hacktrophy

Nová cesta k internetovej bezpečnosti

Hacktrophy je modernou cestou ako efektívne testovať bezpečnosť vašich webov či aplikácií prostredníctvom tzv. bug bounty programov. Vďaka veľkému množstvu etických hackerov objavíte bezpečnostné zraniteľnosti včas a citlivé dáta tak zabezpečíte skôr, než by mohli byť zneužité.

www.hacktrophy.com

Prečo by ste sa mali zaujímať o IT bezpečnosť?

37 000 webstránok sa **každý deň stane terčom hackerského útoku**. Black-hat hackeri vo svete denne ukradnú približne 5 miliónov citlivých záznamov.

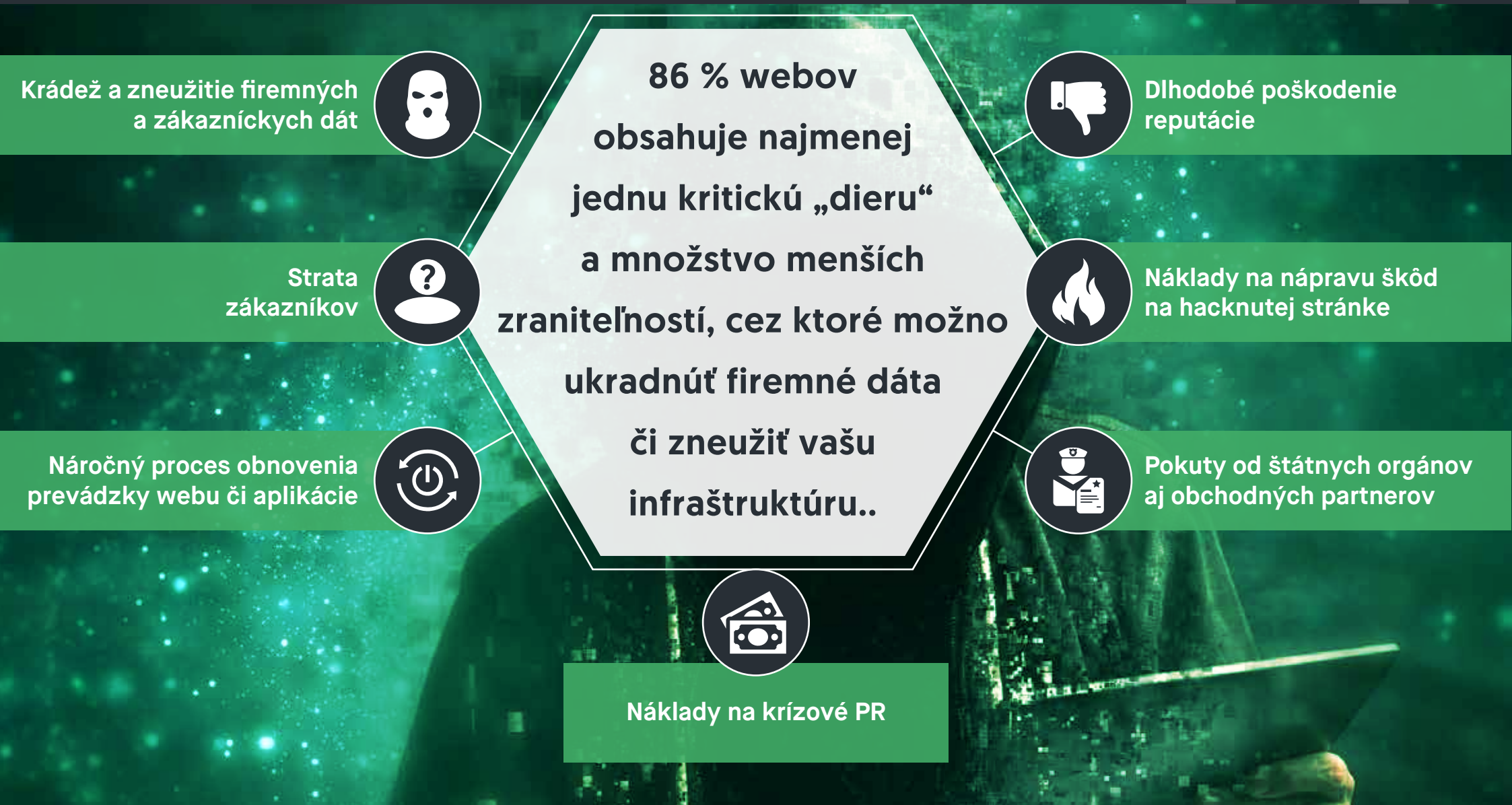
Obeťou hackerského útoku sa stala už **jedna šestina slovenských a českých podnikajúcich v online biznise.***

Skoro **2/3 malých a stredných** podnikov zaznamenalo v roku 2017 kybernetický útok a 54 % z takýchto podnikov bolo obeťou krádeže citlivých dát.

Pokuta **do výšky 20 miliónov EUR alebo 4 % z ročného obratu** hrozí od mája 2018 spoločnostiam, ktoré nedodržia pravidlá nového nariadenia na ochranu osobných údajov (GDPR).

* Prieskum agentúry 2Muse realizovaný pre Hacktrophy, 2016

Čo vám hrozí po úspešnom útoku zlého hackera na váš web?



86 % webov obsahuje najmenej jednu kritickú „dieru“ a množstvo menších zraniteľností, cez ktoré možno ukradnúť firemné dáta či zneužiť vašu infraštruktúru..

- Krádež a zneužitie firemných a zákazníckych dát
- Strata zákazníkov
- Náročný proces obnovenia prevádzky webu či aplikácie
- Dlhodobé poškodenie reputácie
- Náklady na nápravu škôd na hacknutej stránke
- Pokuty od štátnych orgánov aj obchodných partnerov
- Náklady na krízové PR

Útoky black-hat hackerov sú realitou aj na Slovensku či v Čechách

1

Z webu Mall.cz ukradol zlý „black hat" hacker vďaka bezpečnostnej chybe 766 421 hesiel, 735 956 e-mailových adries a obdobný počet telefónnych čísel v čitateľnej podobe. Dáta uverejnil na internete. **Okrem finančných škôd vo výške niekoľko tisíc eur spoločnosť stratila reputáciu** a značnú časť zákazníkov.

2

Komerční banka mala v roku 2013 bezpečnostnú chybu v internetovom bankovníctve. Tá umožnila jednému z klientov **vidieť záznamy penzijného sporenia 47 947 klientov banky**. Prípad bol medializovaný a banka prehlásila, že sa takmer „nič nestalo". Stratila ale dobré meno a časť klientov.

3

Tesne pred spustením nového projektu napadol slovenskú vývojársku firmu black-hat hacker. Do systému vnikol cez nezabezpečenú firemnú aplikáciu a zneužil servery spoločnosti na nelegálne účely. **Dôsledkom bola finančná škoda 45 000 EUR a odloženie štartu pripravovaného projektu o 3 mesiace.***

4

Koncom roka 2016 napadol zlý hacker vďaka bezpečnostnej diere stránku Domina.sk. **Médiám rozposlal ukradnuté citlivé dáta ako dôkaz svojho úspechu**. Súbor obsahoval informácie o viac ako 30 000 používateľoch vrátane ich správ s veľmi citlivým obsahom. Služba stratila veľkú časť klientov a dodnes bojuje o svoju povesť.

* Štúdia firiem Citadelo a Nethemba, ktorých majitelia sú spoluzakladatelia projektu Hacktrophy

Hacktrophy zvýši úroveň vašej IT bezpečnosti

Princíp je jednoduchý – cez Hacktrophy.com vyhlásite odmenu za nájdenie bezpečnostných chýb vo vašich aplikáciách alebo na webe. Zaregistrovaní etickí hackeri sa tieto zraniteľnosti budú snažiť nájsť a oznámiť vám ich skôr, než by mohlo dôjsť k ich zneužitiu.

Odmena sa vyplatí iba za reálne bezpečnostné „diery". Testovanie pritom môže prebiehať tak, aby neohrozilo bežnú prevádzku webu (napr. cez vaše testovacie konto alebo v testovacom prostredí).

Ako funguje Hacktrophy?

1. S našou pomocou určíte kde a čo majú etickí hackeri hľadať, pričom vám pomôžeme nastaviť správne odmeny.

2. Etickí hackeri začnú testovať bezpečnosť vášho webu či aplikácie.

3. Keď nájdu bezpečnostnú zraniteľnosť, nahlásia vám ju.

4. Preveríme, či ide o relevantnú „dieru". Ak áno, akceptujeme hlásenie a vy si chybu opravíte.

5. Uhradíme odmenu hackerovi z financií v rámci balíčka, ktorý ste si zakúpili.

6. Etickí hackeri hľadajú ďalšie zraniteľnosti, až kým sa neminú financie z vášho balíčka.

„

Výhody bug bounty programu Hacktrophy

Dlhodobé testovanie bezpečnosti

Etickí hackeri váš web alebo aplikáciu testujú počas celého roka, resp. až kým sa neminú financie z predplateného balíčka.

Cenová efektivita a kvalita výstupov

Platíte len za diery, ktoré sa skutočne nachádzajú v systéme, preverí ich náš moderátor a spĺňajú vaše zadanie.

Rôznorodosť testerov z celého sveta

Váš online produkt alebo službu testujú desiatky až stovky bezpečnostných expertov, tzv. etických hackerov.

Testovanie máte pod kontrolou

Vy určíte, čo môžu etickí hackeri testovať, v akom prostredí (testovacom alebo produkčnom) a do akej hĺbky vášho systému.

Odbornosť testerov

Zručnosti etických hackerov v oblasti testovania IT bezpečnosti sú rozsiahlejšie ako v prípade bežných IT zamestnancov.

Manuálne testovanie a overovanie

Vašu bezpečnosť testujú reálni ľudia s unikátnymi znalosťami, nie automatizované roboty či skeny.

Čo môžete testovať cez Hacktrophy?

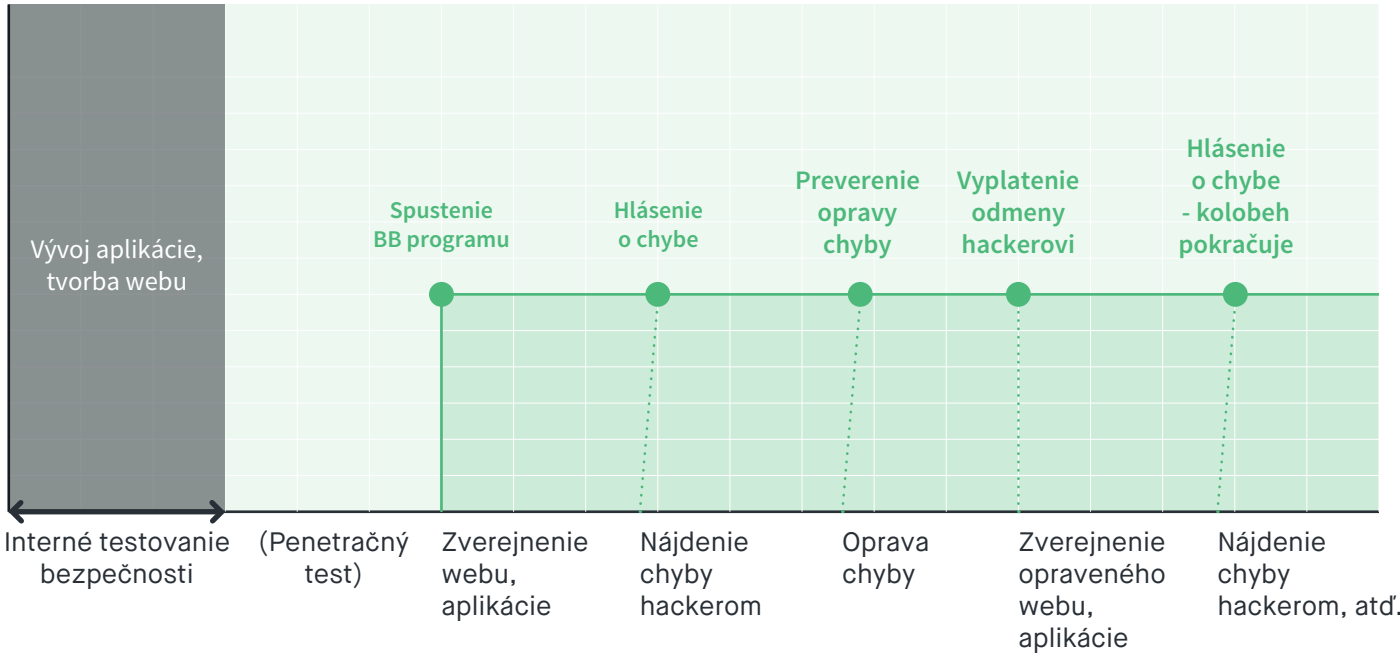
Každý web, aplikáciu či rozhranie dostupné cez internet:

- webstránky, ktoré pracujú s citlivými údajmi vás alebo vašich klientov,
- e-shopy, stávkové portály, online trhoviská,
- CMS jadrá,
- CRM a účtovné systémy, cloud, IoT riešenia,
- mobilné aplikácie alebo hry,
- internet banking, kryptoburzy a platobné brány,
- firemné či priemyselné systémy, ktoré sú pripojené k internetu.

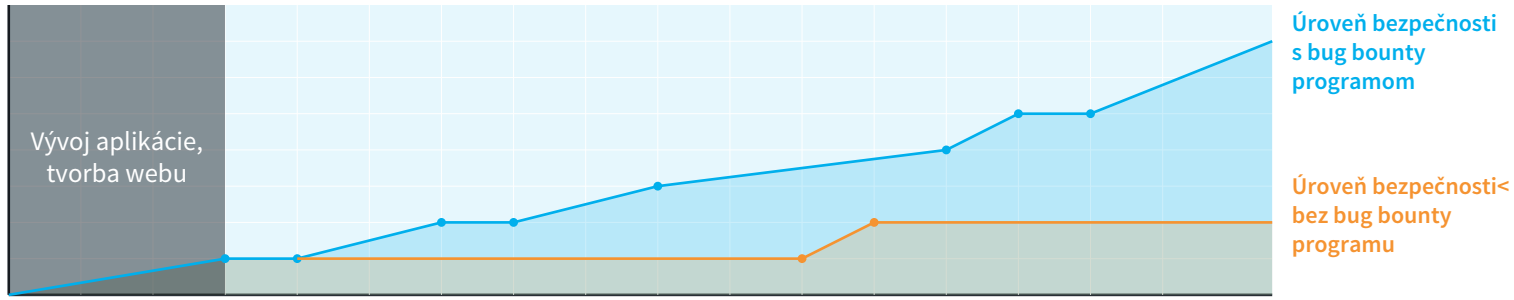
Testovať možno nielen chyby vzniknuté v dôsledku programovania či použitého softvéru, ale aj nastavenie infraštruktúry, na ktorej web či aplikácia bežia. Testovanie môže prebiehať v produkčnom aj testovacom prostredí.

Proces testovania bezpečnosti

BUG BOUNTY PROGRAM HACKTROPHY

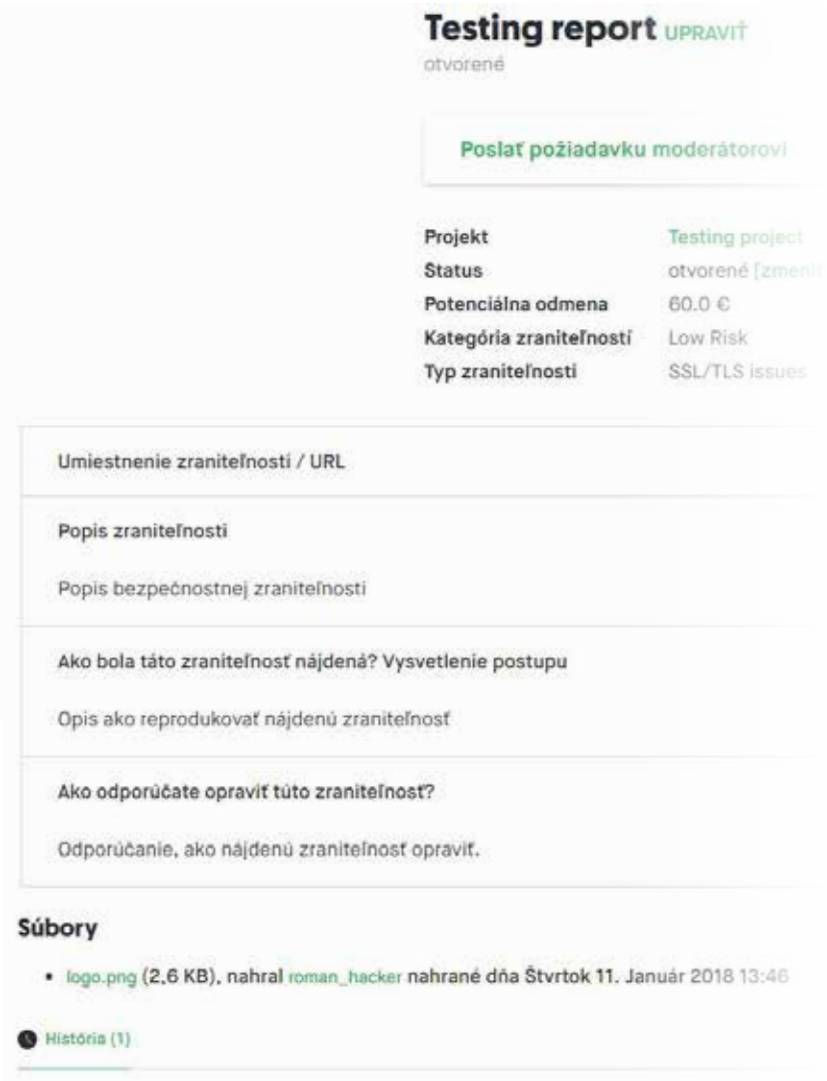


ÚROVEŇ BEZPEČNOSTI



Čo získate od etických hackerov?

Ukážka hlásenia nájdenej "diery"



TOP 5 zraniteľností nahlásených v roku 2017 cez Hacktrophy

- **Špecifická zraniteľnosť (10,35 %)**
  Zraniteľnosť, ktorá sa nenachádza v OWASP TOP 10 hodnotení, ale predstavuje vysoké riziko napadnutia.
- **SPF configuration problems (5,52 %)**
  Chyba v nastaveniach e-mailového servera, ktorá umožňuje vykonávať e-mail spoofing (krádež identity).
- **XSS (4,83 %)**
  Predstavuje možnosť vkladania škodlivého kódu na webstránku s cieľom jeho následného využitia na koncových zariadeniach návštevníkov na krádež citlivých dát.
- **CSRF (4,16 %)**
  Útok, ktorý umožňuje prinútiť používateľa načítať web obsahujúci škodlivú požiadavku. To môže viesť ku krádeži identity alebo citlivých dát používateľov.
- **Session fixation (4,16 %)**
  Ide o útok, ktorý dovoľuje útočníkovi ukradnúť platnú reláciu používateľa, ktorá je následne presmerovaná na server útočníka.

Porovnanie penetračných testov a Hacktrophy

	PENETRAČNÝ TEST	HACKTROPHY
Časové pokrytie	**Nízke.** Jeden alebo niekoľko etických hackerov na obmedzený čas.	**Vysoké.** Veľká skupina etických hackerov bez časového limitu, pričom sa platí len za validné výsledky.
Potrebné úsilie	**Stredné.** Pomerne zložité nastavenie zadania. Prioritou je záverečné hlásenie.	**Nízke.** So zadaním bug bounty projektu vám pomôže pridelený moderátor. Priebežne získavate overené hlásenia o zraniteľnostiach.
Kvalita nájdených zraniteľností	**Vysoká.** Závislá na kvalite dodávateľa pentestu.	**Vysoká.** Počet hackerov garantuje rôzne typy skúseností a formy hackovania.
Náklady za zraniteľnosť	**Vysoké.** Konzultanti sú drahí a ich čas je obmedzený.	**Stredné.** S výškou odmien vám poradí Hacktrophy, pričom ich máte celý čas pod kontrolou. Platíte len za overené zraniteľnosti.

Detailné porovnanie nájdete v našom blogu

Vyberte si jeden zo spôsobov testovania

Balík S

Ideálny pre jednoduchý web či aplikáciu s minimom citlivých údajov.

Doba trvania je 1 rok alebo do minutia odmien pre etických hackerov

1 299 €

vrátane odmien pre etických hackerov

ODPORÚČAME

Balík M

Ideálny pre firemný web, ktorý spracúva niektoré citlivé údaje, napr. po registrácii.

Obsahuje automatizovaný sken zraniteľnosti!

Doba trvania je 1 rok alebo do minutia odmien pre etických hackerov

1 699 €

vrátane odmien pre etických hackerov

Balík L

Ideálny pre web či aplikáciu, ktoré pracujú s financiami alebo viacerými citlivými údajmi.

Obsahuje automatizovaný sken zraniteľnosti **s manuálnym overením!**

Doba trvania je 1 rok alebo do minutia odmien pre etických hackerov

4 299 €

vrátane odmien pre etických hackerov

Každý balík automaticky obsahuje:

- Dlhodobé testovanie bezpečnosti komunitou viac ako 350 etických hackerov z celého sveta
- Flexibilné nastavovanie odmien pre etických hackerov v závislosti od závažnosti hľadaných chýb
- Manuálne overenie nahlásených chýb prideleným moderátorom
- Podpora zo strany moderátora pri tvorbe a manažovaní vášho bug bounty programu počas celej doby trvania balíčka
- Zľava na pokračovanie testovania po vyčerpaní zakúpeného balíčka
- Pravidelné hlásenia o aktuálnom stave vášho bug bounty programu
- Prispôsobenie cieľov testovania podľa vašich potrieb a technických možností (web, mobilná aplikácia, formulár, časť infraštruktúry, atď.)
- Detailné hlásenia o bezpečnostných zraniteľnostiach nájdených etickými hackermi vrátane popisu ich charakteru, umiestnenia a návrhu na opravu

Náročným korporátnym klientom ponúkame spoluprácu "ušitú na mieru". Neváhajte nás kontaktovať pre viac detailov.

Porovnanie balíkov Hacktrophy

Balík	S	M	L	Na mieru
Cena balíka vrátane odmien pre etických hackerov	**1 299 €**	**1 699 €**	**4 299 €**	**podľa dohody, ku každej vyplatenej odmene sa pripočítava 20% provízia**
Doba trvania balíka	1 rok alebo do minutia odmien pre et. hackerov	1 rok alebo do minutia odmien pre et. hackerov	1 rok alebo do minutia odmien pre et. hackerov	na mesačnej báze alebo do minutia odmien pre hackerov
Obsahuje základný sken zraniteľností?	✗	✓ **bez** manuál. preverenia nájdených zraniteľností	✓ **s** manuál. preverením nájdených zraniteľností	podľa dohody
Pomôžeme vám s nastavením testovacieho projektu a odmien pre hackerov	✓	✓	✓	podľa dohody
Je podpora zo strany moderátora súčasťou balíka?	✓	✓	✓	za príplatok 200€ / mes.
Propagácia vášho projektu v komunite etických hackerov na Hacktrophy	e-mail min. 3 x	e-mail 3 x + soc. siete + garancia prizvania min. 10 et. hackerov	e-mail 4 x + soc. siete + garancia prizvania min. 15 et. hackerov	e-mail 1 x mesačne + podľa dohody
Možnosť vyplácať odmeny v rôznych menách či kryptomenách	✓	✓	✓	✓
Detailné hlásenia od hackerov o nájdených bezpečnostných dierach	✓	✓	✓	✓
Manuálne overenie nahlásených bezpečnostných dier moderátorom	✓	✓	✓	v prípade zakúpenia moderátora
Mesačné prehľady o priebehu testovania	✗	✓	✓	✗
Zľava na ďalší testovací balík po minutí prvého balíka	3%	4%	6%	✗

Kto stojí za Hacktrophy

Za projektom stoja etablovaní hráči vo sfére IT bezpečnosti s pozadím vo firmách ako Citadelo, Nethemba alebo ESET. Aj vďaka nim si môžete byť istí, že od Hacktrophy dostanete presne to, čo očakávate.

Miroslav Trnka

zakladateľ spoločnosti ESET,
jedného z popredných
antivírusových riešení na svete.

Tomáš Zaťko

CEO Citadelo,
ktorá sa špecializuje na informačnú bezpečnosť
podnikov akejkoľvek veľkosti.

Pavol Lupták

CEO Nethemba,
ktorá sa už viac ako 10 rokov zameriava
na bezpečnosť webových aplikácií
a penetračné testovanie.

Juraj Bednár

spoluvlastník Citadelo

Kontakt

Roman Jazudek

CEO Hacktrophy

jazudek@hacktrophy.com

+ 421 948 09 09 08

Lukáš Suchoba

Sales Representative

suchoba@hacktrophy.com

+ 421 948 46 69 37

Hacktrophy, s.r.o.

Lazaretská 12, 811 08 Bratislava

Viac informácií nájdete na

Hacktrophy.com