RESPONSIBLE DISCLOSURE POLICY

Introduction

At Dampfin, we've built our business on the simple principle that our customers come first. We aim to keep our website, mobile site and related software applications ("**Website**"), as well as the service offered on our Website ("**Service**") safe for everyone to use, and data security is of the utmost importance. If you have discovered a security vulnerability in our Website or Service, we encourage you to contact us and disclose it to us in a responsible manner.

When security vulnerabilities are reported to us in compliance with this policy, Dampfin will validate and fix such vulnerabilities as soon as reasonably possible, in line with our commitment to the privacy, safety and security of our customers. We will not take legal action against you or terminate your access to the Service if you discover and report security vulnerabilities responsibly in compliance with this policy. Dampfin reserves all of its legal rights in the event of any non-compliance with this policy.

If you are a current customer and observe any unauthorised activity occurring on your account, or suspect that your account might be compromised, please contact us, so that it can be investigated by the relevant teams.

Reporting a Security Vulnerability

If you think that you have found a security vulnerability in our Website or Service, please contact us immediately via sales@dampfin.com When reporting a security vulnerability, you must do the following:

1. Include sufficient information in your report, as we require a way to validate and reproduce the security vulnerability.
2. Proof-of-Concept (**PoC**) scripts or tools are encouraged, and the following information is required:
    i. The URL or API path/parameter where the vulnerability occurs.
    ii. The type of vulnerability, which should include a clear description of the issue.
    iii. Step-by-step instructions to reproduce the vulnerability.
    iv. If applicable, an attack scenario, as this may help demonstrate the risk and get the issue resolved faster.
    v. The test account that was used during testing.

3. Do not share or discuss your findings with anyone. This includes friends or colleagues. It is also strictly prohibited to post on blogs or social media platforms about your findings.
4. Please provide us with your full name.
5. Testing must be performed using a test account that is identifiable by Dampfin and disclosed in your findings.

In-scope Findings

The following types of findings are in-scope and are of interest to Dampfin on the Dampfin.com domain and its subdomains:

1. Web application attacks after a user is authenticated into their Dampfin account.
2. Administrative panels or open ports or services that are accessible to the public.
3. Cross-site scripting, XML External Entity injection and SQL injection attacks.
4. Remote code execution.
5. Circumventing permission limitations.
6. Cross-Site Request Forgery (CSRF) or Server-side Request Forgery (SSRF).
7. Privilege escalation.
8. Authorisation bypass.

Out-of-scope Restrictions

At Dampfin, we welcome “white hat” security researchers and appreciate your research and proactive responsible disclosure. Please note however that Dampfin does not permit you to do any of the following:

1. Access, modify or destroy a Dampfin customer’s account or data. Should you suspect that you are able to view or control a Dampfin customer’s account or data, please reach out to us before attempting such exploits so that Dampfin will take further steps to resolve this.
2. Interrupt or degrade our services.
3. Execute a “Denial of Service” attack, which could affect the availability of our services for any period of time.
4. Post, transmit, upload, link to, send or store any malicious software onto any of our systems. Should you suspect there is an avenue to obtain access into our

internal network, please contact us immediately and Dampfin will take further steps to resolve this.

5. Send any unsolicited or unauthorised mail or messages, this includes attempts to spoof emails, spam or perform phishing attacks.
6. Violate any applicable law or act.
7. Attempt attacks against third-party pages, including payment pages, or any sellers' websites (where applicable). Attempts can only be made against the Dampfin.com domain and its subdomains.
8. You are only allowed to pursue exploiting a vulnerability that contravenes the above-mentioned restrictions further, once the Security team has vetted and given you permission to continue. Should there be any deviations from the agreement with the Security team, this will no longer be regarded as being in accordance with this policy.

Contravening this Policy in any way may result in us suspending or terminating your access to the Website and Service, contacting the relevant authorities and/or pursuing any other remedies we have at law.

Non-qualifying Submissions

1. The risk and value of a vulnerability is determined by its impact and exploitability. If a vulnerability is not directly exploitable or does not lead to a significant threat, it will not form part of this Policy. The following types of disclosures are not part of this Policy:
    1. Informative error messages or banner disclosure.
    2. Expected, known public files or directories, (e.g. robots.txt).
    3. Clickjacking or CSRF on pages without sensitive actions.
    4. Self-XSS.
    5. Captcha-related findings.
    6. Username enumeration on the login, password reset and registration pages.
    7. OPTIONS/TRACE HTTP method enabled.
    8. SSL attacks and weaknesses.
    9. Missing HTTP security headers.
    10. Results and reports from Static Application Security Tools (SAST).
    11. Vulnerabilities in third-party applications that are not directly related to the Website.
    12. Publicly known vulnerabilities.

These findings only become eligible in the event that a reasonable, exploitable attack chain is reported. Please note that, at the discretion of Dampfin, other findings may also be added to the list of non-qualifying submissions on a case-by-case basis.

Our Commitment

If you identify a security vulnerability in compliance with this Policy, Dampfin commits to:

1. acknowledging receipt of your vulnerability report in a timely manner;
2. confirming the validity of your report; and
3. should your submission be the first for an identified, qualifying vulnerability that was previously not known about at Dampfin, a certificate of appreciation will be issued to you and attached to your full name.

Dampfin does not run a bug bounty program, and thus does not offer any monetary rewards for any valid responsible disclosures. Dampfin will however provide certificates of appreciation for the first instance of an identified vulnerability, as mentioned above.