PRAVIDLÁ PRE HACKTROPHY BUG BOUNTY PROJEKTY

Uvedomujúc si zvýšenú úroveň ochrany vyžadovanej našimi zákazníkmi, ponúkame spôsob ako zapojiť do tohto procesu internetovú komunitu etických hackerov. Táto komunita pozostáva z vysoko kvalifikovaných expertov, ktorých by sme radi prizvali k spolupráci a využívali ich schopnosti prostredníctvom programu odmeňovania zraniteľností. Tento Hacktrophy bug bounty program (ďalej len „**Program**“) je vyvinutý a prevádzkovaný bezpečnostnou spoločnosťou Hacktrophy, ktorá garantuje kvalifikovaný manažment Programu. Tieto inštrukcie môžu pomôcť tým, ktorí by chceli pomôcť urobiť internet bezpečnejším miestom.

Popis programu

Tento Program podporuje a odmieňa príspevky (oznámenia kvalifikovaných zraniteľností ako sú tieto opísané v týchto pravidlách) etických hackerov (ďalej len „**Etický hacker**“). Hacktrophy umožní Zákazníkovi (ďalej len „Zákazník“) vstúpiť do Programu a spojiť sa s Etickými hackermi.

Typy Programu, ktoré Hacktrophy ponúka sú špecifikované v Podmienkach pre Zákazníka.

Služby v rozsahu Programu

Akákoľvek webová služba alebo aplikácia, ktorá je vlastníctvom Zákazníka a ktorá obsahuje dôvodne citlivé údaje, vrátane bezpečnostných zraniteľností v API a iných služieb prístupných cez internet.

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 odmeňovať také oznámenia. Bezpečnostné zraniteľnosti v aplikáciách alebo weboch 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.

Pamätajte, ak máte pochybnosti, najprv nás kontaktujte.

Kvalifikované zraniteľnosti

Bezpečnostná zraniteľnosť je chyba, vada, omyl, porucha alebo kaz v počítačovom programe, systéme alebo v infraštruktúre, ktorá vplýva na bezpečnosť zariadenia, systému, siete, alebo údajov a môže spôsobiť skutočnú škodu hmotnú, či nehmotnú. Akákoľvek bezpečnostná zraniteľnosť môže byť vhodná pre tento Program, avšak musí byť nová, predtým neoznámená a nie vylúčená z Programu, aby bola spôsobilá na odmenu a uznanie. Obvykle pôjde o oznámenia zraniteľností s výrazným bezpečnostným dopadom. Avšak odmenená môže byť akákoľvek zraniteľnosť akejkoľvek závažnosti, ktorá môže spôsobiť škodu. Akýkoľvek problém v dizajne, implementácii či nastavení infraštruktúry, ktorý výrazne ovplyvňuje celistvosť údajov užívateľa môže spadať tiež do tohto Programu.

Bežné príklady zahŕňajú:

- 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

Vezmite na vedomie, že rozsah Programu je štandardne obmedzený na technické zraniteľnosti webových aplikácií vo vlastníctve Zákazníka a súvisiacich liniek.

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.

Zákazník môže výslovne určiť aj iné ako vyššie uvedené zraniteľnosti, ktoré sa kvalifikujú na odmenu v jeho zverejnenom Projekte.

Nekvalifikované zraniteľnosti

V závislosti od ich vplyvu, niektoré oznámené problémy sa nemusia kvalifikovať. Hoci ich posudzujeme od prípadu k prípadu, tu sú niektoré bežné problémy s nízkym rizikom, za ktoré obvykle nevzniká nárok na odmenu:

- 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
- Vulnerabilities used to enumerate or confirm the existence of users or tenants
- Vulnerabilities requiring unlikely user actions
- URL Redirects (unless combined with another vulnerability to produce a more severe vulnerability)

Okrem peňažných odmien, Etickí hackeri, ktorí s nami spolupracujú na riešení bezpečnostných zraniteľností môžu byť uvedení na našej web stránke, za podmienok špecifikovaných v Podmienkach pre Etických hackerov.

Zákazník môže výslovne vylúčiť iné ako vyššie uvedené zraniteľnosti, za ktoré nevzniká nárok na odmenu.

Odmeny

Odmeny za kvalifikované zraniteľnosti sa pohybujú od 40,00 € do akejkoľvek sumy určenej vo zverejnenom Projekte v závislosti od závažnosti potenciálneho bezpečnostného dopadu oznámenej zraniteľnosti.

O výške odmien pre Etických hackerov za oznámenia o zraniteľnostiach v rámci konkrétneho Projektu Zákazníka rozhoduje Zákazník na základe návrhu výšky odmien prezentovaných Hacktrophy tak, aby Zákazník efektívne využil služby Hacktrophy v súlade s cieľom svojej účasti v Programe. Zákazník má právo výšku odmien pre Etických hackerov ponúkaných v rámci konkrétneho Projektu meniť kedykoľvek počas trvania Projektu podľa vlastného uváženia.

Výška odmien je určená v každom Projekte osobitne.

Prosím vezmite na vedomie, že na odmenu nie je právny nárok. Nárok na odmeny, určenie ich príjemcov a výška odmeny je ponechaná na zváženie Zákazníka, resp. Hacktrophy.

Výška odmeny pre Etického hackera je obvykle stanovená podľa podmienok určených vo zverejnenom Projekte a kategórie zraniteľnosti vybranej Etickým hackerom, a potvrdenej Hacktrophy, ktorá musí definitívne schváliť kategóriu zraniteľnosti (a výšku odmeny), podľa podmienok špecifikovaných v Podmienkach pre Zákazníka.

Nevyplácame odmeny jednotlivcom, ktorí konajú so zámerom odhaľovať bezpečnostné chyby na iný účel, ako ten, ktorý sleduje tento Program, alebo porušujú zákon, alebo zverejňujú či porušujú alebo zneužívajú údaje akejkoľvek inej osoby, alebo ktorí sú vedení na akýchkoľvek právne záväzných sankčných zoznamoch. Etickí hackeri zodpovedajú za akékoľvek daňové dopady v závislosti od ich krajiny trvalého pobytu a štátneho občianstva. Môžu existovať ďalšie obmedzenia pokiaľ ide o ich spôsobilosť zúčastniť sa na Programe podľa miestnych právnych predpisov.

Sme oprávnení zrušiť Program kedykoľvek bez udania dôvodu.

Testovanie bezpečnosti nesmie porušovať žiadne právne predpisy, zverejňovať, narušovať alebo zneužívať akékoľvek údaje, ktoré nie sú vaše.

Vyhľadávanie a oznamovanie bezpečnostných zraniteľností

Pri vyhľadávaní zraniteľností, prosím, sa nikdy nepokúšajte o prístup k údajom kohokoľvek iného a nezapájajte sa do činností, ktoré môžu ohroziť alebo spôsobiť škodu iným užívateľom alebo Zákazníkovi.

Každý Etický hacker musí byť prihlásený do Programu, aby mohol predložiť oznámenie o zraniteľnosti. Etický hacker sa môže do Programu prihlásiť vyplnením požadovaných údajov v prihlasovacom formulári. 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. V rámci jednotlivých Projektov zvyčajne komunikuje v mene Zákazníka pridelený moderátor. Zákazník má však kedykoľvek možnosť zapojiť sa do rozhovorov s Etickými hackermi o predložených oznámeniach. Prosíme Etických hackerov o aktívnu komunikáciu ohľadom svojich oznámení, najmä o poskytnutie súčinnosti Zákazníkovi pri oprave oznámenej bezpečnostnej zraniteľnosti.

Etický hacker oznámi zraniteľnosť nájdenú vo vybranom Projekte prostredníctvom formulára tak, že vyplní všetky nevyhnutné podrobnosti a údaje opisujúce zraniteľnosť.

Ostatné podmienky predkladania oznámení o zraniteľnosti a ich spracovanie sú ustanovené v Podmienkach pre Zákazníka a v Podmienkach pre Etického hackera.

Ostatné pokyny:

Prosíme, aby ste predložili svoje oznámenie akonáhle ste objavili potenciálny bezpečnostný problém. V prípade, ak Etický hacker neuvedie vo formulári všetky nevyhnutné údaje z akéhokoľvek dôvodu, oznámenie môže byť považované za nespôsobilé.

Prosíme o vykonanie due diligence: potvrďte, že software má nejaké významné zraniteľnosti, a vysvetlite, prečo sa domnievate, že tieto funkcie môžu byť odhalené a zneužité tak, že môžu pri špecifickom použití predstavovať riziko. Oznámenia, ktoré nebudú obsahovať tieto informácie sa obvykle nekvalifikujú na odmenu.

V zásade sa zaväzujeme odpovedať urýchlene a výmenou za to žiadame o oznámenie s rozumným predstihom. Oznámenia, ktoré sú v rozpore s týmto princípom sa obvykle nekvalifikujú, ale budeme ich posudzovať prípad od prípadu. Zároveň prosíme o trpezlivosť pri vyhodnocovaní predložených oznámení, keďže Program môže prijať veľké množstvo oznámení alebo si niektoré druhy zraniteľnosti vyžadujú časovo náročné preverenie.

Je v rozpore s Programom súkromne odhaliť bezpečnostnú chybu tretím osobám na iný účel, než na skutočnú opravu zraniteľnosti cez platformu Hacktrophy. V dôsledku toho sa takéto oznámenia obvykle nekvalifikujú. Takéto konanie je považované za závažné porušenie našich podmienok, ktorého dôsledkom je okamžité vylúčenie Etického hackera z Programu. V takomto prípade nemá Etický hacker nárok na zaplatenie odmeny a môžu mu hroziť trestno-právne dôsledky.

„Kto prvý príde, prvý melie.“ – Na odmenu sa Etický hacker kvalifikuje iba v prípade, ak bol prvou osobou, ktorá nás upozornila na predtým neznámu bezpečnostnú zraniteľnosť.

Pri prihlásení sa do Programu odporúčame vyplniť všetky informácie v prihlasovacom formulári vrátane platobných a iných údajov nevyhnutných na úhradu odmeny. V prípade, ak platobné a iné údaje Etického hackera vyžadované Hacktrophy nebudú vyplnené, Hacktrophy nezodpovedá za to, že odmena nebude z akéhokoľvek dôvodu uhradená.

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.

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.

Odmena bude Etickému hackerovi uhradená len v prípade, ak Zákazník zaplatil odmenu pre Etického hackera Hacktrophy. Následne, Hacktrophy zaplatí odmenu Etickému hackerovi.

Vyhradzujeme si právo upraviť všetky podmienky tohto Programu kedykoľvek. Pred vstupom do Programu musí Etický hacker súhlasiť s Podmienkami pre etických hackerov. Prosíme vás, aby ste túto stránku kontrolovali pravidelne, pretože pravidelne aktualizujeme naše podmienky Programu, ktoré sú účinné ich zverejnením.