

# BUCKVROO

## Responsible Disclosure Policy

Have you discovered a weak spot in a Buckaroo ICT system or website? Report this vulnerability to us as soon as possible via [security@buckaroo.nl](mailto:security@buckaroo.nl) so that we can take appropriate measures.

## **What can you report?**

You can report vulnerabilities in our services. Examples are:

- Cross-Site Scripting (XSS) vulnerabilities.
- SQL injection vulnerabilities.
- Cross-Site request forgery (CSRF)
- Etc.

## **Excluded systems:**

- Matomo.buckaroo.nl
- Servicedesk.buckaroo.nl

## **We ask you:**

- E-mail your findings to [security@buckaroo.nl](mailto:security@buckaroo.nl). Encrypt your findings with our PGP key to prevent the information from falling into the wrong hands.
- Not to abuse the problem or take any action that goes beyond what is necessary to demonstrate the problem. For example, do not download large amounts of data to demonstrate a leak.
- Not to share the vulnerability with others until it has been resolved by us and to delete all confidential data obtained through the vulnerability immediately after the vulnerability has been closed.
- Not to perform attacks on our physical security or third party applications.
- Not to use social engineering methods, DDOS or spam.
- To provide sufficient information to reproduce the problem so that we can resolve it as quickly as possible. This includes information about how and when the vulnerability occurs. Clearly describe how this problem can be reproduced and provide information about the method used and the time of the investigations. More complex vulnerabilities may require more information.
- To communicate with us in a respectful way.

## **What we will do:**

- We will respond to your report within 2 working days with our assessment of the report.
- If you adhere to the above conditions, we will not take any criminal or civil action against you regarding the report.
- We treat the report confidentially and will not share your personal information with third parties without permission unless this is necessary to comply with a legal obligation (for example, a claim from the judicial authorities). You can also report to us anonymously.
- We will fix the vulnerability as soon as possible. Here, too, proportionality plays an important role: the timeframe for resolution depends on various factors, including the severity and complexity of the vulnerability and the systems affected.

**Reward:**

- As a thank you for your help, we can offer a reward for reporting a security issue unknown to us.
- The reward is determined based on the risk of the reported security problem and the quality of the report.
- Buckaroo will not reward any reports if it concerns an already known security problem and / or poses a low risk.
- To be eligible for a reward, the requirements set by the Buckaroo Finance department must be met.
- Bug bounty's from the past are no guarantee for comparable results in the future.

**Public PGP Key:**

[https://www.buckaroo.nl/media/2905/pub\\_key.txt](https://www.buckaroo.nl/media/2905/pub_key.txt)