automated spray-painting robot using Raspberry Pi and Arduino.

Experience

VMukti Solutions, Ahmedabad, India **Jan 2022 – May 2022**

Information Security Intern

- Assisted in preparing internal system documentation and basic security usage guidelines.
- Summarized technical instructions into clear, user-oriented notes.

Hands-On Security Practice **Ongoing**

- Conduct labs involving Nmap scanning, HTTP header inspection, Wireshark packet analysis, and basic Metasploit modules.
- Studied web attack vectors (SQL injection, XSS, directory traversal, file upload issues) and analyzed how requests appear at protocol level.
- Used **WAFW00F** to fingerprint WAF technologies, understand detection behaviours, and examine how different requests trigger or bypass rules in controlled labs.
- Practiced writing simple **regex patterns** for filtering suspicious payload traits.
- Completed all topics from provided Web/HTTP lecture slides: HTTP methods, status codes, cookies, sessions, parameters, content types, and request manipulation workflows.
- Maintain structured GitHub notes and Markdown documentation for each module.

Technical Skills

Programming & Scripting

Python, Bash (basic), Java (basic), C/C++ (basic), Git

Web Security & Detection Concepts

OWASP Top 10, HTTP/HTTPS fundamentals, request/response analysis, WAF fingerprinting (WAFW00F), pattern matching, regex, basic signature logic

Cybersecurity Tools

Nmap, Wireshark, Burp Suite (intro), Metasploit (intro), Snort (intro), WAFW00F

Systems

Linux (beginner to intermediate), Docker (basic familiarity)

Communication

Clear documentation, simplified explanations of technical topics, structured note-taking

Projects

Web Server Enumeration & HTTP Analysis (INE Labs)

- Explored HTTP headers, server banners, status codes, and error responses using curl, Metasploit scanners, and Nmap scripts.
- Mapped request patterns to potential rule triggers, similar to CRS-style logic.
- Analyzed robots.txt, directory exposure, and how WAF-like rules might interpret different inputs.

WAF Fingerprinting & Behaviour Observation (WAFW00F Labs)

- Used **WAFW00F** to detect WAF technologies and observe how different payloads affect fingerprinting results.
- Compared normal vs. malformed HTTP requests to identify potential WAF response patterns.
- Documented detection quirks and basic fingerprinting logic without modifying or exploiting real systems.

XODA File Upload Exploitation (Lab Exercise)

- Performed enumeration, HTTP request tracking, payload structure analysis, and exploit execution in a controlled environment.
- Noted request patterns and indicators relevant for rule-based detection.

Membership Inference Attacks (Semester Project)

github.com/Raptor2807/attacks_against_ML_Models

- Implemented MIA concepts as part of guided coursework.
- Used Python and PyTorch with standard model architectures.

Cybersecurity Practice Portfolio

- **Wireshark Packet Analysis –** Protocol-level interpretation and anomaly observation.
- **Password Cracking Basics –** Simple tasks with Hashcat and John the Ripper.
- **Firewall Configuration –** Tested basic iptables/ufw rules for traffic filtering.

Languages

English: C1 | **German:** B1 (learning)