

समाचार वाणी

खबर जो करें असर !

नाशिक | Thursday, 24 September 2026

गूगल का बड़ा ऐलान : AI सिस्टम में बग खोजने वाले को मिलेगा 26 लाख रुपये तक का इनाम

Publisher

Published on 07 Oct 2025



गूगल ने हाल ही में अपने आर्टिफिशियल इंटेलिजेंस (AI) सिस्टम में बग खोजने वालों के लिए बड़ा पुरस्कार घोषित किया है। इस नए बग बाउंट प्रोग्राम के तहत कोई भी सिक्वोरिटी एक्सपर्ट या एथिकल हैकर अगर गूगल के AI सिस्टम में गंभीर खामी खोजकर दिखाता है, तो उसे 30,000 अमेरिकी डॉलर यानी लगभग 26 लाख रुपये तक का इनाम दिया जाएगा।

यह प्रोग्राम गूगल के पुराने Vulnerability Reward Program का विस्तार है, लेकिन अब इसका विशेष ध्यान AI की दुनिया पर केंद्रित किया गया है। कंपनी ने कहा है कि इस पहल का उद्देश्य अपने AI सिस्टम को और अधिक सुरक्षित बनाना है।

गूगल ने अपने बयान में कहा कि “हम सुरक्षा विशेषज्ञों और शोधकर्ताओं को आमंत्रित कर रहे हैं कि वे हमारे AI सिस्टम में खामियों की पहचान करें और उन्हें रिपोर्ट करें। गंभीर खामियों की रिपोर्ट पर इनाम की राशि 30,000 डॉलर तक हो सकती है।”

इस कार्यक्रम की खासियत यह है कि यह पहले की तुलना में AI मॉडल और उसके इन्फ्रास्ट्रक्चर की सुरक्षा पर केंद्रित है। गूगल ने बताया कि AI सिस्टम में बग खोजने और उसे सही करने के लिए बाहरी विशेषज्ञों की मदद लेना आवश्यक है, क्योंकि बड़े और जटिल AI मॉडल्स में सुरक्षा खामियां सामान्य होती हैं।

इससे पहले भी कई रिसर्चर गूगल के Vulnerability Reward Program का हिस्सा बनकर बड़ी रकम कमा चुके हैं। गूगल के अनुसार, अब तक बग खोजकर शोधकर्ताओं ने कुल मिलाकर 4,30,000 डॉलर से अधिक राशि प्राप्त की है। गूगल का कहना है कि इस बार भी प्रतिभागियों के सामने चुनौती यही होगी कि वे AI सिस्टम की सुरक्षा को मजबूत करें और संभावित खतरों को उजागर करें।

गूगल के AI सिस्टम में बग ढूँढना आसान काम नहीं है। यह सिस्टम लगातार अपडेट होते रहते हैं और नए एल्गोरिदम तथा डेटा मॉडल्स जोड़ते रहते हैं। इसलिए इसमें बग की पहचान करना और रिपोर्ट करना तकनीकी क्षमता और गहन अध्ययन की मांग

करता है।

AI सुरक्षा विशेषज्ञ और एथिकल हैकर्स इस प्रोग्राम को उत्साह के साथ देख रहे हैं। उन्हें उम्मीद है कि इससे न केवल उन्हें वित्तीय लाभ मिलेगा बल्कि उनके कौशल को वैश्विक स्तर पर मान्यता भी मिलेगी।

गूगल का यह कदम इस बात को भी स्पष्ट करता है कि AI तकनीक के बढ़ते इस्तेमाल के साथ सुरक्षा खतरों को नजरअंदाज नहीं किया जा सकता। बड़े AI मॉडल्स का दुरुपयोग होने की संभावना और उनके सिस्टम में मौजूद सुरक्षा खामियों को उजागर करने के लिए यह बग बाउंटी प्रोग्राम बेहद जरूरी है।

विशेषज्ञों का मानना है कि ऐसे कार्यक्रम AI कंपनियों के लिए दोहरे लाभ के साधन हैं। पहला, वे अपने सिस्टम की सुरक्षा सुधार सकते हैं और दूसरा, प्रतिभाशाली शोधकर्ताओं और एथिकल हैकर्स को अपनी तरफ आकर्षित कर सकते हैं। गूगल ने यह भी स्पष्ट किया कि किसी भी खामी की गंभीरता और प्रभाव के आधार पर इनाम की राशि तय की जाएगी।

इस नए प्रोग्राम में गूगल ने स्पष्ट किया कि केवल गंभीर बग्स या सुरक्षा खामियों पर ही 30,000 डॉलर का पुरस्कार मिलेगा। छोटी-मोटी या सामान्य खामियों के लिए अलग श्रेणी में पुरस्कार दिए जाएंगे। इस पहल का उद्देश्य AI मॉडल्स की विश्वसनीयता और उपयोगकर्ताओं के डेटा की सुरक्षा को सुनिश्चित करना है।

गूगल ने आगे कहा कि AI की सुरक्षा पर ध्यान न देना गंभीर परिणाम ला सकता है। अगर AI सिस्टम में खामी का फायदा उठाकर कोई हैकर डेटा चोरी या सिस्टम में अनधिकृत बदलाव करता है, तो इससे न केवल कंपनी को बल्कि उपयोगकर्ताओं को भी नुकसान हो सकता है।

AI के बढ़ते प्रयोग और गूगल के AI मॉडल्स के वैश्विक इस्तेमाल को देखते हुए, यह बग बाउंटी प्रोग्राम समय की मांग है। इससे न सिर्फ तकनीकी खतरों की पहचान होगी बल्कि एथिकल हैकर्स और सुरक्षा शोधकर्ताओं को उनकी प्रतिभा दिखाने का मंच भी मिलेगा।

विशेषज्ञों का मानना है कि यह पहल AI सिस्टम की सुरक्षा में एक महत्वपूर्ण कदम है। गूगल ने इसे पारदर्शी और वैश्विक स्तर पर आयोजित किया है, जिससे दुनिया भर के प्रतिभागी इसमें हिस्सा ले सकते हैं।

इस प्रोग्राम के जरिए गूगल AI सुरक्षा के क्षेत्र में नई मिसाल कायम करना चाहता है। कंपनी ने कहा कि “हम चाहते हैं कि हमारा AI सिस्टम सुरक्षित, भरोसेमंद और भविष्य की चुनौतियों के लिए तैयार रहे।”

गूगल के इस पहल ने एथिकल हैकर्स और तकनीकी विशेषज्ञों में उत्साह भर दिया है। वेम्बु, गूगल और अन्य कंपनियों के बग बाउंटी प्रोग्राम इस बात का प्रमाण हैं कि तकनीकी दुनिया में सुरक्षा को प्राथमिकता देना कितना महत्वपूर्ण है।

DISCLAIMER: the views/contents expressed/presented herein, within this advertorial and promotional feature are the sole and exclusive responsibility of individual clients/expert/their authorised representative/Publisher, to which effect, publication house/its representative/affiliates are not responsible/liable whatsoever.