

Experimental Evaluation of Web Application Firewall Performance in Simulated Real-World Environments

Name: Daudul Islam

Student ID: 2507415

Course: Research Methods and Professional Development

MSc in Cyber Security And Digital Forensic

Research Context

- Primary Target are Web Application like SQLi, XSS, RCE, OWASP Top 10
- WAFs protect web apps by filtering HTTP/HTTPS traffic.
- Traditional WAFs use rule-based detection
- Recent research uses ML and deep learning to improve detection accuracy
- Limited evaluation of WAFs in real-world deployment scenarios



Research Problem

- Focus on lab based datasets
- High detection accuracy reported,
but limited real-world evaluation
- Key missing elements
 - Latency and throughput impact
 - False positive behavior under mixed traffic
 - Operational complexity and configuration



Research Aim

- Aim

Evaluate operational performance and effectiveness of WAFs in simulated real-world environments





Objectives

➤ Objectives

Review existing literature on WAFs (rule-based and ML-based)

Deploy a test environment with a WAF

Simulate legitimate and malicious traffic (OWASP Top 10)

Measure detection accuracy and false positives

Evaluate system performance (latency, CPU, memory)

Analyse trade-offs between security and performance

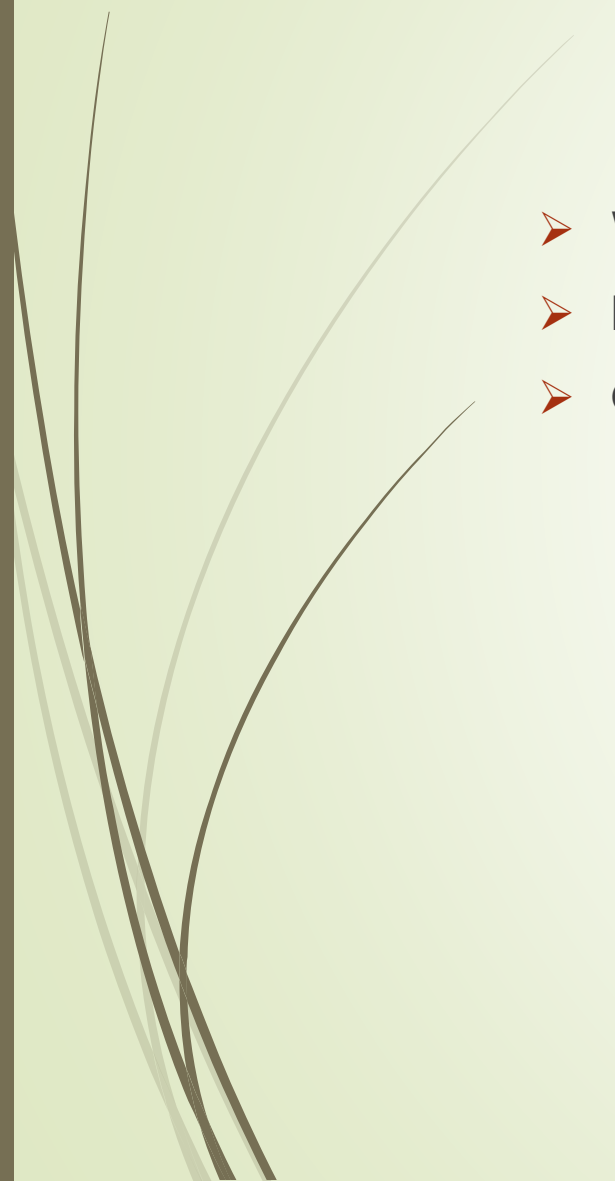


Brief Literature Review

- Most papers focus on ML-based detection accuracy
- Some compare commercial WAF products such as AWS vs Akamai
- Common gaps
 - Lack of deployment evaluation
 - No performance overhead metrics
 - Minimal false positive analysis

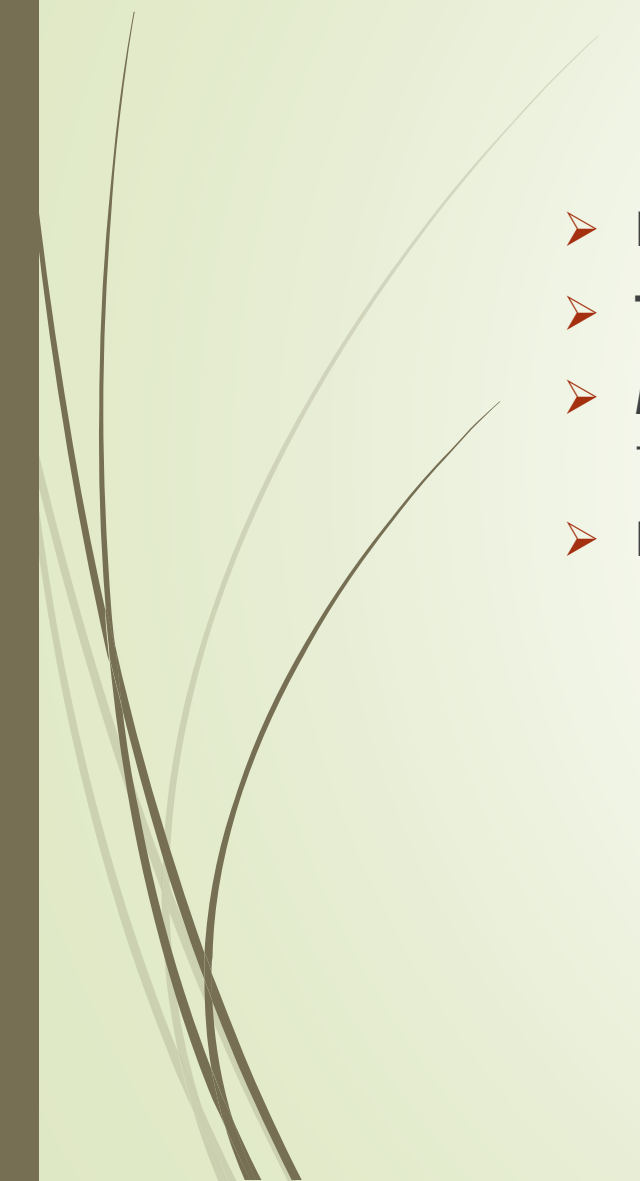


Research Gap

- WAF studies focus on lab datasets, not real traffic
 - Performance impact under real-world load is largely unknown
 - Operational usability and configuration challenges are underexplored
- 



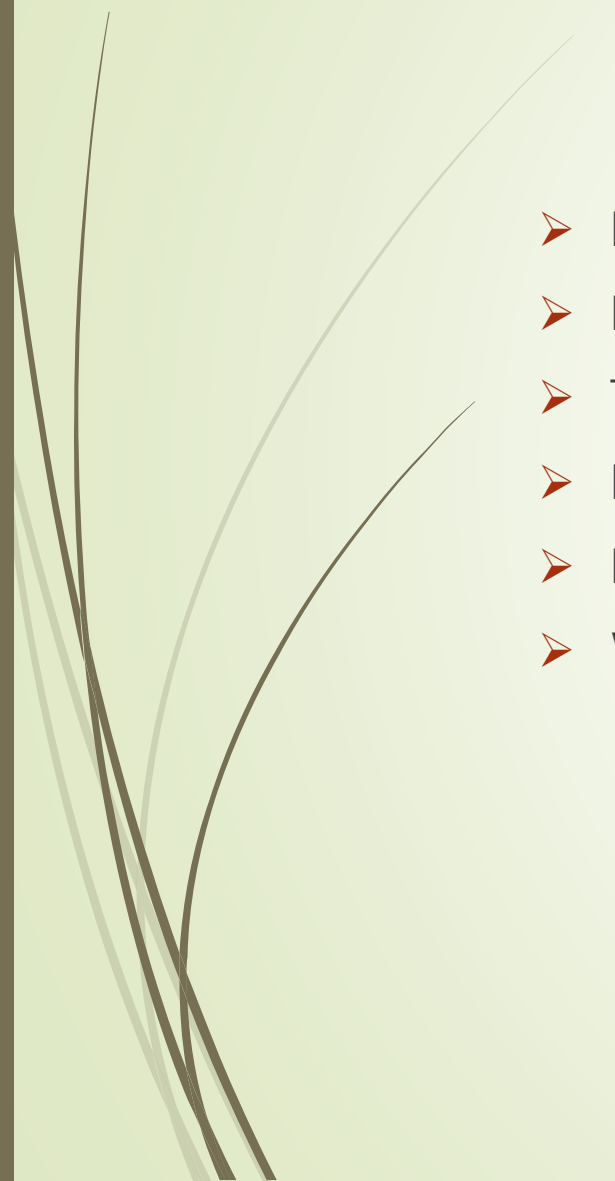
Research Methodology



- **Environment:** Web server + vulnerable web application + WAF deployment
- **Traffic Simulation:** Legitimate + OWASP Top 10 attacks
- **Metrics:** Detection rate, false positives/negatives, latency, CPU/memory, throughput
- **Data Analysis:** Statistical analysis, graphical performance comparison

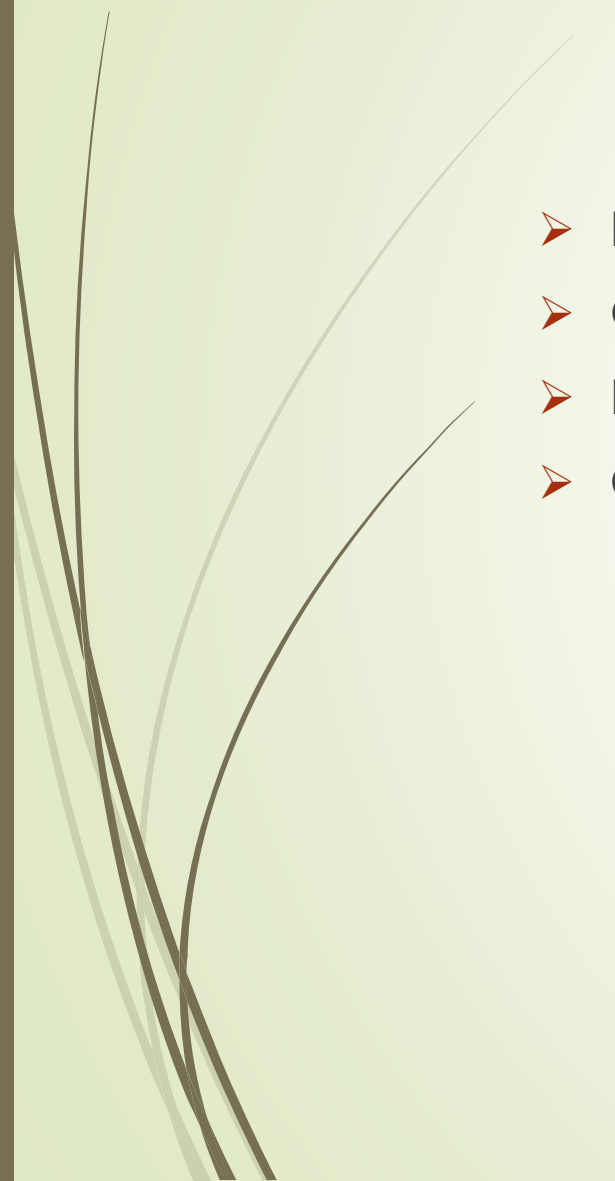


Project Planning and Resources

- 
- Literature Review 4 weeks
 - Environment Setup 3 weeks
 - Traffic & Attack Simulation 4 weeks
 - Data Collection 3 weeks
 - Data Analysis 3 weeks
 - Writing & Revision 4 weeks



Expected Impact

- Practical insights on WAF deployment performance
 - Guidance for organisations selecting WAF solutions
 - Bridge lab-based studies and real-world implementation
 - Contribution to cybersecurity evaluation research
- 

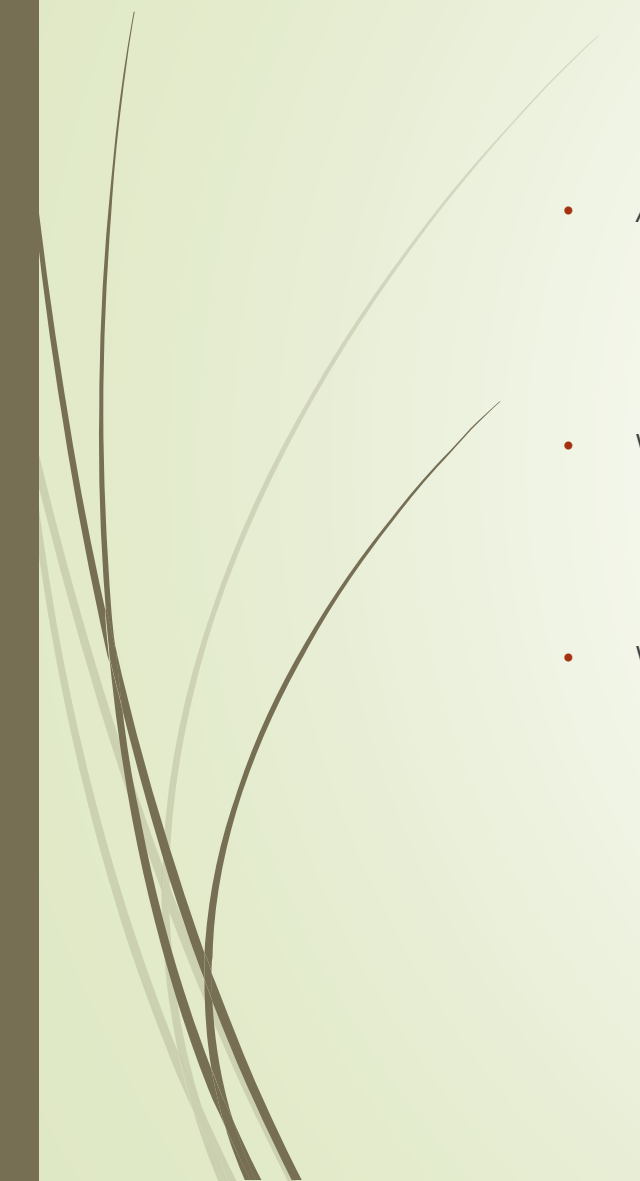


Limitations

- Simulated environment may not replicate full enterprise-scale infrastructure
- Limited WAF solutions evaluated
- Results may vary with traffic patterns and hardware configuration
- Time constraints limit extended long-term testing



References



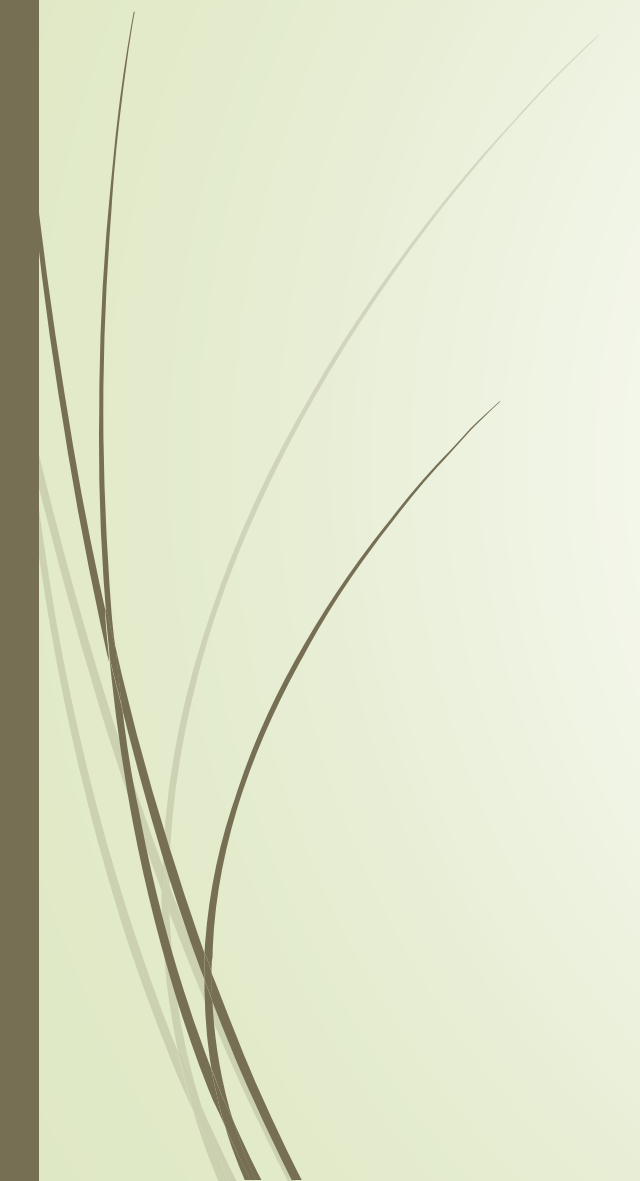
- Akamai WAF vs. AWS WAF A Comparative Analysis of Web Application Firewall Solutions for Cloud Security
Mohit Thodupunuri,
Volume 14, Issue 2,
July-December 2023
- Website Protection: An Evaluation of the Web Application Firewall
Gabriela Elizabeth Cárdenas Rosero, Cathy Pamela Guevara-Vega, Pablo Landeta-López
Accepted: 20-02-2025, Published: 21-02-2025
- Web Application Firewalls (WAFs) in Protecting Software
Ivana Bilic, Karlo Josic, Drazen Pranic & Sanja Ribaric
January 2024,
ISBN 978-3-902734-44-0, ISSN 1726-9679



References

- Identifying and Mitigating Web Application Vulnerabilities: A Comparative Study of Countermeasures and Tools

Sayed Elham Sadat, Mohammed Fahim Naseri, Khosraw Salamzada, Published: 2024-12-01



Thank You