

---

# Software Vulnerability Patch Management

**Sponsored by Coupa Software**

Point of contact: Philip Cox ([phil.cox@coupa.com](mailto:phil.cox@coupa.com))

**Team Members**

Amruta Gadgil / Pramothini Dhandapany / Fei Hao

**Faculty Advisor**

Patrick Tague ([tague@cmu.edu](mailto:tague@cmu.edu))

---

# Agenda

- Introduction
- Motivation
- Related Work
- System Design
- System Implementation
- Demo
- Experiments/Analysis
- Conclusion
- Future work

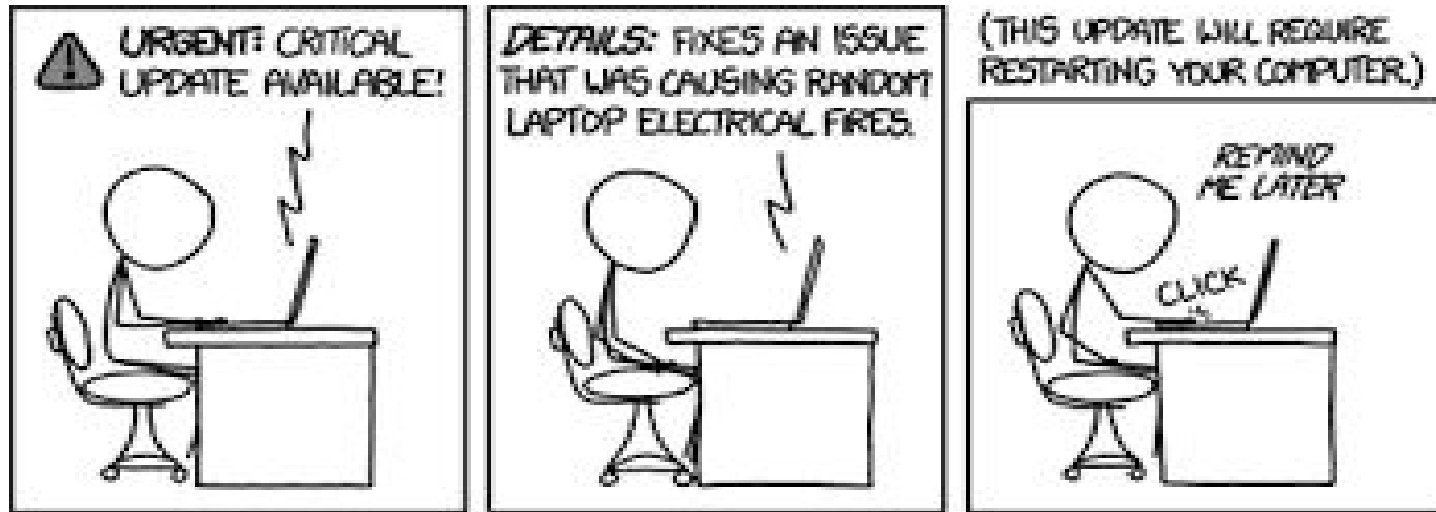


# Introduction



# What is Patch Management

Patch management involves planning when the patches should be applied to systems.



# Project Background

Basic project work involves:

- Build a web application to:
  - Manage software patches
  - Prioritize patches, based on
    - Severity of vulnerabilities
    - Asset importance
  - Provide automation-friendly reports

---

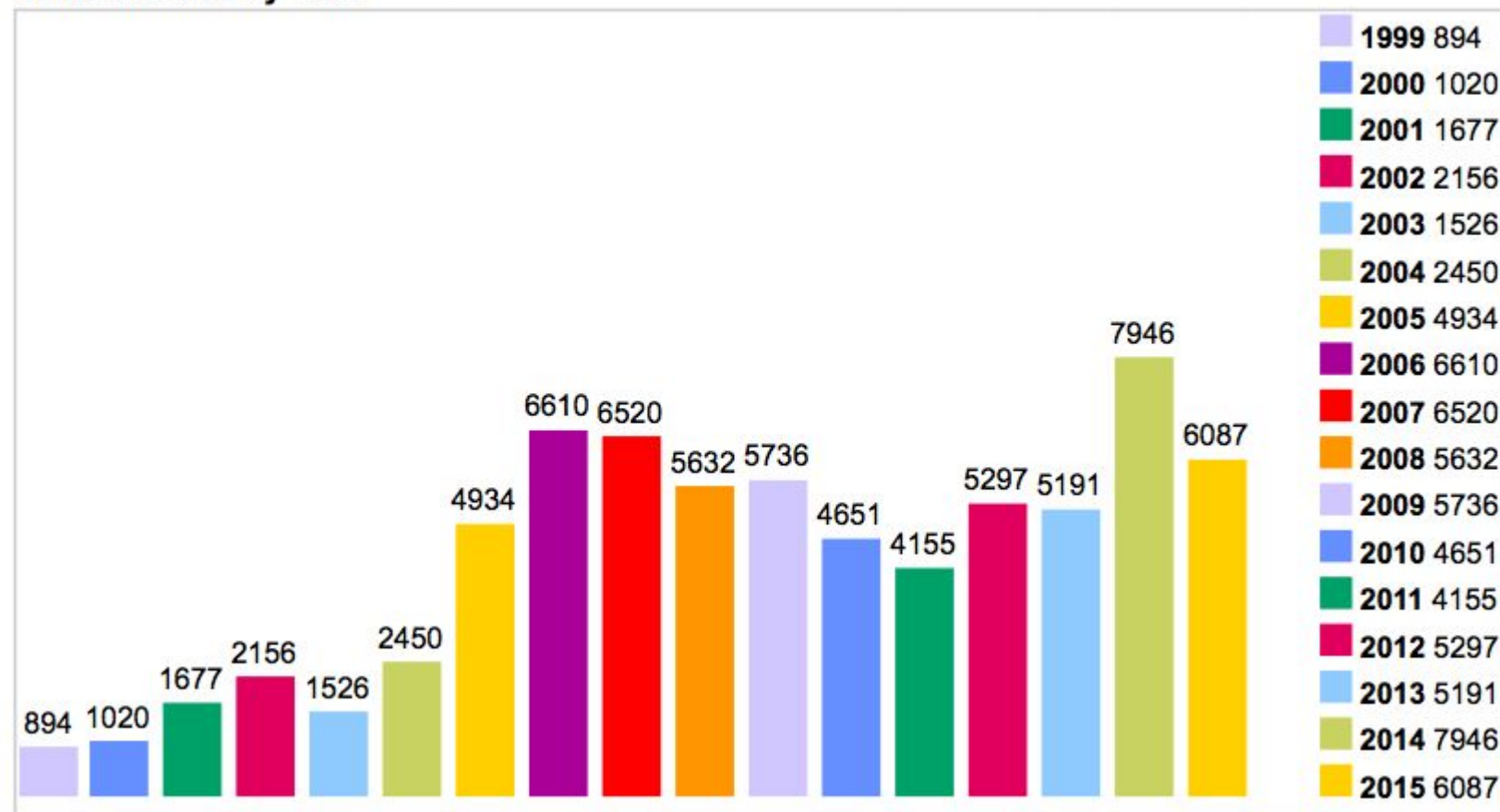
---

# Motivation

---

---

## Vulnerabilities By Year



# Mechanisms to assess the severity of Vulnerability

- CVE: Common Vulnerabilities and Exposures
  - A dictionary of publicly known information security vulnerabilities and exposures
- Rating from 1-10 based on severity of vulnerability
- Been adopted as primary method for quantifying the severity of vulnerabilities by a wide range of organisations and companies
  - NVD (National Vulnerability Database)
  - Qualys



# Asset Importance

- Is CVE Score sufficient? What about environmental impact?
- Environmental impact: the importance of host machine on which patch will be applied
  - Will a software used in a front end server have the same priority as a software that is used in an internal tool?
  - Environmental Impact is different for every organization!
- Environmental impact considers:
  - Where an IP is placed in network (e.g. internal or external server)
  - The importance of services being run on it
  - Availability of backups (load balancing)

---

---

# Related Work

---

---

# Qualys

- <https://www.qualys.com> - “The Leading Provider of Information Security and Compliance Cloud Solutions”
- Network scan support
- Vulnerability reporting
- New Patch Report tool - <https://www.qualys.com/company/newsroom/news-releases/usa/2010-06-21/>
- **NOT Open Source!**
- **NO Custom Business Risk Calculation**

---

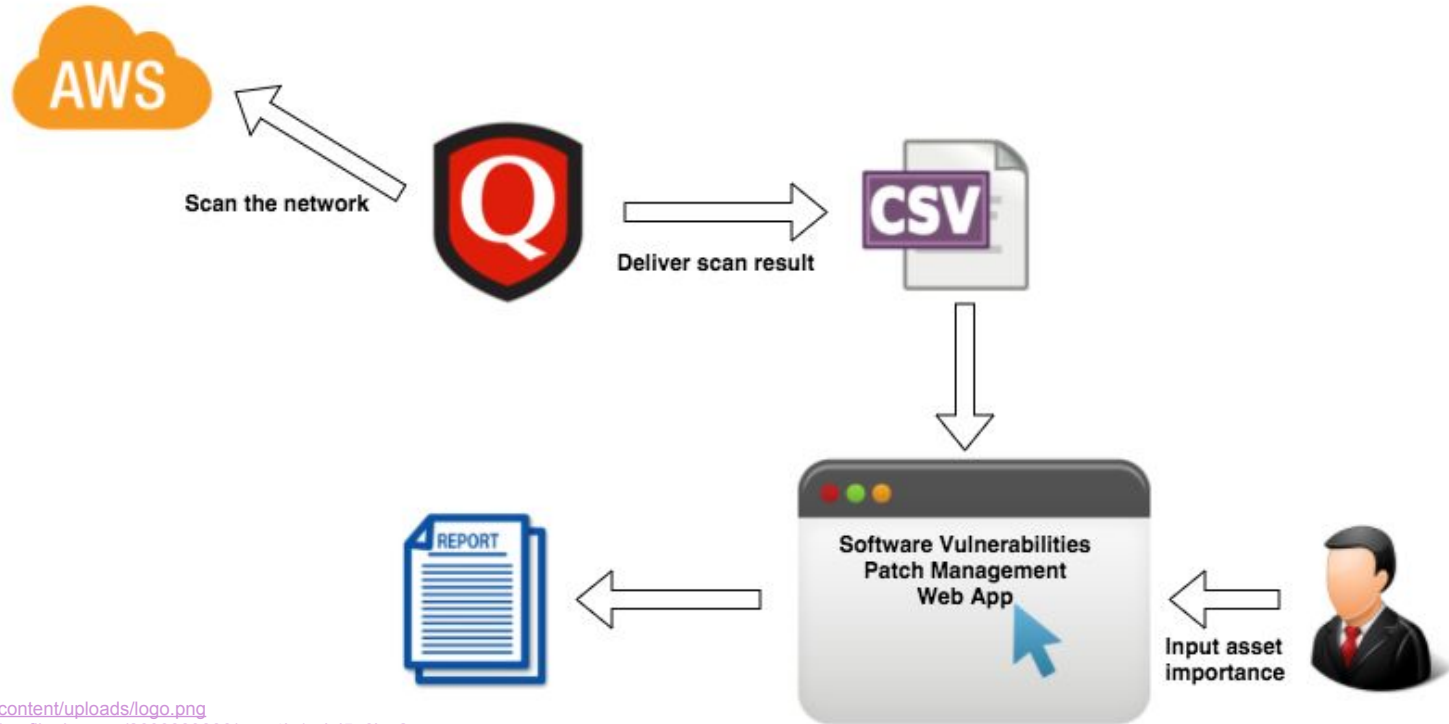
---

# System Design

---

---

# System Diagram



<http://nikuniku.me/wp-content/uploads/logo.png>

[https://pbs.twimg.com/profile\\_images/2600889806/ggrs4jx1qdg5o6hw2zv.png](https://pbs.twimg.com/profile_images/2600889806/ggrs4jx1qdg5o6hw2zv.png)

[http://pgloader.io/img/csv\\_text.png](http://pgloader.io/img/csv_text.png)

[http://www.estormwater.com/sites/default/files/imagecache/article\\_max/report-icon.jpg](http://www.estormwater.com/sites/default/files/imagecache/article_max/report-icon.jpg)

[https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcSIQ1Ep3LnaSQx9weN1gbSW9Nh2vxPQs33E\\_hjkfpjJUdBF7vRDXQ](https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcSIQ1Ep3LnaSQx9weN1gbSW9Nh2vxPQs33E_hjkfpjJUdBF7vRDXQ)

# Project Goals - Planned Tasks

Committed Tasks
Pull a <b>complete system inventory</b> - using a <b>csv file as input</b>
Assign <b>default importance rating</b> for assets
Build a <b>web interface</b> - to take asset importance rating as <b>input from user</b>
Build a <b>web interface</b> - to <b>show the report</b> with <b>prioritized patches</b> to be applied - based on business risk
Provide a way to <b>download the report in csv</b> format
Provide a way to <b>download the report in json</b> format
Provide <b>authentication mechanism</b> to the web application, where users can register and sign-in
Provide <b>user roles</b> in the web application, like admin user and non-admin user
Build a <b>web interface</b> - to take <b>new csv file</b> as input for <b>modified</b> asset data

# Other useful features

Additional (Nice to have) Features implemented based on client feedback
Provided functionality for user to be able to <b>sort</b> the report displayed on web page, based on chosen columns
<b>Pie chart</b> showing <b>distribution</b> of vulnerabilities based on business risk
Provision for <b>bulk edit</b> the asset importance rating
"Select all" option to select all the assets
<b>Search</b> function on asset IPs
'Star'-based <b>rating</b> mechanism

# DB Schema

AssetRating	
PK	IP
	Rating

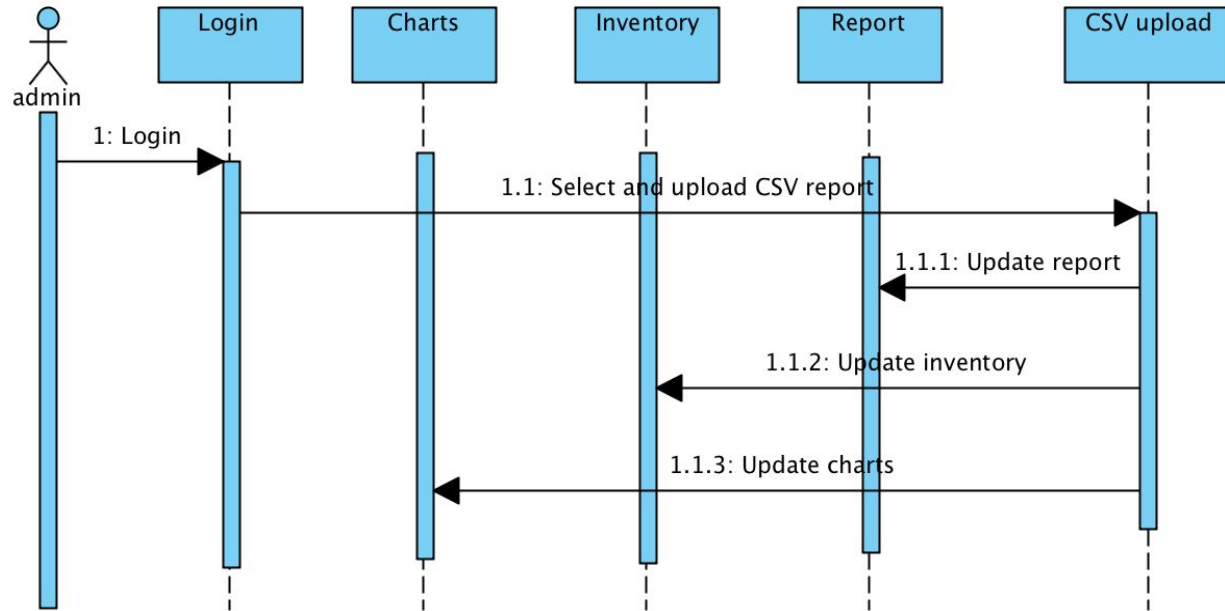
ReportTable	
PK	Id
	title
	cveld
	threat
	impact
	solution
	severity
FK1	assetInfo

UserTable	
PK	id
	username
	password
	email
	first_name
	last_name
	is_staff
	is_active



# System Sequence Diagram

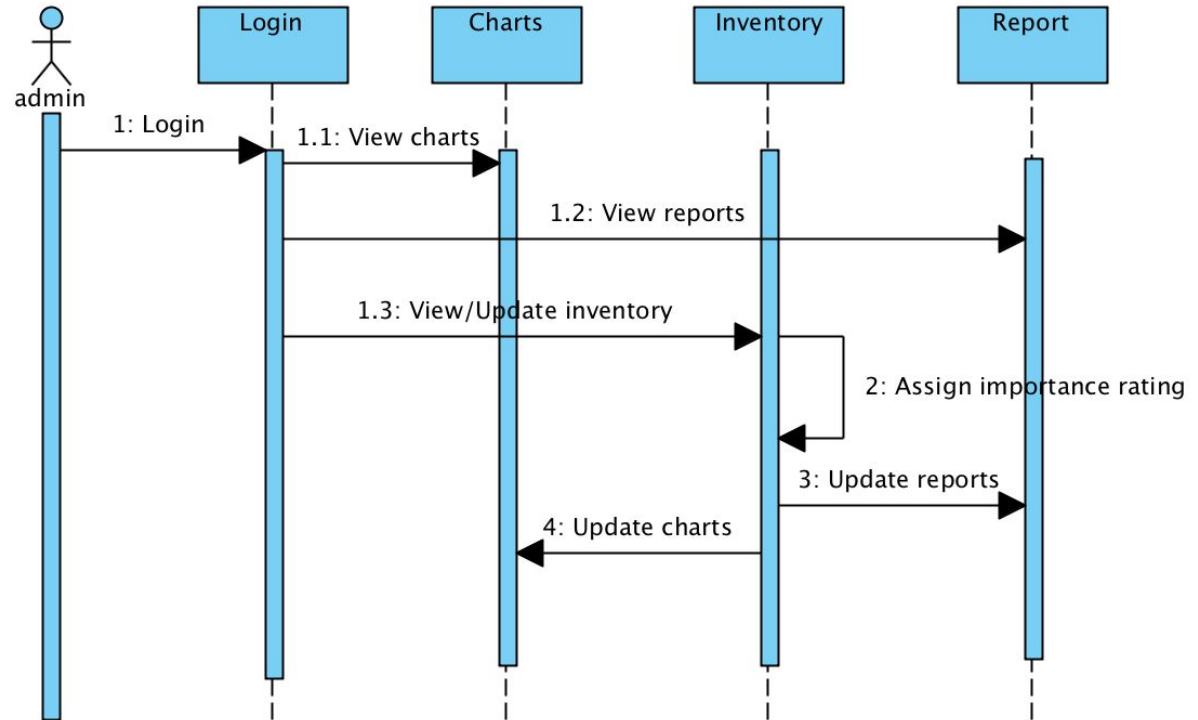
1. Upload new file (csv) and update report, inventory, and chart



# System Sequence Diagram

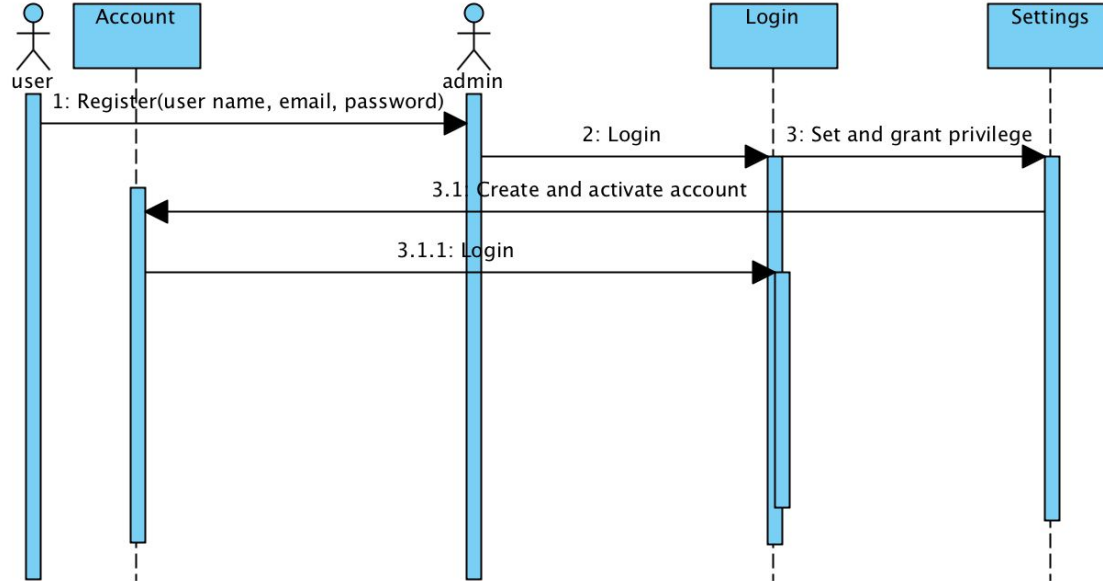
2. View inventory, reports and charts;

Assign/update assets importance rating

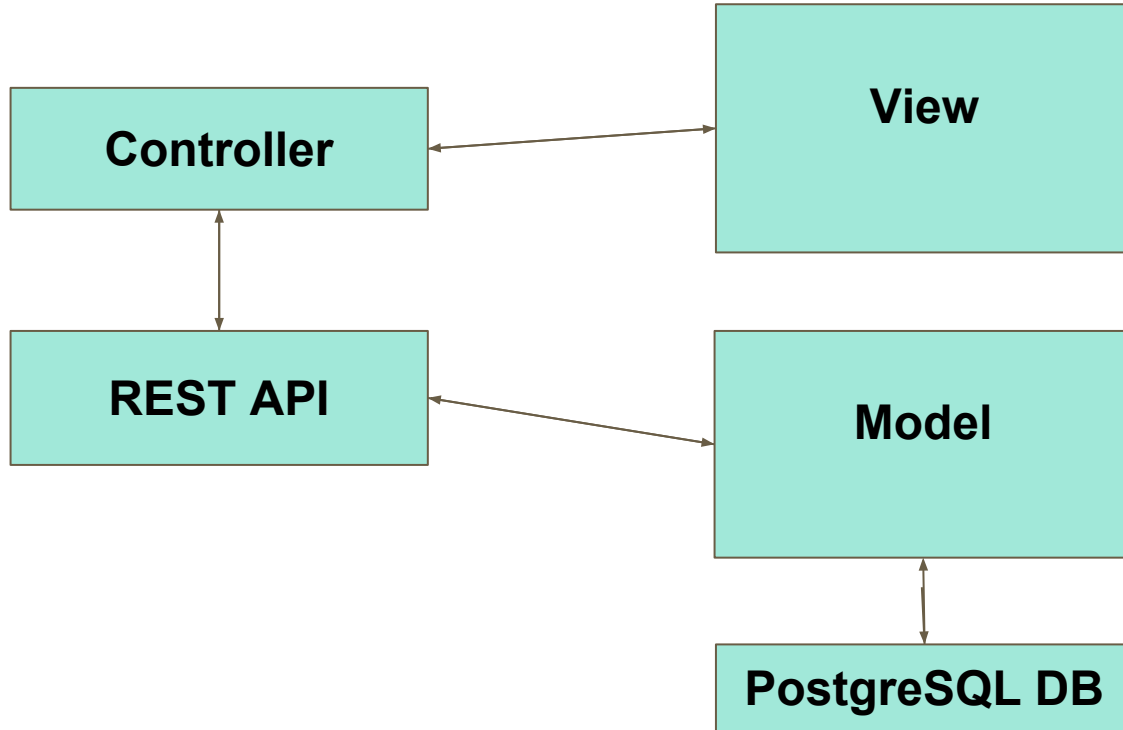


# System Sequence Diagram

## 3. Register and create account



# System design general block diagram



---

---

# System Implementation

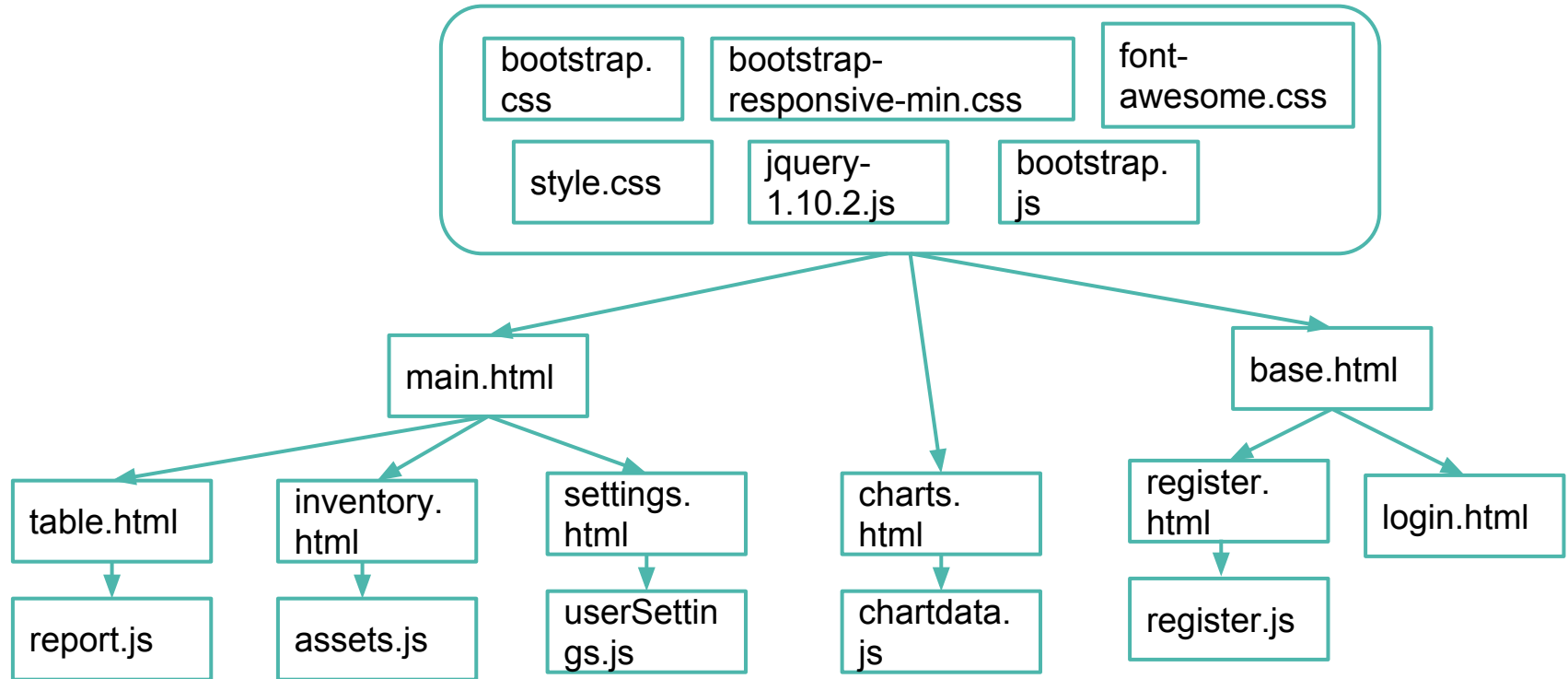
---

---

# Technologies Applied

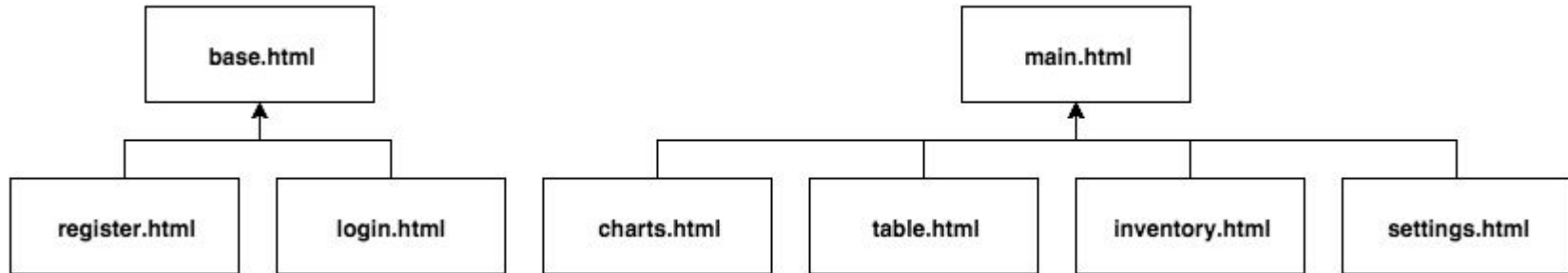
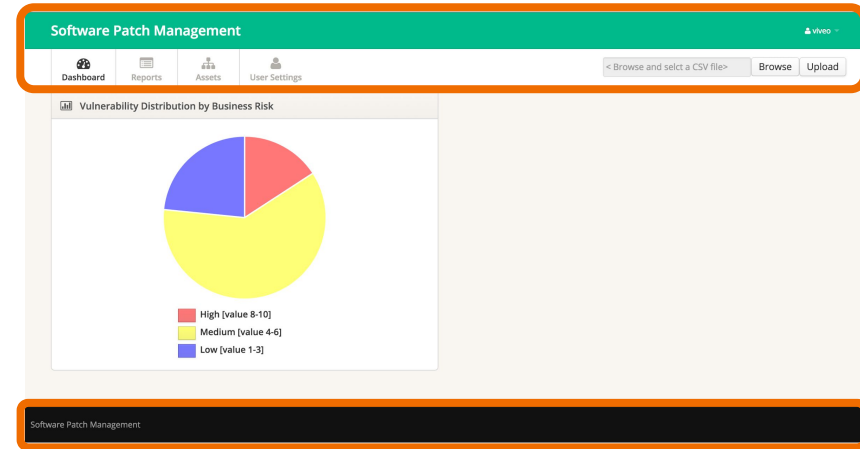
- Python-Django framework for web application development
- PostgreSQL as backend database
- REST API as database connector
- Bootstrap for enhanced UI
- Javascript plugins like jQuery for dynamic contents

# Developed Modular code - UI



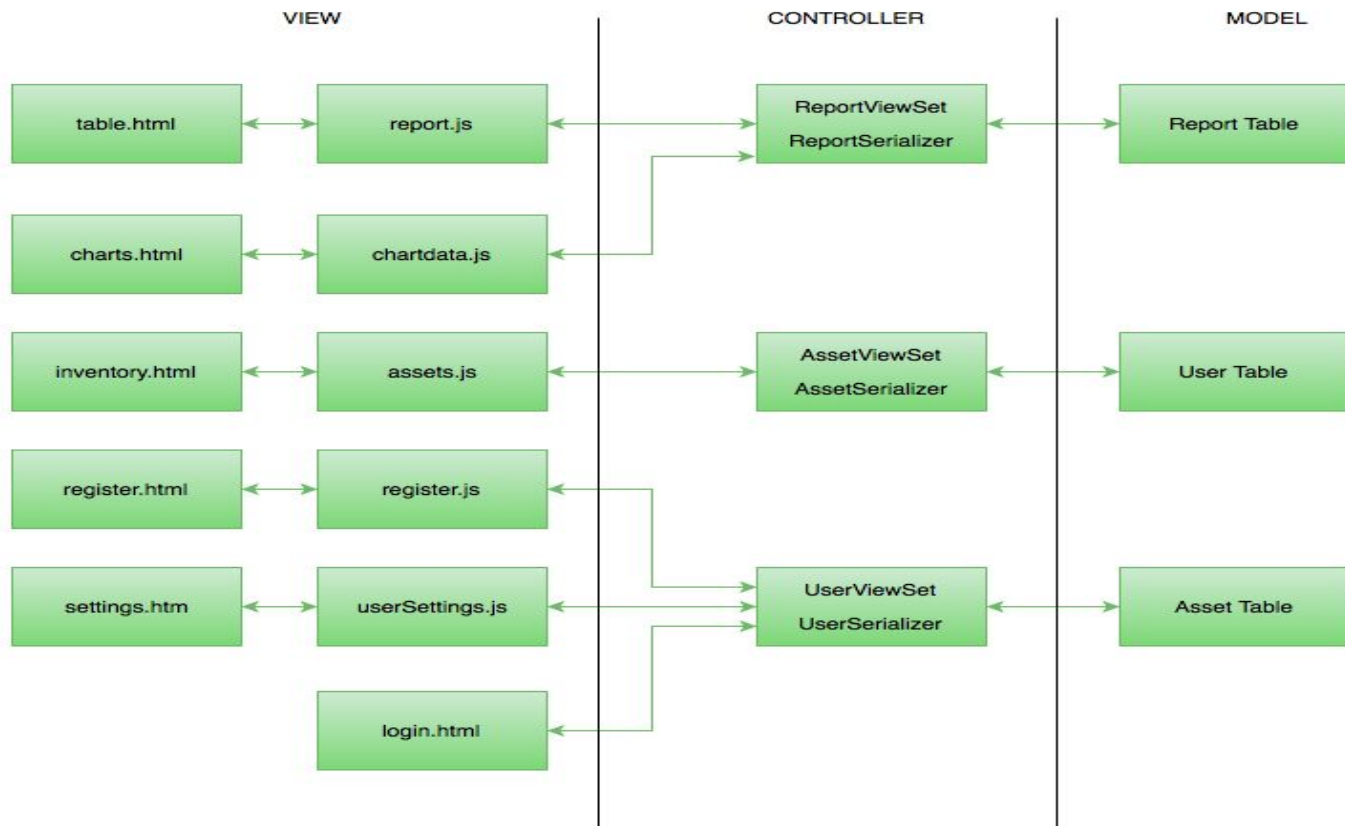
# Template Inheritance in UI

- **Inherit** navigation bar, and footer





# Developed Modular code



---

# Demo

<http://software-patch-management.herokuapp.com/>

---

---

---

# Experiments/Analysis

---

---

# CSV Validation

Failure Scenarios
No uploaded file.
The uploaded file is empty (no content).
The uploaded file is not a CSV file (suffix is not .csv).
The uploaded file's size is too big (larger than 50MB).
The uploaded file does not have a row with its first column as "IP" (no header row).
The uploaded file has the required header but no content (the header row is the last row).
The uploaded file has a header row started with "IP", but the fields in this row are not correct.
The uploaded file has row(s) with incorrect number of columns (record length).
The uploaded file has invalid "IP" value.
The uploaded file has invalid "Severity" value.

# General Functionality: Report page

## Download Reports:

- click csv - report gets saved as export.csv
- click json - report gets saved as export\_as\_json.csv

## Browse:

- explorer pops up to choose csv file

## Upload:

- updated report table page displayed

## Table header click:

- sort the column
- toggle sort on same column

# General Functionality: Assets page

## Search:

- search any ip (only numbers and dots)
- search invalid characters
- search more than 15 characters

## Select all:

- select all displayed assets

## Submit:

- with bulk update checkboxes selected
- without bulk update

## Cancel:





















- with bulk update
- without bulk update

# General functionality: Dashboard

## **Dashboard:**

- Business risk distribution
- Custom business risk calculation
- Sliders on dashboard

# Authentication

User	Login	View Dashboard, Asset and Report table data	View/upgrade other users	upload csv	Download report table details
Admin					
non Admin					
Registered but not approved					
Anonymous					



---

---

# Conclusion

---

---

# Conclusion

- Our project is a small part of a big vision
- Need for a standard software patching system, which is:
  - Automated
  - Organized
  - Well tracked



# Future Work



# Future Work - New features

- Qualys API support
- Logging
- IPv6 address for assets
- Host names for assets
- Use downloaded reports to apply patches without manual intervention
- Support for multiple organizations

# Future work - Enhancements in existing features

- Colored rows in report table based on severity group
- Option to choose download file name
- Forgot password security questions/Reset password support
- Admin user - support to revoke privilege
- After 3 unsuccessful login attempts, block the account

---

---

# References

---

---

# References

- <http://www.patchmanagement.org/pmessentials.asp>
- <https://www.qualys.com/docs/qualys-api-v2-user-guide.pdf>
- <https://community.qualys.com/community/training>
- <http://learn.onemonth.com/ruby-vs-python>
- <http://www.djangobook.com/en/2.0/chapter01.html>
- <https://www.digitalocean.com/community/tutorials/sqlite-vs-mysql-vs-postgresql-a-comparison-of-relational-database-management-systems>
- <https://cve.mitre.org/>
- <http://www.cvedetails.com/browse-by-date.php>
- "Security in Django". Django Project. Retrieved March 25, 2013.
- Socol, James (2012). "[Best Basic Security Practices \(Especially with Django\)](#)". Retrieved March 25, 2013.
- <https://pypi.python.org/pypi/csvvalidator>

# References (Cntd...)

- <http://blog.kevinchisholm.com/javascript/jquery/jquery-ajax-get-post-difference/>
- <http://api.jquery.com/jQuery.ajax/>
- [http://www.w3schools.com/jquery/jquery\\_ref\\_ajax.asp](http://www.w3schools.com/jquery/jquery_ref_ajax.asp)
- [http://www.w3schools.com/jquery/ajax\\_ajax.asp](http://www.w3schools.com/jquery/ajax_ajax.asp)
- <http://stackoverflow.com/questions/8683922/how-can-i-pass-my-context-variables-to-a-javascript-file-in-django>
- <http://www.mkyong.com/jquery/jquery-loop-over-json-string-each-example/>
- <https://css-tricks.com/star-ratings/>
- <http://tympanus.net/codrops/2012/12/17/css-click-events/>
- <http://code.stephenmorley.org/html-and-css/star-rating-widget/>
- <http://www.evotech.net/blog/2007/08/css-javascript-character-entities/>
- <http://www.w3.org/Style/Examples/007/evenodd.en.html>
- <http://egrappler.com/templatevamp-free-twitter-bootstrap-admin-template/>



# References (Cntd...)

- <http://www.freeformatter.com/html-formatter.html#ad-output>
- <http://stackoverflow.com/questions/5871730/need-a-minimal-django-file-upload-example>
- <https://godjango.com/41-start-your-api-django-rest-framework-part-1/>
- <http://django-tastypie.readthedocs.org/en/latest/interacting.html>
- <http://dada.theblogbowl.in/2014/12/how-to-use-requestput-or-requestdelete.html>
- <http://stackoverflow.com/questions/31880227/django-rest-framework-method-put-not-allowed-in-viewset-with-def-update>
- <http://docs.python-requests.org/en/latest/api/#requests.Request>
- <http://www.django-rest-framework.org/topics/3.0-announcement/>
- <http://www.django-rest-framework.org/api-guide/relations/>
- <https://baxeico.wordpress.com/2014/06/25/put-and-delete-http-requests-with-django-and-jquery/>
- <http://stackoverflow.com/questions/14367595/django-rest-framework-posting-foreign-key-field-containing-natural-key>
- [Django Rest Framework in your PJ's:](#)
- <https://www.youtube.com/watch?v=xMtHsWa72Ww>
- <https://github.com/tomchristie/django-rest-framework/issues/2403>
- <http://voorloopnul.com/blog/doing-bulk-update-and-bulk-create-with-django-orm/>
- <https://docs.djangoproject.com/en/dev/ref/models/querysets/#bulk-create>
- <https://editor.datatables.net/examples/styling/bootstrap.html>
- <http://stackoverflow.com/questions/6666532/how-to-force-table-cell-td-content-to-wrap>
- <http://www.stoimen.com/blog/2010/03/31/jquery-get-the-id-of-the-current-element/>
- <http://www.eyecon.ro/bootstrap-slider/>

---

---

# Questions..?

---

---



**Thank you!**

