

# BUCKVROO

## Responsible Disclosure Policy

Heeft u een zwakke plek in een ICT-systeem of website van Buckaroo ontdekt? Meld deze kwetsbaarheid dan zo spoedig mogelijk aan ons via [security@buckaroo.nl](mailto:security@buckaroo.nl) zodat we passende maatregelen kunnen treffen.

## **Wat kun je melden?**

U kunt kwetsbaarheden in onze diensten melden. Voorbeelden zijn:

- Cross-Site Scripting (XSS) kwetsbaarheden.
- SQL injectie kwetsbaarheden.
- Cross-Site request forgery (CSRF)
- Etc.

## **Wij vragen jou:**

- Je bevindingen te mailen naar [security@buckaroo.nl](mailto:security@buckaroo.nl). Versleutel je bevindingen met onze PGP key om te voorkomen dat de informatie in verkeerde handen valt.
- Het probleem niet te misbruiken of handelingen te verrichten die verder gaan dan nodig is om het probleem aan te tonen. Download bijvoorbeeld geen grote hoeveelheden data om een lek aan te tonen.
- De kwetsbaarheid niet met anderen te delen totdat het door ons is opgelost en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het lek te wissen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, DDOS, spam of applicaties van derden.
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Geef informatie over hoe en wanneer de kwetsbaarheid zich voordoet. Beschrijf duidelijk hoe dit probleem gereproduceerd kan worden en geef informatie over de gebruikte methode en het tijdstip van onderzoeken. Bij complexere kwetsbaarheden kan meer informatie nodig zijn.

## **Wat wij zullen doen:**

- Wij reageren binnen 2 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Als je je aan bovenstaande voorwaarden houdt zullen wij geen strafrechtelijke of civielrechtelijke stappen tegen je ondernemen betreffende de melding.
- Wij behandelen de melding vertrouwelijk en zullen jouw persoonlijke gegevens niet zonder toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen (bijvoorbeeld een vordering van justitie. Het staat je ook vrij om de melding anoniem te doen.
- We lossen de kwetsbaarheid zo snel mogelijk op. Ook hier speelt proportionaliteit een belangrijke rol: de termijn voor het oplossen is afhankelijk van verschillende factoren, waaronder de ernst en complexiteit van de kwetsbaarheid en de getroffen systemen.

## **Beloning:**

- Als dank voor uw hulp kunnen wij een beloning aanbieden voor een melding van een ons nog onbekend beveiligingsprobleem.
- De beloning wordt vastgesteld op basis van het risico van het gemelde beveiligingsprobleem en de kwaliteit van de melding.

- Indien de melding een reeds bekend beveiligingsprobleem betreft en/of een laag risico vormt kan het zijn dat er geen beloning wordt toegekend.
- Toegekende beloningen uit het verleden bieden geen garantie voor vergelijkbare resultaten in de toekomst.