

**HEIMDALL: A DIGITAL THREAT MANAGEMENT
PLATFORM**

Design Manual

by

Killian O'Connor

For IT Carlow

10/2/2020

Page **1** of **11**

Table of Contents

Table of Contents.....	2
Table of Figures	3
1. Introduction.....	4
2. Wireframes	4
2.1 Home Page.....	4
2.2 Admin Page.....	4
2.3 Reporting Module	5
2.4 Active Alerts Page.....	5
2.5 Alert Details.....	6
2.6 Closed Alerts.....	6
2.7 AWS S3 Scanner Module Home Page	7
2.8 CVE Scanner Module Home Page	8
3. Sequence Diagrams.....	8
3.1 Generic Sequence.....	8
3.2 Report Generation Sequence.....	9
3.3 Generic Scanner Sequence.....	10
4. ER Diagram	11

Table of Figures

Figure 1, Wireframe: Home Page	4
Figure 2, Wireframe: Admin Page.....	4
Figure 3, Wireframe: Reporting Module.....	5
Figure 4, Wireframe: Active Alerts Page.....	5
Figure 5, Wireframe: Alert Details View.....	6
Figure 6, Wireframe: Closed Alerts.....	6
Figure 7, Wireframe: S3 Scanner Home Page.....	7
Figure 8, Wireframe: CVE Scanner Home Page.....	8
Figure 9, Sequence Diagram: Generic Request.....	8
Figure 10, Sequence Diagram: Report Generation.....	9
Figure 11, Sequence Diagram: Generic Scanner.....	10
Figure 12, Entity Relationship Diagram	11

1. Wireframes

1.1 Home Page

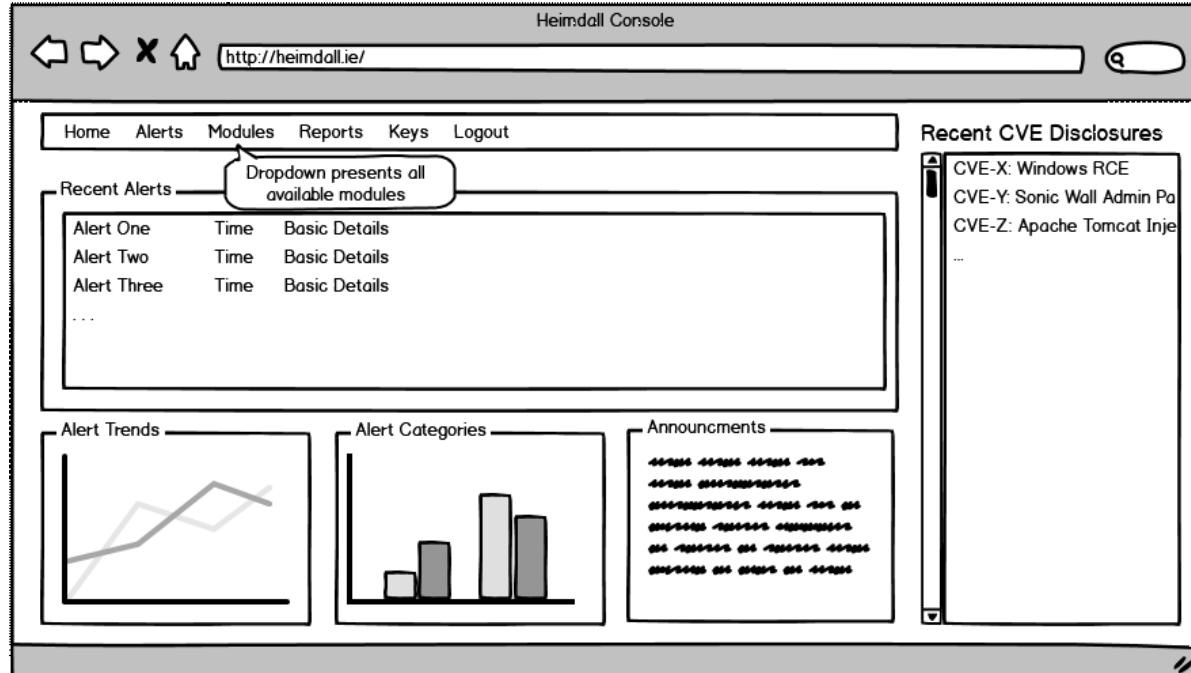


Figure 1, Wireframe: Home Page

1.2 Admin Page

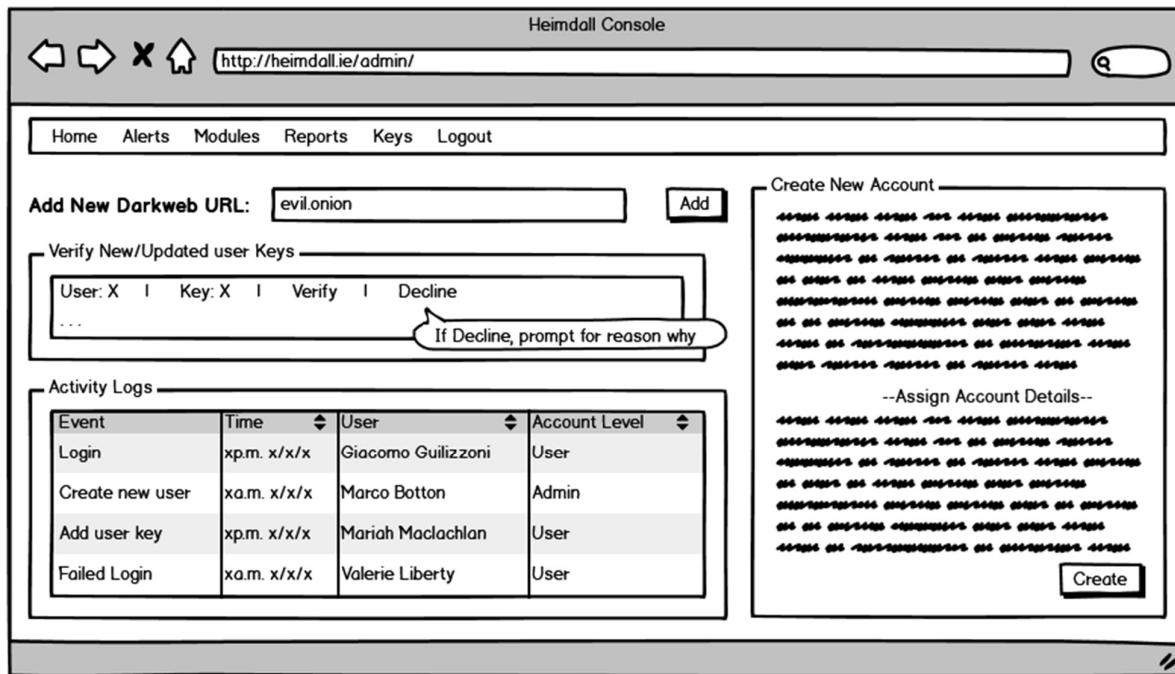


Figure 2, Wireframe: Admin Page

1.3 Reporting Module

The wireframe for the Reporting Module shows a header with a search bar containing the URL <http://Heimdall.ie/report/>. Below the header is a navigation menu with links for Home, Alerts, Modules, Reports, Keys, and Logout. The main content area is titled "Generate New Report". It includes a "Modules to Use" section with a dropdown for "Template" and two date pickers for "Start Date" (y/y/y) and "End Date" (x/x/x). There are four radio buttons for selecting modules: module 1 (selected), module 2, module 3 (selected), and module 4 (selected). To the right of the module selection is a large, illegible scribble. A "Generate Report" button is located at the bottom right of this section. Below this is a "Recent Reports" section listing three entries: Report One, Report Two, and Report Three, each with columns for Time and Modules Used. An ellipsis (...) is shown below the third entry.

Figure 3, Wireframe: Reporting Module

1.4 Active Alerts Page

The wireframe for the Active Alerts Page shows a header with a search bar containing the URL <http://heimdall.ie/module/userAlerts/>. Below the header is a navigation menu with links for Home, Alerts, Modules, Reports, Keys, and Logout. A callout bubble points to the "Alerts" link in the menu with the text "Drop down to choose between active or closed alerts". The main content area is a table displaying active alerts. The table has columns for AlertID, Time, Alert Details, Module, Action, and Close. The table contains three rows of data:

AlertID	Time	Alert Details	Module	Action	Close
001	xp.m. x/x/x	User key present on info dumping site	OSINT Scanner	Action	Close
002	xp.m. x/x/x	User key present on darknet market	Darkweb Scanner	Action	Close
003	xp.m. x/x/x	S3 bucket publically accessible	AWS S3 Scanner	Action	Close
...					

Figure 4, Wireframe: Active Alerts Page

1.5 Alert Details

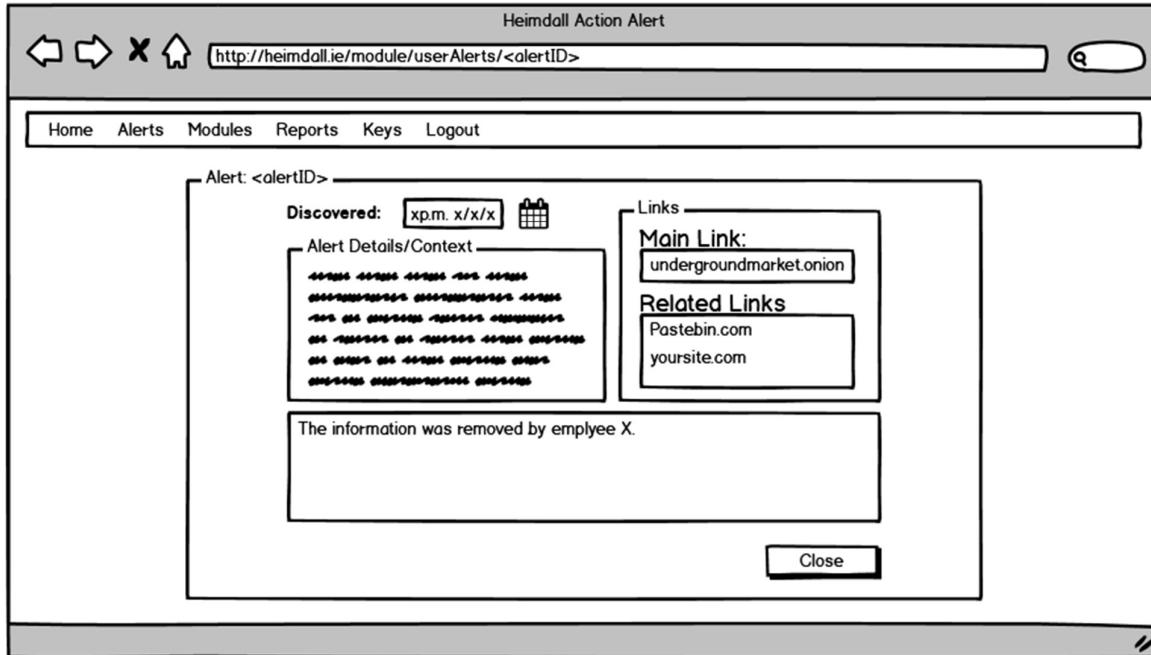


Figure 5, Wireframe: Alert Details View

1.6 Closed Alerts

Heimdall Historic Alerts					
Home Alerts Modules Reports Keys Logout					
AlertID	Time Discovered	Time Closed	Alert Details	Module	Remediation Comments
009	xp.m. x/x/x	xp.m. x/x/x	User key X present on pastebin.com	OSINT Scanner	Request was issued to site and information was removed. Affected email users were notified to be on alert
012	xp.m. x/x/x	xp.m. x/x/x	Application X on IP X is vulnerable to CVE XXXX-X	CVE Scanner	Application updated
013	xp.m. x/x/x	xp.m. x/x/x	S3 bucket x publically accessible	AWS S3 Scanner	Access controls implemented
...					

Figure 6, Wireframe: Closed Alerts

1.7 AWS S3 Scanner Module Home Page

The wireframe shows a web browser interface for the AWS S3 Scanner module. At the top, there are standard navigation icons (back, forward, search) and a URL bar containing <http://heimdall.ie/module/awsScanner/>. Below the header is a horizontal menu bar with links: Home, Alerts, Modules, Reports, Keys, and Logout. The main content area is divided into two sections: "Current AWS Range(s)" and "Active AWS Alerts".

Current AWS Range(s)

Add New AWS Range:

Range	Date Added	Last Associated Alert
x.aws.com	x/x/x	xp.m. x/x/x
192.168.1.1	y/y/y	yp.m. y/y/y

Active AWS Alerts

Alert: ID X x.a.m. x/x/x Basic Description action
Alert: ID Y y.a.m. y/y/y Basic Description action
Alert: ID Z z.a.m. z/z/z Basic Description action
...

Figure 7, Wireframe: S3 Scanner Home Page

1.8 CVE Scanner Module Home Page

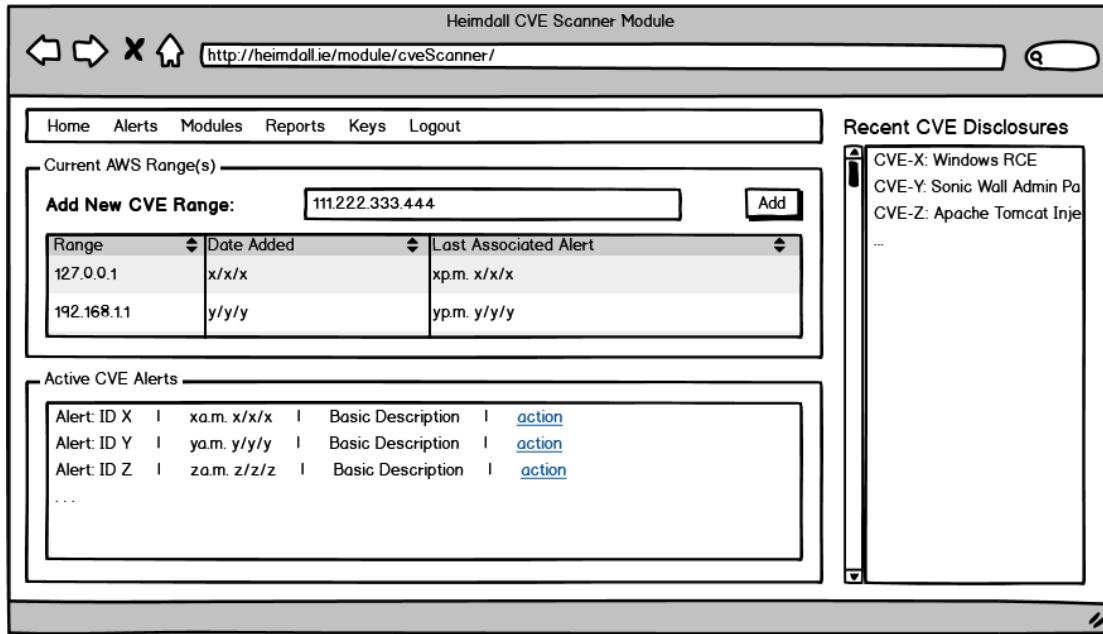


Figure 8, Wireframe: CVE Scanner Home Page

2. Sequence Diagrams

2.1 Generic Sequence

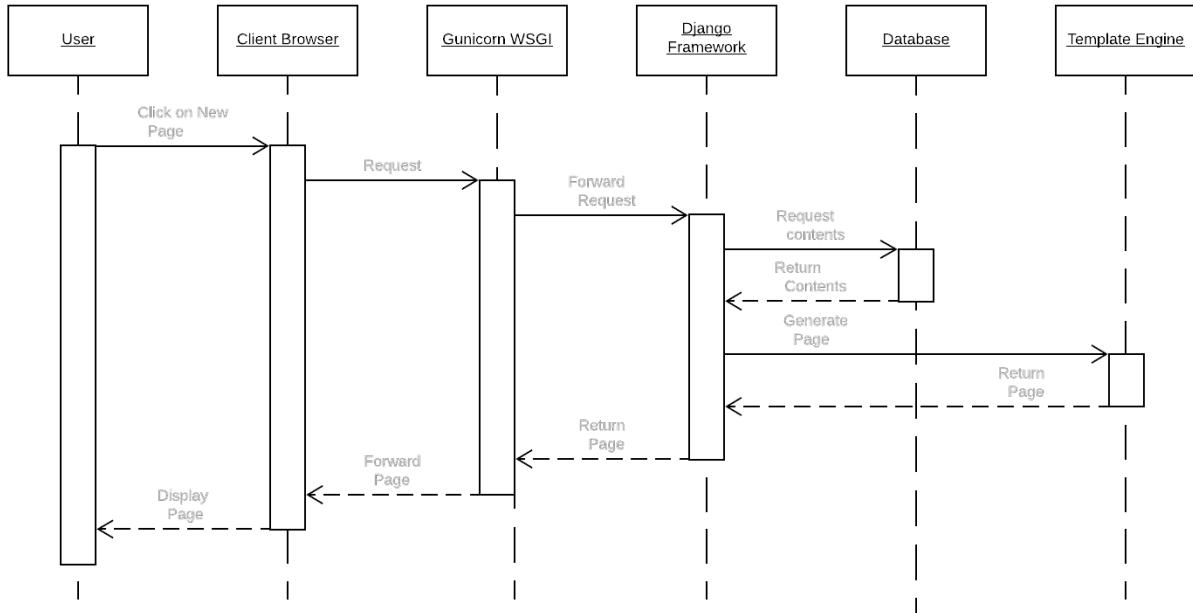


Figure 9, Sequence Diagram: Generic Request

2.2 Report Generation Sequence

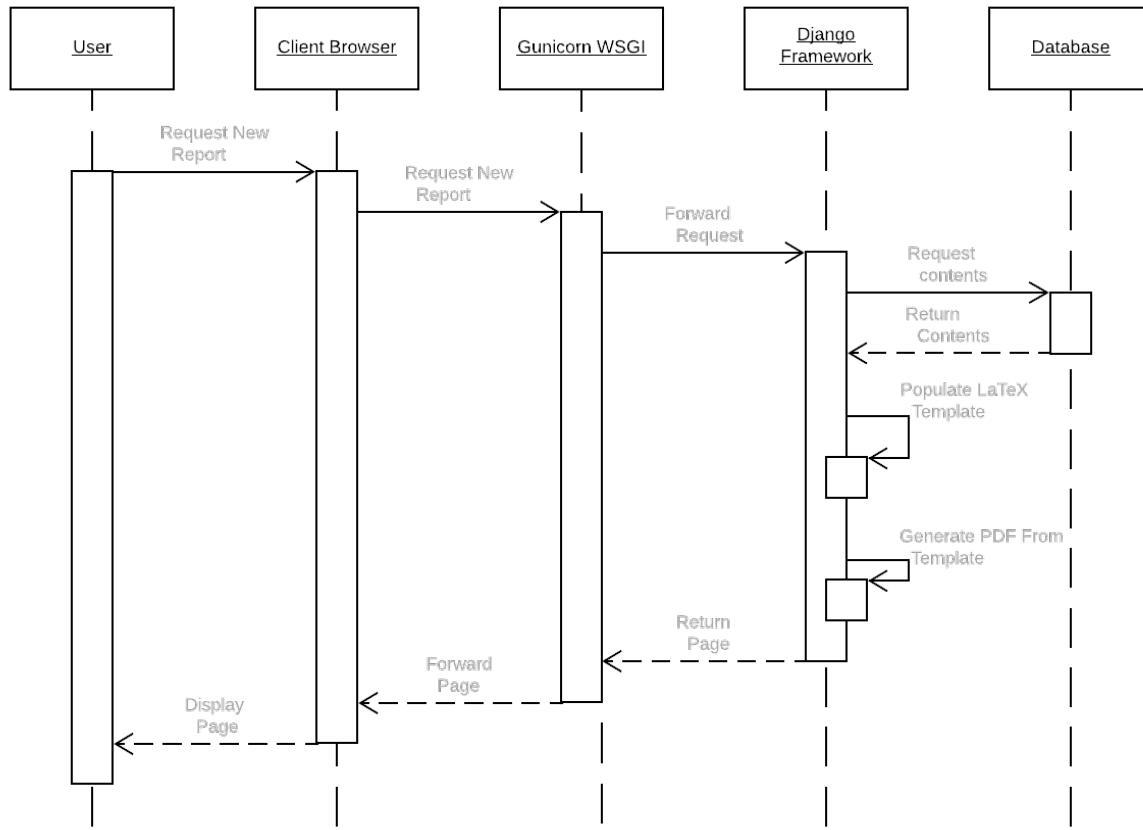


Figure 10, Sequence Diagram: Report Generation

2.3 Generic Scanner Sequence

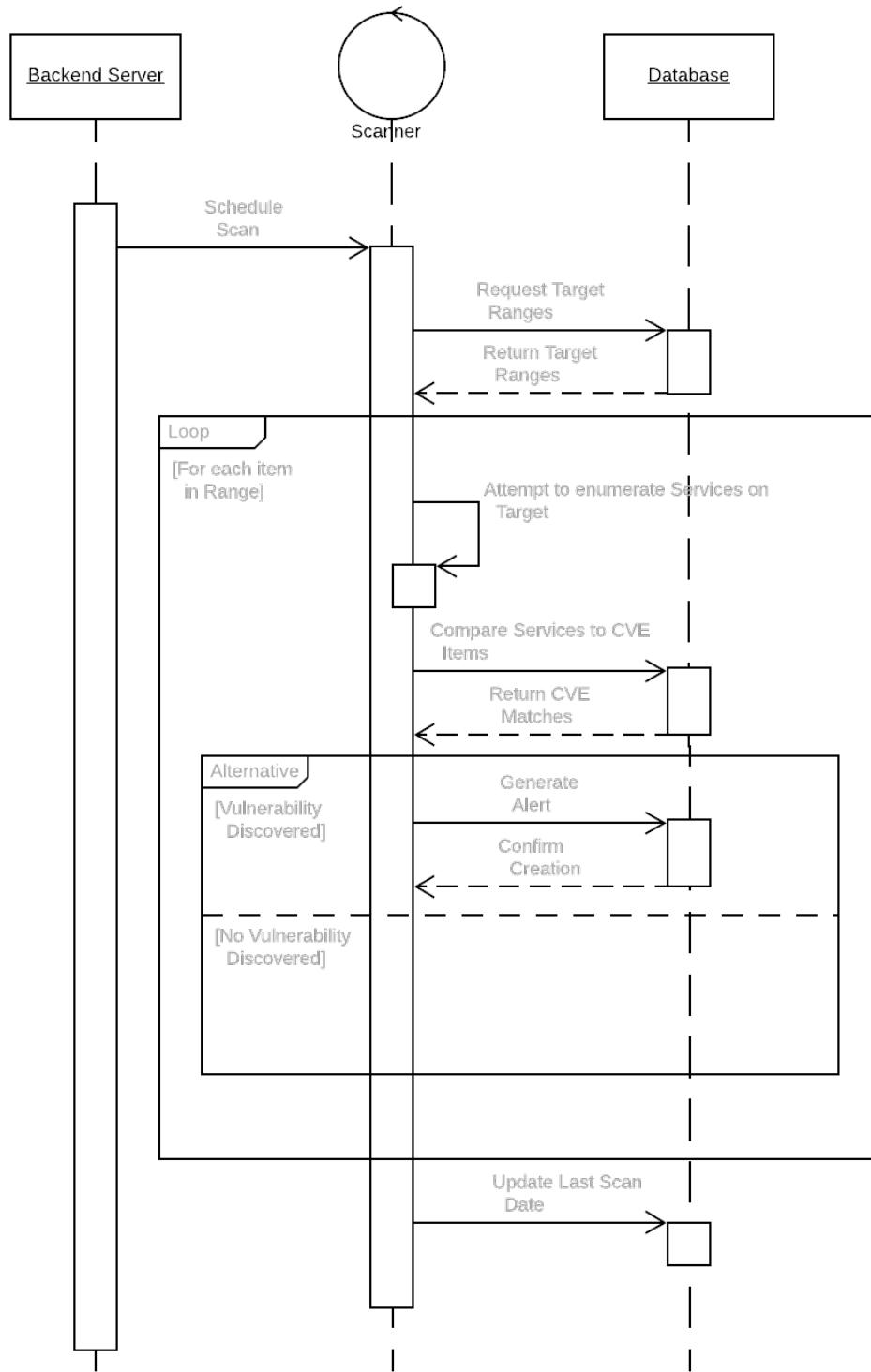


Figure 11, Sequence Diagram: Generic Scanner

3. ER Diagram

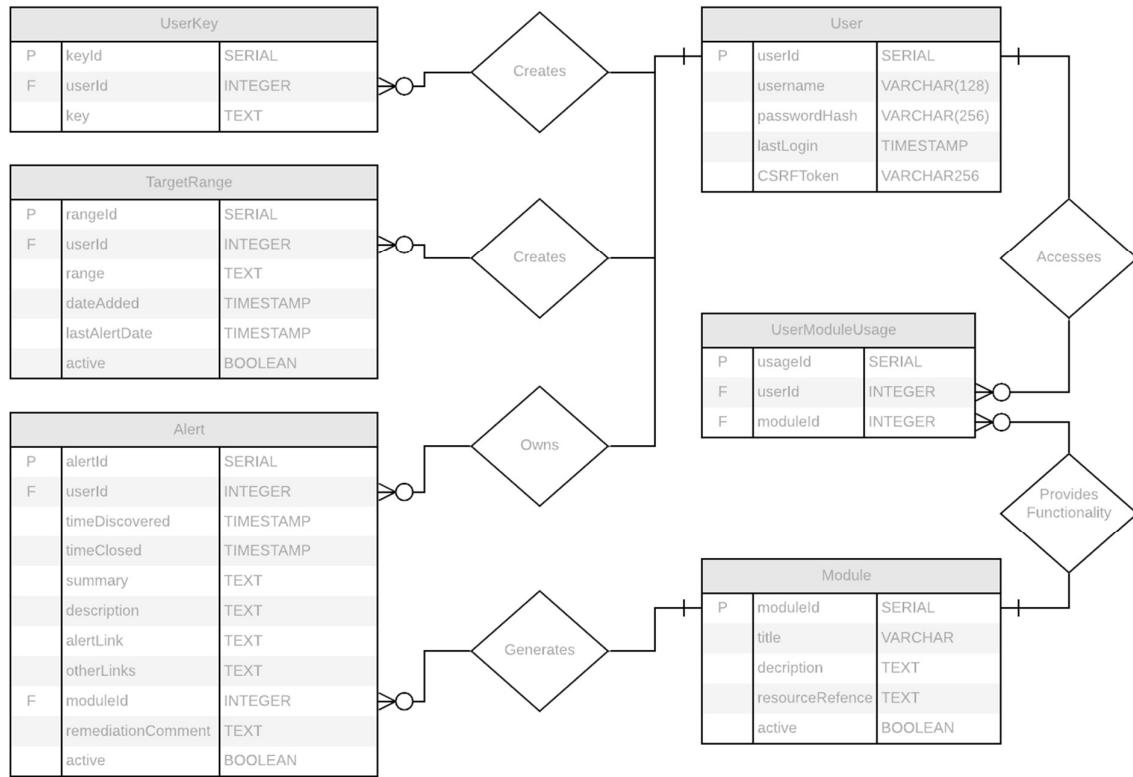


Figure 12, Entity Relationship Diagram