

🔗 Google Discussions



Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

📄 EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 92 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 92

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.

How should you prevent and fix this vulnerability?

- A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

Show Suggested Answer

by Jerrard at Oct. 7, 2020, 8:58 p.m.

Comments

Type your comment...

  **sudarchary** Highly Voted  2 years, 6 months ago

Selected Answer: D

Option D is correct as using web security scanner will allow to detect the vulnerability and templating system

   upvoted 10 times

  **deardeer** Highly Voted  3 years, 5 months ago

Answer is D. There is mention about simulating in Web Security Scanner. "Web Security Scanner cross-site scripting (XSS) injection testing *simulates* an injection attack by inserting a benign test string into user-editable fields and then performing various user actions." <https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#xss>

   upvoted 7 times

  **AzureDP900** 1 year, 8 months ago

Agree with D

   upvoted 2 times

  **ThisisJohn** 2 years, 7 months ago

Agree. Also from your link

"There are various ways to fix this problem. The recommended fix is to escape all output and use a templating system that supports contextual auto-escaping."

So escaping is a way to fix the issue, which is required by the question

   upvoted 1 times

  **AwesomeGCP** Most Recent  1 year, 9 months ago

Selected Answer: D

D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

   upvoted 2 times

  **tangac** 1 year, 10 months ago

Selected Answer: D

clear D everything is explicated here : <https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings>

Web Security Scanner cross-site scripting (XSS) injection testing simulates an injection attack by inserting a benign test string into user-editable fields and then performing various user actions. Custom detectors observe the browser and DOM during this test to determine whether an injection was successful and assess its potential for exploitation.

There are various ways to fix this issue. The recommended fix is to escape all output and use a templating system that supports contextual auto-escaping.

   upvoted 2 times

  **Lancyqusa** 2 years, 7 months ago

It should be C because the web security scanner will identify the library known to contain the security issue as in the examples here - https://cloud.google.com/security-command-center/docs/how-to-use-web-security-scanner#example_findings.

Once the security issue is identified, the vulnerability can be fixed by a secure version of that library.

   upvoted 1 times

  **DebasishLowes** 3 years, 4 months ago

Ans : D

   upvoted 2 times



  **pyc** 3 years, 5 months ago

C,

D is wrong, as Security Scanner can't "simulate" anything. It's a scanner.

B is not right, as Armor can't do input data validation, it just deny/allow IP/CIDR.

   upvoted 1 times

  **desertlotus1211** 3 years, 4 months ago

Yes it can simulate... Read the documentation first...

   upvoted 3 times

  **KarVaid** 3 years, 7 months ago

<https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>

Security Scanner should be able to scan for XSS vulnerability as well. Option D is better.

Security Scanner should be able to scan for XSS vulnerabilities as well. Option D is better.

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **KarVaid** 3 years, 7 months ago

Cloud armor can prevent the vulnerability but to fix it, you would need Security scanner.

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **Fellipo** 3 years, 8 months ago

B , <https://cloud.google.com/armor>

👍 ↩ 🚩 upvoted 5 times

🗨️ 👤 **HectorLeon2099** 3 years, 9 months ago

Answer is B. Web Security Scanner can look for XSS vulnerabilities but can't simulate XSS injection attack.

https://cloud.google.com/armor/docs/rule-tuning#cross-site_scripting_xss

👍 ↩ 🚩 upvoted 3 times

🗨️ 👤 **FatCharlie** 3 years, 8 months ago

Web Security Scanner does appear to be able to simulate an XSS attack.

"Web Security Scanner cross-site scripting (XSS) injection testing simulates an injection attack by inserting a benign test string into user-editable fields and then performing various user actions. Custom detectors observe the browser and DOM during this test to determine whether an injection was successful and assess its potential for exploitation."

<https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#remediate-findings>

👍 ↩ 🚩 upvoted 4 times

🗨️ 👤 **saurabh1805** 3 years, 9 months ago

Agree B is correct answer here.

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **Jerrard** 3 years, 9 months ago

D. <https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>

👍 ↩ 🚩 upvoted 4 times



Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses

