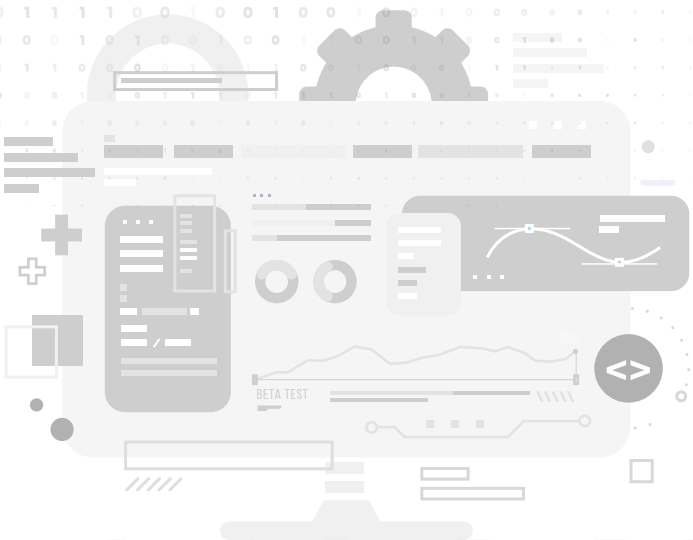
Payatu

Payatu Case Study

Securing the Digital Realm of a Pentesting-as-a-service Provider with Threat Modeling



Payatu Security Consulting Pvt. Ltd.

Project Overview

Anything that is of value needs to be protected!

In the technologically sophisticated and globally interdependent world of modern business, our organizational assets are of the highest value. Technology systems, applications, networks, and critical data, everything needs to be protected. And the first step to protection is identification and evaluation.

Threat modeling is the proactive approach of prioritizing potential security risks to technology systems and applications by understanding, identifying, and then creating a corrective action plan to combat these risks.

A well-recognized platform that offers pentesting-as-a-service was looking to get threat modeling done to ensure that the platform and its modules can be protected proactively.

With this in mind, Payatu took up the challenge of improving the security resilience of this client by identifying threats and defining countermeasures to prevent or mitigate the effects of threats to the system.

Scope

To perform threat modeling of modules of the portal such as

To identify all potential threats and vulnerabilities to the platform

01 Client Onboarding

02 Management of Security Projects

03 Reporting Automation

04 Scan Scheduling

05 Attack Surface Management

Process

01

Scoping, Objective Finalization, and Application Overview

Payatu Bandits first started the threat modeling process by understanding the security objectives that the client wanted to achieve.

Once the objectives were finalized, the scope and the architecture type of the application was discussed to determine the future course of action.

The Bandits also deeply understood the application, how it works, its deployment, types of user roles, data elements, technologies used, and any/all security mechanisms applied.

02

Methodology Decision

Based on the comprehensive understanding of the application, the Bandits decided to follow the STRIDE framework as the methodology of this project.

STRIDE	ATTACK
Spoofing	Cookie Replay Session Hijacking CSRF
Tampering	XSS SQL Injection
Repudiation	Audit Log Deletion Insecure Backup
Information Disclosure	Eavesdropping Verbose Exception
Denial of Service	Website Defacement
Elevation of Privilege	Logic Flow Attacks

STRIDE helps with the identification of threats by classifying attacker goals via common attacks.

03

Application Decomposition

Once the methodology was finalized, the application was decomposed, and application context and scenarios were generated.

Trust levels and trust boundaries were mapped out along with all the entry and exit points.

04

Generation of Data Flow Diagrams

To better comprehend the application, a visual representation of all the processes and modules of the app was generated. This visual representation is known as Data Flow Diagrams or DFD.

The DFD of the client's application logically showed how the data flows through the app from end to end, allowing the Bandits to identify affected components through critical points and the flow of control through these components.

05

Develop the Threat Model Diagram

For this particular project, the team leveraged the Microsoft Threat Modeling Tool to visualize system components, data flows, and security boundaries. With the help of this tool, the Threat Model Diagram for this client was developed, which was then used to define identified assets, present controls and threat agents.

Identify Threats

06

Implementing the STRIDE framework, all the potential threats to the client's application were identified, and later ranked based on the risk factors. It is possible to develop a prioritized list of threats to aid in a risk mitigation strategy, such as determining which threats should be mitigated first, by assessing the level of risk posed by the identified threats.

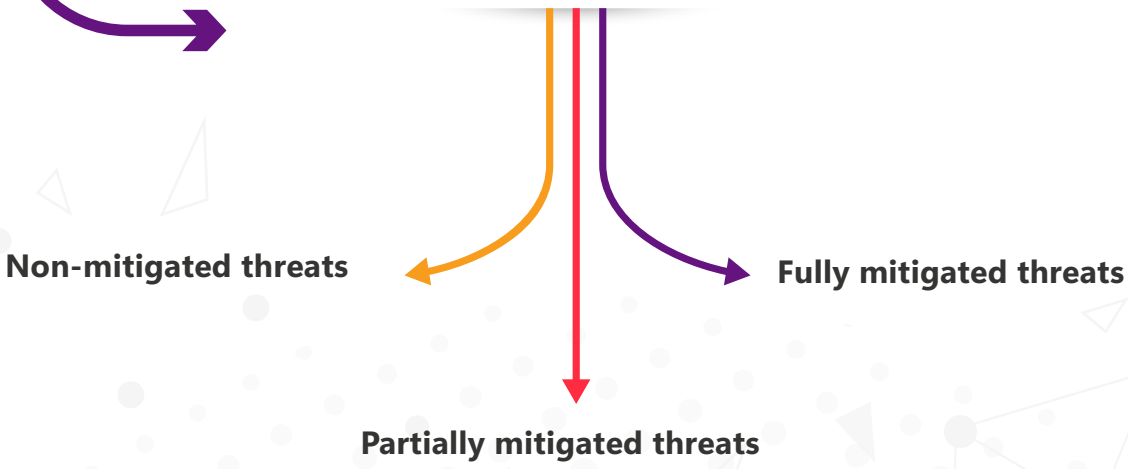
Determining the Countermeasures and Mitigation Techniques

07

Countermeasure identification aims to ascertain whether there are any protective measures, such as security controls or policies, that can hinder the realization of a threat.

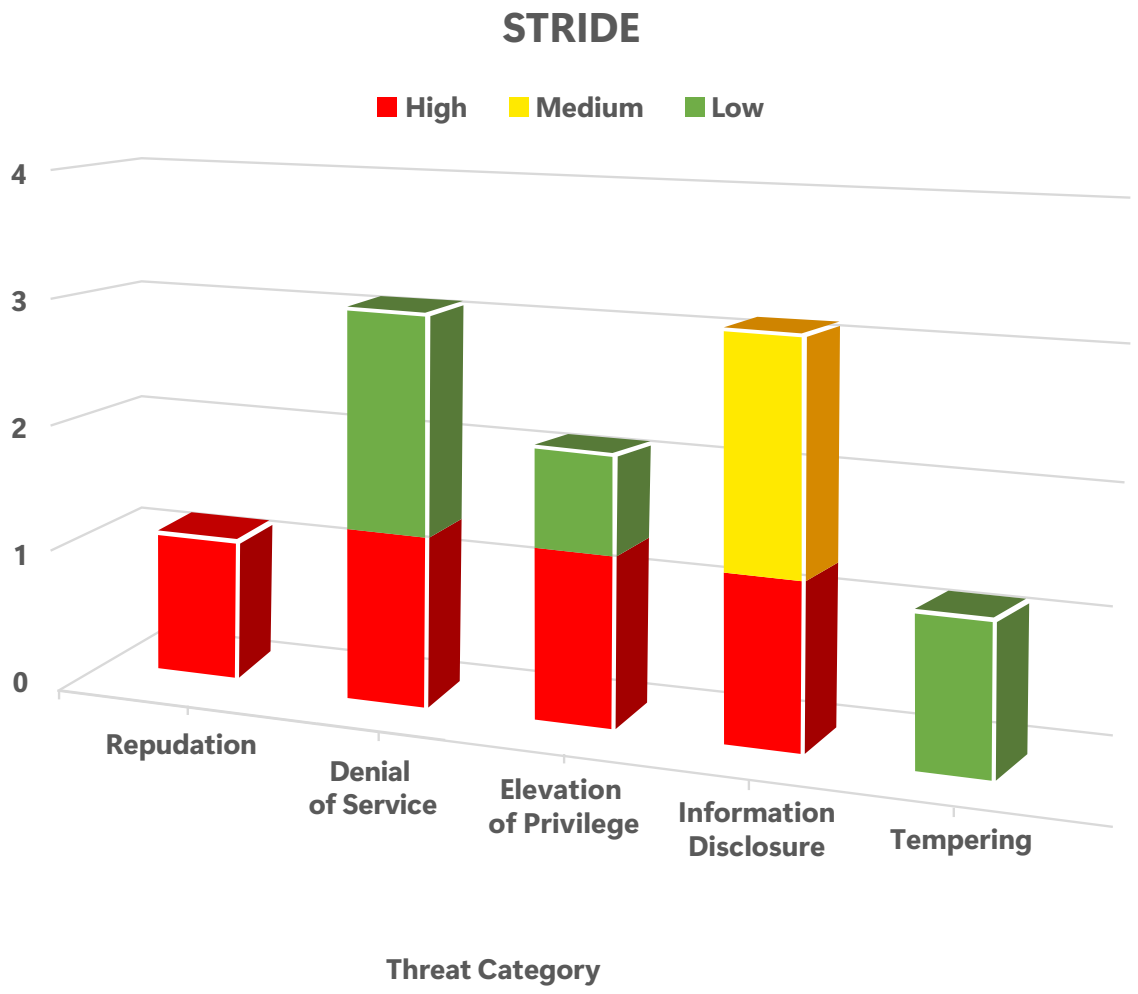
Vulnerabilities are those threats that lack countermeasures. Once the threats are categorized using STRIDE, suitable countermeasures can be identified within each category.

Post identification of the threats and corresponding countermeasures, a threat profile can be generated using the below criteria:



Findings

Vulnerabilities identified based on the STRIDE framework



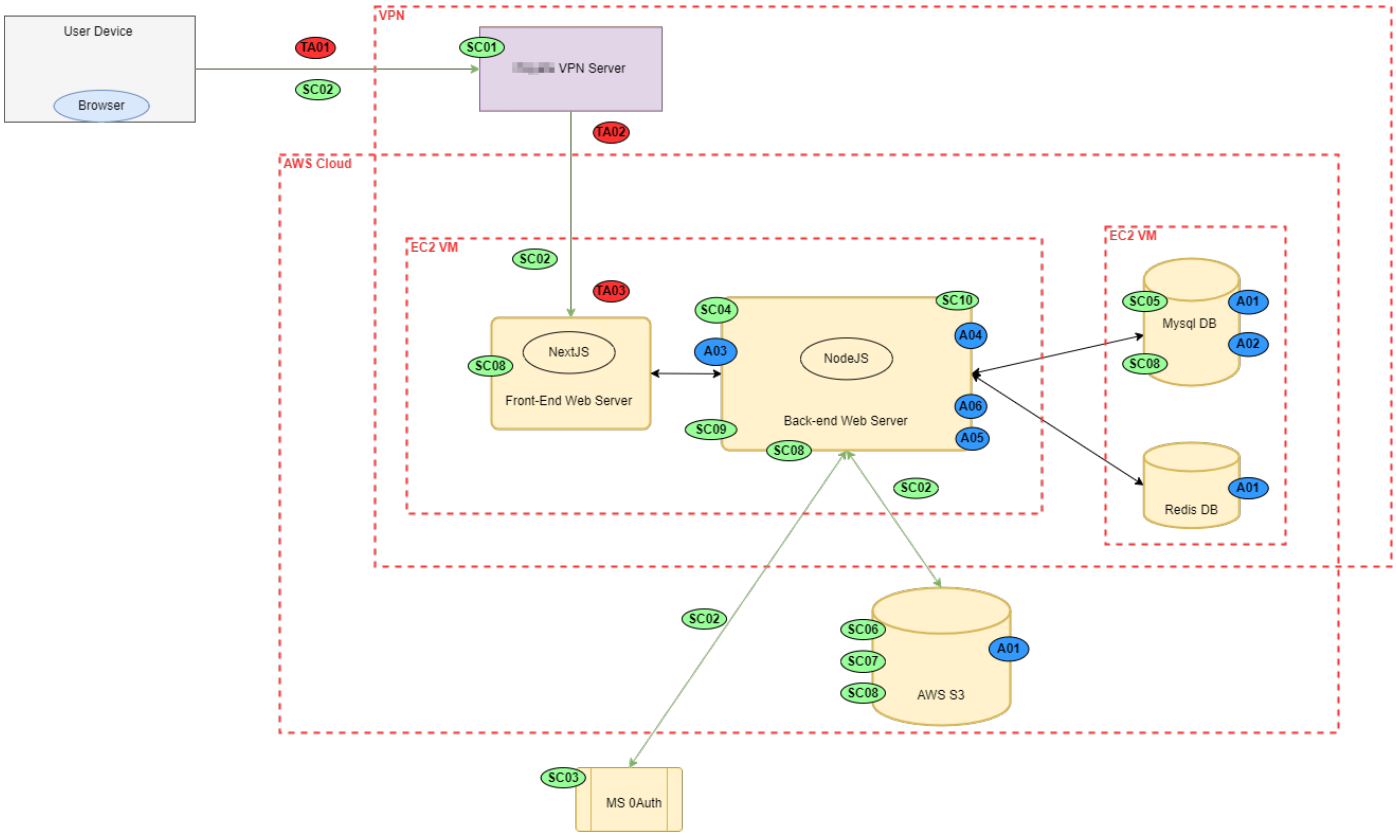
Threat Model Matrix

Threat Agent	Asset	Attack	Attack Surface	Attacker Goal	Severity	Existing Security Controls
Internal Authorized User	Report Information Session Token	Denial of Service	Frontend Web Server, Backend Web Serve	To achieve denial of service	**Low**	
Internal Authorized User	AWS Credentials/ Keys Redis Credentials DB Credentials	Elevation of Privilege	Backend Web Server	To escape docker container and get access to host system	**High**	None
External Un-authorized User, Internal Authorized User, Internal Un-authorized User	Report Information, Client PII	Denial of Service	MySQL DB	To achieve denial of service	**High**	None

Internal Authorized User, Internal Unauthorized User	Report Information, Client PII, Session Token	Repudiation	MySQL DB	Makes tracing of statement execution difficult	**Low**	It used debugging statement to see the log which does not include logging of all user's activity
Internal Authorized User	Report Information, Client PII	Information Disclosure	MySQL DB	Potentially gain access to unencrypted sensitive information	**Medium**	None
External Unauthorized User	Report Information, Client PII	Elevation of privilege	VPN Server	To gain access to services behind VPN	**Low**	None
Internal Authorized User	Report Information	Denial of Service	Redis Server	To achieve denial of service on Redis server	**Low**	

Internal Authorized User	Report Information, Client PII, AWS Credentials/ Keys	Information Disclosure	AWS S3 Bucket	Read the sensitive data contained in AWS S3 Bucket such as report POC	**High**	
Internal Authorized User	Report Information	Tampering	AWS S3 Bucket	Upload malicious files with huge file size	**Low**	Currently the application just checks for file extension.
Internal Authorized User	Report Information, Client PII	Information Disclosure	AWS S3 Bucket	Read the sensitive data such as report POC	**Medium**	Not implemented on data stored before 5th Jan 2023

Threat Model



Asset

A01: Report Information

A02: Client PII

A03: Session Token

A04: AWS Credentials/Keys

A05: Redis Credentials

A06: DB Credentials

Security Controls

SC01: Restricted network access/VPN

SC02: Transport Layer Security

SC03: Authentication

SC04: Input Validation

SC05: Encryption At Rest

SC06: IAM Policies

SC07: IAM Roles

SC08: Logging and monitoring

SC09: Output Encoding

SC10: User Roles

Threat Agent

TA01: External Unauthorized User

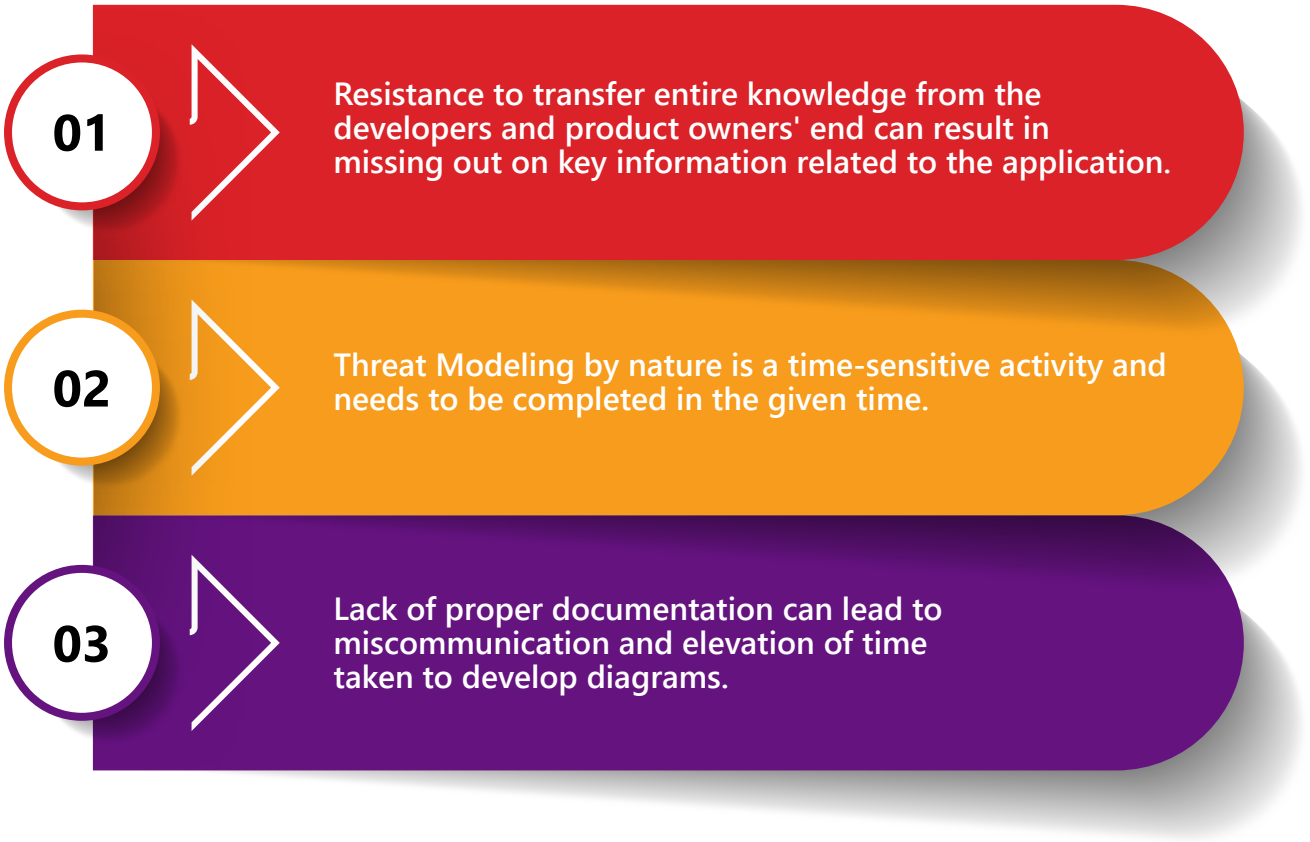
TA02: Internal Authorized User

TA03: Internal Unauthorized User

HTTPS

TCP Connection

Challenges


01
Resistance to transfer entire knowledge from the developers and product owners' end can result in missing out on key information related to the application.
02
Threat Modeling by nature is a time-sensitive activity and needs to be completed in the given time.
03
Lack of proper documentation can lead to miscommunication and elevation of time taken to develop diagrams.

Recommendations

1. Avoid running the container as root user
2. Implement automatic backup
3. Enable logging and monitoring mechanism in all servers/services
4. Enable encryption on DBMS at rest
5. Use MFA/OTP mechanism for added security
6. Maintain an OSS security library inventory
7. Use Shift-Left approach for OSS tool validation
8. Use a licensed VPN provider
9. Limit user input size
10. Implement firewall rules to check for unusual resource consumption
11. Generate temporary security credentials
12. Implement file size restriction check server-side and validate content type
13. Validate file content at runtime and discard malicious files
14. Enable S3 bucket encryption for all old data

The Before and After Threat Modeling Picture of the Client's Application

To simply put, the client was not aware of any threats to its application but had certain general controls (14 to be specific) in place.

Post conducting the threat modeling exercise, the client was made aware of 24 threats, vulnerabilities, and threat agents within its application. Of which, the general control could combat 14 threats, but 10 new control recommendations were made.

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.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

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.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared responsibility to secure the information stored in their cloud. Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure. pipeline to increase the visibility of security threats.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

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.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.

CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting - social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

More Services Offered by Payatu

- AI/ML Security Audit
- Trainings

More Products Offered by Payatu

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.io

+91 20 41207726