PRAVIDLÁ PRE HACKTROPHY BUG BOUNTY PROJEKTY

Uvedomujúc si zvýšenú úroveň ochrany vyžadovanej našimi zákazníkmi, hľadáme 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 program odmeňovania zraniteľností. Tento Hacktrophy bounty program (hereinafter only as the "**Program**") je vyvinutý a prevádzkovaný bezpečnostnou spoločnosťou Hacktrophy, ktorá garantuje kvalifikovaný manažment Programu. Nasledovné inštrukcie môžu pomôcť tým, ktorí by chceli pomôcť urobiť internet bezpečnejším miestom.

Popis programu

Tento Program podporuje a odmieňa príspevky (oznámenie 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.

Hacktrophy ponúka dva typy Programu:

Basic Program – spracovanie oznámenia Etického hackera nasledujúce po zverejnení Projektu prebieha bez kontroly moderátora. Všetky oznámenia sa posielajú priamo Zákazníkovi, ktorý o nich rozhodne. Zákazník je výlučne zodpovedný za opravu oznámenej zraniteľnosti a konzultuje postup opravy s Etickým hackerom.

Premium Program – kompletné spracovanie oznámenia Etického hackera je kontrolované moderátorom určeným zo strany Hacktrophy. Moderátor Hacktrophy posúdi každé oznámenie a ohodnotí jeho spôsobilosť a relevanciu. Zákazník je výlučne zodpovedný za opravu oznámenej zraniteľnosti a konzultuje proces opravy v Etickým hackerom a moderátorom.

Služby v rozsahu Programu

Akákoľvek webová služba alebo aplikácia, ktorá je vlastníctvom Zákazníka a ktorá obsahuje dôvodne citlivé údaje, vrátane bugov 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 odmieňať také oznámenia. Bezpečnostné bugy 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. Bugy 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.

Vždy si pamätaj, ak máš pochybnosti, najprv nás kontaktuj.

Kvalifikované zraniteľnosti

Bezpečnostný bug je chyba, vada, omyl, porucha alebo kaz v počítačovom programe alebo systéme, ktorý vplýva na bezpečnosť zariadenia, systému, siete, alebo údajov a môže spôsobiť skutočnú škodu hmotnú, či nehmotnú. Akýkoľvek bezpečnostný bug môže byť vhodný pre tento Program, avšak musí byť nový, predtým neoznámený a nie vylúčený z Programu, aby bol spôsobilý na odmenu a uznanie. Obvykle pôjde o oznámenia bugov s výrazným vplyvom. Avšak odmenená môže byť akákoľvek zraniteľnosti akejkoľvek závažnosti, ktorá môže spôsobiť škodu. Akýkoľvek problém v dizajne či implementácii, ktorý výrazne ovplyvňuje celistvosť údajov užívateľa môže spadať do tohto Programu.

Bežné príklady zahŕňajú:

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Mixed-content scripts
- Unauthorized cross-tenant data tampering or access (for multi-tenant services)
- Insecure direct object references
- Injection Vulnerabilities (such as SQL Injection, XML injection or ORM injection)
- Authentication Vulnerabilities
- Server-side Code Execution
- Privilege Escalation
- Significant Security Misconfiguration
- Server-side code execution bugs

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

Zákazník môže výslovne určiť 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
- 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)
- Vulnerabilities in platform technologies that are not unique to the online services in question
- ”Cross Site Scripting” bugs in SharePoint that require “Designer” or higher privileges in the target’s tenant.
- Low impact CSRF bugs (such as logoff)
- Cookie replay vulnerabilities

Okrem peňažných odmien, Etický hackeri, ktorí s nami spolupracujú na riešení bezpečnostných bugov budú 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 bugy sa pohybujú od 40,00 € do akejkoľvek sumy určenej Zákazníkom vo zverejnenom Projekte. Nasledovná tabuľka načrtáva obvyklý priemer odmien za niektoré najbežnejšie triedy bugov, navrhnutý zo strany Hacktrophy:

Úroveň rizika	Príklady zraniteľností	Suma odmeny (€)
Kritická	• Remote Code Execution • Vertical Privilege Escalation • XML External Entities Injection with significant impact • SQL Injection with significant impact • LFI/RFI	Rozsah 500 – 7500
Vysoká	• 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	Rozsah 300 – 1500
Stredná	• Direct object reference • CSRF with impact • Path Traversal • DOM XSS	Rozsah 80 – 550
Nízka	• SSL misconfigurations with little impact • SPF configuration problems • XSS with limited impact • CSRF with limited impact • SSL/TLS issues • URL redirect • Clickjacking	Rozsah 40 – 160
Akceptovateľné riziko	• Debug information • Use of CAPTCHAs • Code obfuscation • Rate limiting, etc.	0

Avšak, Zákazník môže určiť akúkoľvek výšku odmien vo svojom Projekte bez ohľadu na odporúčanie Hacktrophy.

Zákazník určí výšku odmien v každom svojom zverejnenom Projekte osobitne.

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

V Basic Programe je výška odmeny pre Etického hackera obvykle stanovená automaticky na základe podmienok určených vo zverejnenom Projekte a kategórie zraniteľnosti vybranej Etickým hackerom, za podmienok špecifikovaných v Podmienkach pre Zákazníka.

V Premium Programe je výška odmeny pre Etického hackera obvykle stanovená podľa podmienok určených vo zverejnenom Projekte a kategórie zraniteľnosti vybranej Etickým hackerom, a potvrdenej moderátorom, ktorý musí definitívne schváliť kategóriu zraniteľnosti (a výšku odmeny), podľa podmienok špecifikovaných v Podmienkach pre Zákazníka.

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

Sme oprávnení zrušiť Program kedykoľvek bez udania dôvodu.

Tvoje testovanie nesmie porušovať žiadne právne predpisy, zverejňovať, narušovať alebo zneužívať akékoľvek údaje, ktoré nie sú tvoje.

Vyhľadávanie a oznamovanie bugov

Pri vyhľadávaní zraniteľnosti, prosím, sa nikdy nepokúšaj o prístup k údajom kohokoľvek iného a nezapájaj sa do činností, ktoré sú rušivé alebo škodlivé pre iných užívateľov alebo pre Zákazníka.

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. Etický hacker tiež bude informovaný, či je Projekt zverejnený v Basic Programe alebo v Premium Programe.

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 v Basic Programe a v Premium Programe, sú ustanovené v Podmienkach pre Zákazníka a v Podmienkach pre Etického hackera.

Ostatné pokyny:

Prosím predlož svoje oznámenie akonáhle si objavil potenciálny bezpečnostný problém. V prípade, ak Etický hacker neuvedie vo formulári všetky nevyhnutné údaje z akéhokoľvek dôvodu, oznámenie môže byť považované za nespôsobilé.

Prosím vykonaj due diligence: potvrď, že software má nejaké významné zraniteľnosti, a vysvetli, prečo sa domnievaš, že tieto funkcie môžu byť odhalené a môžu pri špecifickom použití predstavovať riziko. Oznámenia, ktoré nebudú obsahovať tieto informácie sa obvykle nekvalifikujú.

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 od prípade k prípadu.

Je v rozpore z Programom súkromne odhaliť vadu tretím osobám na iný účel ako na skutočnú opravu bugu. V dôsledku toho sa také oznámenia obvykle nekvalifikujú. Také konanie je považované za závažné porušenie našich podmienok, ktorého dôsledkom je okamžité vylúčenie Etického hackera z Programu. V takom prípade nemá Etický hacker nárok na zaplatenie odmeny.
Kto prvý príde, prvý melie. Na odmenu sa kvalifikuješ iba v prípade, ak si bol prvou osobou, ktorá nás upozornila na predtým neznámu vadu.

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.

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 týmito podmienkami. Prosím kontroluj túto stránku pravidelne, pretože neustále upravujeme naše podmienky Programu, ktoré sú účinné ich zverejnením.