```
From e864c7f67f8d10cef7f1ef126cf066353ab585c4 Mon Sep 17 00:00:00 2001
From: 13 <alizsalari13@gmail.com>
Date: Wed, 3 Dec 2025 01:03:18 +0330
Subject: [PATCH] am-legal-safe-har

---
 ...ub-bug-bounty-program-legal-safe-harbor.md | 38 ------------------
 1 file changed, 38 deletions(-)
 delete mode 100644 content/site-policy/security-policies/github-bug-bounty-program-legal-safe-
harbor.md

diff --git a/content/site-policy/security-policies/github-bug-bounty-program-legal-safe-harbor.md
b/content/site-policy/security-policies/github-bug-bounty-program-legal-safe-harbor.md
deleted file mode 100644
index 1818712ee97e..000000000000
--- a/content/site-policy/security-policies/github-bug-bounty-program-legal-safe-harbor.md
+++ /dev/null
@@ -1,38 +0,0 @@
----
-title: GitHub Bug Bounty Program Legal Safe Harbor
-redirect_from:
-  - /articles/github-bug-bounty-program-legal-safe-harbor
-versions:
-  fpt: '*'
-topics:
-  - Policy
-  - Legal
----
-
-## Summary
-
-1. We want you to coordinate disclosure through our bug bounty program, and don't want
researchers put in fear of legal consequences because of their good faith attempts to comply with
our bug bounty policy. We cannot bind any third party, so do not assume this protection extends
to any third party. If in doubt, ask us before engaging in any specific action you think _might_
go outside the bounds of our policy.
-1. Because both identifying and non-identifying information can put a researcher at risk, we
limit what we share with third parties. We may provide non-identifying substantive information
from your report to an affected third party, but only after notifying you and receiving a
commitment that the third party will not pursue legal action against you. We will only share
identifying information (name, email address, phone number, etc.) with a third party if you give
your written permission.
-1. If your security research as part of the bug bounty program violates certain restrictions in
our site policies, the safe harbor terms permit a limited exemption.
-
-## 1. Safe Harbor Terms
-
-To encourage research and coordinated disclosure of security vulnerabilities, we will not pursue
civil or criminal action, or send notice to law enforcement for accidental or good faith
violations of this policy. We consider security research and vulnerability disclosure activities
conducted consistent with this policy to be “authorized” conduct under the Computer Fraud and
Abuse Act, the DMCA, and other applicable computer use laws such as Cal. Penal Code 502(c). We
waive any potential DMCA claim against you for circumventing the technological measures we have
used to protect the applications in this bug bounty program's scope.
-
-Please understand that if your security research involves the networks, systems, information,
applications, products, or services of a third party (which is not us), we cannot bind that third
party, and they may pursue legal action or law enforcement notice. We cannot and do not authorize
security research in the name of other entities, and cannot in any way offer to defend,
indemnify, or otherwise protect you from any third party action based on your actions.
-
-You are expected, as always, to comply with all laws applicable to you, and not to disrupt or
compromise any data beyond what this bug bounty program permits.
-
```

-Please contact us before engaging in conduct that may be inconsistent with or unaddressed by this policy. We reserve the sole right to make the determination of whether a violation of this policy is accidental or in good faith, and proactive contact to us before engaging in any action is a significant factor in that decision. If in doubt, ask us first!
-
-## 2. Third Party Safe Harbor
-
-If you submit a report through our bug bounty program which affects a third party service, we will limit what we share with any affected third party. We may share non-identifying content from your report with an affected third party, but only after notifying you that we intend to do so and getting the third party's written commitment that they will not pursue legal action against you or initiate contact with law enforcement based on your report. We will not share your identifying information with any affected third party without first getting your written permission to do so.
-
-Please note that we cannot authorize out-of-scope testing in the name of third parties, and such testing is beyond the scope of our policy. Refer to that third party's bug bounty policy, if they have one, or contact the third party either directly or through a legal representative before initiating any testing on that third party or their services. This is not, and should not be understood as, any agreement on our part to defend, indemnify, or otherwise protect you from any third party action based on your actions.
-
-That said, if legal action is initiated by a third party, including law enforcement, against you because of your participation in this bug bounty program, and you have sufficiently complied with our bug bounty policy (i.e. have not made intentional or bad faith violations), we will take steps to make it known that your actions were conducted in compliance with this policy. While we consider submitted reports both confidential and potentially privileged documents, and protected from compelled disclosure in most circumstances, please be aware that a court could, despite our objections, order us to share information with a third party.
-
-## 3. Limited Waiver of Other Site Policies
-
-To the extent that your security research activities are inconsistent with certain restrictions in our [relevant site policies](/site-policy) but consistent with the terms of our bug bounty program, we waive those restrictions for the sole and limited purpose of permitting your security research under this bug bounty program. Just like above, if in doubt, ask us first!