AlpCaps

RESPONSIBLE DISCLOSURE PROGRAM

At ALPCAPS, we prioritize the security of our digital infrastructure and services. Ensuring the confidentiality, integrity, and availability of our systems is a core principle of our operations. We are committed to working together with the cybersecurity community to maintain a secure and trusted environment for our clients and partners.

The Program

While ALPCAPS does not currently operate a bug bounty program, we strongly encourage the responsible disclosure of any vulnerabilities you may discover within our systems or services. We appreciate the collaboration of security researchers in identifying and addressing vulnerabilities to enhance the safety of our infrastructure.

Reporting Guidelines

If you identify a security vulnerability, please report it to us using the following contact details:

Email: support@alpcaps.com

When submitting your vulnerability report, please include the following information:

A description of the vulnerability and its potential impact.
A list of affected systems, services, or URLs.
Steps required to reproduce the vulnerability.
How you discovered the vulnerability.
Your contact information.
We ask that you submit only one vulnerability per report unless a sequence of vulnerabilities is necessary to demonstrate their combined impact. While we will acknowledge the receipt of your report, please note that we may not provide specific details on our findings or resolution progress.

Strictly Forbidden Activities

To ensure a safe and cooperative environment, the following activities are strictly prohibited and actively monitored:

Any activity that could disrupt our services (e.g., Denial of Service (DoS), Distributed Denial of Service (DDoS), spamming, etc.).
Any actions that could jeopardize the integrity of user data.
Any actions that breach the confidentiality of user data.
The use of automated tools for vulnerability scanning.
Any fraudulent activities or transactions.
ALPCAPS reserves the right to pursue legal actions against individuals involved in illegal, harmful, or unauthorized activities that violate the above principles.

Scope

This Responsible Disclosure Program applies to:

Domains where ALPCAPS is listed as the Registrant Organization, particularly alpcaps.com and its subdomains.
Mobile applications published by ALPCAPS on the Android Play Store and Apple Store.
Please note that certain types of vulnerabilities fall outside the scope of this program, including:

Vulnerabilities in outdated or unsupported software versions without demonstrable exploitability.
Bugs that require non-trivial prior knowledge (e.g., session tokens) to exploit.
Missing or inadequate SSL/TLS configuration best practices.
Social engineering attacks or tactics.
Physical security vulnerabilities related to ALPCAPS' property or facilities.
Got Further Questions?
If you have any questions or need clarification regarding this program, please refer to our support team or consult other relevant Help sections on our website. We value your contribution to improving the security of ALPCAPS' services.