Payatu

Payatu Casestudy

AWS Cloud Configuration Review & Pentesting of a Thriving Fintech Start-Up

Payatu Security Consulting Pvt. Ltd.

Project Overview

Founded in 2019, the client is a fintech company that is stepping up its game by introducing a credit card for the mobile generation. Their product will allow users to control all aspects of credit cards, including credit limit, instant rewards redemption, domestic and international use, online or offline transactions, contactless payments, and more. Enabling customers to get a fully digital experience allowing them to control the rewards they wish to avail themselves. However, a lack of cyber security makes their product vulnerable and leaves them struggling to build brand confidence.

Investing in AWS Cloud Configuration Assessment helped the brand to improve cloud security and implement controls for their compliance requirements, discovering security loopholes by getting a detailed report with a mitigation plan.

The Scope

The thriving fintech startup opted for the most prominent services offered by Payatu.

AWS CLOUD CONFIGURATION REVIEW

01 To check whether Appropriate Access Control mechanisms and User Rights Management are in place

02 To review the incorporation of proper Logging and Monitoring into the infrastructure

03 Check the implementation of proper security groups

04 HTTP communication is allowed with S3 buckets and Load Balancers

05 Check proper data backups and disaster recovery have been implemented or not

06 Check the rotation of access keys and if there are unused credentials for more than 90 days

INTERNAL & EXTERNAL PENTEST

01 To check configuration mistakes that might leak important information

02 HTTP communication is allowed with 3 buckets and Load Balancers

03 Assessing the cloud infrastructure for any vulnerabilities, and gaps

04 Assess the overall security postures of the application

The Challenge

The Payatu Bandits performed a real-time security assessment on the cloud AWS infrastructure, considering the below common security issues:

Scoping the Service

The brand follows Multi-Account Architecture, making it challenging to define the scope within a time frame for the assessment. With the help of an architectural diagram of the application, Payatu Bandits decoded the number of resources, estimated time and scope of work.

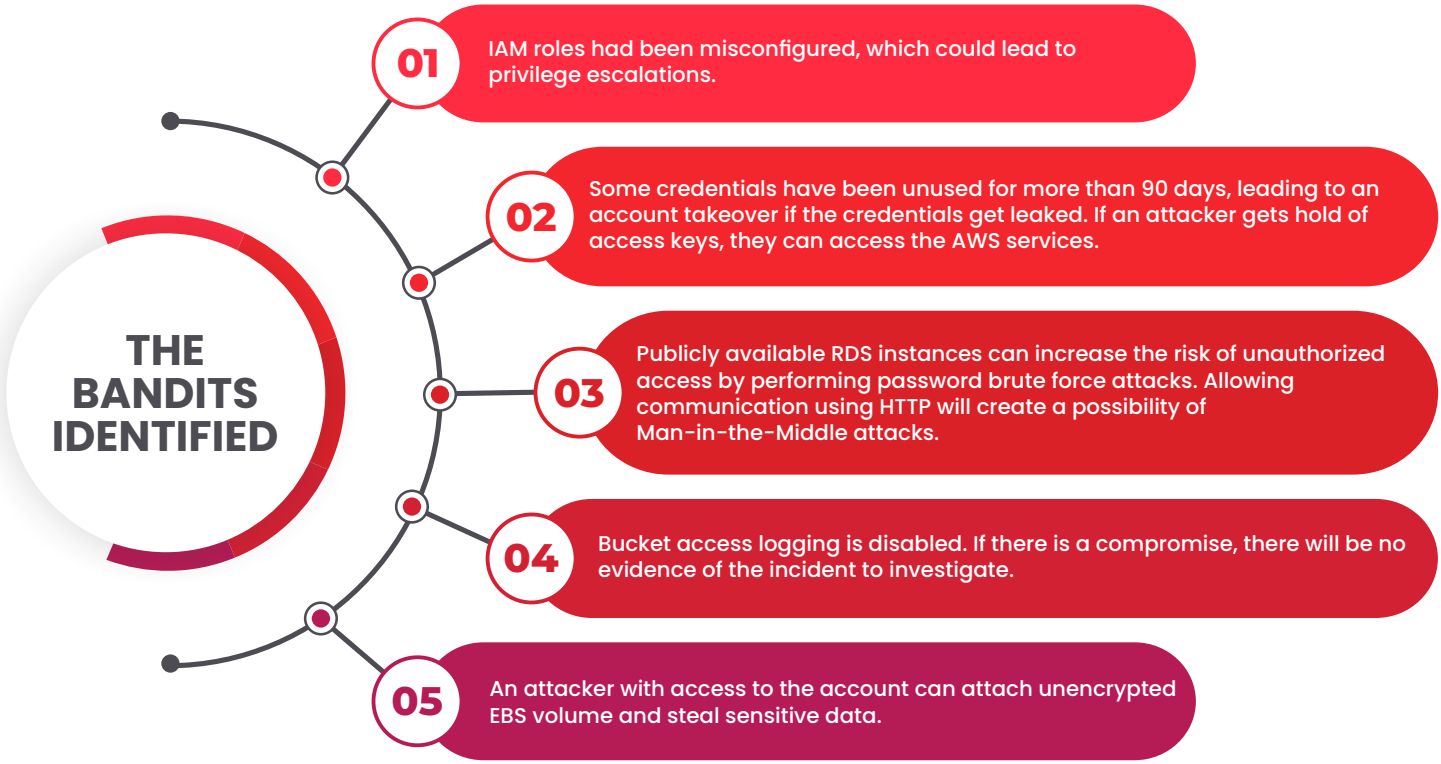
Permissions

As a financial organization, the client was reluctant to share SSH access and overpermissive IAM Role. The Bandits minimized the required permissions and easily performed the audit with the brand's approval.

The Assessment

Payatu Bandits performed a real-time security assessment on the cloud infrastructure. These assessments uncovered all the security issues in the assessed infrastructure, explained the impact and risks associated with the misconfiguration, and guided the team in prioritizing and remediating the issues.

Technical Impact



Business Impact

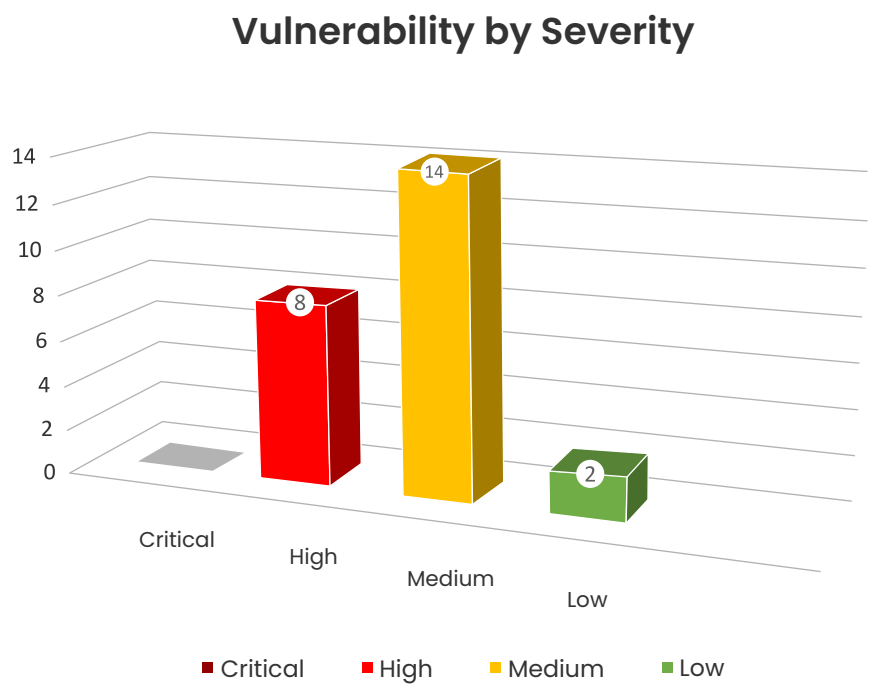
THE BANDITS IDENTIFIED

1. Successful exploitation will allow an attacker to gain higher privileges. With higher privileges the attack can disrupt day-to-day business logic (The attacker can also destroy resources, data etc from the cloud).
2. Implement a key rotation policy for access keys; 90 days is the recommended value.
3. If there is no key rotation policy, and key gets leaked it can lead to the cloud environment being compromised.
4. Avoid using root level administrator accounts for any administrative tasks. If this account gets compromised in any way, then it could potentially damage the whole AWS infrastructure, you would probably end up harming your business!
5. MFA adds another layer of protection so that even if user credentials are compromised, the attacker would need a one-time password to log in. If MFA is disabled, the attacker will be able to log in with just the compromised credentials. It may lead to loss of data, stolen identity and financial loss.
6. If an attacker manages to breach the public RDS instance, it will allow the attacker to access business-sensitive data. It may be possible for the attacker to access other internal services.

Vulnerability Chart

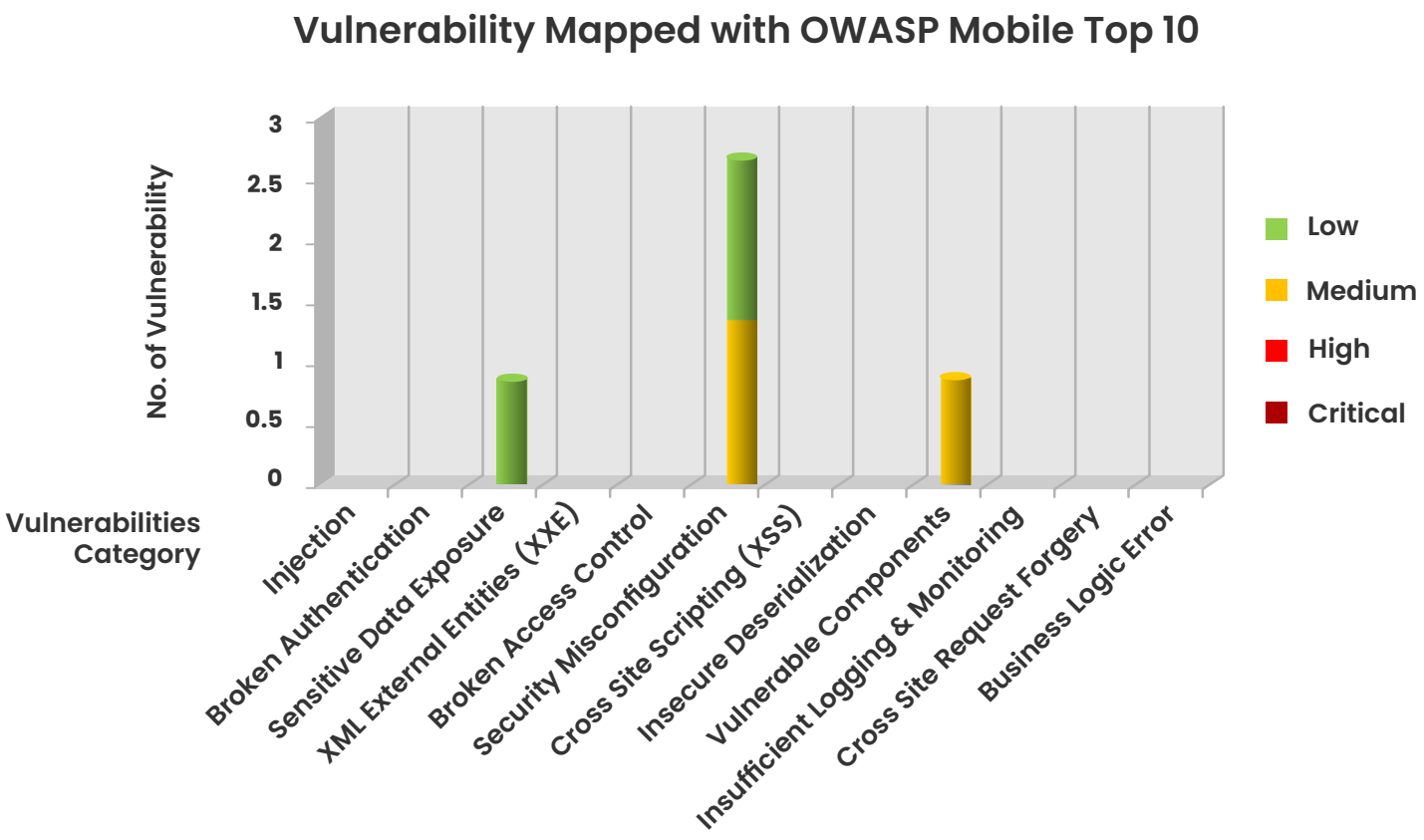
The discovered vulnerabilities table and chart illustrated below, provides a snapshot view of the number and severity of issues discovered during this security assessment.

Critical	This issue can impact the application severely and should be addressed immediately. Attackers can gain root or super user access or severely impact system operation.
High	This issue can cause a problem like unprivileged access and should be addressed as soon as possible.
High	This issue may pose a significant threat over a longer period of time.
High	This issue is more likely an information disclosure and may be an acceptable threat.



VULNERABILITIES BY CATEGORY

Below given chart shows the vulnerability matrix based on category of vulnerabilities.



Expert Bandit's Recommendations

IAM

1. Avoid IAM: Pass Role; if not, implement a filter to restrict the IAM: PassRole permission with the resources element of the IAM policy.
2. Implement a resource filter so that can assume only allowed roles. Identify and ensure that all access keys have not been used in the last 90 days and disable them as a security best practice.
3. Implement a key rotation policy for access keys; 90 days is the recommended value.
4. Lock down the root account usage and stop using the root credentials for your everyday operations or administrative ones. Implementing the principle of least privilege is recommended by creating AWS IAM users with minimal actions required to perform just the desired task.
5. Identify and deactivate any unnecessary IAM access keys as a security best practice. AWS allows two active access keys only during the key rotation process. However, it is strongly recommended that the old keys are deactivated once the new one is created so only one access key will remain active for the IAM user.
6. Set up MFA for all users.

RDS

01 Enable the "Auto Minor Version Upgrade" settings for receiving patches and updates for the RDS engine.

02 Set the "Backup Retention Period" to 30 days, or as per business requirements.

S3

Ensure that the AWS S3 Server Access Logging feature can record access requests useful for security audits. By default, server access logging is not enabled for S3 buckets.

Implement the access policy to enforce SSL-only (encrypted) access to S3 data.

Enable the "Versioning" property of the S3 bucket containing business-critical files. It will allow the owner to recover and retain overwritten and deleted files.

Enable the "MFA-Delete" property of the S3 bucket containing business-critical files. Setting this property, S3 bucket will prevent the deletion of the file by an unauthenticated user.

Ec2

1. Implement encryption to protect it from attackers or unauthorized personnel. With Elastic Block Store encryption enabled, the data stored on the volume, the disk I/O and the snapshots created from the volume are all encrypted.

2. Implement encryption to protect it from attackers or unauthorized personnel. With Elastic Block Store encryption enabled, the data stored on the volume, the disk I/O and the snapshots created from the volume are all encrypted. Snapshots created from an encrypted volume are always encrypted with the same key as the volume.

3. Allowing IAM actions to all principals is contrary to the principle of least privilege and presents an opportunity for abuse. Review the policy to ensure it is secure and in line with the resources intended.

4. For every KMS Customer Master Keys (CMKs), ensure rotation of the key is enabled.

5. Disable the EBS listeners with HTTP protocol and enable only the TLS listener.

6. Ensure that your Load Balancers have the Access Logging feature enabled for security, troubleshooting and statistical analysis.

7. Ensure ELBv2 Load Balancers have the Deletion Protection feature enabled.

8. It is recommended to enable dropping invalid header fields to mitigate the risk of request smuggling attacks.

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

Our deep technical security training and state-of-the-art research methodologies and tools ensure the security of our client's assets.
At Payatu, we believe in following one's passion, and with that thought, we have created a world-class team of researchers and executors who are willing to go above and beyond to provide best-in-class security services. We are a passionate bunch of folks working on the latest and cutting-edge security technology.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

Want to know more about the distinct premium services security services offered by Payatu? Tell us about your specific requirements here, and we will get back to you with a customized sample report.

Payatu Security Consulting Pvt. Ltd.

www.payatu.com
info@payatu.com
+91 20 41207726