Responsible Disclosure

Responsible Disclosure Program

If you are a security researcher and have found a vulnerability, an abuse risk, or a security-related bug in an Advantage Club product, domain, or website, you can report it to us under Advantage Club's Responsible Disclosure Program.

To report a potential security vulnerability/risk/bug send an email to security@advantageclub.in with details in the below format, and we'll get in touch. The more elaborate the initial details, the easier it will be for Advantage Club to evaluate the relevance and validity of the report.

Reporting Format

Email Subject: External Bug Report <single line bug summary>

Email Body:

1. Description of the bug
2. Description of the attack scenario
3. The impact of this scenario
4. Steps to reproduce the reported vulnerability
5. Proof of exploitability (e.g., screenshot, video): (file upload button)
6. Perceived impact on another user or the organization
7. List of URLs and affected parameters
8. Other vulnerable URLs, additional payloads, Proof-of-Concept code
9. Browser, OS, and/or app version used during testing
10. Bug resolution and fix.

Program Rules

Advantage Club encourages the responsible and ethical discovery and reporting of vulnerabilities. The following conduct is expressly prohibited:

- When experimenting, please only attack test accounts you control. A PoC unnecessarily involving accounts of other guests or Advantage Club employees may be disqualified. It's also best practice to tell us the accounts you are using for testing even when they are under your control;
- Do not run automated scans without checking with us first;
- Do not test the physical security of Advantage Club offices, employees, equipment, partners, vendors, or contractors;
- Do not test using social engineering techniques (phishing, spear-phishing, pretexting, etc.);
- Do not perform DoS or DDoS attacks. You are welcome and encouraged to look for vulnerabilities that can be leveraged for DoS or DDoS attacks, we just don't want you actually exploiting the issue outside of a tightly controlled environment;
- Do not, in any way, attack our end users/guests or engage in the trade of stolen user credentials;
- Do not access, or attempt to access data, information, or physical building units that do not belong to you;
- Do not violate any applicable law or breach any agreements in order to discover vulnerabilities, or otherwise utilize unethical means to gain access and/or information;
- Only the first reporter is eligible to receive Recognition.

Important to mention

- Please do not publicly disclose the details of any potential security vulnerabilities without written consent from Advantage Club's authoritative department.
- Advantage Club does not condone any malicious or illegal behavior in identifying and reporting security vulnerabilities and you should not engage in any activity that violates applicable laws.
- If you discover personally identifiable information (PII) while exploring a suspected security vulnerability, please cease your investigation and immediately report the vulnerability that led to such discovery.

In Scope & Out of Scope Targets

All parts of our applications and services available to customers/guests are in scope and are our primary interest. Please have a look below for in-scope targets.

- *.advantageclub.in

Advantage Club uses a number of third-party providers and services. Our disclosure program does not permit you to perform security testing on their systems. Vulnerabilities in third-party systems will be assessed on a case-by-case basis, and most likely will not be eligible for recognition. The following third-party systems are excluded:

- Direct attacks against any part of AWS's infrastructure

Non-Qualifying Vulnerabilities

Low-severity, purely theoretical, and best-practice issues do not qualify for submission. Here are some examples:

- Descriptive error messages (e.g., Stack Traces, application or server errors)
- Theoretical sub-domain takeovers with no supporting evidence
- HTTP 404 codes/pages or other HTTP non-200 codes/pages
- Information leakage, fingerprinting/banner disclosure on common/public services
- Disclosure of known public files or directories, (e.g., robots.txt)
- Clickjacking on a public page and issues only exploitable through clickjacking
- CSRF on forms that are available to anonymous users (e.g., the contact form)
- Logout Cross-Site Request Forgery (logout CSRF)
- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Lack of Secure/HTTPOnly flags on non-sensitive Cookies
- Weak Captcha/Captcha Bypass
- Forgot Password page brute force and account lockout not enforced
- OPTIONS HTTP method enabled
- Reflected file downloads
- Missing Cache-control
- Host Header Attack
- Directory Listing
- Missing HTTP security headers, (specifically OWASP list of useful HTTP headers)
- SSL Issues (BEAST, BREACH, Renegotiation attack, Forward secrecy not enabled, weak ciphers)
- Not performing rate limiting on non-login endpoints
- Content spoofing
- HPKP/HSTS preloading

- Generic examples of Host header attacks without evidence of the ability to target a remote victim
- Reports exploiting the behavior of, or vulnerabilities in, outdated browsers
- SPF, DKIM, or DMARC settings & Email Spoofing
- Mixed Content Scripting & Self XSS
- EXIF Geolocation data
- Open WordPress JSON API without an exploit
- Password Reset token leakage (This is known and we will implement a fix)
- Password policy

Recognition

- By helping Advantage Club continuously keep our data secure, once the security vulnerability is verified and fixed as a result of the report, we would like to put your name on our Hall of Fame page
- Of course, we will need to know if you want the recognition, in which case you will be required to give us your name and Twitter handle, LinkedIn Profile as you wish it to be displayed on our Hall of Fame page.

We currently do not offer any monetary compensation. However, we may send out Advantage Club swag in some cases (decided by our security team).

Requests or demands for monetary compensation in connection with any identified or alleged vulnerability are non-compliant with this Responsible Disclosure Policy.