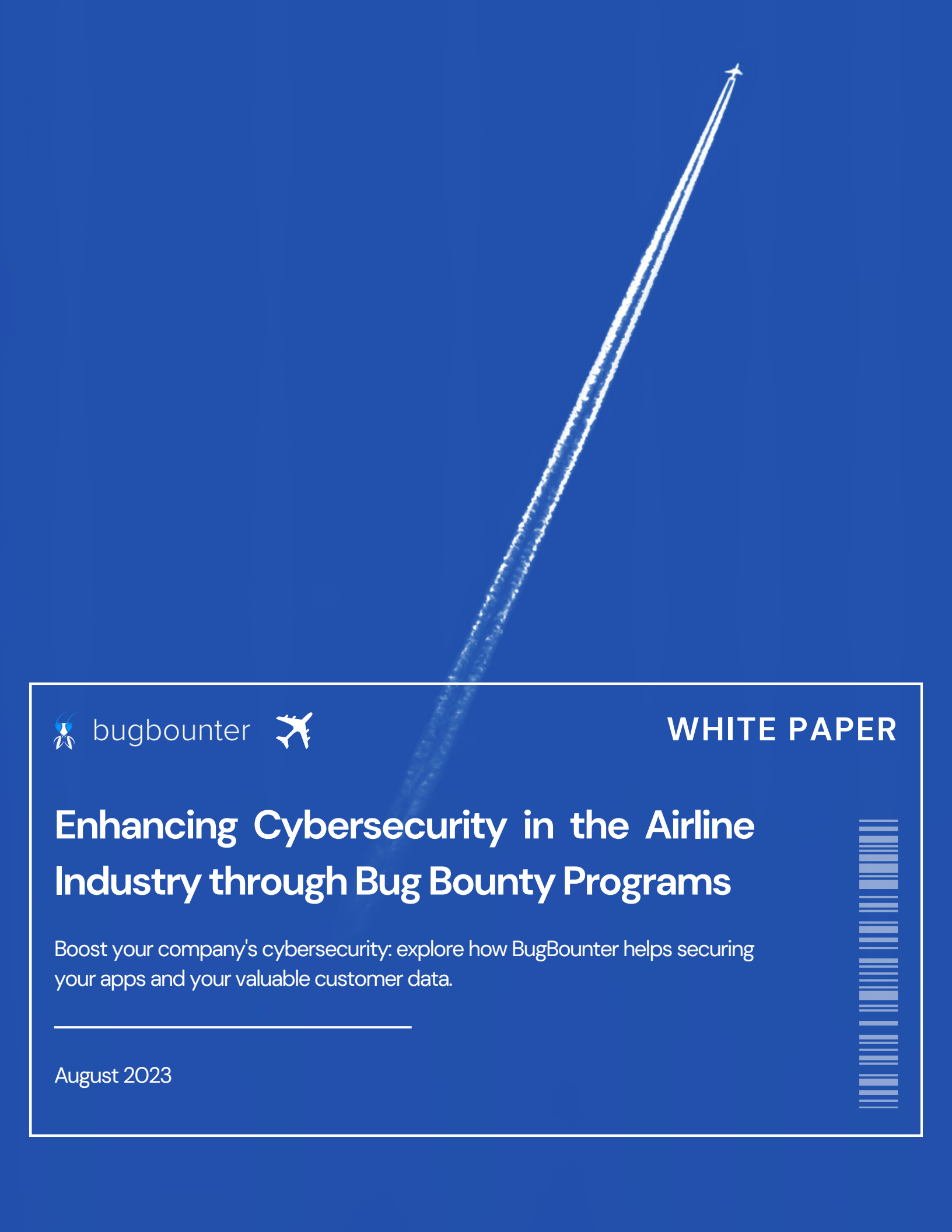


bugbounter

WHITE PAPER

Enhancing Cybersecurity in the Airline Industry through Bug Bounty Programs

Boost your company's cybersecurity: explore how BugBounter helps securing your apps and your valuable customer data.

August 2023

ABSTRACT

In an era defined by rapid technological advancements, the **airline industry's reliance on digital infrastructure has grown significantly.** With increased connectivity comes an **augmented risk of cyber threats.** To secure the integrity of critical systems and customer data in the airline sector, **bug bounty programs have emerged as a valuable instrument.** This paper explores the **role of bug bounty programs in enhancing cybersecurity within airlines**, their impact on the industry, and **how such programs can be leveraged to fortify application security.**

WHITE PAPER bugbounter

INTRODUCTION

The airline industry, which includes top operators in the world, need to perform in an environment where the fusion of cutting-edge technology and complex networks is paramount. As the industry continues to embrace digital transformation, the threat landscape expands, exposing airlines to a variety of cyber threats. **To counteract risks of latest releases of apps and ensure the safety and reliability of their customers and members data, the concept of bug bounty programs has gained traction.**

BUG BOUNTY: THE PRIMER

Bug bounty programs represent a collaborative methodology of research to cybersecurity vulnerability assessments. In essence, bounty programs leverage the skills and expertise of **freelance cybersecurity experts, also known as bug bounty hunters, to discover vulnerabilities in an organization's systems and applications.** By incentivizing ethical hackers through **bug bounty rewards, airline companies encourage the discovery of security flaws before malicious actors can exploit them.**

WHITE PAPER

bugbounter

BUG BOUNTY IN AIRLINES: WHY?

In recent days, the dangers in the cyber world are disguising themselves, along with various actors in cybercrime such as script kiddies, hacktivists, criminal gangs, nation-state hackers, and malicious insiders. Cybercriminals can access private details such as names, passport IDs, credit card passwords, and addresses, and manipulate bookings by creating fake reservations with privilege escalation for free or tickets for 2 EUR. **They can also cancel 100 bookings in a matter of minutes, significantly affecting the flights.**

WHITE PAPER bugbounter

BUG BOUNTY IN AIRLINES INDUSTRY

In recent years, top airline companies have started embracing bug bounty programs to bolster their cybersecurity measures.

Crowdsourced cybersecurity testing, facilitated by bug bounty platforms such as BugBounter, has enabled airlines companies to tap into a global network of security experts. By welcoming their collective intelligence, airlines have effectively extended their defense lines against cyber threats:

- ☑ Hundreds of engaged experts
- ☑ Diversity of thought
- ☑ Rapid response
- ☑ Recheck of fix
- ☑ Advisory for remediation
- ☑ Motivation to uncover

WHITE PAPER

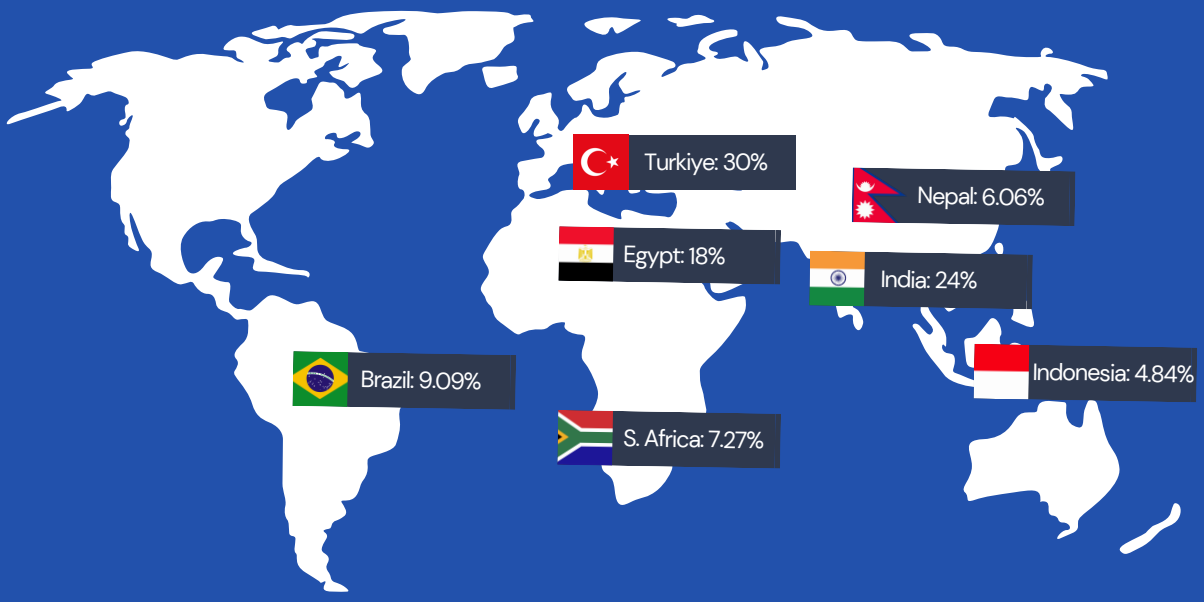
bugbounter

STATISTICAL INSIGHTS: COUNTRIES

Data extracted from BugBounter's bug bounty program participation provides valuable insights into the efficacy of bug bounty initiatives within the airlines industry.

Distribution of Experts by Submission

130 cybersecurity experts within the BugBounter Community submitted reports on the airlines bug bounty projects. Turkiye is the country with the highest number of reports were submitted from, while Indonesia is #7 at the rank.

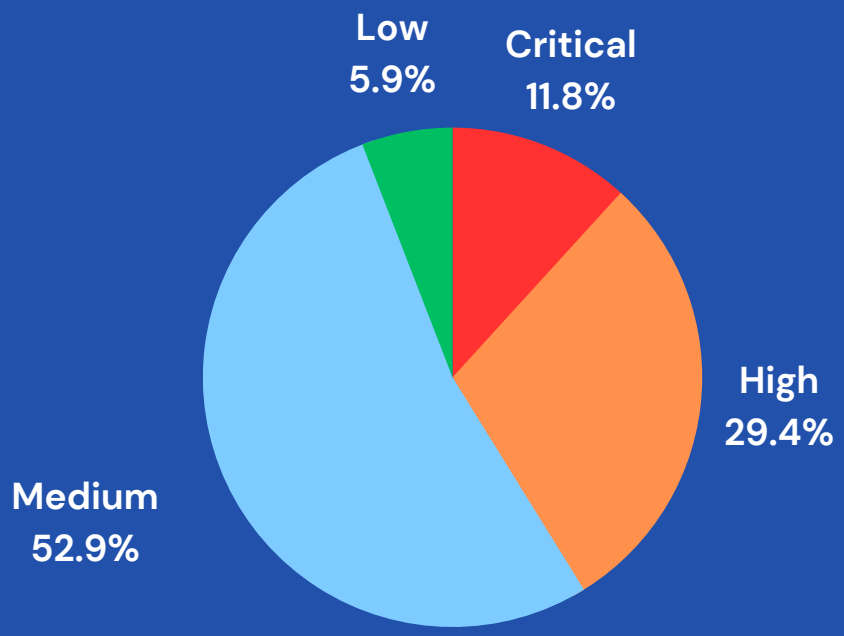


STATISTICAL INSIGHTS: SEVERITY

Data extracted from BugBounter's bug bounty program participation provides valuable insights into the efficacy of bug bounty initiatives within the airlines industry.

Distribution of Reports' Severity Levels

Among all the reports submitted, 40% were rejected due to duplication. The remaining 60% were validated by the triage and cybersecurity teams. Based on CVSS 3.0 scoring system, **medium level vulnerabilities are the most discovered.**



STATISTICAL INSIGHTS: FINDINGS

The statistics below show the number of the vulnerabilities reported by the BugBounter Community, and the platforms where the vulnerabilities were identified.

Top Vulnerability Types Reported Across the Programs

The revealed stats shed light on complex cybersecurity challenges airlines face. From logic errors to data leakage, diverse vulnerabilities underline **urgency for strong code checks, access controls, and data safeguards to ensure comprehensive digital defense.**

See the top 3 vulnerabilities reported across the programs.

Vulnerability	Rate
Information Leakage	20%
Business Logic Error	16%
Cross-Site Scripting (XSS)	12%
Others	52%

IMPACT ON CYBERSECURITY

Bug bounty programs contribute significantly to the overall cybersecurity posture of airlines. By uncovering critical vulnerabilities, bounty programs provide an opportunity for companies to rectify weaknesses before malicious actors exploit them. The collaborative nature of **bug bounty initiatives fosters a symbiotic relationship between airlines and the security community, thereby creating a safer cyber environment for the entire industry.**

APPLICATION SECURITY

The integration of bug bounty programs into airlines' cybersecurity strategies is instrumental in fortifying application security. As airlines invest in advanced cyber threat solutions, **bug bounty programs offer an additional layer of defense.** They enable organizations to harness the collective expertise of cybersecurity professionals from diverse backgrounds, **identifying vulnerabilities that might have been overlooked in internal assessments.**

WHITE PAPER

bugbounter

CONCLUSION

In an era where cyber threats continue to evolve, the airline industry must remain resilient in securing its digital infrastructure. **Bug bounty programs serve as a beacon of innovation, allowing airlines to harness the power of collective cybersecurity knowledge.** The partnership between airlines and bug bounty hunters not only enhances the overall security of top airlines in the world but also exemplifies a collaborative approach to combating cyber threats. As the industry continues to progress, **bug bounty programs stand as a testament to the airlines' dedication to providing safe and secure air travel experiences for all passengers.**

THANK YOU FOR READING

Elevate airline cybersecurity with insights into bug bounty programs. Explore the white paper and thank you for prioritizing safety. We appreciate your dedication to securing the skies.

FOLLOW BUGBOUNTER

- BugBounter
- bugbounterr
- bugbounterr
- bugbounter

bugbounter.com