



Payatu Casestudy

Global IT Services Consultancy Conducts Web Application Assessment on 12 Apps

Project Overview

One of India's giant multinational companies was served as a client for a huge cybersecurity-related project. This company is a leading global IT services consulting and business solutions provider, highly recognized for its deep domain expertise in several industry verticals.

The client is not just a mega organization, it is also a leader in digital transformation services provider along with designing high quality cognitive business operations for its customers.

Needless to say, it is also an employer to thousands and lakhs of employees.

With such a high volume of operations and employees, it can get difficult for MNCs to have a centralized system that can securely keep track of all the business processes alongside employee management activities.

For this, the said client has a central internal ERP system in place that manages and automates over 10 solutions such as accounting, project management, sales, etc.











Payatu was given the charge of conducting a web application assessment for a mission-critical set of 12 applications that were covered under this single system.



This was one of the many projects where all the 12 applications assessed were found to be vulnerable and over 120 vulnerabilities were identified.

The Scope




CONDUCT A PENTEST ON THE PARENT SYSTEM THAT CONSISTS OF 12 APPLICATIONS

Web Application Assessment of

-  The application suite that caters to implementations, enhancements and production support to enable financial activities of the client
-  The application suite that is used to automate and enable lender-related financial activities of the client and its subsidiaries
-  The project management system that maintains the records of the employees' work time for proper payment to the employees
-  An application where contacts of different stakeholders/resources are saved that can be shared across. This application also allows people to schedule meetings
-  Accounts app that is used by business units to maintain the client's customer accounts globally. Accounts are linked to external data providers (D&B etc.) to keep the account owners updated about the customer
-  Access management application that is used for managing the access of the users to several types of functionalities across the parent application
-  An offerings application that is a sub-app of the parent sales application in which a new offering can be created and sent for approval
-  Opportunities app, used for creating opportunities, managing timelines, linking contracts to a particular opportunity and adding offerings to the opportunity
-  The project resource management application that holds and shows all the data required for the allocating a resource in the project and dealing with other related operations
-  The project commercial management app that manages contracts with the customers. The creator can create projects with these contracts and assign them to users

-  The work management application that is used to allocate work to the employees
-  The contract management system that manages contracts and enables governance on accounting of projects executed under a contract. It captures the signed contract document and metadata of the contract like parties, duration and valuation, and signed contract document. Contract management lifecycle workflow is part of CMS. Hence, it acts as an enterprise repository of contracts between our client and its customers

To identify any vulnerabilities that can be exploited to

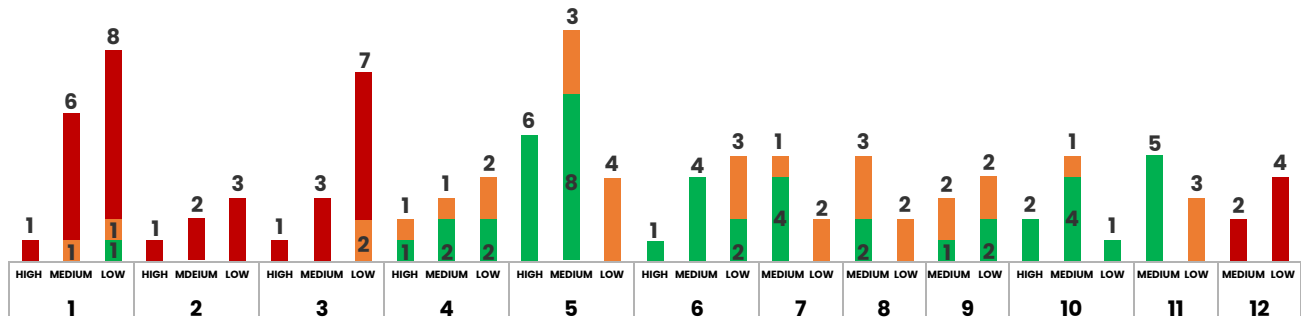
-  1 Gain access to internal networks
-  2 Copy/Access data
-  3 Bypass the security controls implemented

The Challenge

- 1** Crunched timelines – The client needed all the applications to be tested within 3 months and to come back with fixed vulnerabilities in the next 3 months
- 2** Overall project timeline – 6 months for 12 applications
- 3** Getting access to the applications was a little challenging
- 4** The process of receiving the application and conducting the assessment one by one proved to be extremely time-consuming
- 5** Redesigning the process flow became crucial to ensure timely delivery of the project
- 6** Lack of bandwidth on the client's side for fixing the bugs proved to stretch the time supposed to be taken for retesting
- 7** Regular movement of timelines when fixing the bugs translated into change in the process agreed upon
- 8** Lack of alignment in the internal communication of the client's stakeholders led to revisiting the same issues with multiple people repeatedly

Findings

STATUS ■ OPEN ■ NOT FIXED ■ FIXED



APPLICATION NAME **SEVERITY**

Application No.	Severity	Status Fixed	Not Fixed	Open	Grand Total
1	HIGH MEDIUM LOW	1	1	8	10
Total		1	2	15	18
2	HIGH MEDIUM LOW			1 2 3	1 2 3
Total				6	6
3	HIGH MEDIUM LOW		2	1 3 7	1 3 9
Total			2	6	6

Application No.	Severity	Status	Not Fixed	Open	Grand Total
4	HIGH	1	1		1
	MEDIUM	2	1		4
	LOW	2	2		5
Total		5	4		9
5	HIGH	6			6
	MEDIUM	8	3		11
	LOW		4		4
Total		14	7		21
6	HIGH	1			1
	MEDIUM	4			4
	LOW	2	3		5
Total		7	3		10
7	MEDIUM	4	1		5
	LOW		2		2
Total		4	3		7
8	MEDIUM	2	3		5
	LOW		2		2
Total		2	5		7
9	MEDIUM	1	2		3
	LOW	2	2		4
Total		3	4		7

Application No.	Severity	Status	Not Fixed	Open	Grand Total
10	HIGH	2			2
	MEDIUM	4	1		5
	LOW	1			1
Total		7	1		8
11	MEDIUM	5			5
	LOW		3		3
Total		5	3		8
12	MEDIUM			2	2
	LOW			4	4
Total				6	6
Grand Total		48	34	38	120

Common vulnerabilities identified



Recommendations

OUR RECOMMENDATIONS

- 1 An authentication and authorization check function should be implemented throughout the application
- 2 User input must be sanitized before being added to a CSV file. Ensure that no cells begin with any special characters such as =,+,- etc
- 3 Add checks on the server side to prevent users from filling data for previous dates
- 4 Implement proper server-side authorization for all endpoints
- 5 For any security checks that are performed on the client side, ensure that these checks are validated on the server side as well
- 6 Enforce Strong Access Control over resources
- 7 Check the user authorization before issuing the resource when the user requests it
- 8 Do not map the object with a direct id instead use of hash is handy in this case
- 8 Apply account unlock mechanisms depending on the risk level. In order from lowest to highest assurance:
 - 1 Use captcha in login page
 - 2 Time-based lockout and unlock
 - 3 Self-services unlock (sends unlock email to registered email address)
 - 4 Manual administrator unlocks

The Takeaway

With the help of Payatu's recommendations, this client of theirs was made aware of its actual security posture and the gaps that needed to be filled by the security team. The client was glad to apprehend the fact its system of multiple web applications needed to be worked on, in order to make them intrusion-free from any attackers.

The result of all these activities, findings, and quality of output was that the client could fix critical bugs in its system and it utterly secure. It is a matter of pride for the Payatu Bandits to ensure that each and every client of theirs leaves with utmost satisfaction and an improved security structure.

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

