


Application Testing for Cryptocurrency Company

PROJECT DETAILS

 Application Testing

 Jan. 2023 - Dec. 2023

 Confidential

 *"The ability to scale our team up with TimsparK's wide range of professionals was invaluable."*

PROJECT SUMMARY

A cryptocurrency company hired TimsparK to provide application testing services. The team conducted security and penetration tests using recognized methodologies, such as OWASP and NIST 800-115.

PROJECT FEEDBACK

TimsparK successfully tested various components and assessed vulnerabilities and configuration flaws to ensure proper fixes. They completed everything on time and listened to all the client's needs. Moreover, they offered alternative solutions, communicated effectively, and led a seamless process.






The Client

Please describe your company and position.

I am an Executive at PassimPay

Describe what your company does in a single sentence.

Cryptocurrency

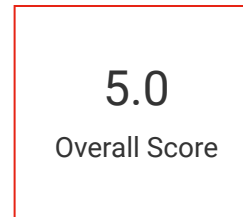
-  Executive, PassimPay
-  Financial services
-  Poland

The Challenge

What specific goals or objectives did you hire TimsPark to accomplish?

- Security testing
- Penetration testing

CLIENT RATING



Quality: 5.0



Schedule: 5.0



Cost: 5.0



Would Refer: 5.0



The Approach

How did you find Timspark?

Referral

Why did you select Timspark over others?

Good value for cost

How many teammates from Timspark were assigned to this project?

2-5 Employees

Describe the scope of work in detail. Please include a summary of key deliverables.

The security testing was conducted in accordance with recognized practices and methodologies such as OWASP and NIST 800-115.

The web application penetration testing included:

- Gathering information about the tested application.
- Testing the security of the web application's external perimeter infrastructure.
- Testing authentication and authorization mechanisms.
- Testing session management mechanisms.
- Testing user input validation and application resilience against various injections (XSS, SQL, NoSQL).
- Testing the resilience of applied cryptography.
- Testing the application's business logic and identifying design flaws.
- Identifying outdated and vulnerable application components.

The penetration testing of the web application's API interfaces included:

- Testing authentication mechanisms.
- Detecting excessive data exposure.
- Testing authorization (BOLA, BFLA).



- Testing using fuzzing methods.
- Testing mass assignment vulnerabilities.
- Testing code injection vulnerabilities.
- Testing security configurations.
- Testing limitations on requests and resource consumption.
- Testing asset management flaws.

The Outcome

What were the measurable outcomes from the project that demonstrate progress or success?

During the year 2023, Timspace specialists conducted testing on multiple components of the Passimpay application using diverse testing techniques and tools. Furthermore, each testing phase included an assessment of previously identified vulnerabilities and configuration flaws to ensure proper remediation efforts were implemented.

Describe their project management. Did they deliver items on time? How did they respond to your needs?

All tasks are completed on time. All our wishes were taken into account. I would like to note that the Timspace team offered alternative solutions if our wishes could have caused risks that we had not initially considered.

What was your primary form of communication with Timspace?

- In-Person Meeting
- Virtual Meeting
- Email or Messaging App

What did you find most impressive or unique about this company?



The ability to scale our team up with Timspark's wide range of professionals was invaluable. The exceptional DevOps engineer they supplied made a significant impact, enhanced by the company's effective communication and seamless organizational processes.

Are there any areas for improvement or something Timspark could have done differently?

No, they delivered what I expected from the kind of contract work we asked them to do.

