

# HAAVOITTUVUUSPALKINTO-OHJELMAN SÄÄNNÖT JA EHDOT

Hackrfi Oy järjestää Suomessa haavoittuvuuspalkinto-ohjelmia. Tässä ohjelmassa tarkoituksena on palkita Suomen kansalaisia tai Suomessa vakituisesti asuvia henkilöitä, jotka raportoivat liiketoiminnan kannalta kriittisistä tietoturvaluushaavoittuvuuksista Hackrfi Oy:n Hackr.fi -palvelussa. Maailmalla vastaavat ohjelmat tunnetaan yleisesti nimellä Bug Bounty.

Näitä sääntöjä ja ehtoja sovelletaan Hackrfi Oy:n omaan haavoittuvuuspalkinto-ohjelmaan, muiden haavoittuvuuspalkinto-ohjelmien säännöt voivat poiketa tässä esitetystä.

Epäselvyyksien ja turhan työn välttämiseksi suosittelemme, että luet huolella seuraavan ohjeistuksen ennen ohjelmaan osallistumista.

## OHJELMASTAMME YLEISESTI

Haluamme tietää kaikista mahdollisista tietoturvaluushaavoittuvuuksista palvelusivullamme.

Kannustaaksemme tietoturvaluusongelmien löytämiseen ja julkaisemiseen vastuullisella tavalla tarjoamme tuotepalkkioita hyväksytyistä tietoturvaluushaavoittuvuuksista, jotka raportoidaan meille Hackrfi-palvelun kautta.

Tietoturvaluushaavoittuvuudeksi luokitellaan tapahtuma, joka yleisen termistön mukaisesti aiheuttaa häiriön tiedon tai palvelun luottamuksellisuudelle, eheydelle tai saatavuudelle. Ohjelman erityisenä tarkastelukohteena on Suomen henkilötietolainsäädännön noudattaminen. Mikä tahansa ohjelman piirissä havaittu Suomen henkilötietolainsäädäntöä rikkova toiminta luetaan tietoturvaluushaavoittuvuudeksi. Lisäksi kiinnitämme huomiota liiketoimintapalveluamme kriittisesti haittaaviin haavoittuvuuksiin.

Tässä dokumentissa annettuja sääntöjä on noudatettava, jotta haavoittuvuuspalkinto-ohjelmaan osallistuminen ja siihen liittyvän tietoturvaluustutkimuksen suorittaminen ei aiheuta ennalta arvaamattomia tietoturvariskejä Hackrfi Oy:n asiakkaille, asiakastiedoille tai liiketoiminnalle.

## OHJELMAN LAAJUUS

Hackrfi Oy:n haavoittuvuuspalkinto-ohjelmaan kuuluu tällä hetkellä Hackr.fi -palvelusivusto. Palvelusivusto löytyy Internet-osoitteesta [www.hackr.fi](http://www.hackr.fi).

## PERIAATTEELLISET RAJAUKSET

Haluamme, että ohjelmaan osallistuessasi sitoudut seuraaviin periaatteisiin:

- Lain kunnioitus: Tietoturvatutkimuksessa on noudatettava Suomen lakia ja näitä sääntöjä.
- Riippumattomuus: Haavoittuvuuspalkinto-ohjelmaan osallistuja ei saa olla Hackrfi Oy:n tai sen yhteistyökumppanin palveluksessa.
- Tutkijan oma toiminta: Tietoturvallisuustutkimus on suoritettava tutkijan itse omistamalta ja ylläpitämältä laitteelta tai laitteilta.
- Vahingon rajoittaminen: Tietoturvatutkimuksessa ei saa käyttää haitallista tai häiriötä aiheuttavaa kuormaa tai syötettä sen enempää kuin mitä teknisen tietoturvallisuushaavoittuvuuden olemassaolon todentaminen edellyttää.
- Liiketoiminnan salliminen: Tietoturvallisuustutkimuksen suorittaminen ei saa merkittävällä tavalla vaikuttaa ohjelman kohteena olevan palvelun saatavuuteen.
- Salassapito: Jos löydät haavoittuvuuden, jonka vuoksi saat näkyville sellaista tietoa, joka ei olisi ilman haavoittuvuutta nähtävissäsi, pidät tällä tavoin saamasi tiedot salassa etkä välitä tai ilmaise niitä kolmansille osapuolille.

Epäselvissä tilanteissa pyydämme olemaan meihin yhteydessä osoitteen [www.hackr.fi](http://www.hackr.fi) kautta ennen kuin osallistut ohjelmaan.

## KIELLETYT TOIMET JA MENETELMÄT

Seuraavien toimien suorittaminen johtaa haavoittuvuuspalkinto-ohjelmaan osallistumisen hylkäykseen sekä mahdollisesti viranomaistoimiin toimien luonteesta riippuen:

- "Brute-force" –menetelmän käyttäminen.
- Koodi-injektiot taustajärjestelmiin (esimerkiksi SQL-injektio).
- "DoS"- (Denial of Service) eli palvelunestohyökkäykset.
- Haavoittuvuusskannaukset tai automaattiset skannaukset Hackrfi Oy:n tai sen toimittajien palvelimiin, kaupallisilla tai avoimeen lähdekoodiin perustuvilla skannereilla; ethän siis käytä esimerkiksi Nessus-skanneria.
- Nk. social engineering ei kuulu ohjelman piiriin.

## HAAVOITTUVUUDEN RAPORTOINTI

Havaittu haavoittuvuus on ilmoitettava osoitteessa [www.hackr.fi](http://www.hackr.fi) olevan ohjelasivun oman raportointilomakkeen kautta. Noudatathan sivustolla annettua ohjeistusta.

Olemme sinuun yhteydessä kolmen (3) arkipäivän sisällä ilmoituksen jättämisestä ohjelasivun kautta. Jos et kuitenkaan saa vastausta, olethan meihin yhteydessä uudestaan.

## RAPORTIN SISÄLTÖ

Pyydämme sinua ilmoittamaan vähintään seuraavat asiat:

- Mistä kohdasta löysit haavoittuvuuden (palvelin, URL, toiminto tms. yksilöivä tunniste).
- Miten tarkalleen ottaen haavoittuvuuden löysit ja miten sen voi toistaa tai todentaa (esimerkiksi, jos haavoittuvuus liittyy tiettyyn verkko-osoitteen parametriin, ilmoita kaikki mahdolliset tiedot yksityiskohtineen).
- Minkä tyyppinen haavoittuvuus on eli mitä mielestäsi haavoittuvuuden kautta voi tapahtua tai saada aikaiseksi.

Raportissa ilmoitettu haavoittuvuus pitää pystyä todentamaan. Jos emme voi todentaa ilmoitusta toistamalla sitä, emme voi myöskään palkita ko. havainnosta.

Internetselaimen toimintaan liittyvät tietoturvasuushaavoittuvuudet on pystyttävä toistamaan HTML5-yhteensopivalla Internet-selaimella.

## MUUTA HUOMIOITAVAA

Jos lähetät meille haavoittuvuusraportin, sinua koskee julkaisukielto raportin sisältämään haavoittuvuuteen. Palkkiota ei siis makseta, jos jokin kolmas osapuoli saa tiedon ilmoittamastasi haavoittuvuudesta.

Halutessasi voimme julkistaa nimesi tai nimimerkkisi.

Jos ilmoitettu haavoittuvuus ei tulkintamme mukaan muodosta riskiä tai ei ole tietoturvasuushaavoittuvuus, pidätämme oikeuden olla palkitseematta ko. havainnosta.

Jos useampi henkilö raportoi saman haavoittuvuuden, lähtökohtaisesti vain ensimmäinen ilmoittaja saa palkinnon. Myöhemmille ilmoittajille kerrotaan että haavoittuvuus on jo käsitelty.

## PALKINNOT

Tässä ohjelmassa palkinnot ovat tavarapalkkioita.

Viranomaisvaatimuksista johtuen asioimme aina vain alkuperäisen raportoijan kanssa. Noudatathan siis ilmoituksen jälkeen saamiasi ohjeita.

## OIKEUDELLISET LISÄVAATIMUKSET

Raportoimalla haavoittuvuudesta Hackrfi Oy:lle myönnät Hackrfi Oy:lle kaikki oikeudet raportin sisältämiin tietoihin ja niiden hyödyntämiseen löydöksen korjaamiseksi.

Hackrfi Oy:llä on oikeus keskeyttää tai sulkea tämä haavoittuvuuspalkinto-ohjelma milloin tahansa. Hackrfi Oy:llä on oikeus muuttaa tämän haavoittuvuuspalkinto-ohjelman ehtoja, myös ilman erillistä ilmoitusta.