
hacktrophy
Nová cesta k internetovej bezpečnosti

Stav bezpečnosti v online svete

- 37 000 hacknutých webov denne
- Ktorýkoľvek web je terčom útoku v priemere každých 120 dní
- 86 % pravdepodobnosť, že web obsahuje kritickú zraniteľnosť
- 25 % útokov spôsobili svojou nedbalosťou samotní zamestnanci = 75 % všetkých kybernetických útokov za posledný rok prišlo z vonkajšieho prostredia firmy

hacktrophy

Stav bezpečnosti online projektov u nás

- 89 % firiem je mierne až veľmi spokojných s IT bezpečnosťou v ich firme
- Až 48 % českých a slovenských spoločností vôbec nerieši bezpečnosť svojich webov a aplikácií
- 16 % slovenských a českých firiem má priamu skúsenosť s hacknutím, ďalších 28 % nepriamu
- 49 % firiem má strach z napadnutia hackerom

hacktrophy

Hackerské a iné "cyber-crime" útoky sa nedejú iba v amerických filmoch

hacktrophy

Najčastejšie druhy útokov v ČR a SR

Škody spôsobené online zločinom v ČR presiahli 1,2 miliardy CZK (44 mil. €).

1. **Hacknutie cez dieru v systéme** a slabé šifrovanie uložených hesiel (Mall.cz)
2. Škodlivá **mobilná aplikácia**, ktorá sa vydávala za produkt Alzy
3. **Phishing** - zasiahol zákazníkov väčšiny našich bánk
4. **Nedostatočná aktualizácia** - napr. Orange doplatil na starý firmvér routerov
5. **Zraniteľnosť v systéme 3. strany** viedol k hacknutiu e-shopu Xzone.cz
6. Šírenie škodlivých **kódov a ransomvéru** (WannCry, Petya, u nás ExPetr...)
7. Nedostatočná **zamestnanecká politika** v oblasti bezpečnosti (únik dát v T-mobile)

hacktrophy

Prípadová štúdia 1

Poškodená reputácia e-shopu

- Stredne veľký český e-shop.
- **Forma hacknutia:** Útočník sa zaregistroval na webe e-shopu. Ako prihlásený používateľ odhalil kritickú SQL injection zraniteľnosť, pomocou ktorej získal kompletný prístup k databáze klientov a ich osobných údajov. Klient sa o tom dozvedel, až keď zoznam jeho klientov „putoval“ po internete.
- **Škoda:** Kombinácia ťažko vyčísliteľného poškodenia reputácie s reálnou škodou vo výške tisícok EUR.
- **Náprava následkov:** 2 týždne

Prípadová štúdia 2

Hacknutie viedlo k rozposielaniu spamu z firemného e-mailu

- Slovenský e-shop s asi 25 zamestnancami
- **Forma hacknutia:** Chyby v kóde samotnej aplikácie, ktoré útočník našiel cez kontaktný formulár. Následne mu to umožnilo rozosielať spam bez vedomia firmy.
- **Škoda:** Kombinácia poškodenia reputácie kvôli rozposielaniu spamu a komplikácií pre zaradenie mailového servera do blacklistov na celom svete. Navyše sa to stalo v období pred Vianocami, takže vznikla aj priama finančná škoda.
- **Náprava následkov:** 3 dni

Ako sa firma môže brániť?

hacktrophy

Základné možnosti ochrany

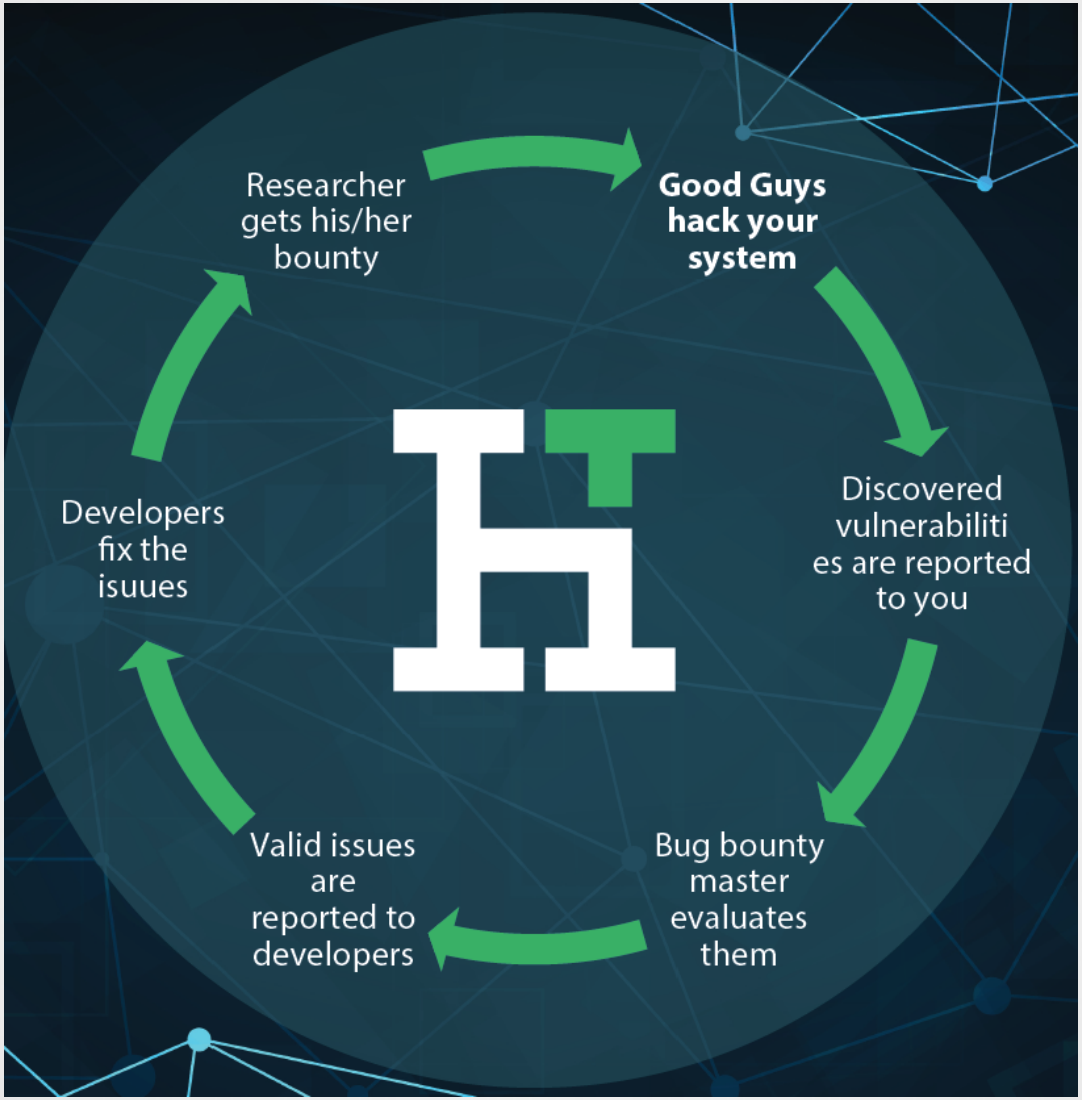
- **Interné testovanie** - limitované počtom a kvalitou zamestnancov, navyše často ide o programátorov, nie security špecialistov
- **Certifikáty** - tie kvalitné sú drahé, u nás sú často zamerané len na formálne aspekty bezpečnosti
- **Penetračný test** - malý počet odborníkov za vysokú cenu, pričom výsledok je viazaný na konkrétny čas
- **Bezpečnostný audit** - komplexné, ale drahé riešenie
- **Bug bounty programy** - nový spôsob testovania bezpečnosti online projektov

Ako fungujú bug bounty programy?

- V strednej Európe ide o nový spôsob, v anglosaskom svete sa už využíva viac ako 15 rokov
- "Bug bounty" v podstate znamená "odmena za nájdenie bezpečnostnej diery"
- **Princíp je jednoduchý** – vyhlásite odmenu za nájdenie bezpečnostných chýb vo vašich aplikáciách. Etickí hackeri sa tieto zraniteľnosti snažia nájsť a oznámiť vám ich skôr, než by mohlo dôjsť k ich zneužitiu. Vy si nájdenú dieru opravíte a vyplatíte etickému hackerovi odmenu.

Etická hackeri vs. Black-hat hackeri

Ako funguje Hacktrophy?



hacktrophy

Hlavné výhody Hacktrophy

- Do hľadania bezpečnostných dier sa zapájajú **stovky expertov** - web alebo aplikáciu tak otestujete dôkladnejšie a lacnejšie ako interne či cez pentest.
- **Testujete priebežne**, nie jednorazovo, pričom vzniká súboj medzi etickými hackermi, aby nahlásili dieru ako prví.
- Platíte odmeny len za **relevantné bezpečnostné diery a v mesačnom limite**, ktorý si vopred stanovíte.
- Testovanie bezpečnosti máte **celý čas v rukách** - sami určíte jeho cieľ, povolené hackerské techniky aj odmeny a potom už len dostávate hlásenia o zraniteľnostiach.

Kedy má zmysel siahnuť po Hacktrophy?

Ak **hrozí zneužitie bezpečnostných dier cez web, mobilnú aplikáciu či IoT rozhranie**, najmä ak:

- prevádzkujete e-shop, CRM či CMS systém, cloud, stávkový či iný portál s citlivými údajmi,
- spúšťate nový online produkt alebo mobilnú aplikáciu,
- prevádzkujete akýkoľvek typ platby cez internet,
- máte web postavený na riešení 3. strán, no umiestnený na vlastnom serveri,
- zavádzate novú funkcionalitu, ale nechcete robiť pentest,
- používate "skryté" rozhranie pre zamestnancov či zákazníkov.

Aký výstup dostanete od etických hackerov?

Skusobny08 UPRAVIT

otevřené

Poslat požadavek moderátorovi

Projekt	TestFirmicky
Status	otevřené [změnit]
Potenciální odměna	1200.0
Kategorie zranitelností	High Risk
Typ zranitelnosti	Internal SSRF

Umístění zranitelnosti / URL	www

Popis zranitelnosti

www

Jak byla tato zranitelnost nalezena? Vysvětlení postupu

www

Jak opravit tuto zranitelnost? Doporučený postup

www

hacktrophy

Koľko stoja služby na Hacktrophy?

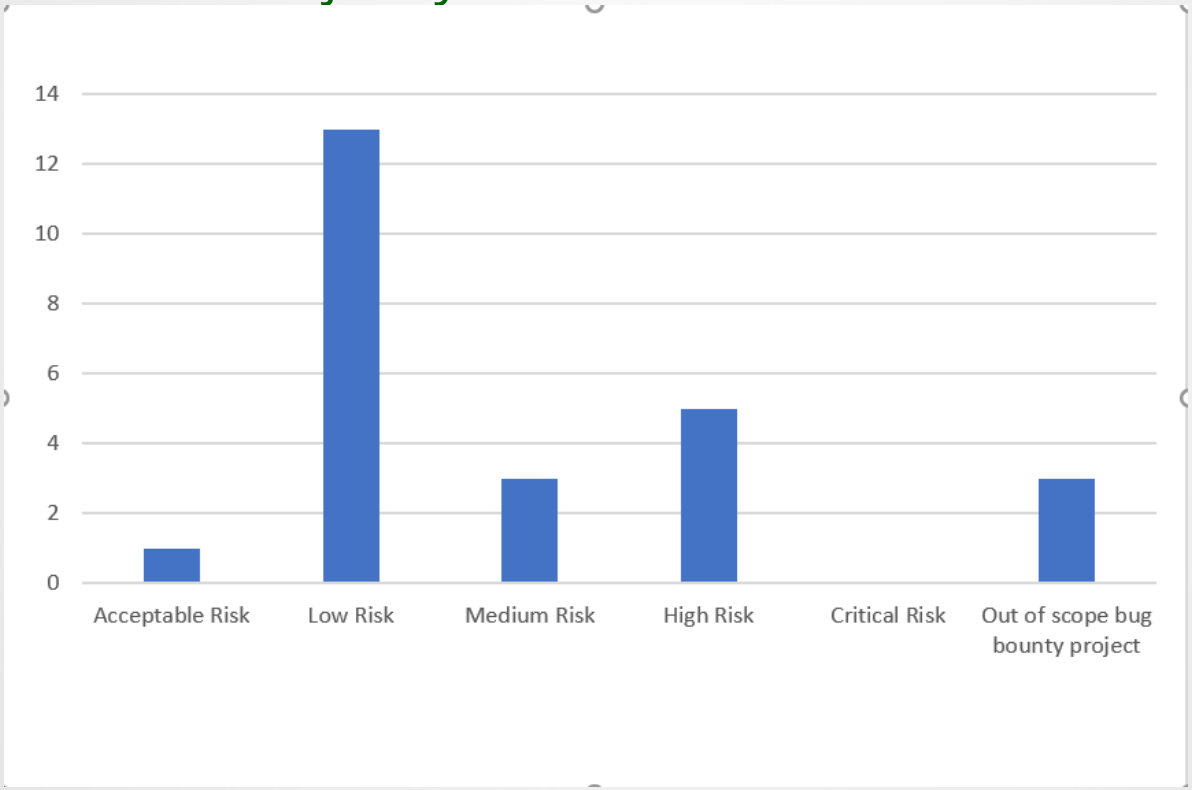
- **Cena závisí** tak od zadania a programu, ktorý využívate (BASIC alebo PREMIUM), ako aj od typu zraniteľnosti, ktorú etický hacker nájde.
- BASIC program je zadarmo, PREMIUM v cene 200 e/mesiac.
- Všetky odmeny si **sami vopred stanovíte**.
- Provízia pre Hacktrophy je fixných 20 % z každej odmeny.
- Pre odmeny si môžete stanoviť **mesačný limit**.
- **Bežný mesačný rozpočet** na testovanie začína od 500-700 eur až po niekoľko tisíc až desaťtisíc eur.

Aká je odporúčaná výška odmien?

Priority	Vulnerability Types	Pricing in EUR
Critical	RCE, SQLi, XXE, Vertical Authentication Bypass	700 / 2200 / 6000
High	Stored XSS, CSRF, Lateral Authentical Bypass	400 / 750 / 1200
Medium	Reflective XSS, URL redirect	125 / 250 / 425
Low	SSL misconfigurations, XSS/CSRF with limited impact	45 / 60 / 135

Doterajšie skúsenosti s Hacktrophy

- Zaregistrovaných skoro 300 etických hackerov.
- Priemerná výška priznaných odmien bola 204 eur.
- Najvyššia vyplatená odmena bola zatiaľ 400 eur.
- Charakter nájdených zraniteľností:



hacktrophy

Ďakujem za vašu pozornosť

Roman Jazudek
jazudek@hacktrophy.com
0948 09 09 08