Web Application Security Assessment of Honeygain

Honeygain is the first-ever app that allows its users to make money online by sharing their Internet connection. When you install the app, it securely utilizes the user's unused bandwidth for data intelligence tasks, such as web crawling and content delivery.

Objective: The objective of this task is to assess the security of a target web application using a black box testing methodology. Students are requested to identify and document potential vulnerabilities within the web application by employing ethical hacking techniques.

Note: Participation in security assessment is voluntary and subject to terms and conditions delineated in this task. By submitting a report, a student acknowledges reading and agreeing to the terms and conditions listed in this document.

In-Scope:

https://www.honeygain.com, including the following subdomains:

- https://dashboard.honeygain.com

Any service not expressly listed above, such as any connected and internal services, is excluded from scope and is not authorized for testing. Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing be conducted only on the systems and services covered by the scope of this document.

Out-of-Scope Vulnerabilities:

- Network-level Denial of Service attacks
- Application Denial of Service by locking user accounts
- Descriptive error messages or headers (e.g., Stack Traces, banner grabbing)
- Disclosure of known public files or directories (e.g., robots.txt)
- Outdated software/library versions

- OPTIONS/TRACE HTTP method enabled
- Cookies that lack HTTP Only or Secure settings for non-sensitive data
- Attacks requiring physical access to a user's device
- SSL/TLS best practices
- SSL attacks, such as BEAST, BREACH, or Renegotiation attack
- Use of a known-vulnerable library without a description of an exploit specific to our implementation

Guidelines, AKA The Process

Under this policy, "research" means activities in which you:

- Provide us a report in a free form notifying us about your findings until 31st May 2024.
- Only test vulnerabilities using your own accounts or accounts that you have explicit permission to test with.
- Once you've established that a vulnerability contains sensitive data (including personally identifiable information, financial information, proprietary information, or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else. Otherwise, we expect you to send a report containing your findings at the end of the research.

While we encourage you to discover and write a report to us about vulnerabilities you find in a responsible manner, the following conduct is expressly prohibited:

- Performing actions that may negatively affect Honeygain or its users (e.g., Spam, Brute Force, Denial of Service, etc.)
- Specialized custom scripts and fuzzing tools are permitted, but please keep your traffic to six requests per second or less when using them.

- Accessing or attempting to access data or information that does not belong to you.
- Destroying or corrupting, or attempting to destroy or corrupt data or information that does not belong to you.
- Retaining any personally identifiable information discovered in any medium. Any personally identifiable information discovered must be permanently destroyed or deleted from your device and storage.
- Any exploitation actions that go beyond what is required for the initial “Proof of Vulnerability.” This means your actions to obtain and validate the Proof of Vulnerability must stop immediately after initial access to the data or a system.
- Conducting any kind of physical or electronic attack on Honeygain personnel or property.
- Social engineering is any Honeygain service desk, employee, or contractor.
- Require financial compensation in order to disclose any vulnerabilities outside of a declared policy (such as holding an organization to ransom).

Writing a vulnerability report

We accept vulnerability reports via e-mail at security@honeygain.com. Information submitted under this policy will be used to mitigate or remediate vulnerabilities. By submitting a vulnerability report, you acknowledge that you have no expectation of payment and that any decisions related to your submission are solely at the discretion of Honeygain.

Your side:

In order to help us triage and prioritize submissions, your report should have:

- Full description of the vulnerability, including the exploitability and impact.
- Affected URL(s).
- IPs that were used while testing.

- Document all steps required to reproduce the vulnerability.
- PoC in screenshots.
- Files attempted to upload.

Our side:

When you choose to share your contact information with us, we commit to coordinating with you as openly and quickly as possible.

- If you share contact information, we will acknowledge receipt of your report within 3-4 business days.
- Depending on the length of the report. We will respond with feedback within 14 business days. We will maintain an open dialogue to discuss issues.

Questions

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please contact us at security@honeygain.com before going any further.