

MICHIGAN STATE
UNIVERSITY

Alpha Presentation

Predictive Engine for Long-Term Malware Detonation

The Capstone Experience

Team Proofpoint

Izzy Dove

Samuel Gendelman

Alexander Kendall

Joshua Wilson

Geoffrey Witherington-Perkins



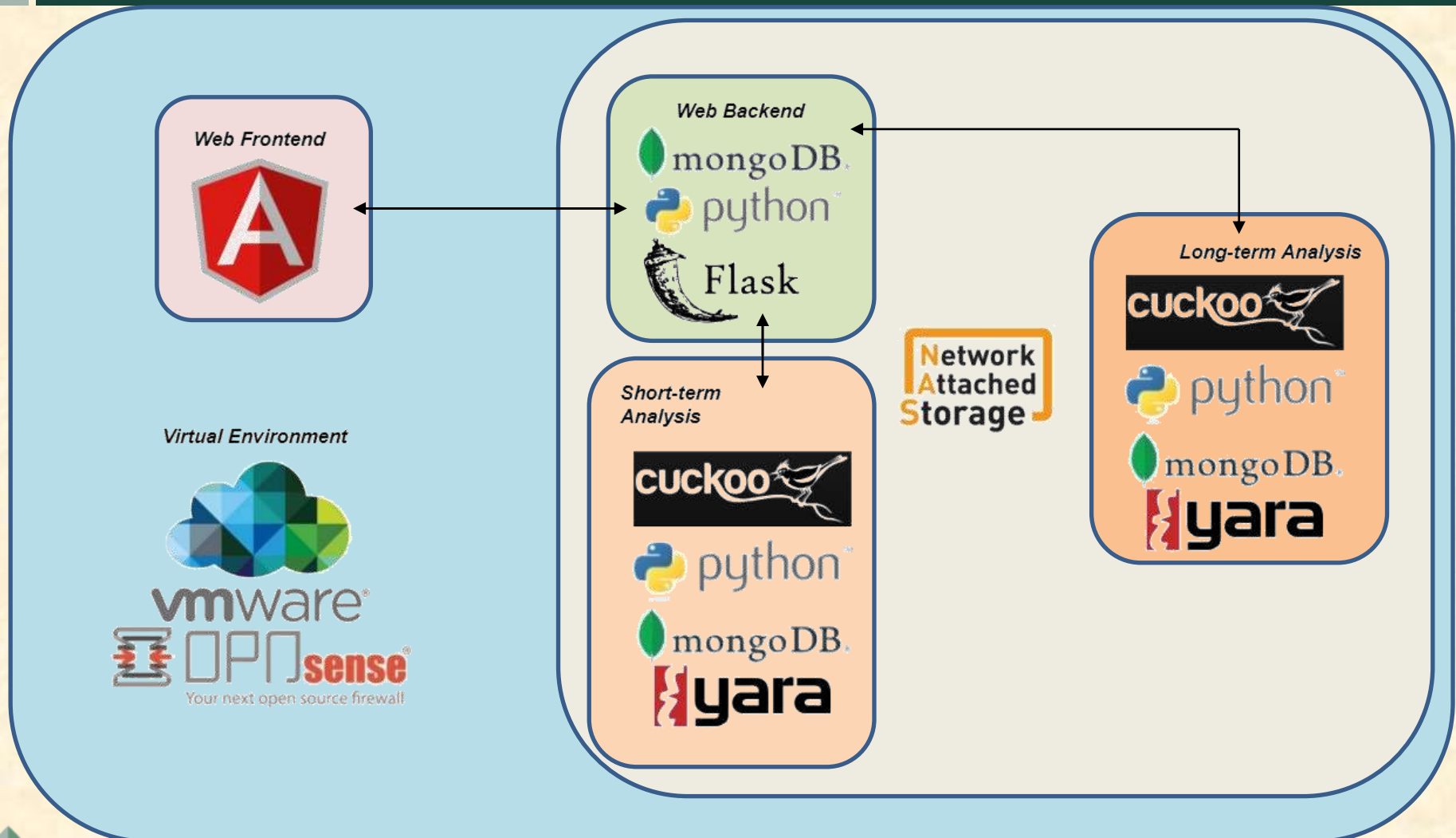
From Students...
...to Professionals

Department of Computer Science and Engineering
Michigan State University
Spring 2020

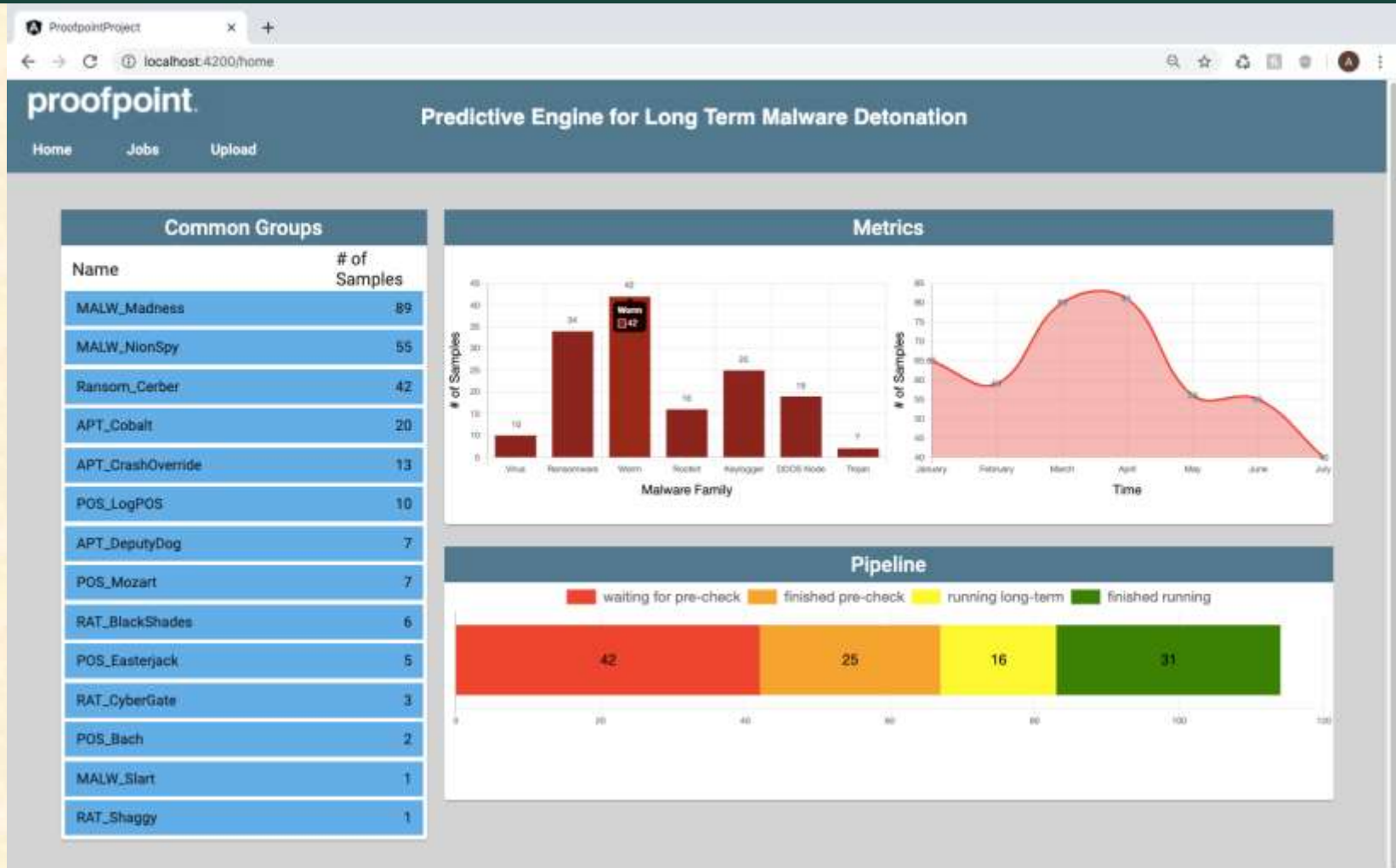
Project Overview

- Long-term malware detonation & analysis
- Automatic categorization of malware
- Web app to display analysis data

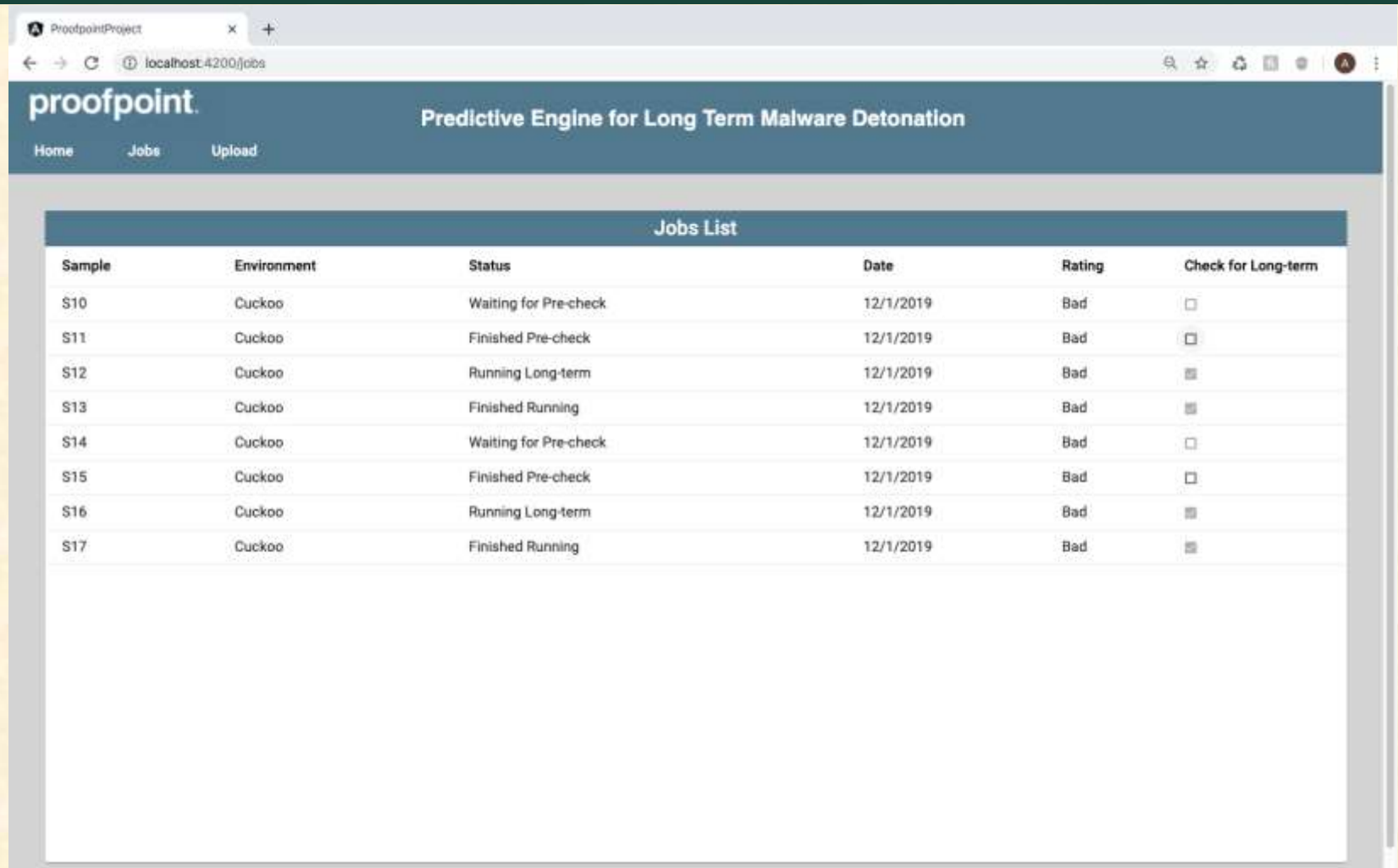
System Architecture



Dashboard



Jobs List

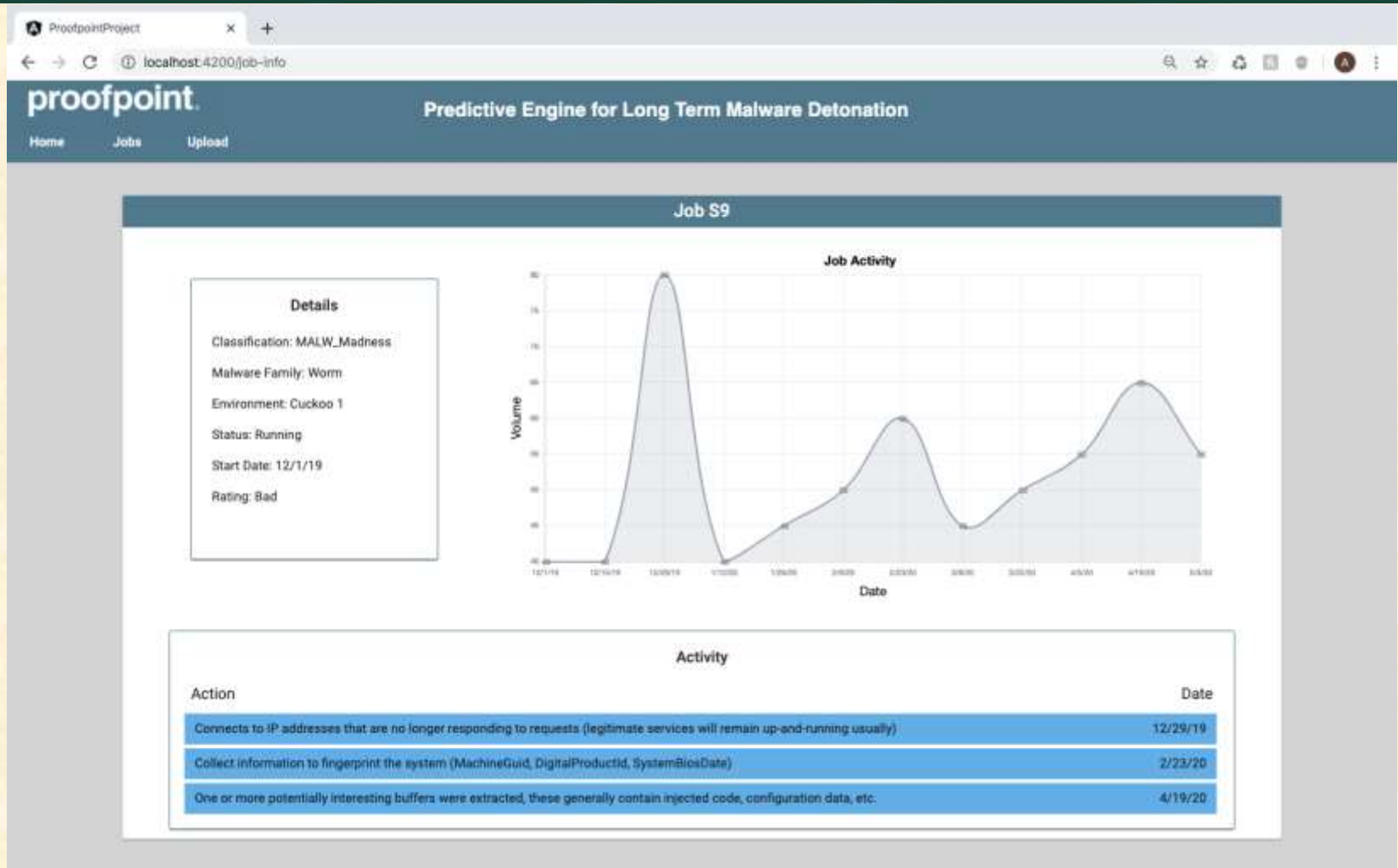


The screenshot shows a web browser window with the URL `localhost:4200/jobs`. The page header includes the Proofpoint logo and the title "Predictive Engine for Long Term Malware Detonation". Below the header is a navigation bar with links for "Home", "Jobs", and "Upload". The main content area displays a table titled "Jobs List" with the following data:

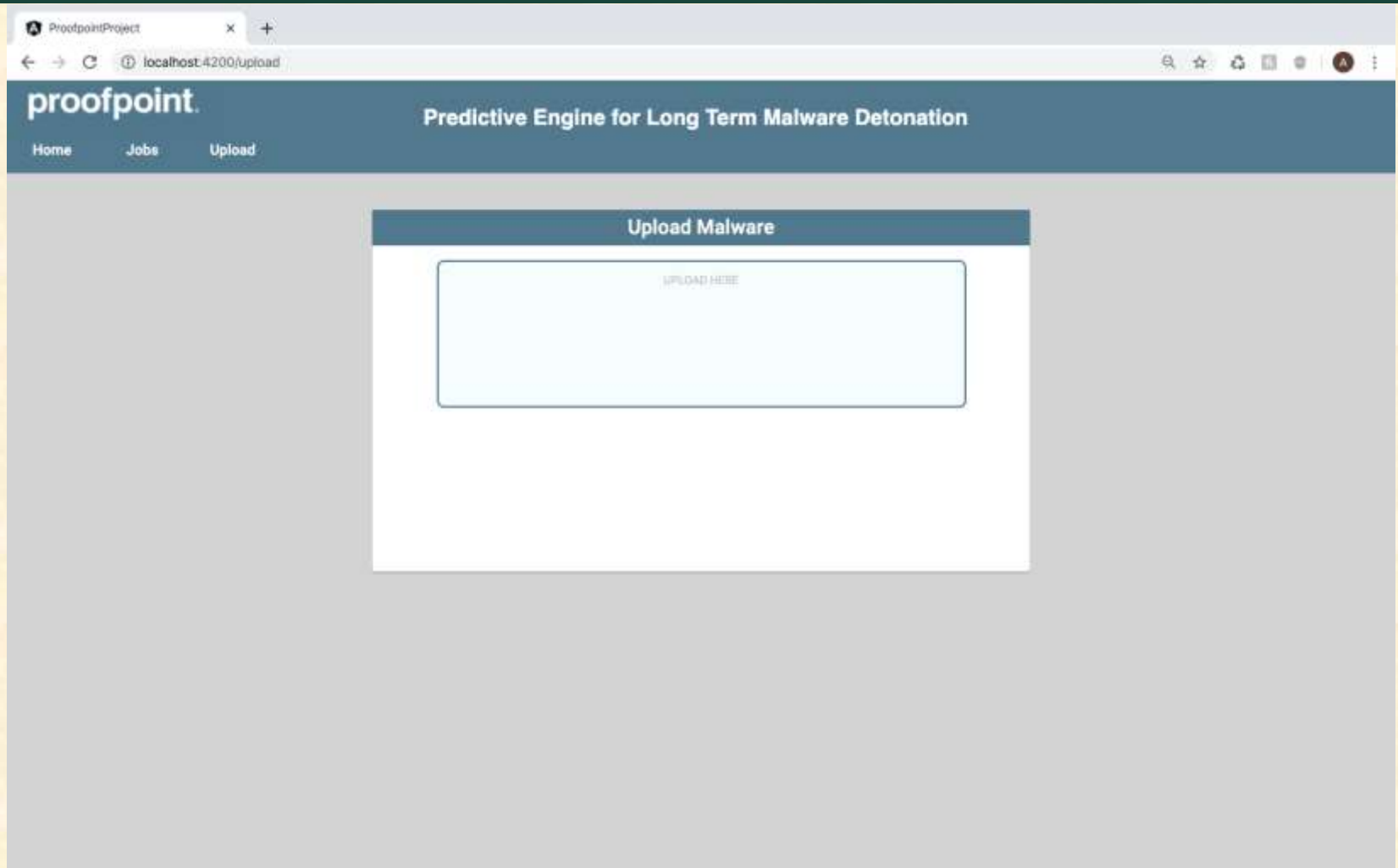
Sample	Environment	Status	Date	Rating	Check for Long-term
S10	Cuckoo	Waiting for Pre-check	12/1/2019	Bad	<input type="checkbox"/>
S11	Cuckoo	Finished Pre-check	12/1/2019	Bad	<input type="checkbox"/>
S12	Cuckoo	Running Long-term	12/1/2019	Bad	<input checked="" type="checkbox"/>
S13	Cuckoo	Finished Running	12/1/2019	Bad	<input checked="" type="checkbox"/>
S14	Cuckoo	Waiting for Pre-check	12/1/2019	Bad	<input type="checkbox"/>
S15	Cuckoo	Finished Pre-check	12/1/2019	Bad	<input type="checkbox"/>
S16	Cuckoo	Running Long-term	12/1/2019	Bad	<input checked="" type="checkbox"/>
S17	Cuckoo	Finished Running	12/1/2019	Bad	<input checked="" type="checkbox"/>



Individual Job



Upload Page



What's left to do?

- Connect long-term Cuckoo machines
- Get malware files for analysis
- Improve similarity checking algorithm
- Improve data parsing on backend
- Explore optional Cuckoo features
- Implement analysis automation options
- Enable real-time database updates

Questions?

?

?

?

?

?

?

?

?

?

