hacktrophy

New Approach to Internet Security

Hacktrophy is a modern way to test the security of your webs or applications effectively through so-called bug bounty programs. With a large number of ethical hackers, you will discover security vulnerabilities in a time and secure sensitive data before it can be misused.

www.hacktrophy.com

Why should you care about IT security?

There is **86 % chance that your website** contains at least one critical vulnerability. Every day, black-hat hackers steal about 5 million sensitive records all around the world.

The average cost of a data breach is $1.3 million **for enterprises and $117,000 for small and medium-sized businesses** (SMBs).

Almost **2/3 of small and medium-sized** businesses reported a cyber attack in 2017, and 54% of such businesses were the victims of the sensitive data theft.

Since May 2018, companies failing to comply with the rules of the new personal data protection directive (GDPR) might be fined **up to EUR 20 million or 4% of annual turnover.**

What are the possible consequences of a successful hacker attack on your website?

Black-hat hacker attacks present an everyday reality

Bad hackers attacked the UK TalkTalk operator system and, thanks to a simple SQL Injection, stole data of 150,000 customers, including 15,000 payment data. **The operator had to pay a fine of 400,000 £ (€ 445,000) and suffered a loss of reputation.**

1

Zomato – the restaurant search and rating service became a target of a hacker attack in 2017. The black-hat hacker **stole e-mails and passwords of 17 million users from its servers, and was selling themonline for $ 1,000**. The company has suffered great damage to reputation.

2

Russian websites of Rambler.ru and VK.com have become targets of hackers who **stole data from 100 million users from each server** due to security vulnerabilities. All 200 million accounts were then sold over the Internet.

3

At the end of 2016, the black-hat hacker attacked Dailymotion servers due to lack of security and **gained 85.2 million users' unique email addresses**. The reputation of server was damaged and some part of clients has probably never come back.

4

Hacktrophy will increase your IT security

Procedure is simple – you will advertise a reward for finding of vulnerabilities in your applications via Hacktrophy. Registered ethical hackers will do their best to find them before they could be misused.

The reward will be paid only for real security vulnerabilities. Testing is done in such a way that it does not endanger the normal operation of the website (e.g. via your test account or in the test environment).

How does Hacktrophy work?

1. We will help you determine where and what should ethical hackers look for, and also set the right rewards for them.
2. Ethical hackers will start testing your application or website.
3. As soon as they find vulnerability, they will report it to you.
4. We will examine whether it is a relevant vulnerability. If so, we will accept a report and you will fix the problem.
5. We will pay the hacker from the money in the package you have purchased.
6. Ethical hackers will look for other vulnerabilities until there is the credit in your package.

The benefits of Hacktrophy bug bounty programme

Long-term safety testing

Ethical hackers test your website or app throughout the year, or until there is credit in your prepaid package.

Cost effectiveness and delivery quality

You pay only for the vulnerabilities that are actually in the system, they are reviewed by our moderator and meet the requirements of your program.

Variety of testers from around the world

Your online product or service is tested by tens of hundreds of security experts, so-called ethical hackers.

Testing is under your control

You determine what an ethical hacker can test, in what environment (test or production) and into what depth of your system.

Testers' expertise

The skills of ethical hackers in the field of IT security testing are more extensive than of regular IT staff.

Manual testing and verification

Your security is tested by real people with unique knowledge, not automated robots or scans.

What can you test through Hacktrophy?

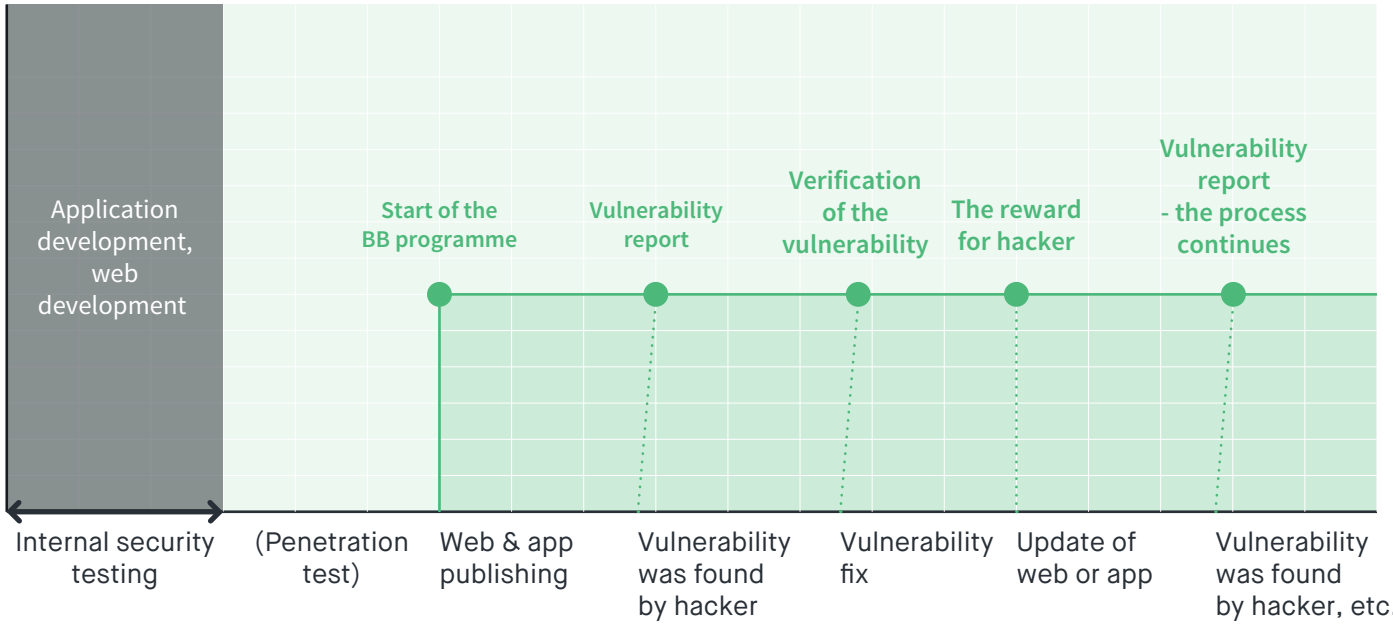
Any web, application, or interface available over the Internet:

- websites that work with sensitive data from you or your clients,
- e-shops, betting portals, online marketplaces,
- CMS kernels,
- CRM and accounting systems, cloud, IoT solutions,
- mobile apps or games,
- Internet banking, crypto currency markets and payment gateways,
- business or industrial systems that are connected to the Internet.

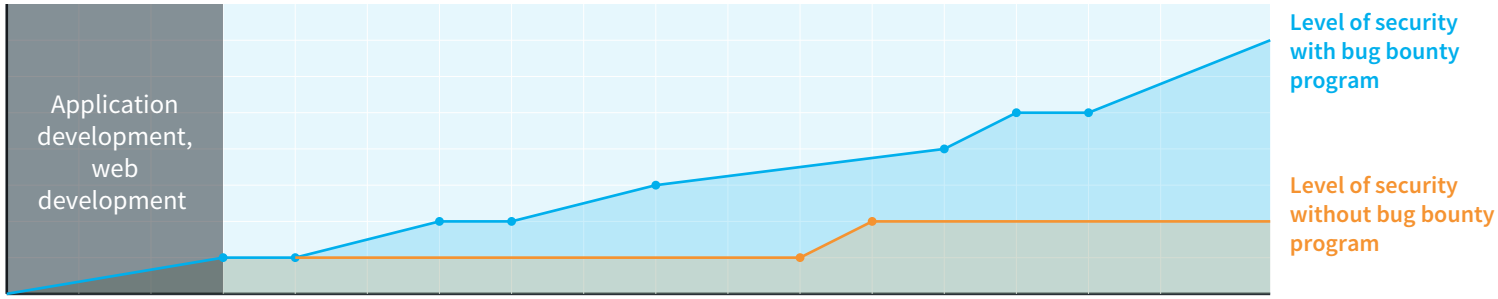
It is possible to test not only the errors caused by the programming or software used, but also the setting of the infrastructure on which the web or the application are running. Testing can take place in production or test environments.

Security testing process

BUG BOUNTY PROGRAM HACKTROPHY

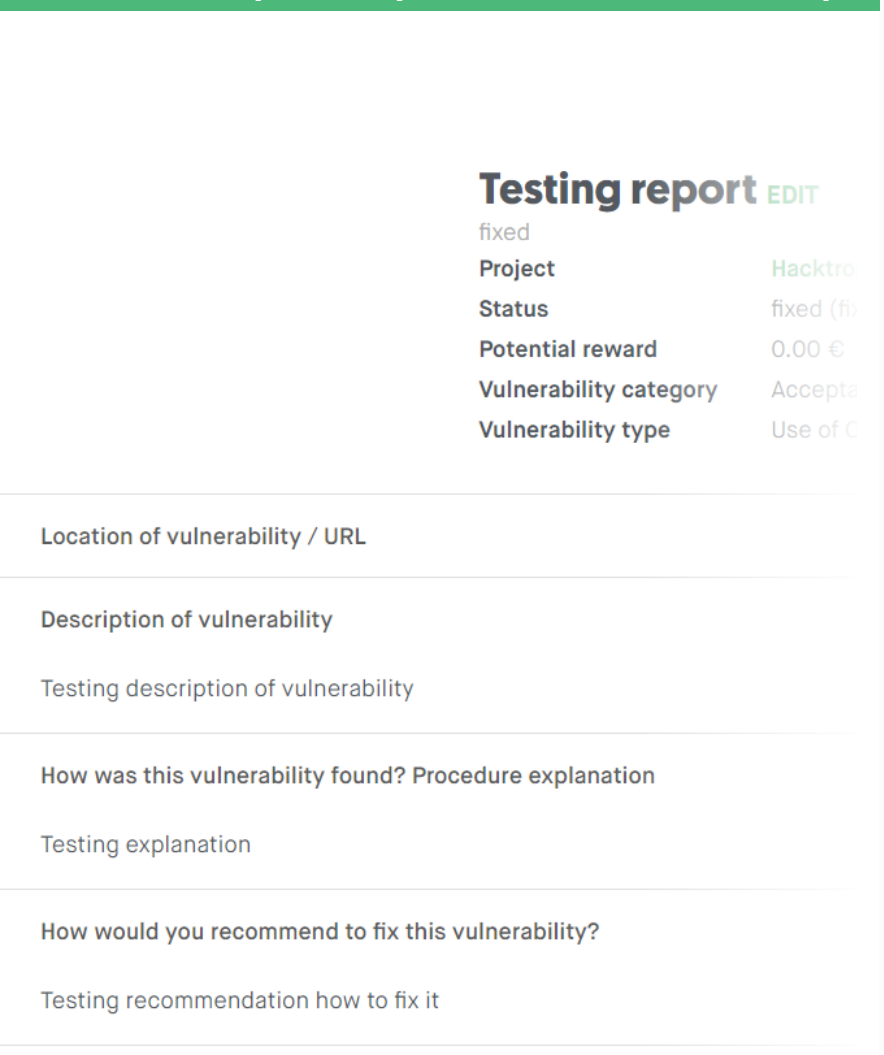


SECURITY LEVEL



What do you get from ethical hackers?

Preview sample of report of found vulnerability



TOP 5 vulnerabilities reported in 2017 via Hacktrophy

- **Specific vulnerabilities (10,35 %)**
  Vulnerabilities not found in OWASP TOP 10 ratings, but poses a high risk of attack.
- **SPF configuration problems (5,52 %)**
  Error in the email server settings that allows you to perform email spoofing.
- **XSS (4,83 %)**
  It represents the possibility of inserting malicious code into a website for the purpose of its subsequent use on the terminal devices of visitors to the theft of sensitive data.
- **CSRF (4,16 %)**
  An attack that allows a user to open a site containing a malicious request. This can lead to identity theft or sensitive user data.
- **Session fixation (4,16 %)**
  This is an attack that allows an attacker to steal a valid session of the user, which is then redirected to the attacker's server.

Comparison of penetration tests and Hacktrophy

	PENETRATION TEST	HACKTROPHY
Time	**Low.** One or several ethical hackers for limited time.	**High.** A large group of ethical hackers without a time limit. You only pay for results.
Effort	**Medium.** It is quite difficult to submit a task. Final report is the priority.	**Low.** You will be given a moderator to help you with the setting of bug bounty project. You are continuously getting verified vulnerability reports.
Quality of found vulnerabilities	**High.** Depending on quality of pen-test provider.	**High.** Several hackers mean various types of experiences and forms of hacking.
Expenses/vulnerability	**High.** Consultants are expensive and their time is limited.	**Medium.** Hacktrophy will advise you with all the rewards. You pay only for verified vulnerabilities.

You can find a detailed comparison in our blog

Choose one of the testing methods

Package S

Ideal for a simple web or application with minimal amount of sensitive data.

Valid for 1 year, or until the rewards for ethical hackers are spent

1 299 €

including rewards for ethical hackers

WE RECOMMEND

Package M

Ideal for a company website that processes some sensitive data, e.g. after registration.

Includes automated vulnerability scan!

Valid for 1 year, or until the rewards for ethical hackers are spent

1 699 €

including rewards for ethical hackers

Package L

Ideal for the web or app that works with finances or multiple sensitive data.

Contains an automated vulnerability scan with **manual verification!**

Valid for 1 year, or until the rewards for ethical hackers are spent

4 299 €

including rewards for ethical hackers

Each package automatically includes:

- Long-term security testing by a community of more than 350 ethical hackers from around the world
- Flexible setting of rewards for ethical hackers, depending on the severity of the vulnerabilities that are being searched
- Manual verification of reported vulnerabilities by assigned moderator
- Support from the moderator when creating and managing your bug bounty program over the entire duration of the package
- Discount for testing after the termination of purchased package
- Regular reports of the current status of your bug bounty program
- Customizing the test objectives to suit your needs and technical capabilities (web, mobile app, form, cast infrastructure, etc.)
- Detailed reports of security vulnerabilities found by ethical hackers, including a description of their nature, location, and repair proposal.

We offer the custom-made cooperation to demanding corporate clients. Do not hesitate to contact us for more details.

Comparison of Hacktrophy packages

Package	S	M	L	Custom-made
Package price including fees for ethical hackers	**1 299 €**	**1 699 €**	**4 299 €**	**based on agreement, 20% commission is charged to each reward**
Package Validity	1 year, or until the rewards for ethical hackers are spent	1 year, or until the rewards for ethical hackers are spent	1 year, or until the rewards for ethical hackers are spent	on a monthly basis, or a until the rewards for ethical hackers are spent
Does it contain a basic vulnerability scan?	✗	✓ **without** manual verifi. of found vulnerabilities	✓ **with** manual verifications of found vulnerabilities	based on the agreement
We'll help you set up a test project and hacker rewards	✓	✓	✓	based on the agreement
Is support from the moderator part of the package?	✓	✓	✓	for an extra charge of 200 € / month.
Promotion of your project in the Hacktrophy ethical hacker community	e-mail minimum 3 x	e-mail 3 x + social media + call guarantee for minimum of 10 ethical hackers	e-mail 4 x + social media + call guarantee for minimum of 15 ethical hackers	1 e-mail per month + by agreement
The option to pay rewards in different currencies or crypto currencies	✓	✓	✓	✓
Detailed reports from hackers about security vulnerabilities found	✓	✓	✓	✓
Manual verification of reported security vulnerabilities by moderator in the event of a moderator purchase	✓	✓	✓	in case of purchase of moderator
Monthly reviews of the course of the test	✗	✓	✓	✗
Discount for the next test package after spending the first one	3%	4%	6%	✗

People behind Hacktrophy

There are prestigious IT security experts behind Hacktrophy with the background in companies such as Citadelo, Nethemba and ESET. These ensure that you will get exactly what you expect from Hacktrophy.

Miroslav Trnka

co-founder of ESET

Tomáš Zaťko

CEO Citadelo

Pavol Lupták

CEO Nethemba

Juraj Bednár

co-owner Citadelo

Contact

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, Slovakia

More information you will find:

www.hacktrophy.com