

Challenge 4: Enhancing System Security in Response to Industry Breach #13

2 of 5 tasks

Jordan-sparks-po bot opened this yesterday · 8 comments

Closed

Edit New issue

Jordan-sparks-po bot commented yesterday · edited by smoothsailor

Challenge 4: Enhancing System Security in Response to Industry Breach

As the CISO of Globeticket, I want to implement rigorous security practices to ensure our systems are fortified against vulnerabilities similar to those that led to a competitor's significant data breach. This proactive approach will help maintain customer trust and ensure the security of sensitive information. To overcome this, we have purchased the tool GitHub Advanced Security to help addressing these issues.

Why:

- Industry Breach Alert:** A major competitor has suffered a data breach involving thousands of credit card records due to vulnerabilities in the System.Data.SqlClient package. This incident has raised concerns about the potential risks in our own systems.
- Immediate Action Required:** The urgency is highlighted by our CISO's concern about our exposure to similar vulnerabilities, prompting a comprehensive review and update of our security practices.

Acceptance Criteria:

- Security Tool Activation:**
 - Enable GitHub Advanced Security (GHAS) along with all its separate features to scan and monitor our repository for vulnerabilities.
- Software Bill of Materials (SBOM):**
 - Export an SBOM and rename it into sbom.json. Create a folder on the main branch called sbom and put the exported sbom.json in it for a detailed audit and tracking of all components used in our software.
- Dependency Management:**
 - Address all Dependabot alerts, prioritizing fixes from critical to high and then medium, ensuring all dependencies are up-to-date and secure.
- Code Quality Assurance:**
 - Resolve all CodeQL alerts, either by fixing the issues directly or dismissing them as false positives after thorough evaluation.
- OWASP Compliance Check:**
 - Conduct a comprehensive check for common OWASP vulnerabilities, particularly SQL Injection. Transition to using SQL parameters to prevent such risks.
 - Utilize GitHub Copilot to assist in identifying and resolving these security issues effectively.

Challenge Tasks:

- ☒ Turn on GHAS and activate all its features.
- ☒ Generate a SBOM, rename it to 'sbom.json', place it in a 'sbom' folder in the root, and commit it to the main branch.
- ☐ Tackle Dependabot alerts, starting with the most severe.
- ☐ Address all CodeQL alerts appropriately.
- ☐ Check and fix any OWASP top 10 vulnerabilities, especially those related to SQL practices.

"Security is not a product, but a process." — Bruce Schneier

Assignees

No one—[assign yourself](#)

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Create a branch for this issue or link a pull request.

Notifications

Unsubscribe

You're receiving notifications because you commented.

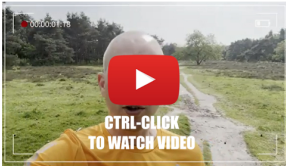
1 participant

Lock conversation

Pin issue

Transfer issue

alex-fletcher-lead bot commented yesterday



Alex Fletcher

Hey team! 🙌 Just had an "aha" moment thinking about our security setup after diving into some awesome resources recently. This stuff is right up our alley, especially with that similar issue we tackled last month.

Feeling pretty stoked about the solution path! We are going to leverage a lot of things from GitHub Advanced Security! I've quickly read up on this. Based on those insights, I've put together a quick Wiki page with some key pointers. Check out the details and get the full scoop [here on our Wiki](#) to catch the vibe 🎉

- Need a hand or stuck on a step? Just type `/help` for some pro tips. 📖
- Craving a full-on, step-by-step guide? Pop over to `/expert-tip`. 📖
- Want to verify if your fixes meet our high standards? `/verify` is just a click away. 🛡️
- Ready for me to dive in and take care of these items? Hit `/fix` and consider it handled. 🛠️

Oh! And don't forget, when you're ready to move on to a new challenge, type `/fixskip`. Emily will handle closing the issue, so don't do it yourself. But first, hit `/fix` and make sure you've used the provided code to gear up for the next challenge.

smoothsailor commented yesterday

/expert-tip

alex-fletcher-lead bot commented yesterday

I managed to find some time and wrote a detailed step-by-step guide for setting up GHAS! Check it out here on the [Wiki page!](#)

smoothsailor commented yesterday

/fix

emily-chase bot commented yesterday

Got it! I've coordinated with the offshore team to get this done. It will incur some costs, but they've written the code. Alex will be creating a PR for you to review and merge. Stay tuned!


alex-fletcher-lead bot commented yesterday

🚀 Fast! Got the code and pushed PR! You can merge that!

#22

smoothsailor commented yesterday

/finish





emily-chase


bot

commented yesterday

...

 You nailed it! Robert will be ecstatic! I'll inform the corporate communication team to showcase this on the intranet. Well done! Closing the issue now! Just navigate to the [Glibofickat Intranet](#) to continue!






emily-chase

bot










closed this as completed yesterday




Add a comment


Write


Preview


H B I         

Add your comment here...

 Markdown is supported

 Paste, drop, or click to add files

 Reopen issue

 Comment

Remember, contributions to this repository should follow our [GitHub Community Guidelines](#).