HAAVOITTUVUUSPALKINTO-OHJELMAN SÄÄNNÖT JA EHDOT

Tässä ohjelmassa tarkoituksena on palkita löydetyistä ja raportoiduista tietoturvallisuushaavoittuvuuksista Bonusway'n ohjelman kohteena olevista komponenteista (katso tarkemmin kohdasta "Ohjelman laajuus"). Hackrfi Oy toimii haavoittuvuuspalkkio-ohjelman koordinaattorina.

Tässä dokumentissa olevia sääntöjä ja ehtoja sovelletaan Bonusway Bug Bounty -haavoittuvuuspalkinto-ohjelmaan. Epäselvyyksien ja turhan työn välttämiseksi suosittelemme, että tutustut tähän ohjeistukseen huolellisesti ennen ohjelmaan osallistumista.

Bonusway on Helsingissä 2011 perustettu kasvuyritys. Bonusway on verkkopalvelu, jonka avulla käyttäjät voivat kerätä ostohyvitystä (engl. cashback) verkko-ostoksista. Tavallinen käyttäjä voi säästää vuodessa jopa satoja euroja tekemällä verkko-ostoksensa palvelumme kautta.

Bonusway'llä on toimintaa 14 maassa ja se on markkinajohtaja Pohjois- ja Itä-Euroopassa. Maailmanlaajuisesti Bonusway'llä on 3,8 miljoonalla asiakasta ja 3500 verkkokauppakuppania.

Esimerkkejä Bonusway'n sivuista ovat: https://www.bonusway.fi, https://www.bonusway.se, https://www.artiway.com.tr, https://www.kopikot.ru.

Haavoittuvuuspalkinto-ohjelma on perustettu, jotta voisimme löytää vakavia virheitä suhteessa meidän tuotelupaukseemme.

OHJELMASTAMME YLEISESTI

Kannustaaksemme tietoturvallisuusongelmien löytämiseen ja julkaisemiseen vastuullisella ja läpinäkyvällä tavalla tarjoamme palkintoja hyväksytyistä tietoturvallisuus-haavoittuvuuksista, jotka raportoidaan meille Hackrfi-palvelun kautta. Tietoturvallisuushaavoittuvuudeksi luokitellaan tapahtuma, joka yleisen termistön mukaisesti aiheuttaa häiriön tiedon tai palvelun luottamuksellisuudelle, eheydelle tai saatavuudelle.

Tässä dokumentissa annettuja sääntöjä on noudatettava, jotta haavoittuvuuspalkinto-ohjelmaan osallistuminen ja siihen liittyvän tietoturvallisuustutkimuksen suorittaminen ei aiheuta ennalta arvaamattomia tietoturvariskejä Bonusway'n asiakkaille, asiakastiedoille tai liiketoiminnalle.

OHJELMAN LAAJUUS

Ohjelmaan kuuluvat Bonusway'n seuraavat komponentit:

Verkkosivusto Bonusway Suomi, sen mobiiliapplikaatiot, kaikki APIt ja verkkopalvelut.

- https://www.bonusway.fi/
- https://itunes.apple.com/fi/app/bonusway-suomi/id1097718776 (itse sovellus)
- https://play.google.com/store/apps/details?id=com.bonusway.finland (itse sovellus)

Jos haavoittuvuus löytyy kolmannen osapuolen palvelusta, se ei kuulu ohjelmaan.

Bonusway –selainlaajennus ja sen käyttämät APIt eivät kuulu ohjelmaan.

Ohjelmaan eivät kuulu kolmansien osapuolien virheet tai ongelmat kuten varusohjelmistojen virheet, operaattorien virheet tai tietoliikenneongelmat eivätkä myöskään päätelaitteissa olevat virheet, tietokoneen tai mobiililaitteen suojauksessa olevat virheet tai haittaohjelmista aiheutuvat välilliset virheet tai muut vastaavat. Laitteen ID/token data ja MFA eivät kuulu ohjelmaan.

PERIAATTEELLISET RAJAUKSET

Arvostamme sitä, että saamme toimia raportoijien kanssa yhteistyössä Bonusway-alustan tietoturvallisuuden parantamiseksi. Seuraavassa lyhyesti periaatteita, joilla ohjelmassa tulee toimia:

- **Lain kunnioitus**: Tietoturvatutkimuksessa on noudatettava oman maasi lakeja sekä näitä sääntöjä.
- **Riippumattomuus**: Haavoittuvuuspalkinto-ohjelmaan osallistuja ei saa olla Bonusway'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 löytyy haavoittuvuus, jonka vuoksi saadaan näkyville sellaista tietoa, joka ei olisi ilman haavoittuvuutta mahdollista, on raportoijan pidettävä tällä tavoin saamansa tiedot salassa välittämättä tai ilmaisematta niitä kolmansille osapuolille.

Epäselvissä tilanteissa pyydämme olemaan yhteydessä palkinto-ohjelman koordinaattoriin Hackrfi Oy:öön osoitteen www.hackr.fi kautta ennen ohjelmaan osallistumista.

Kunnioitamme raportoijan tähän käyttämää aikaa, ja toivomme siksi myös raportoijan kunnioittavan meidän palvelu-, vaste- ja korjausaikojamme.

KIELLETYT TOIMET JA MENETELMÄT

Jos käy ilmi, että jokin seuraavista toimista on ollut käytössä tietoturvatutkimustyössä, se johtaa hylkäämiseen palkinto-ohjelmasta ja mahdollisesti rikosoikeudelliseen vastuuseen. Emme salli mitään seuraavista toimista jotka voivat vaikuttaa häiritsevästi tarjoamiemme palvelujen saatavuuteen ja Bonusway'n asiakkaisiin, mukaan lukien

- Koodi-injektiot taustajärjestelmiin (esimerkiksi SQL-injektio) siten että järjestelmässä tai taustajärjestelmässä olevia tietoja muutetaan tai poistetaan tai luetaan tarpeettomassa laajuudessa. Koodi-injektio sinänsä ei ole kielletty, rajoitus on vain PoC-koodin toiminnallisuuden tyyppiin ja laajuuteen.
- Palvelunestohyökkäykset ("DoS"- Denial of Service) - tämä koskettaa myös automaattisia skannereita ja muita työkaluja, joiden käytöstä saattaa syntyä palveluestohyökkäyksen kaltaista kuormaa.
- Social engineering ja MitM-hyökkäykset (man-in-the-middle) eivät kuulu ohjelman tietoturvatutkimuksen piiriin.
- Liiketoimintaa haittaavat (tai suurella todennäköisyydellä haittaavat) toimet tulee jättää suorittamatta tämän ohjelman piirissä oleviin tai sen ulkopuolella oleviin järjestelmiin.
- Yksilön turvallisuuden uhkaaminen.

HAAVOITTUVUUDEN RAPORTOINTI

Tietoturvahaavoittuvuus on raportoitava osoitteen www.hackr.fi olevan ohjelmasivun oman raportointilomakkeen kautta. Raportoitaessa on huomattava seuraavaa:

- Raportoijan on jaettava kaikki mahdollinen tieto ja yksityiskohdat, jotta haavoittuvuus voidaan todentaa. Jos havaintoa ei voida toistaa, ei myöskään palkkiota voida tarjota. Tietoa ei saa jättää pois raportista mahdollista myöhempää raporttien tai havaintojen ketjuttamista varten.
- Pyrimme olemaan raportoijaan yhteydessä keskimäärin 3 työpäivän kuluessa havainnosta kertoaksemme raportin käsittelyn etenemisestä.
- Pyrimme vahvistamaan raportin oikeellisuuden keskimäärin 14 työpäivän sisällä. Pyydämme kuitenkin huomioimaan, että raportista riippuen sen vahvistaminen saattaa kestää tätä pitempään. Vahvistamiseen kuluva aika riippuu myös raportin kattavuudesta sekä havainnon toistamisen helppoudesta.
- Tutkimustyö ei saa uhata tai vaarantaa muita palvelun käyttäjiä - tarvittaessa annetaan raportoijalle lisää tunnuksia käyttöön.
- Jos raportoijalla on epäilys, että seuraava askel tutkimuksessa aiheuttaa palveluun häiriöitä, voidaan raportti toimittaa keskeneräisenä ja hakea meiltä lupa tutkimusten

jatkamiseen.
- Liitteet ja liitetiedostot pyydämme tarvittaessa erikseen vastaanotettuamme raportin.

Muuhun kuin tietoturvaan tai tietosuojaan liittyvät raportit tai asiakaspalveluyhteydenotot, jotka lähetetään tämän osoitteen kautta, jätetään huomiotta. Jos teillä on muuhun kuin tietoturvaan liittyvä kysymys, pyydämme teitä ystävällisesti olemaan yhteydessä Hackrfi Oy:n asiakaspalveluun osoitteessa www.hackr.fi.

RAPORTIN SISÄLTÖ

Raportoijalle on tarjolla tähän ohjelmaan soveltuvat raportointipohjat. Niiden käyttö on vapaaehtoista, mutta suotavaa.

Raportissa ilmoitettu haavoittuvuus pitää pystyä todentamaan. Jos emme voi todentaa ilmoitusta toistamalla sitä, emme voi myöskään palkita ko. havainnosta. Internet-selaimen toimintaan liittyvät haavoittuvuudet on pystyttävä toistamaan modernilla (HTML5-yhteensopivalla) Internet-selaimella.

Koska ohjelma keskittyy mobiilisovellusten ja -rajapintojen tietoturvaa, seuraavista asioista lähetettyjä raportteja emme välttämättä hyväksy osaksi ohjelmaa:

- Automaattiskannereiden (useasti erittäin spekulatiiviset ja epätarkat) tulokset
- Sähköpostipalvelimiin liittyviä konfiguraatioita (SPF, DMARC, ...)
- SSL/TLS konfiguraatioiden parhaita käytäntöjä tai niiden puutteita (ellei havaintoon liity selkeästi hyväksikäytettävissä olevaa uhkaa tai heikkoutta)
- SSL/TLS konfiguraatioihin liittyviä yksittäisiä CVE-havaintoja tai havaintoja jotka on löydettävissä SSLabs-skannerilla (tai vastaavalla)
- HTTP security headereihin liittyviä parhaita käytäntöjä tai niiden puutteita
- Lomakkeita, joissa on teoreettinen CSRF-haavoittuvuus (ilman toimivaa PoCia joissa osoitetaan uhka ja sen toteuttaminen)
- Logout CSRF -havaintoja
- Salasanapolitiikkoihin tai salasanojen vahvuuteen liittyviä havaintoja
- Web-sisällön injektointia (engl. content spoofing / text injection)
- Palvelun teknisestä alustasta vuotavia versionumero yms. tietoja, joihin ei liity selkeästi osoitettavissa ja hyväksikäytettävissä olevaa uhkaa tai heikkoutta.
- Havaintoja, jotka liittyvät iTunesiin ja PlayStoreen, tai muihin kolmannen osapuolen palveluihin/sovelluksiin, jotka liittyvä mahdollisesti ohjelman kohteena olevan palvelun/sovelluksen hallinnointiin.
- Evästekonfiguraatioihin liittyviä havaintoja
- Virhesivukonfiguraatioihin liittyviä havaintoja
- XSS johon ei liity mitään osoitettua uhkaa tai heikkoutta
- Havaintoja puutteista, haavoittuvuuksista tai ongelmista, jotka eivät ole suoranaisesti Bonusway'n vaikutuksen alaisia

MUUTA HUOMIOITAVAA

Lähettäessään raportin raportoija sitoutuu olemaan julkaisematta raportin sisältämää haavoittuvuutta. Palkkiota ei makseta, jos jokin kolmas osapuoli saa tiedon raportoidusta haavoittuvuudesta.

Raportoijan niin halutessa voimme julkistaa hänen nimensä tai nimimerkkinsä mahdollisella kiitos-sivulla tai top-listauksessa.

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

PALKINNOT

Ohjelman suurin palkinto on 5.000€ ja pienin palkinto on 50€. Palkinnot maksetaan työkorvauksena.

Suurimman palkkion saaminen edellyttää esim. loppukäyttäjän yksityisen avaimen ("private key") saaminen haltuun tai käyttäjän sähköpostin haltuunotto. Palkkion saaminen edellyttää hyvää näyttöä ja hyvin dokumentoidun PoCin siitä, miten käyttäjän sähköposti puretaan tai avain varastetaan.

Palkinnon suuruuden määrittelee Bonusway. Palkkioiden määrittelyyn käytetään riski- ja impaktipohjaista arviointia. Havainnot arvioidaan pääasiallisesti haavoittuvuuden mahdollisen seurauksen näkökulmasta. Jos raportoitu haavoittuvuus ei tulkintamme mukaan muodosta riskiä tai ei ole tietoturvallisuushaavoittuvuus, pidätämme oikeuden olla palkitsematta ko. havainnosta.

Pyrimme olemaan perusteluissamme avoimia ja läpinäkyviä ja perustelemalla päätöksiämme raportoijalle. Jos yhdestä bugista on monta ilmentymää, esim bugi jaetussa kirjastossa, voidaan raportit ja palkkiot yhdistää. Yleisesti käytössä olevista ja julkisesti saatavilla olevista kirjastoista löytyneistä haavoittuvuuksista saatamme maksaa normaalia pienemmän korvauksen.

Jos raportoitte meille useita havaintoja, jotka ovat saman tietoturvahaavoittuvuuden ilmentymiä useammassa palvelussa (esimerkiksi samassa koodissa, jota suoritetaan eri alustoilla), tai tietoturvahaavoittuvuus on osa laajempaa ongelmaa, kaikki nämä havainnot saatetaan palkitsemismielessä yhdistää.

Viranomaisvaatimuksista johtuen asioimme vain ja ainoastaan alkuperäisen raportoijan kanssa.

OIKEUDELLISET LISÄVAATIMUKSET

Bonusway sekä Hackrfi Oy pidättävät oikeuden lopettaa tämän palkinto-ohjelman hetkellä millä hyvänsä sekä muuttaa sen ehtoja ilman erillistä ilmoitusta. Kaikki palkintomaksupäätökset ovat lopullisia. Tämän palkinto-ohjelman säännöt tai mikään palkinto-ohjelmaan liittyvä kommunikaatio eivät tuota Hackrfi Oy:lle minkäänlaisia velvoitteita.

Ilmoittamalla Hackrfi Oy:lle tietoturvahaavoittuvuudesta myönnätte Hackrfi Oy:lle ja Bonuswaylle ikuisen, maailmanlaajuisen, royalty-vapaan, peruuttamattoman ei-eksklusiivisen lisenssin ja oikeuden käyttää, muuttaa ja integroida raportin sisältämiä tietoja Hackrfi Oy:n ja Bonusway'n palveluihin, tuotteisiin ja testijärjestelmiin. Hackrfi Oy:llä tai Bonusway'llä ei ole palkinto-ohjelmaan liittyviä velvoitteita raportin tekijälle.