Project Economics

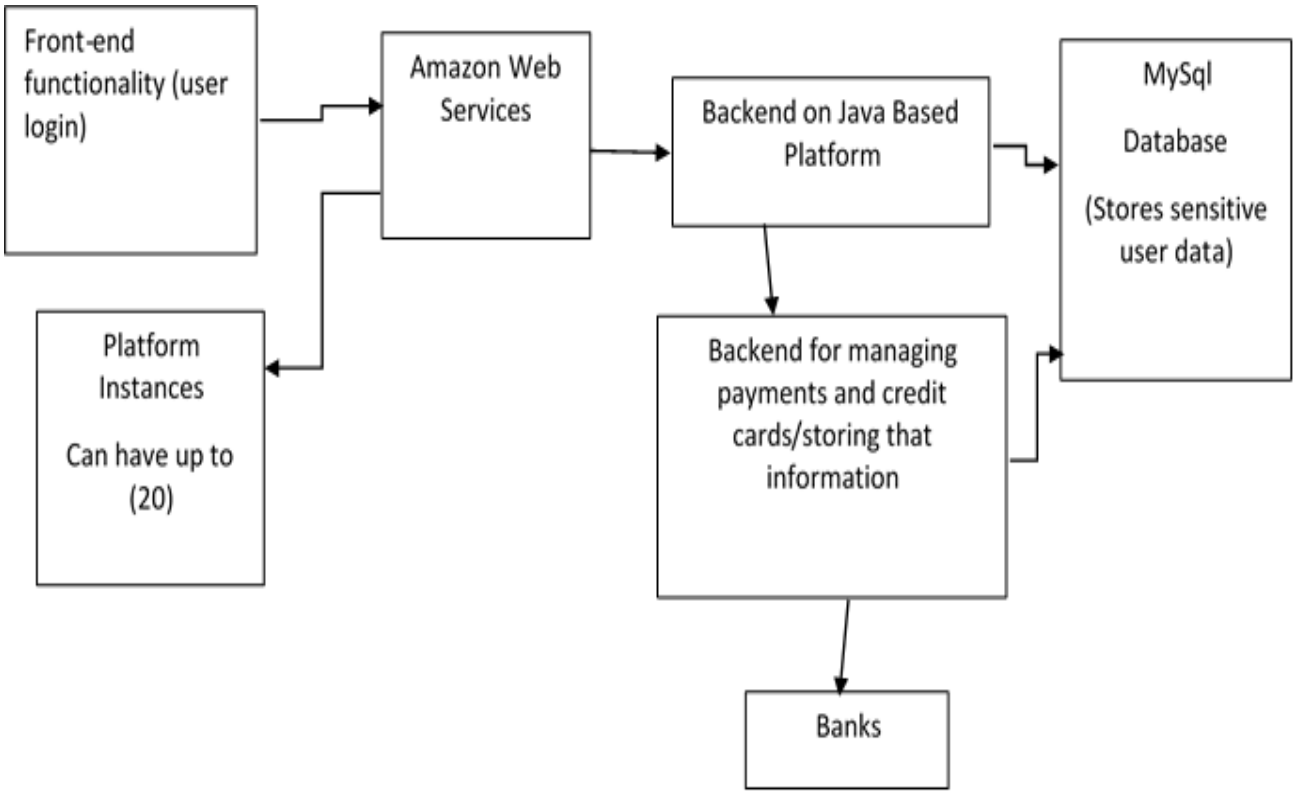
SECURITY ANALYSIS

August Tan, Piyush Jadhav | Application Security | October 6, 2015

Introduction

- Project economics is a behind the meter origination platform that allows stakeholders to manage project life-cycles and their repayment terms electronically.
- The startup gives companies, specifically energy and utility companies, a tool to manage their finances and schedule their workflow accordingly.
- What this means security-wise is that the startup has to manage sensitive user data such as finances while giving them instances of their platform to work with.

Architecture Overview



- The Front End is View that enables clients to see contents on their instances
- The Users can create up to 20 instances on AWS.
- The Backend is based upon JAVA based platform.
- This Backend then Connects to MYSQL Database that Stores Sensitive Information. The Backend is also responsible for payment authentication.

Security Concerns

AWS Vulnerabilities

- There is a vulnerability in AWS that makes it possible to map the internal cloud infrastructure, identify where a particular target VM is likely to reside, and then instantiate new VMs until one is placed co-resident with the target.
- Such placement can then be used to mount cross-VM side-channel attacks to extract information from a target VM on the same machine.
- This vulnerability can be avoided by using dedicated AWS Instances.
- This choice is mainly dependent on how much do want want to protect the data. This is a direct trade-off between cost and security

Password Security

- Keep up to speed with the state of the art in password storage
- Using just salted password is not enough these days. The attackers, with today's hardware can calculate ridiculously high number of hashes quickly. Below are the numbers that demonstrate how many hashes can be generated in a second on a 25-GPU rig.

Scheme	**Tries/sec**
NTLM	350,000,000,000
MD5	180,000,000,000
SHA1	63,000,000,000
SHA512Crypt	364,000
Bcrypt	71,000

- Therefore it advised that you use modern techniques like scrypt ,bcrypt or PBKDF2
- When a password is entered wrong, what feedback do you give? Is there a difference in response time if the user does not exist in the database? This could be used for username enumeration.

Security against DDOS Attacks

- With the sheer volume of today DDOS attacks, it is very difficult to keep them out. Akamai Technologies shared new details recently of an existing botnet that is now capable of launching 150+ gigabit-per-second (Gbps) DDoS attacks from Linux systems infected by the XOR DDoS Trojan.
- There should be an clear process defined in event of a Denial of service attack.

SQL Injection Attack

- Sanitize All User Inputs
- Use Prepared Statements (Parameterized Queries) everywhere
- Use of Stored Procedures wherever possible

Script Insertion

- Various Script injection attacks are possible. Therefore it is very important to ensure that the input data is properly sanitized.