YES WE HACK

Brittany Ferries

BRITTANY FERRIES

Case Study

France Cyber Maritime is a non-profit association dedicated to providing practical and customised cybersecurity solutions to the maritime industry. Its mission is to enhance the industry's resilience and promote French expertise in maritime cybersecurity on a global scale, with a particular focus on Europe.

As cyber-attacks continue to proliferate, particularly within the maritime industry, France Cyber Maritime is committed to delivering cutting-edge solutions to safeguard the industry's IT systems and infrastructure.

To that end, France Cyber Maritime has partnered with YesWeHack, a member of the association, to introduce Battleship - the first-ever live Bug Bounty program designed specifically for the maritime industry in Europe. This initiative aims to bolster the cybersecurity defenses of maritime companies by proactively identifying potential vulnerabilities before they can be exploited by malicious actors.

In May 2022, the inaugural edition of Battleship was held, featuring the participation of Brittany Ferries, a prominent shipping company.

Founded in 1972, the French maritime company BAI became Brittany Ferries in 1974 and is today the leading shipping company on the Western and Central Channel. With a fleet of 10 ships, Brittany Ferries operates crossings between France, the UK, Ireland and Spain and carries around 2 million passengers per year.

Over a period of 48 hours, dozens of cybersecurity experts from the YesWeHack community tested Brittany Ferries' online booking platform, seeking to uncover any potential security weaknesses. This initial edition of Battleship proved to be a resounding success, enabling Brittany Ferries to reinforce the security of its booking system.

We had the pleasure of speaking with Ian Frens, CISO at Brittany Ferries, who graciously shared his experience of participating in this unprecedented event. Ian Frens provided valuable insights into how the company prepared for the event, as well as the significant impact that the initiative had on the overall IT security of the organisation.

YES WE HACK

CAN YOU EXPLAIN THE REASONS BEHIND BRITTANY FERRIES' PARTICIPATION IN BATTLESHIP?

IAN FRENS, CISO, BRITTANY FERRIES:

Brittany Ferries had recently revamped its online booking system, which had become a critical application for the company, as a majority of ferry bookings were now made online.

Despite undergoing a penetration test before going live, the system revealed two significant vulnerabilities that raised concerns about its security.

When France Cyber Maritime extended the invitation to participate in the Live Bug Bounty program, we saw this as a valuable opportunity to evaluate the security of our booking application, even though we had no prior experience in this area.

Given our lack of expertise in the Bug Bounty domain, we decided to focus solely on the main online booking application, though we had initially considered testing other web applications as well. In hindsight, this decision proved to be wise, as it enabled the researchers to concentrate on a specific scope.

HOW DID YOU PREPARE YOUR PARTICIPATION IN THIS LIVE BUG BOUNTY?

IAN FRENS, CISO, BRITTANY FERRIES:

As this was a completely new approach for Brittany Ferries, our first step was to attend meetings with France Cyber Maritime and YesWeHack to understand the event's structure and organisation. These meetings enabled us to prepare adequately and anticipate what to expect during the Live Bug Bounty.

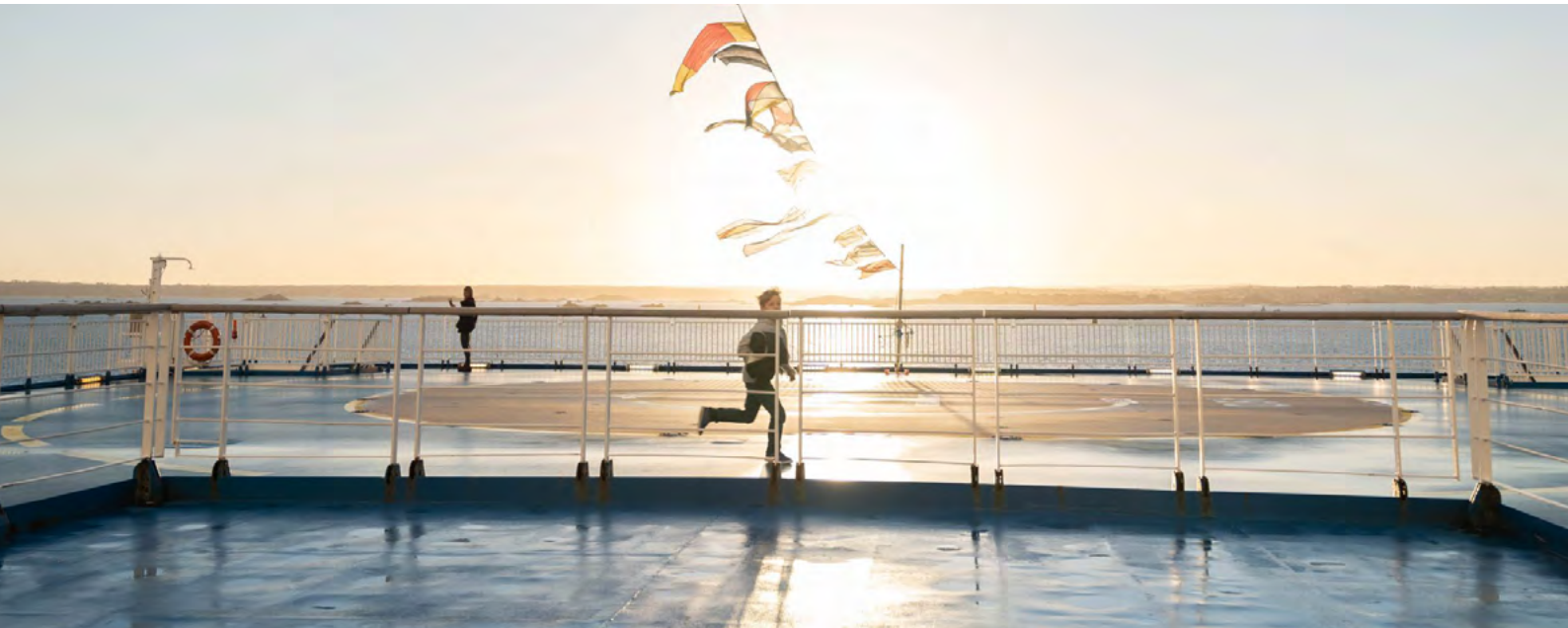
Next, we focused on defining our program. Even though we already intended to test the application, it was crucial to define:

- The vulnerabilities to look for and those to exclude
- The rewards to grant
- The rules for researchers to follow during the event

We collaborated closely with the YesWeHack team and involved the application teams from the outset.

Once the program was defined, Brittany Ferries' internal teams, including the application team, the CISO and the production team, were mobilised for the two-day event. Participation in such an event requires in-house security skills in both the application and web domains, not only to write the program but also to assess the vulnerabilities discovered during the event.

Although the YesWeHack team conducts a pre-qualification process during the event, it is essential to fully understand the reports to determine whether to accept the vulnerabilities and award corresponding rewards.



WERE THERE ANY CONCERNS OR FEARS WITHIN BRITTANY FERRIES BEFORE JOINING THIS LIVE BUG BOUNTY?

IAN FRENS, CISO, BRITTANY FERRIES:

From the outset, we recognised the potential benefits of participating in the Bug Bounty program, despite its novelty. As such, the idea was met with a positive response. Of course, we had to obtain approval from management by addressing certain concerns such as the selection of security researchers, the impact on production, and the confidentiality of results. Fortunately, these concerns were quickly addressed, and we were able to participate in Battleship with confidence.

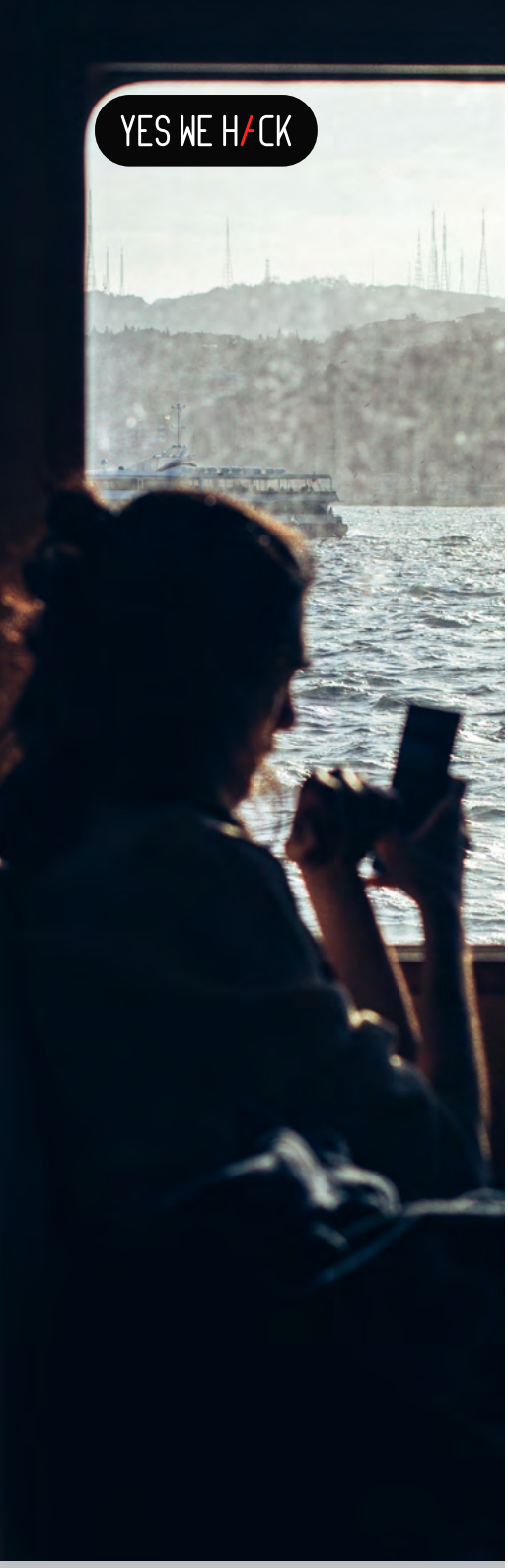
WHAT DO YOU THINK ABOUT THE CONCERNS COMPANIES MAY HAVE ABOUT LAUNCHING A BUG BOUNTY PROGRAM IN A PRODUCTION ENVIRONMENT?

IAN FRENS, CISO, BRITTANY FERRIES:

The program definition does not prevent some side effects indeed. In order to facilitate the identification of Bug Bounty attacks, we asked participating researchers to include a specific header in all of their test requests.

During the event, we faced a situation where a researcher used a bruteforce tool to test one of our APIs. Thankfully, our production team was quickly alerted by our monitoring tools, and we were able to discuss the issue with the researcher to find a solution. Once the incident was resolved, we did not encounter any further similar issues.

It's worth noting that during a Bug Bounty event, it's always possible to interact with participating researchers to adjust or reframe their research if necessary. This highlights the importance of having internal teams readily available throughout the event.



Brittany Ferries

WHAT BENEFITS DID PARTICIPATING IN BATTLESHIP BRING TO YOU AND YOUR COMPANY?

IAN FRENS, CISO, BRITTANY FERRIES:

To begin with, our participation in the Bug Bounty program provided us with reassurance about the security level of our application. Although a few vulnerabilities were discovered, none of them were deemed critical. Overall, the researchers considered the security level of the application to be good.

Furthermore, the vulnerabilities that were discovered allowed us to address them promptly. We found that the cost-effectiveness ratio was excellent compared to our usual penetration testing.

Our internal development teams found the event to be highly engaging. The interactive collaboration facilitated by Bug Bounty enabled them to gain a better understanding of attackers' thought processes and the techniques they employ. It also heightened their awareness that minor coding or configuration errors could be exploited for malicious purposes. This awareness is a significant advantage of Bug Bounty over penetration testing.

Lastly, we realised that communicating our participation in this event could help establish trust among our customers and partners by demonstrating that cybersecurity was a top priority for Brittany Ferries.

Overall, the event had a positive outcome, which is why we decided to integrate Bug Bounty into our annual audit plan in addition to more conventional methods.

> **"We found that the cost-effectiveness ratio was excellent compared to our usual penetration testing.**

ABOUT

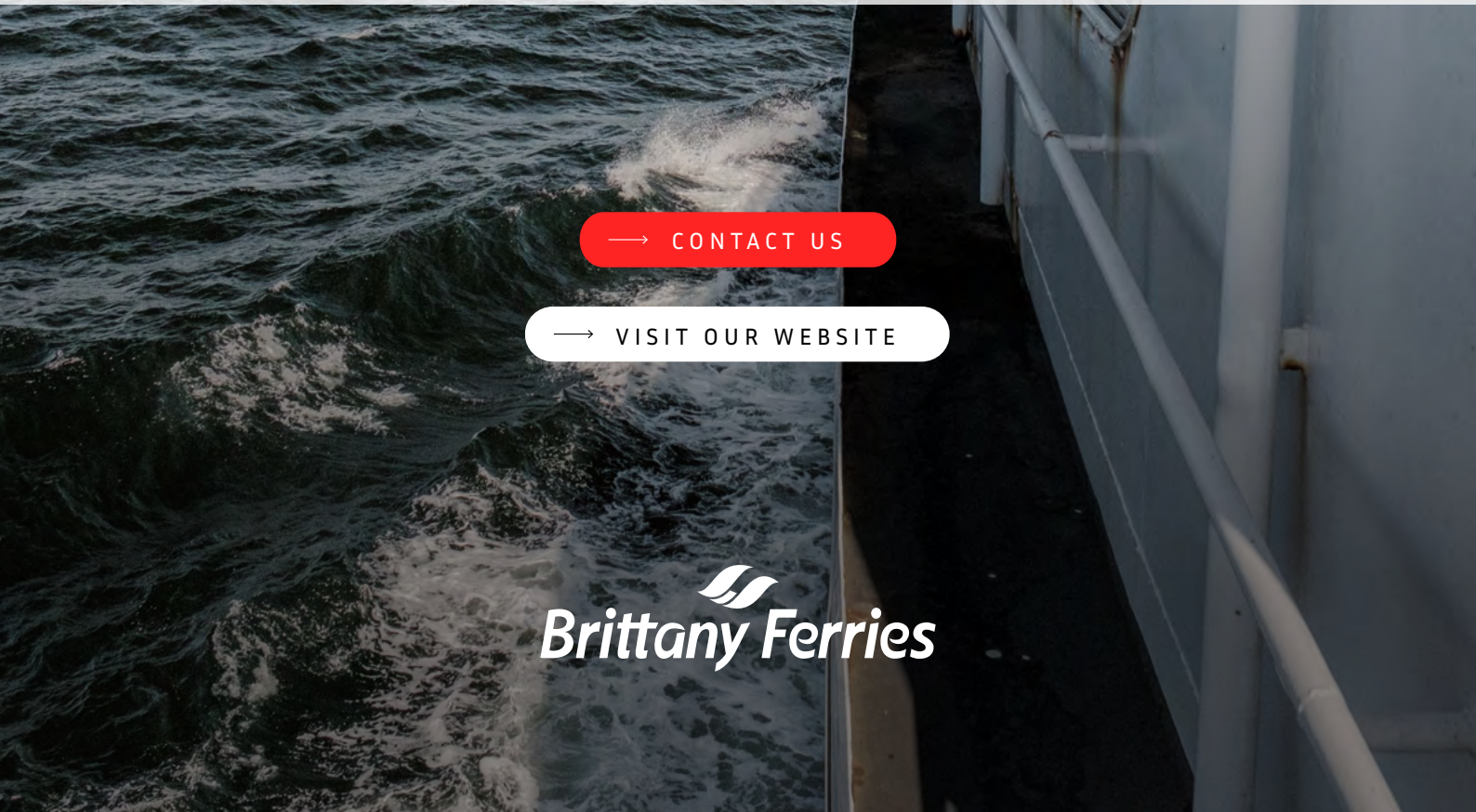
YES WE HACK

Founded in 2015, YesWeHack is a Global Bug Bounty & VDP Platform.

YesWeHack offers companies an innovative approach to cybersecurity with Bug Bounty (pay-per-vulnerability discovered), connecting tens of thousands of cybersecurity experts (ethical hackers) across 170 countries with organisations to secure their exposed scopes and reporting vulnerabilities in their websites, mobile apps, infrastructure and connected devices.

YesWeHack runs private (invitation based only) programs and public programs for hundreds of organisations worldwide in compliance with the strictest European regulations.

In addition to the Bug Bounty platform, YesWeHack also offers: a creation and management solution for Vulnerability Disclosure Policy (VDP), a pentest management platform, a learning platform for ethical hackers called Dojo and a training platform for educational institutions, YesWeHackEDU.



⟶ CONTACT US

⟶ VISIT OUR WEBSITE

Brittany Ferries