KAMI LIMU

Group Members and Roles

1. Thaddeus Mwai - Team Lead, Systems Admin
2. Dorcas Anono Litunya - Business Analyst
3. Mark Tanui - Cloud Infrastructure Engineer
4. Catherine Kemunto - Penetration Tester

Mentor's Name: Matthew Macharia

Sentinel Master

'Here for you'

Date of Submission: May 12, 2022

Introduction

According to the Bertelsmann Stiftung's Transformation Index (**BTI**) report, 33.4% of Kenya's population lives below the poverty line. This means that more than one-third of the country's population survives on less than $1.90 per day. This financial crisis makes it hard for these Kenyans to access loans from the banks. For this reason, Microfinance Institutions in Kenya play a crucial role. The World Bank defines Micro Finance Institutions (MFIs) as organizations that offer relatively small financial loans to low-income households, micro-enterprises, small-scale farmers, and others who lack access to traditional banking services. These MFIs provide an enormous potential to support the economic activities of the less fortunate and thus contribute to poverty alleviation. By the year 2020, there were more than 147 large microfinance institutions

in Kenya, which provided approximately Ksh.6.5 billion to approximately 1.5 million active borrowers.
With the Covid-19 pandemic, the digitization of financial services has been a focus for banks and microfinance institutions alike. Unfortunately, this migration into the digital space in the year 2019/2020 has exposed financial institutions to more cyberattacks with the main focus being sensitive data and customer funds.

According to a report by the Central Bank Kenya and Sacco Societies Regulatory Authority in 2021, MFIs lose an equivalent of KSh6.23 million per month or KSh208,000 daily to cybercrimes. In spite of the high rate of cyber attacks, the Serianu Africa Cybersecurity Report reports that 97% of these MFIs spend less than USD 10,000 a year on cybersecurity.

One of the ways to reduce the risk of cyberattacks is through the use of Web Application Firewalls(WAFs). A WAF is a network security software that protects web applications from cyberattacks by monitoring and filtering all incoming and outgoing HTTP traffic between a web application and the Internet. Most MFIs have gone out of their way to seek help from third-party companies to build and train their staff on the use of WAFs, however, a gap still exists. While these MFIs are able to procure on-premise and cloud-based WAF solutions from vendors such as Fortinet and Checkpoint, they still lack in-house expertise, customized WAF solutions, and funds to successfully manage and monitor all HTTP traffic to prevent cyberattacks.

To address this gap, Sentinel Master aims to meet the following objectives:

1. Build an affordable and customizable WAF for Microfinance Institutions
2. Monitor and handle potential cyber-attacks through the WAF
3. Partner with other companies to improve the functionality of the WAF. For example, a partnership with a consulting firm such as Serianu.

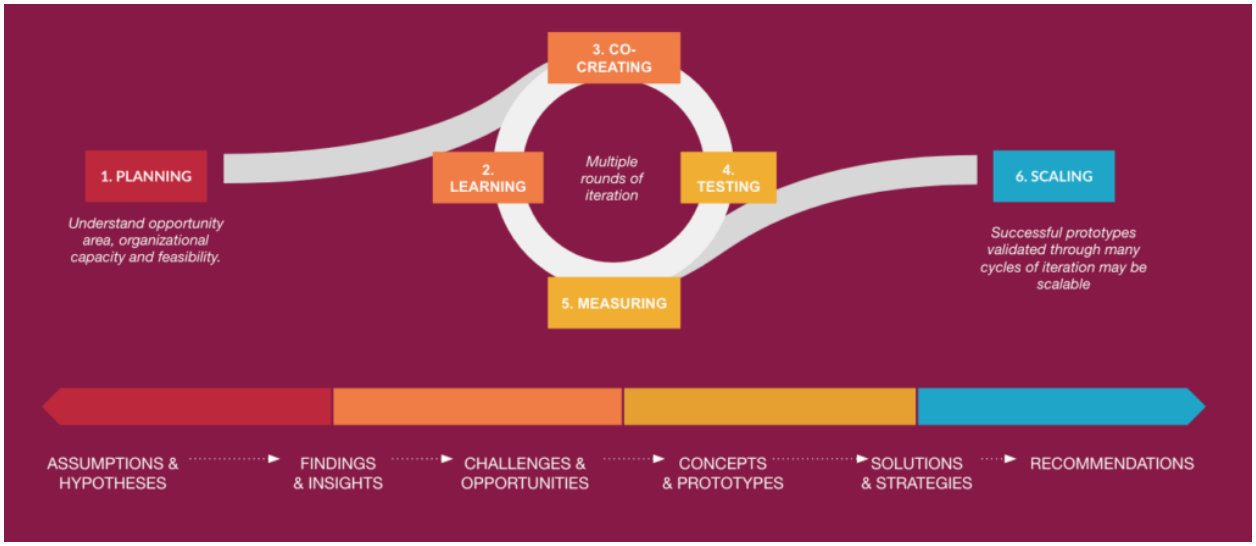
Description of Solution

Sentinel Master aims to protect micro-finance institutions against data breaches that result in the loss of hundreds of millions. We aim to achieve this by providing a hybrid WAF-as-a-Service, tailored to use both blacklists and whitelists to distinguish between legitimate and malicious traffic. We deliver a WAF-as-a-Service, that requires no customer setup or maintenance, is low cost, and offers greater protection than other WAFs due to filtering traffic before it reaches protected websites and web applications.

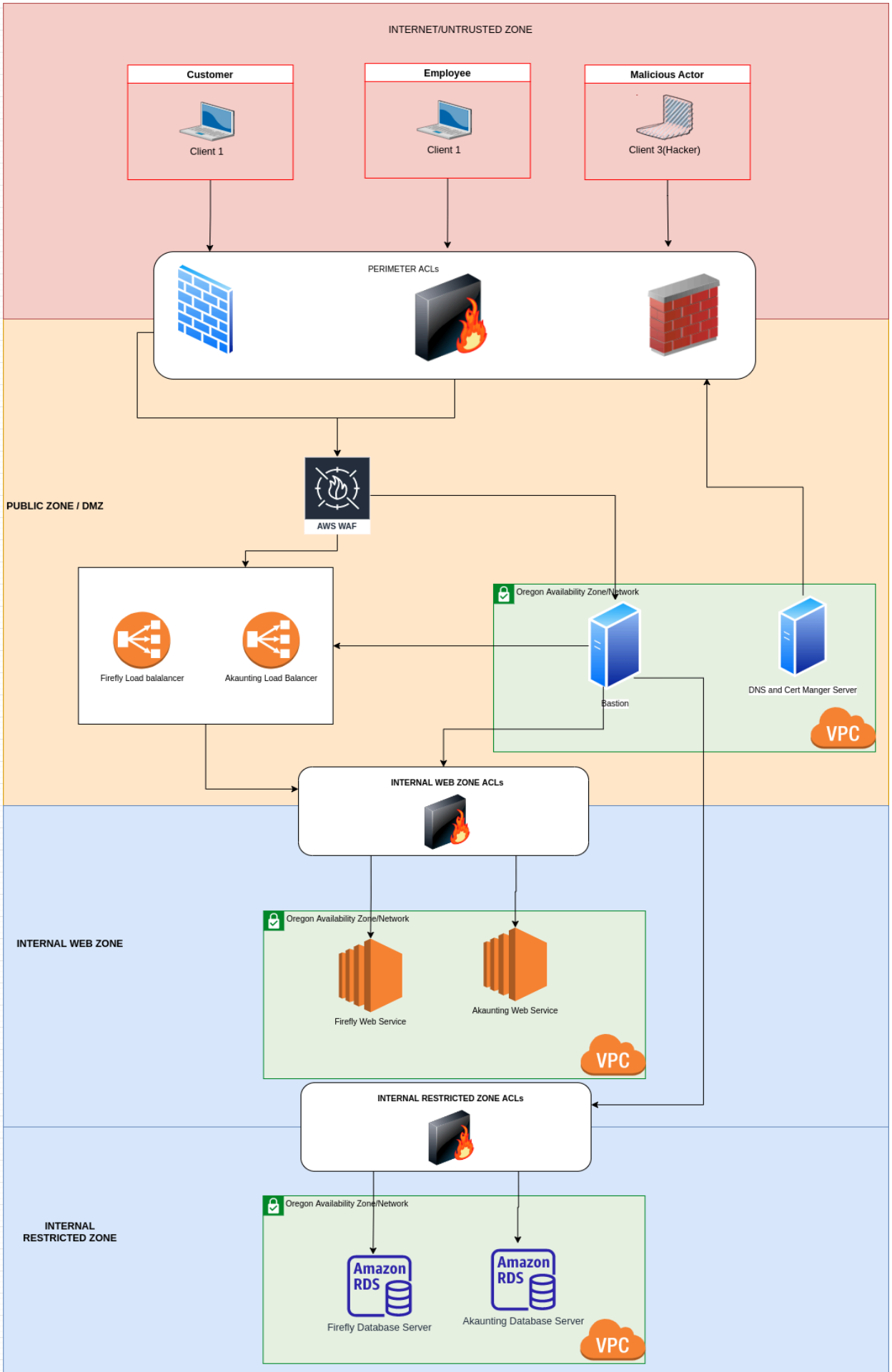
Micro-finances institutions are more susceptible to cyber-attacks and data breaches due to their non-investment in security infrastructure: estimated to be under $10,000. MFIs have more clientele due to low-interest rates and more competitive products, giving attackers an incentive to attempt exploitation of vulnerabilities within MFIs systems. Statutory bodies tasked to control cybersecurity within MFIs also fail to comprehensively address the existing gaps. Hence, leaving these institutions more and more vulnerable.

Given that hundreds of millions are lost by micro-finance institutions due to successful cyber breaches, it is the top priority for these institutions to protect their services. A WAF as a service is the tool of choice to protect web assets. And, given the potential consequences of a successful cyberattack such as revenue loss and brand damage, the price of overconfidence can be high.

Our approach to solving the existing gap was human-centered, iterative, and results-driven. We focused on understanding the dynamics between stakeholders across the ecosystem. For example, we worked with Serianu Limited, an award-winning Pan-African-based Cybersecurity and Business consulting firm that enables organizations to extract value from their information. From the case studies done by Serianu, we were able to quantify our hypothesis and prove them. We learned that MFIs have a challenge with expertise and financial capital to maintain ISO cybersecurity standards for financial institutions.



We prototyped to create and design Sentinel Master using draw.io and X. The prototype was utilized to test alternative approaches and to validate that they represent real improvements. It included decoupling of Sentinel Master cloud architecture: Virtual Private Clouds, network subnetting, and zoning of instances. This further enabled decision-making for the ideal position for the WAF, load balancer, and other components.

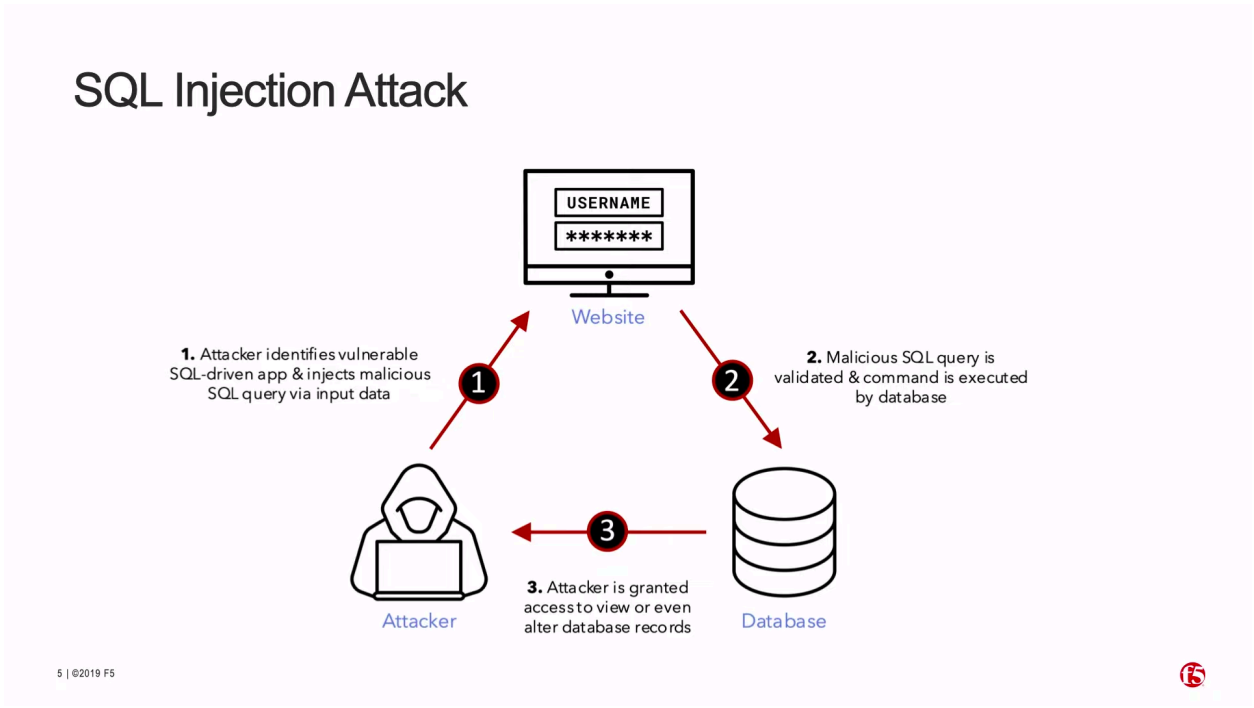

INTERNET/UNTRUSTED ZONE
Customer
Client 1
Employee
Client 1
Malicious Actor
Client 3(Hacker)
PERIMETER ACLs
PUBLIC ZONE / DMZ
AWS WAF
Firefly Load balalancer
Akaunting Load Balancer
Oregon Availability Zone/Network
Bastion
DNS and Cert Manger Server
VPC
INTERNAL WEB ZONE ACLs
INTERNAL WEB ZONE
Oregon Availability Zone/Network
Firefly Web Service
Akaunting Web Service
VPC
INTERNAL RESTRICTED ZONE ACLs
INTERNAL RESTRICTED ZONE
Oregon Availability Zone/Network
Amazon RDS
Firefly Database Server
Amazon RDS
Akaunting Database Server
VPC

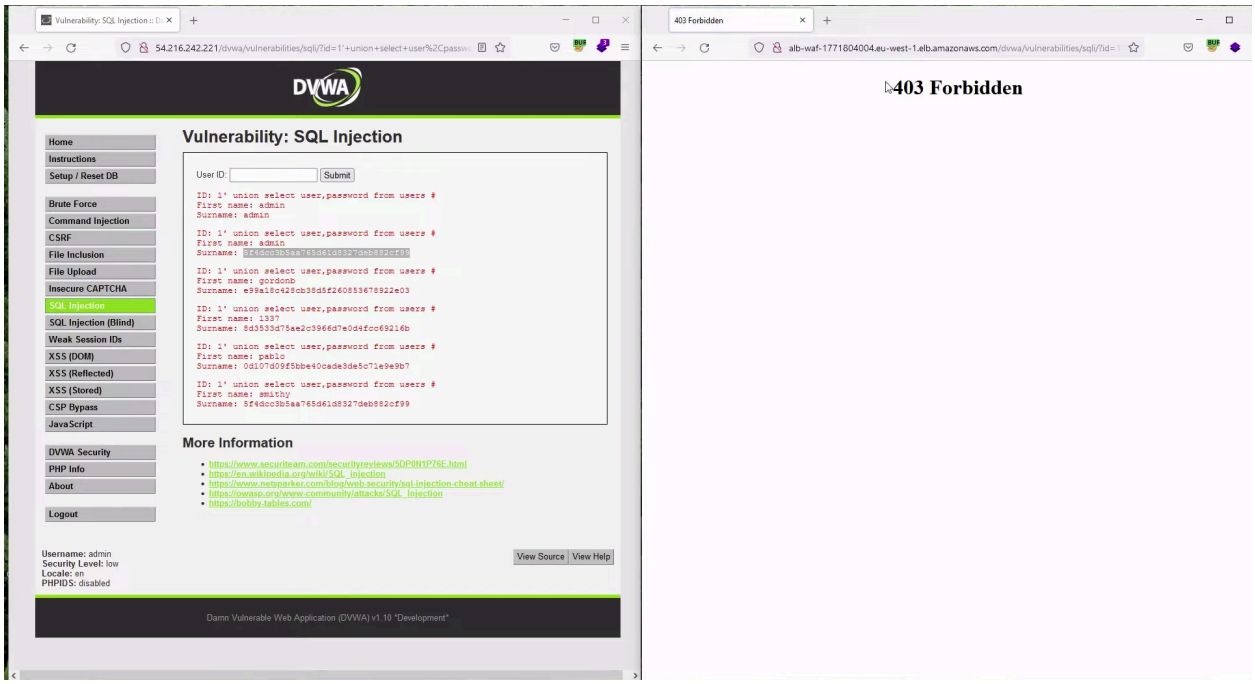
Sentinel Master sits between web applications and the Internet and protects them by monitoring and filtering traffic. When working correctly, WAFs monitor all incoming traffic and filter anything that could be a threat.

From the OWASP top ten mitigation techniques, the use of a well-managed WAF is listed as a comprehensive measure to combat attacks. Sentinel Master provides targeted, instantaneous, and managed virtual patching against identified risks to ensure micro-finance institutions not only mitigate the risk but also track the attackers who are trying to exploit the risk and update their defense policy against those attackers.

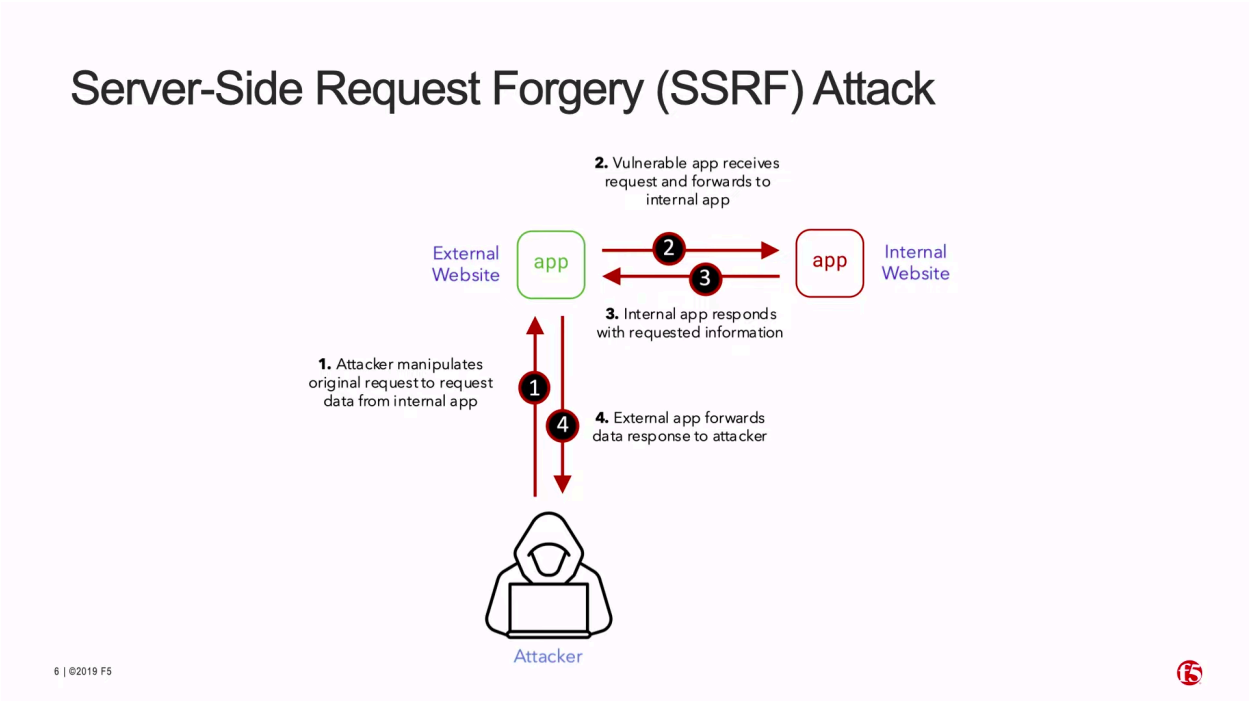
Sentinel Master protects the application layer of the OSI Model against attacks. The application layer is the hardest to defend as the application is accessible only over Port 80 (HTTP) or Port 443 (HTTPS). Systemweakness.com tells us that most exploits are used to compromise applications using the seventh layer-application layer- of the OSI Model.

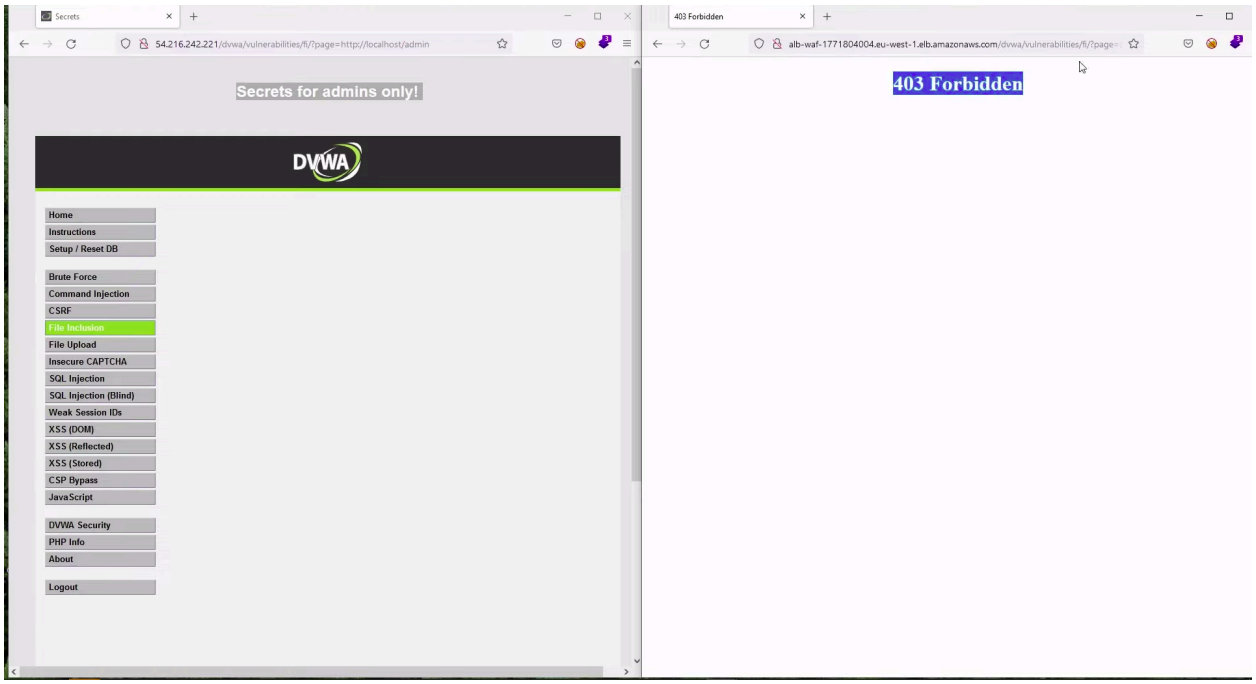
Sentinel Mater has been tested for its effectiveness in two ways. Using the Damn Vulnerable Web App (DVWA) which is damn vulnerable we tested our tool to ensure it protects against OWASP top ten. The web app is built with PHP and MySQL which is also used by most MFIs. Using this legal environment helped to better understand the process of securing other services as well.
The attached screenshots showcase Sentinel Master defending against SQLi and Server Side Request Forgery attacks.





The left side shows DVWA without Sentinel Master and the right side with Sentinel Master



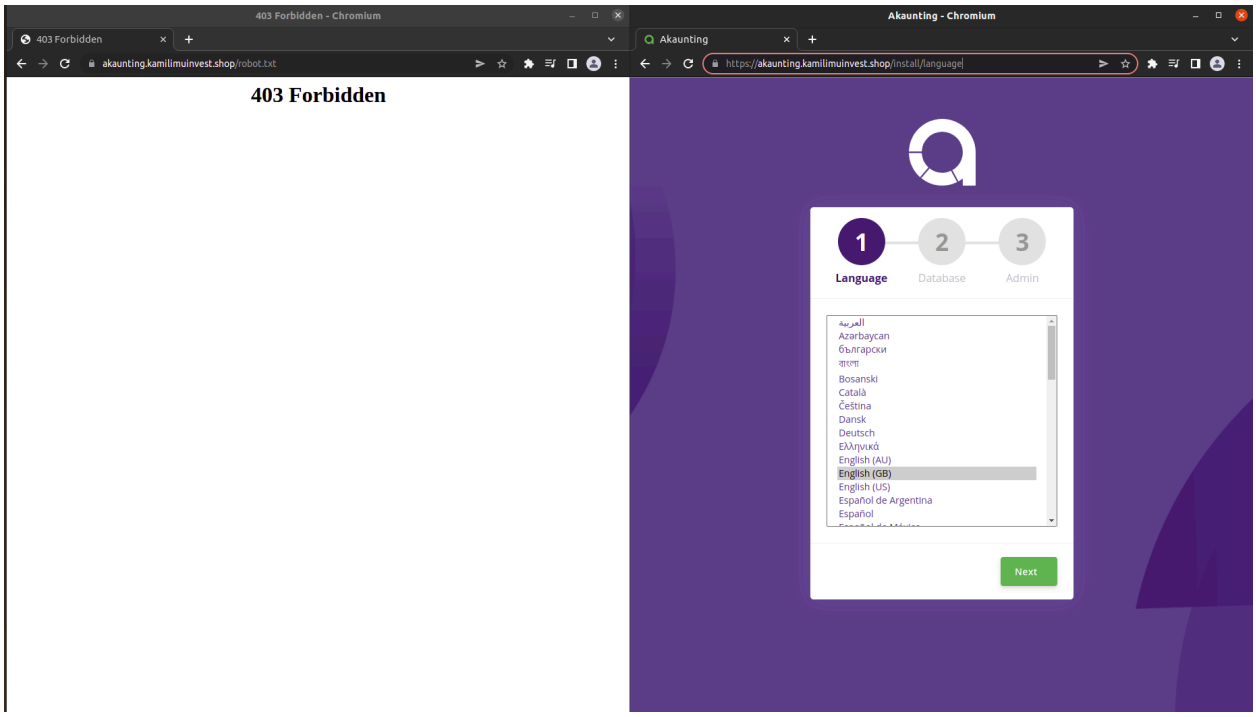


The left side shows DVWA without Sentinel Master and the right side with Sentinel Master

Data from one of the case studies by Serianu, helped us select two open-source financial accounting software that MFIs use: akaunting and firefly. The services were hosted in AWS and

were secure with Sentinel Master as well. Tests and scans to ascertain WAF rules revealed that the services were shielded from specified attacks.

The following screenshot demonstrates Sentinel Master shielding akaunting, one of the open-sources services that we hosted from a user accessing the robot.txt file.



The left side shows Sentinel Master defending, right side showing service without Sentinel Master.

Sentinel Master also protects against distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks.

Value proposition

- Subscription-based services
- Ease of scalability for businesses
- Multi-tenancy thus compounded resources

Competition

The main competitors of Sentinel Master are companies that offer on-premise WAF solutions and/or cloud-based WAF solutions. On-premise WAF Solutions involve hardware or software being set up within the organization's physical server environment and it is accessed and managed by the organization through the Local Area Network(LAN). Cloud-based WAF solutions provide protection over the cloud and it is accessed and managed by the organization through a web interface or mobile app. An example of an on-premise WAF solution is WAPPLES whereas an example of a cloud-based WAF solution is Prophaze.

Competitive Advantage

As opposed to on-premise WAF solutions and cloud-based WAF solutions, Sentinel Master offers the Web Application Firewall as a service. This means that Sentinel Master will be in charge of setting up, monitoring, and managing the WAF for all its clients. Other advantages include:

Customized WAF for MFIs- Sentinel Master customizes the WAF from a generic model to a model that better suits MFIs.

Management- As opposed to the on-premise WAFs that require an organization to have its own staff manage the operations of the WAF, Sentinel Master offers experts to monitor the organization's WAF 24/7/365.

Cost- The monthly incurred cost associated with the Sentinel Master's WAFs is relatively predictable as it consists of only the monthly subscription cost and add-ons if any.

Scalability- Sentinel Master offers greater flexibility when it comes to scalability. The WAF's capacity can be automatically scaled up to handle newer threats or increased web traffic.

Security-Maintaining data security is critical regardless of which option you go with. With Sentinel Master, the software is hosted within the highly secured AWS data center and the AWS is responsible for data security. An on-prem WAF is only as good as the company's ability to

secure access to that data. Within many organizations, data security is not their primary focus which in turn creates data vulnerabilities, exposure, and increased risk.

Business Model

For our business to be fully functional, we have divided it into 4 sections that will be working collaboratively in order for optimal results.

1. Design and Solutions Architect team

   The design team creates the network infrastructure diagrams that will be implemented by our cloud engineers. These network diagrams will be based on our user needs as we deploy their solutions.

   .

2. Cloud Engineering

   This team creates the Web application Firewall(WAF) on the cloud. The WAF is subscription-based. The features and functionalities are customized based on client needs.

3. Sales & Marketing

   This team manages our social media platforms and looks for fresh new ways to penetrate the market. It also controls the pricing of the product and makes sure the company's assets and liabilities are in sync and we're sustainable.

4. Service and Product

   This team is responsible for all market research and discovering the trends in our users' preferences. The team also analyses our competitor strategies and develops new ways to keep Sentinel Master ahead. It is also responsible for the deployment of the product to the consumer

As we grow as a business, we hope to partner with Amazon Web Services(AWS) and Serianu. AWS, a cloud service provider, would be our partner to provide a platform where we can set up the WAF service on their cloud platform. Moreover, training through AWS would be beneficial in order to grow the team’s expertise. Serianu, a cybersecurity and Business consulting firm, would also assist us in monitoring and evaluating the platform. These resources will be beneficial to expanding our business.

Sentinel Master will generate revenue by selling WAFs as a service. Our main revenue stream will be from setting up WAF for Microfinance institutions. Moreover, we also intend to offer

monitoring and evaluation solutions to Microfinance Institutions that have a WAF already set up. These services will be subscription-based thus ensuring continuous cash flow. The cost of the service will depend on client needs such as the number of web applications uploaded, load balancer setup, and required WAF privileges. Since the service is a multi-tenancy model, we are able to maximize profits as we can have different tenants on the same platform. Through this, we have become Managed Service Providers for the WAF. Our consumers will pay through any platform that can deposit to our bank account.

Here is a sample cost of our product:

Export date: **5/11/2022** Language: **English**

Estimate title: **My Estimate**

Estimate URL: **https://calculator.aws/#/estimate?id=7008fd708183595a7baa0ccc85effd5749da5f60**

Estimate summary

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	**294.87 USD**	**3,538.38 USD** Includes upfront cost

Detailed Estimate

Name	Group	Region	Upfront cost	Monthly cost
Amazon EC2	No group applied	US East (Ohio)	0.00 USD	27.67 USD
Description: **Config summary:** Operating system (Linux), Quantity (1), Pricing strategy (Compute Savings Plans 1 Year No Upfront), Storage amount (100 GB), Instance type (t4g.medium)				
Amazon Route 53	No group applied	US East (Ohio)	0.00 USD	2.60 USD
Description: **Config summary:** Hosted Zones (1)				
Elastic Load Balancing	No group applied	US East (Ohio)	0.00 USD	22.27 USD
Description: **Config summary:** Number of Application Load Balancers (1)				

Milestones so far

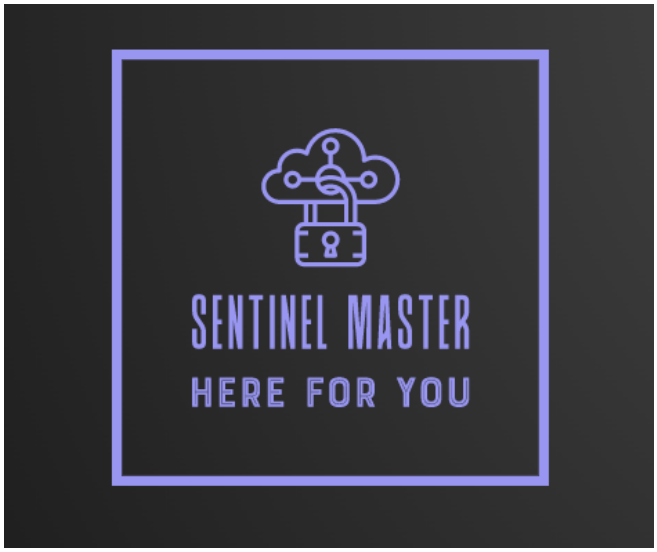
1. **Branding**

The name Sentinel Master came up in one of our brainstorming meetings due to the fact that we want to become sentinels that guard business resources. Just as a sentinel's duty is to guard and protect a master's property, we want to guard and protect Microfinance Institutions from any malicious attacks. We are determined to make our customers have the best and most secure systems guarding their resources. Our brand personality is that we are:

Convenient, Skilled, and customer-obsessed.

For our brand colors, we wanted them to be appealing to the eye of the user and also tie in with the main idea that we are selling. Our main colors are **blue** which symbolizes trustworthiness and loyalty to our customers and **black** which expresses power and sophistication, an accurate description of the solutions we hope to offer our customers. Our slogan, **Here for You**, was something random that we thought of during our meetings that's in relation to the type of services we want to provide as Sentinel Master. We want our customers to feel seen and protected through the services we offer.

Below is a picture of our logo that we later plan on printing on shirts and wearing as a method of brand promotion.



2. **Pilot Product**

We have Tested the app with two web services such as Akaunting and Firefly. Through these two platforms, we obtained feedback on how to improve our services and are currently incorporating this feedback to use for the next iteration of the product.

3. **Partnerships**

We have partnered with Serianu, which is a cybersecurity consulting firm that assists us with monitoring and evaluation. Moreover, Serianu has also provided training for our IT experts to enable them to be skilled at their craft.

Scaling Plans

FIRST YEAR	Word of mouth-For the first 3 months, we ought to market through the official websites that we intend to share with Microfinance Institutions by having them use our service and share it with their social circles. We also plan to advertise on social media like Twitter and LinkedIn. This would reach about five people. We will also sell our product in business conferences.
SECOND	We anticipate having around seven users in our service. We'll take into consideration feedback from the current users and incorporate it in the second version of our service. Social media advertising will increase the number of ads we put forward on these platforms to reach more people. We will also do online ads on websites to create more traffic for our application. We will then dive into print media advertising by having columns in business magazines and local newspapers talking about our activities as Sentinel Master and giving people tips on building secure systems thus drawing more people into our application.

What are the plans for the next 1-5 years?

- Build an official Sentinel Master's website to help create brand awareness and showcase our brand to prospective customers.

- Obtain a business license, business bank account, and company credit card
- Improve our services based on user feedback.
- Partner wit other firms such as Serianu which is a cybersecurity consulting firm to improve our service delivery.
- Secure funding through loans, angel investors, and grants. Examples of companies looking for cyber security companies to fund include Strategic Cyber Ventures, AllegisCyber Capital, Cyber Capital Partners, and TenEleven Ventures.

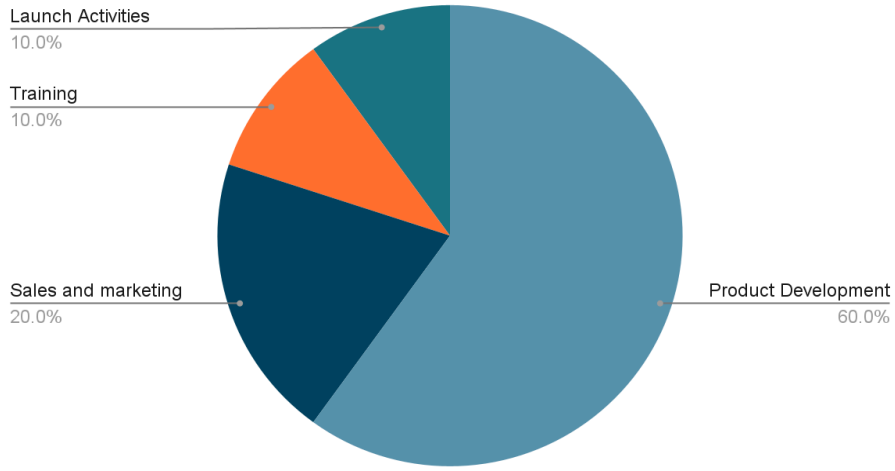
What potential impact do you hope to achieve?

Sentinel Master aims to create awareness on the importance of having a Web Application Firewall Service and reduce MFIs Web Application attacks. In addition, Sentinel Master aims to reduced the money lost due to breaches by close to 86%, as quoted by the MFI statutory body of Uganda. This is attributed to the fact that Sentinel Master would protect MFIs against eight of the ten OWASP vulnerabilities.

Funding/Support Need

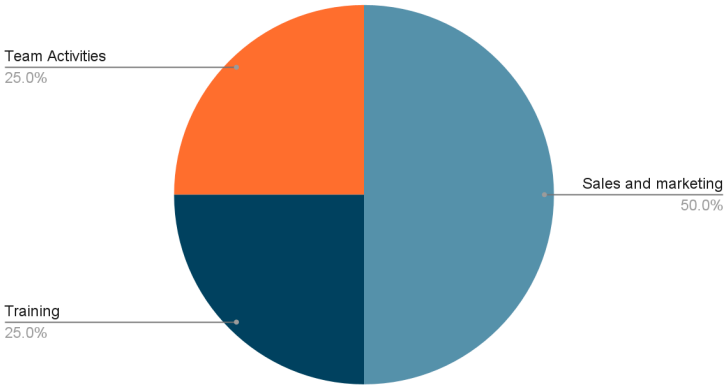
Pilot Plan funding

	Period 1	
Product Development and Company setup	3000000	
Sales and marketing	1000000	
Training	500000	
Launch Activities	300000	



Post Pilot funding budget monthly

	Period 1(Amount in Ksh)	
Sales and marketing	100000	
Training	50000	
Team Activities	50000	



Scaling Plans

We hope to expand through consistent marketing and delivering customer-centred services. The potential impact that we hope to have is to ensure all microfinance Institutions in Kenya are secure. This would help reduce the number of cyber-related threats and make people's finances more secure.

Over the next few years, we hope to incorporate our initial user feedback and improve our services.

Moreover, we hope to add new services in Cybersecurity such as :

- Offer Access Control as a service
- Monitoring as a service
- Manage service provider for infrastructure

Sentinel Master’s Theory of Change

Problem Statement	

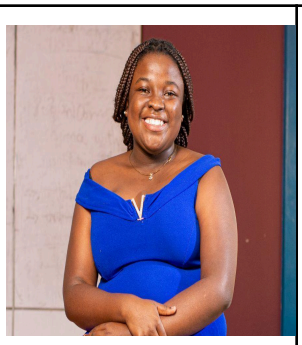
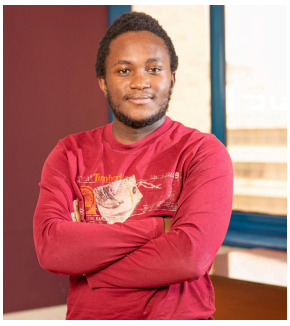
Inputs	Activities	Outputs	Short-Term Outcomes	Mid-Term Outcomes	Long-Term Outcomes

Resources needed to conduct activities efficiently	Activities needed to reach outcomes	Tangible immediate results of our activities	Outcomes expected of our intervention.	Outcomes we want to see in our intervention timeframe.	Outcomes we hope to observe beyond our intervention timeframe
● Human resources: skilled cybersecurity practitioners ● Technology: web apps/accounting platforms, the WAF	● Development ● Training: the web developers & cybersecurity professionals ● Deployment	● Do we have stats on impact? ● Targeted businesses/companies ● Selling alongside an accounting software? ● % of reduced attacks (finance sector)	● Secure transactions	● Increased customer trust/confidence & loyalty. ● Increased profitability - reduction in losses due to cybercrime	● Business expansion - they focus on improving Ops.

Assumptions	The MFIs are willing to adopt the WAF solution. The WAF does not obstruct any Data Protection laws.

Impact	MFIs can focus on improving business operations and revenue.

Our team

			
DORCAS A. LITUNYA	TED W. MWAI	CATHERINE K. MAKORI	MARK TANUI
BUSINESS ANALYST	TEAM LEAD & SYSTEM ADMIN	PENETRATION TESTER	CLOUD INFRASTRUCTURE ENGINEER