bugbounter

How a FinTech Company Secured Its Customer Data from a Potential Exploit With BugBounter

Overview

FinTech companies are on the rise as they are disrupting the finance industry’s not-so-modern processes. They constantly develop new technologies to deal with monetary transactions and personally identifiable information (PII).

Yet, this innovativeness and drastic technology-led changes bring vulnerabilities to organisations because each innovation introduces unexplored and uncontrollable digital territories for malicious hackers to exploit. That’s why, both FinTechs and the organizations that utilise their services have to be on alert at all times.

Goals and Challenges

Challenges

In accordance with the above-mentioned reasons, **a well-established FinTech company was in search of ways to strengthen its security posture** as a result of increased cyber-attacks and data breaches amid the pandemic.

Like many tech-led industries, FinTech companies are constantly under cyber attacks. For this reason, the FinTech company was running pentests regularly. However, the company was in **need of further coverage** of its web applications, mobile applications and public APIs **due to the pentests' limited resources and uniformity.**

In addition, one of the company's strongest competitors faced a dramatic security exploit which caused a major data breach of thousands of clients. The competitor was fined over 100.000 USD (in regards to the GDPR/KVKK regulations) and lost its reputation.

Goals

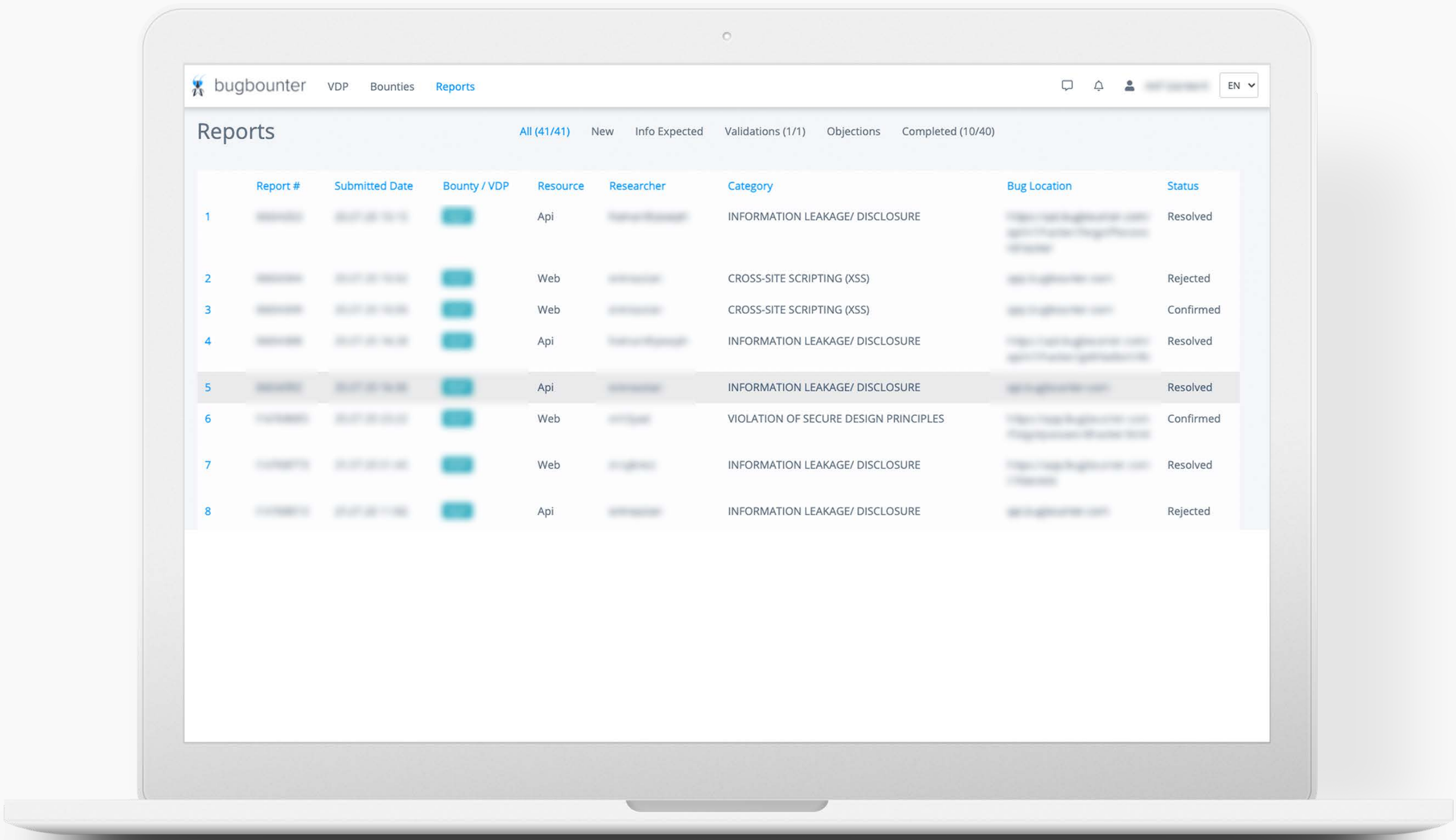
Taking all of these into consideration, the FinTech company had to take action urgently and
needed:

- An additional solution that accelerates, extends and deepens, the testing process next to regular pentests and internal red-team.
- A larger pool of diverse offensive security researchers who can introduce fresh perspectives to the testing process and who are able to use similar tools, techniques, motivation to discover unknown vulnerabilities matched to black-hat hackers
- A business model that utilizes such expertise in a budget-friendly way
- To discover security vulnerabilities as quickly and effectively as possible to not share the same fate with its competitor.

Solution: BugBounter's CrowdSourced Testing Services

Founded to tackle these issues, BugBounter's aim is to **gather expert freelance security researchers together to discover, validate and report security vulnerabilities through success-based bug bounty programs.** With a crowdsourced ecosystem of talented researchers joining from different countries, cultures, backgrounds and expertise areas, BugBounter utilizes their collective brainpower to outperform insufficient testing methods which became industry standards these days.

The FinTech company decided to run a complementary bug bounty program through BugBounter to meet the security testing goals while dealing with ever changing cyber attacks.



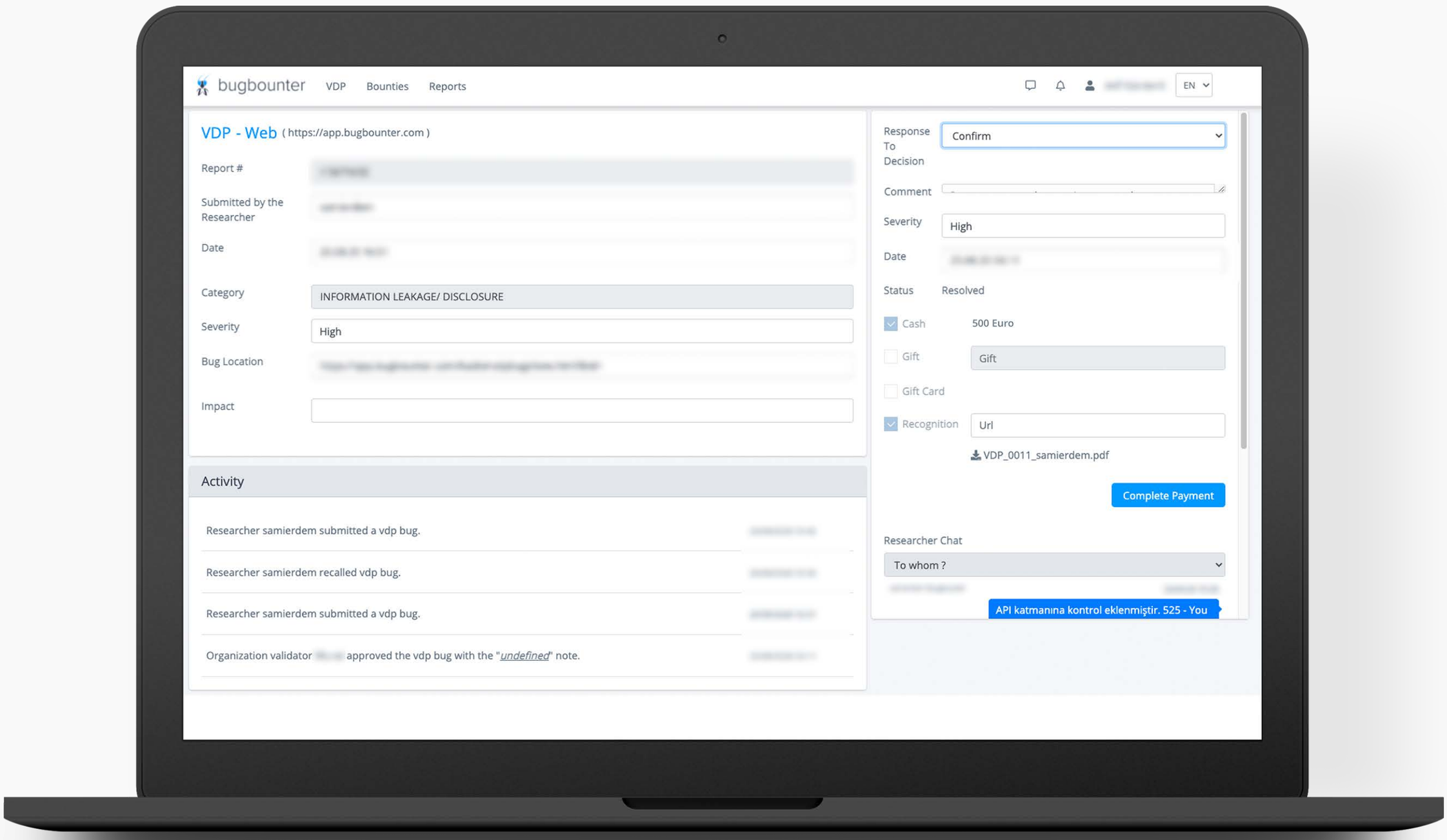
Method: Bug Bounty Program

Bug Bounty is a platform service that operates with numerous offensive security professionals on a success-based business model. This approach is:

Highly effective: Ethical hackers registered to the platform aim to discover vulnerabilities within the company's digital assets and attack surfaces. They are acknowledged as experts in the industry and are familiar with the most exploited security vulnerabilities.

Time-saving: While racing against the clock, ethical hackers also race with each other. The first researcher to spot a weakness claims the reward and because of that, vulnerabilities are discovered much faster - often within the same day.

Cost-efficient: Since the program is bounty-based, a reward structure is designed according to the severity of the vulnerabilities which matches the budget of the companies. When the bounty budget is achieved the company may suspend the program or keep receiving the reports that will be evaluated with an additional budget.



The BugBounter Approach

BugBounter analysed the attack surfaces and advised the scope for the bug bounty program that meets the needs of the FinTech company. After the bug bounty structure was designed, it was announced within the BugBounter ecosystem. This enabled the testing invitation to reach out to a specific group of talents to participate in the challenge.

The results of the most recent pentest were excluded from the scope of the bounty program. This was done to optimize the budget to prevent already known issues being reported and eventually get rewarded.

Within the first 3 days, BugBounter's researchers found 4 critical/high (according to CVSS 3.0 scoring system) severity level vulnerabilities. One of those critical vulnerabilities appeared to be a similar breach reason that the FinTech company's competitor faced. As the Fintech fixed the reported bugs, reporting researchers validated those fixes which ended up in resolving the issues as fast as possible.

Results

Thanks to the diverse pool of talented researchers in the BugBounter ecosystem, the FinTech company:

- Spotted the vulnerabilities quickly and stayed one step ahead of malicious attackers.
- Discovered the bugs in a cost-effective way.
- Verified the security patches and solidified its security posture.
- Prevented its customer data from a potential exploit and preserved their reputation.