**Final Year Research Topic**

**Vulnerability Tracker**

There is government compliance to scan the servers so currently it is scanned manually those tasks are automated by this system. In this system, the servers’ vulnerabilities will be fixed by assigning them to the relevant person in the organization. When it is fixed by the assigned user it will be forwarded to the department that assigned the task. That department will be checked if it is fixed by scanning the server then the status will be updated as the vulnerability is fixed if it is still not fixed the status will be not updated. There are some scenarios the assigned user will reject the assigned tasks since it is not related to them. So, tasks must be assigned to a related user again by that assigning department.

### **Maintain the Server details with the priority level**

#### Include the live server details on a priority basis.

#### Include the vulnerability scanning schedule according to the priority basis of the servers.

#### Include tags related to server details (Ex:- O/S version, Web application, Service)

#### Include scan details, follow-up details, and escalation details.

#### The system shall allow browsing on a particular server and viewing the details.

#### The system shall display detailed information about the onboarded server.

### **Manage server details (Add/Remove/Update)**

#### The system shall allow adding/removing/updating server details on a user basis.

#### The system shall allow adding vulnerability scan details on the following categories App

DB, O/S

# The system shall allow to update of the Vulnerability status after fixing by the responsible party.

### **Provide a Search facility.**

# The system shall enable the user to search for particular server details by providing a keyword.

# The system shall enable users to select multiple options on the screen to search.

# The system shall display all the matching products based on the search.

# The system shall enable the user to navigate between the search results.

# The system shall notify the user when no matching product is found on the search.

### **Maintain user profiles**

# The system shall allow the user to create a profile and set his credential.

# The system shall authenticate user credentials to view the profile.

# The system shall all the ow user to update their profile information.

# The system shall allow the user to commit the fixed vulnerability from the system.

# The system shall display assigned vulnerabilities of the particular servers to the users.

### **Provide personalized profile**

### .

1. The system shall display V/A scan history in the user profile.
2. The system shall allow users to assign vulnerabilities to particular business units.
3. The system shall display detailed information about the selected server.
4. The system shall allow to over-right of committed tasks of a particular user by the admin account.

### **Email confirmation**

1. The system shall maintain the user’s email information as a required part of the customer profile.
2. The system shall send an email to the respective user when a particular vulnerability was assigned.
3. The system shall send follow-up emails to the users based on the assigned vulnerabilities.
4. The system shall escalate the follow-up to the next line of command when the first two follow-ups didn’t get any reply.
5. The system shall display all the follow-up details.

### **Report Generation**

1. The system shall display customized reports based on the imputed content.

Domain controller

Database

Application

Server Type

Non - Critical

Public facing

Critical Servers

V/A scan Schedule

Escalation party

Fixing schedule

Criticality

Vulnerabilities

Vulnerabilities

V/A scan Schedule

Followup dates

Previous Scan dates

Next Scan Date

Scan Date

Non - Critical

Public facing

Critical

Server Criticality

Responsible person

Server Name

Current V/A scan status

IP Address

Server Type

Scan Date

Server Criticality

Server