HACKTROPHY BUG BOUNTY PROJEKTY
PODMIENKY PRE ETICKÉHO HACKERA

Vitaj v Hacktrophy Bug Bounty Programe (ďalej len "**Program**"). Tento Program podporuje a odmieňa príspevky (oznámenie kvalifikovaných zraniteľností ako sú tieto opísané v Pravidlách projektov a týchto podmienkach) etických hackerov (ďalej len "**Etický hacker**"), ktorý pomáhajú, aby bol internet bezpečnejší. Prostredníctvom tohto Programu Hacktrophy poskytuje peňažné odmeny a prípadne verejné uznanie za bezpečnostné zraniteľnosti zodpovedne odhalené Etickými hackermi za nasledovných podmienok.

Ak ste v našom Programe nový, prosím preštudujte si tieto Podmienky pre Etického hackera a Pravidlá projektov, aby ste sa dozvedeli ako vstúpiť do Programu, predložiť oznámenia o zraniteľnosti a získať za to odmeny.

Popis Programu

Za podmienky, že Etický hacker súhlasil s týmito podmienkami, Hacktrophy umožní Etickému hackerovi vstúpiť do Programu a spojiť sa zo Zákazníkmi predkladaním oznámení o kvalifikovaných zraniteľnostiach podľa týchto podmienok. Zákazníci využívajúci Program vytvárajú Projekty, v ktorých ponúkajú odmeny za oznámenie kvalifikovaných zraniteľností Etickými hackermi podľa týchto podmienok (ďalej len "**Projekt**"). Etickí hackeri si môžu prostredníctvom Programu prezerať Projekty a predkladať oznámenia o zraniteľnostiach.

Z Programu sú vylúčené:

- **Web stránky tretích strán.** Niektoré služby **Zákazníka** na menej bežných doménach môžu byť prevádzkované obchodníkmi alebo partnermi. Nemôžeme umožniť Etickému hackerovi testovať tieto systémy v mene vlastníka a preto nebudeme odmieňať také oznámenia. Bezpečnostné zraniteľnosti v aplikáciách alebo web stránkach tretích strán (napr. java, plugins).
- **Útoky proti infraštruktúre Zákazníka, ktorá nie je prístupná cez internet, sociálne inžinierstvo a phishingové útoky proti zamestnancom Zákazníka.**
- **Nedávne akvizície.** Keďže pre internú kontrolu a opravy je potrebný čas, novo založené spoločnosti podliehajú šesť mesačnej ochrannej dobe. Zraniteľnosti oznámené skôr sa obvykle nekvalifikujú na odmenu.
- **Denial of service (DoS)** útoky a obdobné metódy, ktoré vyžadujú veľký objem dát a leverage black hat SEO techniky.

Kvalifikované zraniteľnosti

1. Obvykle pôjde o oznámenia zraniteľností s výrazným vplyvom. Avšak odmenená môže byť akákoľvek zraniteľnosť akejkoľvek závažnosti, ktorá môže spôsobiť škodu. Spôsobilé oznámenia budú zahŕňať zraniteľnosti nasledovných typov:

    - Remote Code Execution
    - Vertical Privilege Escalation
    - XML External Entities Injection with significant impact
    - SQL Injection with significant impact
    - LFI/RFI
    - Horizontal Privilege Escalation
    - Stored XSS with significant impact
    - CSRF with significant impact
    - Direct object reference with significant impact
    - Internal SSRF

- Session fixation
- Reflective XSS with impact
- Insecure Deserialization with significant impact
- Direct object reference
- CSRF with impact
- Path Traversal
- DOM XSS
- SSL misconfigurations with little impact
- SPF configuration problems
- XSS with limited impact
- CSRF with limited impact
- SSL/TLS issues (weak crypto, improper setup)
- URL redirect
- Clickjacking

2. V prípade oznámenia zraniteľnosti s možným viacnásobným výskytom je Zákazník oprávnený odmietnuť ďalšie oznámenia takej zraniteľnosti po dobu 30 dní a v tejto lehote takú zraniteľnosť opraviť. Po uplynutí tejto lehoty je Zákazník povinný akceptovať oznámenie, predmetom ktorého je rovnaká zraniteľnosť v prípade, ak ju z vlastnej viny neopravil.

3. Hacktrophy si vyhradzuje právo odmietnuť akékoľvek oznámenie na základe vlastného uváženia a určiť na základe vlastného uváženia, ktoré zraniteľnosti budú považované za kandidátov na odmenu, ako aj konečných prijímateľov odmeny, berúc do úvahy pravidlá stanovené v týchto podmienkach.

Nekvalifikované zraniteľnosti

1. Účelom Programu je odhaliť závažné zraniteľnosti, ktoré majú priamy a preukázateľný vplyv na bezpečnosť našich Zákazníkov. Aj keď našou službou podporujeme akékoľvek oznámenia, ktoré opisujú bezpečnostné zraniteľnosti, dole uvádzame príklady zraniteľností, ktoré nebudú odmeňované:

    - Missing HTTP Security Headers (such as X-FRAME-OPTIONS) or cookie security flags (such as “httponly”)
    - Server-side information disclosure such as IPs, server names and most stack traces
    - Bugs used to enumerate or confirm the existence of users or tenants
    - Bugs requiring unlikely user actions
    - URL Redirects (unless combined with another vulnerability to produce a more severe vulnerability)

2. Hacktrophy si vyhradzuje právo rozhodnúť o odmietnutí akéhokoľvek oznámenia, ktoré, na základe nášho uváženia, spadá do ktorejkoľvek z týchto kategórií zraniteľností, aj keby inak bolo spôsobilé na odmenu, berúc do úvahy pravidlá stanovené v týchto podmienkach.

Ako sa prihlásiť do Programu

Etický hacker sa môže do Programu prihlásiť vyplnením požadovaných údajov v prihlasovacom formulári. Etickému hackerovi bude doručený e-mail potvrdzujúci prihlásenie. Následne, na dokončenie registrácie, bude Etický hacker požiadaný o potvrdenie registračnej e-mailovej adresy v jeho prihlasovacom formulári.

Pri prihlásení sa do Programu odporúčame vyplniť všetky informácie v prihlasovacom formulári vrátane platobných údajov nevyhnutných na úhradu odmeny. V prípade, ak

platobné údaje Etického hackera nebudú vyplnené, Hacktrophy nezodpovedá za to, že odmena nebude z akéhokoľvek dôvodu uhradená.

Po prihlásení získa Etický hacker prístup k zoznamu Projektov zverejnených Zákazníkmi s kategóriami zraniteľností kvalifikovaných na odmeny a výškou odmeny za každú takú oznámenú zraniteľnosť.

Oznamovanie

Vezmite na vedomie, že v prípade, ak v prihlasovacom formulári nie sú vyplnené platobné údaje Etického hackera, Hacktrophy nezodpovedá za to, že odmena nebude z akéhokoľvek dôvodu uhradená.

Etický hacker oznámi zraniteľnosť nájdenú vo vybranom Projekte prostredníctvom formulára tak, že vyplní všetky nevyhnutné podrobnosti a údaje opisujúce zraniteľnosť. V prípade, ak Etický hacker neuvedie vo formulári všetky nevyhnutné údaje z akéhokoľvek dôvodu, oznámenie môže byť považované za nespôsobilé.

Moderátor Hacktrophy posúdi každé oznámenie a ohodnotí jeho spôsobilosť a relevanciu.

Moderátor rozhodne o každom oznámení do 5 dní od jeho predloženia Etickým hackerom.

Rozhodnutia moderátora o oznámení

1. Moderátor akceptuje oznámenie bez výhrad:
   - výška odmeny pre Etického hackera je stanovená na základe podmienok určených vo zverejnenom Projekte a kategórie zraniteľnosti vybranej Etickým hackerom, a potvrdenej moderátorom, ktorý musí definitívne schváliť kategóriu zraniteľnosti (vrátane výšky odmeny).
   - Etický hacker dostane prostredníctvom svojho užívateľského rozhrania informáciu o úhrade odmeny alebo informáciu, že sa očakáva úhrada odmeny pre Etického hackera od Zákazníka (v závislosti od balíka služieb využívaného Zákazníkom), ktorú Hacktrophy následne zaplatí Etickému hackerovi.

2. Moderátor odmietne oznámenie, lebo:
   - oznámenie bolo vyhodnotené ako falošne pozitívne oznámenie;
   - oznámenie je mimo rozsahu Projektu, v takom prípade je moderátor oprávnený určiť osobitnú odmenu v prípade, ak to bolo vopred dohodnuté so Zákazníkom;
   - v prípade, ak bola určená osobitná odmena pre Etického hackera, Etický hacker dostane od Hacktrophy prostredníctvom svojho užívateľského rozhrania informáciu o priznaní nároku na úhradu osobitnej odmeny;

Poznámky:

V prípade, ak Etický hacker oznámi zraniteľnosť iného druhu, t.j. zraniteľnosť, ktorá nie je presne stanovená vo zverejnenom Projekte s výškou odmeny pre takú zraniteľnosť, definitívne o nej rozhodne Zákazník v spolupráci s moderátorom. V takom prípade sa hore uvedený postup aplikuje obdobne.

Zákazník je výlučne zodpovedný za opravu oznámenej zraniteľnosti a konzultuje proces opravy s Etickým hackerom a moderátorom.

Na základe žiadosti Etického hackera môže Zákazník rozhodnúť o odhalení a zverejnení záverečnej správy. Zákazník je oprávnený odhalenie záverečnej správy odmietnuť bez udania dôvodu. Avšak, Zákazník sa zaväzuje rešpektovať, ak si Etický hacker neželá byť odhalený.

Úhrada odmeny

V prípade, ak bolo oznámenie Etického hackera akceptované podľa týchto podmienok, Etický hacker dostane prostredníctvom svojho užívateľského rozhrania informáciu o úhrade odmeny alebo informáciu, že sa očakáva úhrada odmeny pre Etického hackera od Zákazníka (v závislosti od balíka služieb využívaného Zákazníkom), ktorú Hacktrophy následne zaplatí Etickému hackerovi.

Len oznámenia predložené v súlade s týmito podmienkami prihláseným Etickým hackerom v rozsahu podmienok zverejneného Projektu budú považované za platné oznámenie o zraniteľnosti. O akýkoľvek výnimkách musí výslovne a osobitne rozhodnúť Zákazník v spolupráci s moderátorom, ako je uvedené v týchto podmienkach.

Odmena bude Etickému hackerovi uhradená len v prípade, ak Zákazník splnil všetky svoje finančné záväzky voči Hacktrophy. Následne, Hacktrophy zaplatí odmenu Etickému hackerovi.

Etický hacker berie na vedomie, že v prípade, ak má Etický hacker trvalý pobyt v štáte, s ktorým nemá Slovenská republika uzatvorenú medzinárodnú zmluvu o zamedzení dvojitého zdanenia alebo medzinárodnú zmluvu o výmene informácií týkajúcich sa daní alebo v štáte, ktorý nie je zmluvným štátom medzinárodnej zmluvy obsahujúcej ustanovenia o výmene informácií pre daňové účely v obdobnom rozsahu, ktorou je tento štát a Slovenská republika viazaná, môže byť odmena pre Etického hackera znížená o daň vybranú zrážkou vo výške ustanovenej zákonom o dani z príjmov platným a účinným v Slovenskej republike. Etický hacker je povinný túto informáciu poskytnúť Hacktrophy v prihlasovacom formulári pri prihlásení sa do Programu.

Ostatné podmienky

1. Stranami tejto dohody sú Etický hacker a Hacktrophy. Pred vstupom do Programu musí Etický hacker súhlasiť s týmito podmienkami.

2. Etický hacker sa kvalifikuje na odmenu iba ak bol prvou osobou, ktorá upozornila Hacktrophy na dovtedy neznámy bezpečnostný problém.

3. Na odmenu nie je právny nárok. Spôsobilosť na odmeny, určenie ich príjemcov a výška odmeny je ponechaná na zváženie Zákazníka, resp. Hacktrophy.

4. Služby podľa tejto dohody sú poskytované na serveroch a prostredníctvom softvéru, ktoré sa nachádzajú v Slovenskej republike. Vzhľadom na túto skutočnosť je miestom dodania služieb podľa tejto dohody Slovenská republika (členská krajina Európskej únie).

5. Testovanie Etického hackera nesmie porušovať žiadne právne predpisy, alebo narušiť, odhaliť alebo zneužiť akékoľvek údaje alebo prístup k údajom iných osôb. Testovacie aktivity Etického hackera nemôžu mať negatívny vplyv na Hacktrophy, Zákazníka alebo na dostupnosť alebo výkon online prostredia Hacktrophy či Zákazníka. Etický hacker musí dodržiavať právne predpisy pri vykonávaní všetkých činností spojených s testovaním. Miestne zákony môžu ustanoviť ďalšie obmedzenia.

6. Predložením oznámenia o zraniteľnosti Etický hacker potvrdzuje, že nevyzradil a súhlasí, že nevyzradí zraniteľnosť alebo obsah oznámenia komukoľvek inému ako Zákazníkovi alebo Hacktrophy prostredníctvom Programu. Akékoľvek prezradenie bez predchádzajúceho písomného súhlasu Zákazníka alebo Hacktrophy je porušením tejto dohody a spôsobí stratu nároku na odmenu. Strany berú na vedomie a dohodli sa, že finančné odškodné nebude dostatočnou náhradou za akékoľvek porušenie týchto

podmienok Etickým hackerom alebo jeho zástupcom/ami a že Zákazník a/alebo Hacktrophy má nárok na osobitné plnenie ako náhradu za akékoľvek také porušenie, vrátane súdneho príkazu niečo konať či nekonať. Taká náhrada sa nepovažuje za jediný prostriedok náhrady škody za akékoľvek také porušenie, ale len jeden z prostriedkov náhrady škody, ktoré má Zákazník a/alebo Hacktrophy k dispozícii podľa právnych predpisov.

7. Všetci jednotlivci, ktorí boli odmenení, môžu byť následne uvedení na verejnej Hacktrophy stránke, pokiaľ si výslovne neželajú, aby neboli, alebo dostanú inú nepeňažnú odmenu poskytovanú zo strany Hacktrophy.

8. Okrem iných aktivít, ktoré sú protiprávne, sú výslovne zakázané tieto aktivity, ak Zákazník výslovne neurčí inak:

    - Denial of Service testing.
    - Vykonávanie automatizovaných testov, ktoré výrazne zaťažia server.
    - Exploitácia nad rámec jednoduchého konceptu. Napríklad dôkaz, že útočník získal prístup do databázy pomocou sqli je akceptovateľný, avšak následne vykonávanie príkazov na úrovni operačného systému nie je (xp_cmdshell).
    - Využívanie akýchkoľvek údajov, ktoré nie sú vaše akýmkoľvek spôsobom.
    - Vykonávanie phishingových alebo iných útokov sociálneho inžinierstva proti Hacktrophy, zamestnancom Hacktrophy, zmluvných partnerov, zákazníkov alebo akýchkoľvek iných osôb. Rozsah tohto Programu je obmedzený na technické zraniteľnosti.

    V prípade akýchkoľvek pochybností, kontaktujte pred začatím testovania Hacktrophy.

9. Vo všeobecnosti je Etický hacker spôsobilý zúčastniť sa tohto Programu, ak:

    - má 18 a viac rokov. Ak má Etický hacker aspoň 18 rokov, ale je v mieste svojho trvalého pobytu považovaný za maloletého, musí požiadať svojich rodičov alebo zákonných zástupcov o súhlas pred tým ako sa tohto Programu zúčastní; a
    - je buď individuálny etický hacker, ktorý sa zúčastňuje na základe vlastných schopností, alebo pracuje pre organizáciu, ktorá mu účasť umožňuje. Etický hacker zodpovedá za to, že si preštudoval pravidlá svojho zamestnávateľa pre účasť v tomto Programe.

10. Počet kvalifikovaných oznámení jednotlivca, za ktoré možno vyplatiť odmenu nie je obmedzený.

11. V prípade viacnásobných oznámení bezpečnostných zraniteľností od rôznych strán bude odmena udelená prvému oznámeniu.

12. V prípade, ak chcete ostať v anonymite, rešpektujeme Vašu žiadosť, ale musíme poznať Vaše údaje, aby sme Vám mohli zaplatiť. Na úhradu odmeny musíte poskytnúť svoje platobné údaje a iné údaje vyžadované Hacktrophy podľa týchto podmienok.

13. Etický hacker je zodpovedný za všetky súvisiace daňové povinnosti spojené s odmenou, ktorú dostane od Hacktrophy. Hacktrophy môže znížiť akúkoľvek odmenu o sumu dane, ktorú je Etický hacker povinný zaplatiť a ktorú musí odviesť Hacktrophy priamo daňovému alebo inému vládnemu orgánu.

14. Ak sa na tom Hacktrophy a Etický hacker dohodnú a za podmienok stanovených všeobecne záväznými právnymi predpismi platnými v Slovenskej republike, môže byť odmena za oznámenie zraniteľnosti Etickému hackerovi zaplatená aj v niektorej z kryptomien.

15. Etický hacker je zodpovedný za súlad s akýmikoľvek postupmi alebo pravidlami svojho zamestnávateľa, ktoré môžu ovplyvniť jeho spôsobilosť zúčastniť sa na tomto Programe. Ak účasť Etického hackera porušuje pravidlá jeho zamestnávateľa, môže byť vylúčený z účasti na Programe alebo mu nemusí byť vyplatená odmena. Všetky platby budú v súlade s miestnymi zákonmi, predpismi a etickými pravidlami. Hacktrophy nezodpovedá za spory medzi zamestnancom a jeho zamestnávateľom s tým súvisiace.

16. V prípade, ak bolo oznámenie akceptované, prosím, vezmite na vedomie:

    - Etický hacker nemôže určiť inú osobu ako príjemcu odmeny, okrem prípadu, ak je považovaný za maloletého v mieste svojho trvalého pobytu.
    - V prípade, ak Etický hacker nemôže, alebo nechce prijať odmenu, vyhradzujeme si právo zrušiť ju.
    - Etický hacker môže odmenu venovať charite. V takom prípade Etický hacker požiada Hacktrophy o zaplatenie odmeny špecifikovanej charitatívnej organizácii.
    - Etický hacker môže oznámiť zraniteľnosť aj bez uplatnenia nároku na vyplatenie odmeny.
    - Ak Etický hacker akceptuje odmenu, je výlučne zodpovedný za všetky aplikovateľné dane spojené s prijatím platby / platieb.
    - Ak je Etický hacker spôsobilý zúčastniť sa na tomto Programe, ale je považovaný za maloletého v mieste svojho trvalého pobytu, Hacktrophy môže uhradiť odmenu jeho rodičom / zákonným zástupcom na ich účet.

17. Predložením svojho oznámenia, Etický hacker:

    - Zaväzuje sa prezradiť bezpečnostnú zraniteľnosť alebo obsah svojho oznámenia len prostredníctvom Programu a berie na vedomie, že prezradenie zraniteľnosti komukoľvek inému ako Zákazníkovi alebo Hacktrophy (prostredníctvom Programu), akýmkoľvek spôsobom, odplatne, či bezodplatne, bude kvalifikované ako trestný čin so zodpovedajúcimi dôsledkami.
    - Súhlasí, že poskytne Hacktrophy licenciu na všetky práva duševného vlastníctva, ktoré sú obsahom jeho oznámenia, ktorá zahŕňa neodvolateľné, časovo neobmedzené, bezodplatné, celosvetové, nevýhradné právo a licenciu v neobmedzenom rozsahu vrátane práva poskytovať sublicencie (i) využívať, upravovať, ohodnotiť, testovať, a inak analyzovať obsah jeho oznámenia; reprodukovať, modifikovať, distribuovať, zobrazovať a vykonávať verejne, a obchodovať a vytvoriť odvodené diela z obsahu jeho oznámenia a všetkých jeho častí, v celku alebo čiastočne, v súvislosti s týmto Programom; a (ii) uvádzať obsah jeho oznámenia a všetky jeho časti v spojení s marketingom, predajom, alebo propagáciou tohto Programu (vrátane ale nielen pokiaľ ide o interné alebo externé obchodné rokovania, prezentácie na konferenciách, veľtrhoch a screen shoty oznámení v mediálnych výstupoch) vo všetkých médiách (známych alebo neskôr vyvinutých).
    - Rozumie a berie na vedomie, že Hacktrophy mohla vyvinúť alebo si objednala tvorbu podobného alebo rovnakého materiálu ako je jeho oznámenie, a vzdáva sa všetkých nárokov, ktoré by mohli vyplývať zo zameniteľnosti s obsahom jeho oznámenia.
    - Rozumie, že má nárok na jednorazovú platbu za každú spôsobilú zraniteľnosť a nemá garantovanú žiadnu dodatočnú náhradu alebo plnenie za využitie obsahu jeho oznámenia.
    - Berie na vedomie jeho zákonnú povinnosť spolupracovať s vyšetrovacími orgánmi a inými orgánmi činnými v trestnom konaní v súlade s platnými právnymi predpismi.

18. Tento Program pochádza zo Slovenskej republiky a oznámenia sú zbierané na počítačoch v Slovenskej republike. Tento Program sa spravuje právnym poriadkom Slovenskej republiky (vrátane priamo aplikovateľných aktov Európskej únie) a Zákazník súhlasí s

výlučnou právomocou a príslušnosťou súdov v Slovenskej republike pre všetky spory, ktoré vzniknú v súvislosti s týmto Programom.

19. Všetky rozhodnutia Hacktrophy v rámci tohto Programu sú konečné a záväzné. Hacktrophy môže zmeniť alebo zrušiť Program kedykoľvek, z akéhokoľvek dôvodu.

20. Hacktrophy vám ďakuje za účasť.

    Šťastný lov!