Network Detection Techniques (Web Application Firewall)

Anil Prajapati (18162101027)
Mihir Manek (18162101012)
Jay Mehta(18162171012)

Index

Introduction

- Web Application Firewall (WAF) helps webapplication to filter HTTP traffic comes from public internet.
- WAF has rules that allow and deny the traffic and that’s called policy.

There are 3 solutions

- Network-based
- Host-based
- Cloud-based

Background

- web applications may face attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection.
- layer 7 is not design to defend against these attacks.
- By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet.
- While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server

Feasibility Study

- If you’re in charge of any sensitive data—credit card information, social security numbers, or health or financial records—you’ve likely spent a few late nights thinking about all the scary things that can happen to that information.
- Installing a firewall that can analyze traffic for suspicious activity may help set your mind at ease.
- By constantly scanning for vulnerabilities, WAFs often notice weak points long before you do even some WAFs can automatically patch the weak point.

SWOT Analysis

STRENGTHS

Data Security

Data Leak Prevention

Authentication

S

WEAKNESSES

Latency

Extra Budget for Security

Extra annoying steps for users to follow

W

Banks

Government / Defence Forces

Companies who owns Website

OPPORTUNITIES

O

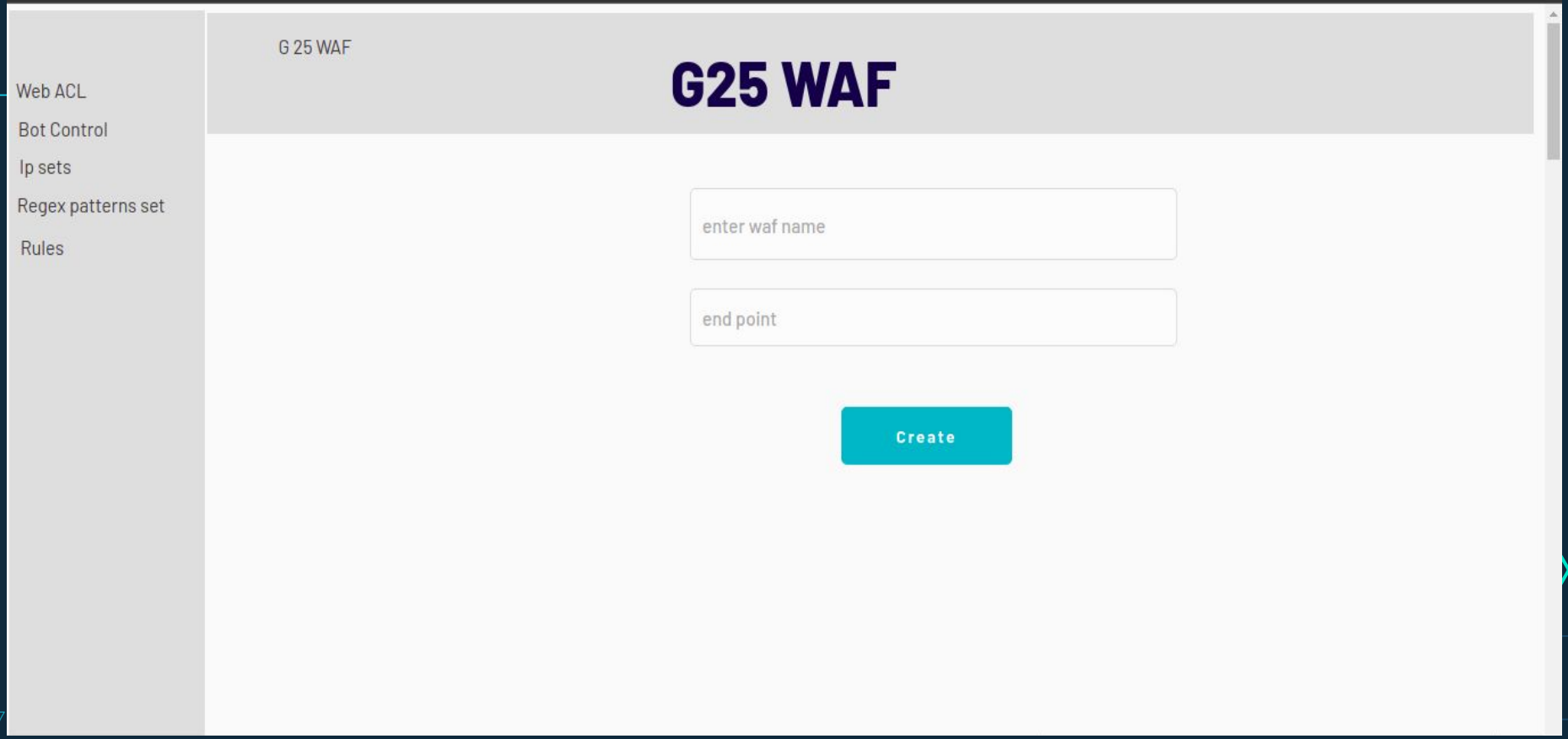
Third Party Data Control

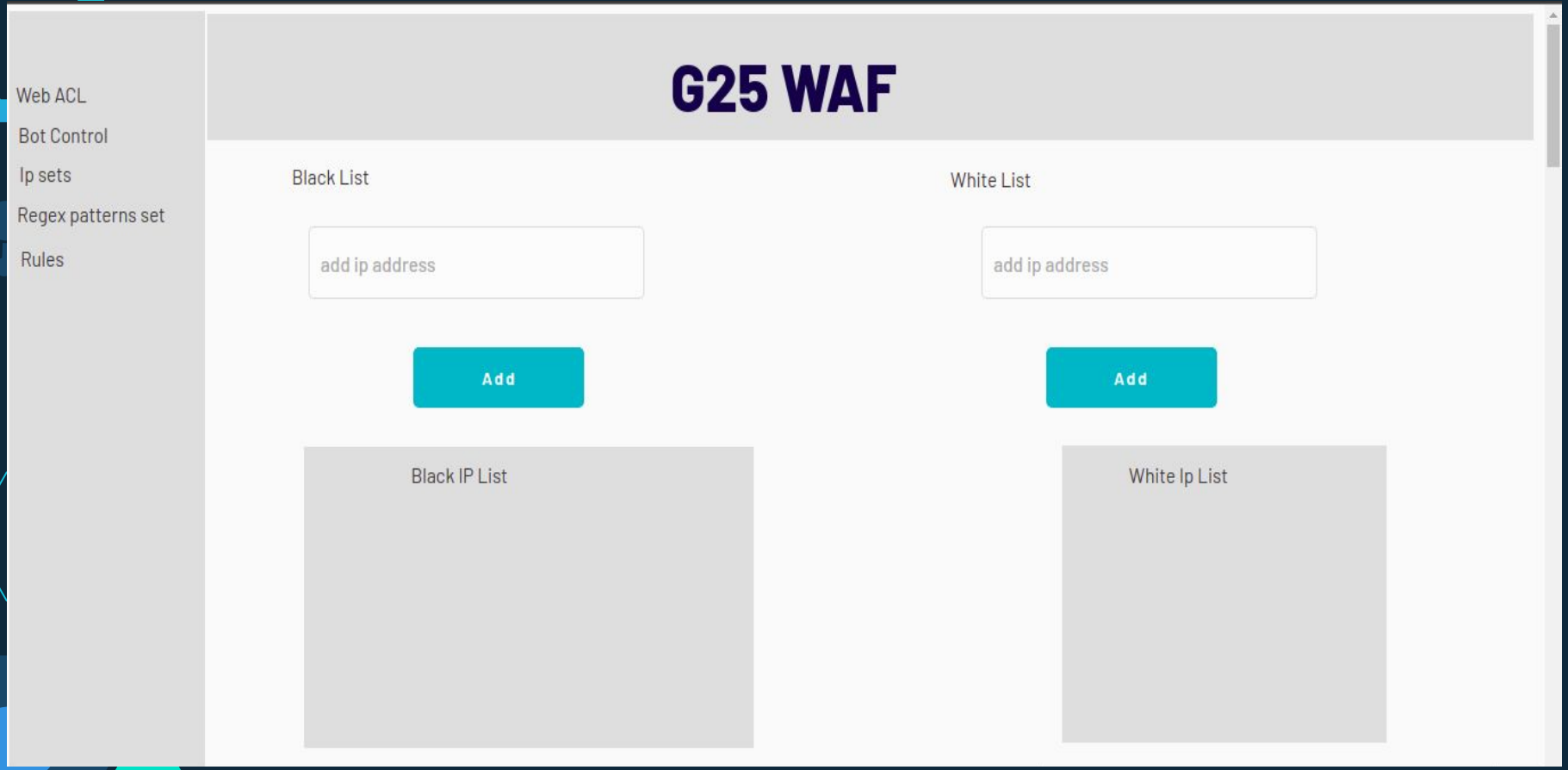
Not Compatible for New Attacks

THREATS

T

Prototype


G 25 WAF
G25 WAF
Web ACL
Bot Control
Ip sets
Regex patterns set
Rules
enter waf name
end point
Create


G25 WAF
Web ACL
Bot Control
Ip sets
Regex patterns set
Rules
Black List
add ip address
Add
Black IP List
White List
add ip address
Add
White Ip List


G 25 WAF
G25 WAF
Web ACL
Bot Control
Ip sets
Regex patterns set
Rules
Pricing
Add Protection Type
SQL Injection
DDOS
Cross-Site Scripting (XSS) Attacks:
Zero-day Attacks:
Man-in-the-middle attacks
Man-in-the-middle attacks
Add

Approach

- deploy web application on AWS
- Add proper incoming allow rules as First Line of Defence.
- Save logs of incoming request
- Real time analysis of logs and detect malicious activity

Types of Attacks

- DDos
- SQL Injection
- MITM
- Zero Day Attack
- Cross site Scripting (XSS)

Recommended Tools & Technologies

- Zabbix
- Nagios
- AWS cloud
- Network access list/Security group
- Python
- Shell Script
- Linux

Conclusion

- Considering these day value of data fetched from user is crucial enough to carry out many important work on basis of that, it's demand has also been increased and so is the way of possession of that information. Hence providing security should be the top most priority of the service provider which our project can help with it.
- WAF is more reliable then the whole Security Team in the company.

Thank You

Happy to hear from you

- anilprajapati18@gnu.ac.in
- mihirmanek18@gnu.ac.in
- jayhmehta18@gnu.ac.in