bugbounter

How an E-Commerce Company Secured Its App Software Releases With BugBounter

Overview

E-commerce is one of the pioneer industries to constantly implement new technologies in order to meet never-ending customer needs and improve customer experience.

However, new features in their web/mobile applications and continuous tech investment are a threat for e-commerce businesses’ digital assets as they bring security vulnerabilities. That’s why e-commerce organisations have to be on alert for cyberattacks at all times.

Goals and Challenges

Challenges

In accordance with the above-mentioned reasons, **a leading e-commerce company was in search of more effective ways to secure its app software releases as compared to pentests.**

The e-commerce company has been running regular pentests every quarter to secure its network. However, since they were also updating their web & mobile app almost biweekly, the periodic pentests weren’t meeting their needs. Their internal red-teams could not employ enough workforce to test every new functionality before going live.

Furthermore, as the frequency and sophistication of cyber-attacks have skyrocketed in recent years, the company was in need of a trustworthy approach to continually check the strength of its mobile app’s cybersecurity and take action before malicious hackers do.

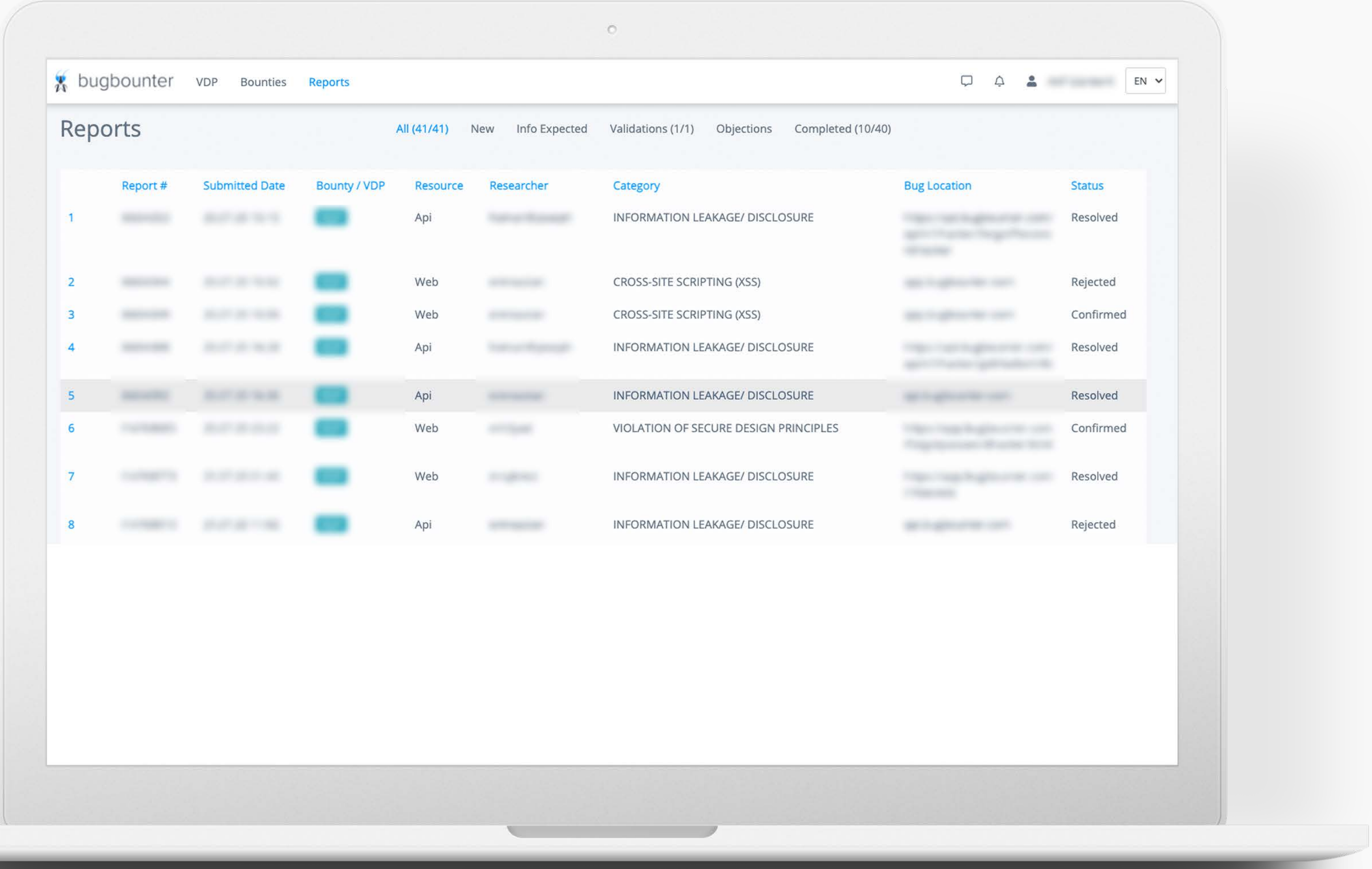
Therefore the e-commerce company needed:

- To achieve continuous security checks on its mobile app updates
- Agile mobilisation capabilities to keep up with the frequent updates
- A team of diverse professionals accustomed to new technologies and discovering unknown vulnerabilities
- A method to utilize such expertise in a budget-friendly and time-saving way

Solution: BugBounter's CrowdSourced Testing Services

Founded to tackle these issues, BugBounter's aim is to **gather expert freelance security researchers together to discover and report security vulnerabilities through 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 usual testing methods such as pentests, automated scans and expensive red-team services.

The e-commerce company decided to run a bug bounty program through BugBounter to accelerate, extend and deepen its periodic testing process.



Reports

	Report #	Submitted Date	Bounty / VDP	Resource	Researcher	Category	Bug Location	Status
1	[redacted]	[redacted]	[redacted]	Api	[redacted]	INFORMATION LEAKAGE/ DISCLOSURE	[redacted]	Resolved
2	[redacted]	[redacted]	[redacted]	Web	[redacted]	CROSS-SITE SCRIPTING (XSS)	[redacted]	Rejected
3	[redacted]	[redacted]	[redacted]	Web	[redacted]	CROSS-SITE SCRIPTING (XSS)	[redacted]	Confirmed
4	[redacted]	[redacted]	[redacted]	Api	[redacted]	INFORMATION LEAKAGE/ DISCLOSURE	[redacted]	Resolved
5	[redacted]	[redacted]	[redacted]	Api	[redacted]	INFORMATION LEAKAGE/ DISCLOSURE	[redacted]	Resolved
6	[redacted]	[redacted]	[redacted]	Web	[redacted]	VIOLATION OF SECURE DESIGN PRINCIPLES	[redacted]	Confirmed
7	[redacted]	[redacted]	[redacted]	Web	[redacted]	INFORMATION LEAKAGE/ DISCLOSURE	[redacted]	Resolved
8	[redacted]	[redacted]	[redacted]	Api	[redacted]	INFORMATION LEAKAGE/ DISCLOSURE	[redacted]	Rejected

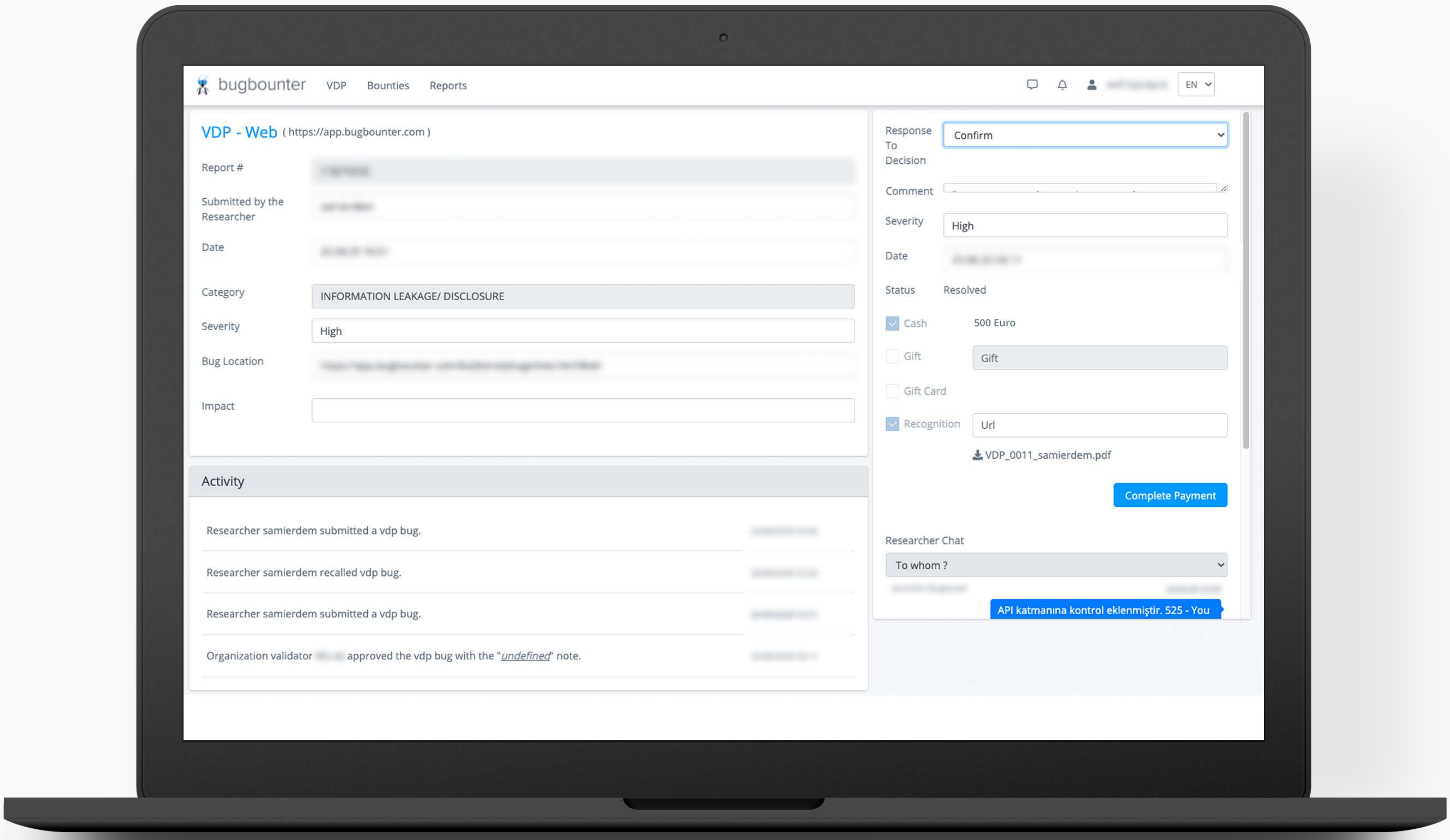
Method: Bug Bounty Program

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 ecosystem aim to discover vulnerabilities within the company's scoped 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 bug claims the prize and because of that, vulnerabilities are found much faster - often within the same day following the publishing of new bounty.

Cost-efficient: Since the program is bounty-based, a reward structure is structured according to the budget and the risk factor 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.



VDP - Web (https://app.bugbounter.com)

Report #	[redacted]
Submitted by the Researcher	[redacted]
Date	[redacted]
Category	INFORMATION LEAKAGE/ DISCLOSURE
Severity	High
Bug Location	[redacted]
Impact	

Activity

Researcher samierdem submitted a vdp bug.	[redacted]
Researcher samierdem recalled vdp bug.	[redacted]
Researcher samierdem submitted a vdp bug.	[redacted]
Organization validator [redacted] approved the vdp bug with the "*undefined*" note.	[redacted]

Response To Decision	Confirm
Comment	
Severity	High
Date	[redacted]
Status	Resolved
☑ Cash	500 Euro
□ Gift	Gift
□ Gift Card	
☑ Recognition	Url

VDP_0011_samierdem.pdf

Researcher Chat

To whom ?

[redacted]

API katmanına kontrol eklenmiştir. 525 - You

The BugBounter Approach

BugBounter analysed the attack surfaces and advised the scope for the bug bounty program that meets the needs of the e-commerce company. After the bug bounty structure was designed (in-scope targets, out-of-scope targets, exclusion lists, reward structure, special terms, validation method, fees, researcher criteria etc), it was announced within the BugBounter ecosystem. This enabled the testing invitation to reach out to a diverse group of talents to participate in the challenge.

BugBounter published a limited-time bug bounty program that would cover the company's new web and mobile applications. This bug bounty program was integrated into their DevOps cycle, which stays active for 7-10 days to cover the testing of new software versions that are just released. This cycle was repeated for every new software release.

Results

Thanks to the continuous programs and the diverse ecosystem of talented researchers in the BugBounter ecosystem, the e-commerce company:

- **Secured its new software releases effectively and cost-efficiently**
- **Attained a great reliability between their customers and suppliers**
- **Went live with an affordable testing budget and great confidence in vulnerability discovery**
- **Spotted the vulnerabilities quickly and stayed one step ahead of malicious attackers**