Richtlijn ethisch hacken

Wat verwacht Thor van een hacker?

1. **Ethisch handelen.** Er wordt van uit gegaan dat de hacker de vereniging wil verbeteren door fouten bloot te leggen, dus er zal in ieder geval geen onomkeerbare schade worden toegebracht. Dit betekent onder andere: de hacker zal in ieder geval niet, tenzij met goedkeuring van de ExpertCommissie:
    a. Eventueel verkregen data na afhandeling bewaren
    b. Onomkeerbare veranderingen aanbrengen aan data en/of systemen
    c. Bevindingen en/of toegang delen met derden
    d. Relevante informatie achterhouden

2. **Snelle, duidelijke melding.** Na een succesvolle hack moet binnen 24 uur de ExpertCommissie (expertcommissie@thor.edu) ingelicht zijn. Mocht het financiën betreffen, zal de ExpertCommissie ook de KasCo inlichten. Onder inlichten verstaan we het volgende:
    a. Binnen 24 uur een beknopt stappenplan om de hack volledig mee te reproduceren, inclusief opsomming waar toegang tot verkregen is.
    b. Binnen een week een gedetailleerd rapport, dit bevat:
        i. Gedetailleerd stappenplan om de hack mee te reproduceren
        ii. Ruwe beschrijving hoe het gevonden is
        iii. Opsomming waar toegang tot verkregen is
        iv. Eventueel een suggestie voor een oplossing

3. **Discretie.**
    a. De hacker houdt alle informatie voor zich totdat de Expertcommissie in samenspraak met de CoCo en indien relevant de KasCo heeft besloten dat kennis over de hack gedeeld mag worden.
    b. Verkregen informatie wordt niet gedeeld met derden.
    c. Na afhandeling van de hack door de ExpertCommissie wordt de eventueel verkregen data en/of informatie verwijderd. Het gedetailleerd rapport mag hierna wel bewaard en gedeeld worden mits deze geen gevoelige informatie bevat.

Wat mag een hacker in dat geval van Thor verwachten?

1. **Beloning.** De Expertcommissie besluit in overleg met de CoCo en eventueel de KasCo over de omvang van beloning.
2. **Nette, professionele behandeling.** De ExpertCommissie zal de hacker ondersteunen in het informeren van de vereniging over de hack.
3. **Tijdige afhandeling.** Na melding van de hack zal de ExpertCommissie er op toezien dat binnen 3 weken de hele hack afgehandeld is en de hierbij gevonden fouten waar mogelijk opgelost zijn door de verantwoordelijke commissie.
4. **Discretie.** Mocht het zo zijn dat de hacker zichzelf niet kenbaar wenst te maken, zal de ExpertCommissie er op toezien dat de identiteit van de hacker alleen bekend zal zijn bij personen waarbij dit strikt noodzakelijk is. Denk hierbij aan de CoCo die met genoemde persoon moet kunnen overleggen.

Wat verstaan we onder een hack?

Onder een hack wordt in ieder geval verstaan een actie die aan één of meer van de volgende criteria voldoet:

a. Toegang verschaffen tot digitale data en/of systemen buiten de daarvoor bestemde wegen.
b. Beschikbaarheid van digitale data en/of systemen beïnvloeden buiten de daarvoor bestemde manieren.

Dit document betreft een richtlijn voor de besluitvorming van de ExpertCommissie. De Expertcommissie kan hiervan afwijken.

Beloning ethisch hacken

De bugs zijn volgens dit systeem in vier gradaties verdeeld, dit om de impact van de grotere bugs te benadrukken en dit dan ook te belonen met meer strepen geldig in Het Walhalla en tegelijkertijd ook het vinden van meerdere kleine bugs te belonen.

Onbelangrijke data is data die in principe bij alle Thorleden en externen bekend mag zijn, denk hierbij aan de quotes, memes, of bijvoorbeeld foto's van Thor.
Belangrijke data is data die bekend zou moeten zijn bij slechts een selecte groep mensen, denk hierbij aan alle financiële data, persoonsgegevens, wachtwoorden, en data van het Bestuur.

Personen uit commissies die (gedeeltelijke) verantwoordelijkheid hebben voor digitale systemen binnen Thor, waaronder het Bestuur, de CoCo, de ExpertCommissie, de WebCo en de LANCo, worden uitgesloten van onderstaande beloningen. Mocht daar onenigheid over zijn, dan besluit de ExpertCommissie.

1. Kleine bugs, 4 strepen
   - Toegang tot onbelangrijke data
   - Debug output van individuele commando's kunnen opvragen
   - Significante visuele bugs
2. Middelgrote bugs, 16 strepen
   - Kunnen inloggen als willekeurige mensen, exclusief beheerders
   - Access en/of debug logs van een volledige site, server of container bemachtigen
   - Onbelangrijke data kunnen wijzigen en/of verwijderen
   - Inzage in belangrijke data
3. Grote bugs, 32 strepen
   - Beheerders rechten op een virtual machine, Linux-containers of de hoofdwebsite thor.edu verkrijgen
   - Belangrijke data kunnen wijzigen en/of verwijderen
   - Zelf gekozen programmacode kunnen uitvoeren binnen een virtuele machine (RCE)
4. Epische bugs, 256 strepen
   - Volledige overname van de systemen of root op de hypervisor verkrijgen. Hierbij geldt de helft van de beloning voor usermode hacks.
     Eventuele manieren:
     - Uit een container of virtual machine breken
     - CoCo SSH private keys verkrijgen
     - Black magic, gelieve uit te leggen

Bovenstaande beloningen zijn een richtlijn en de ExpertCommissie zal de uiteindelijke beloning vaststellen, daarbij in acht nemend de maximale vergoeding die Thor volgens de wet mag geven aan één persoon.