
دوازدهمین دوره
جشنواره
لینوکس
امیرکبیر
انجمن علمی دانشکده مهندسی کامپیوتر دانشگاه صنعتی امیرکبیر برگزار می کند:
24-26 Feb 2021

How can we make the internet safer?

Open Bug Bounty Project

Who am i?

Cyber Security Consultant
Co-Founder at Ravro.ir

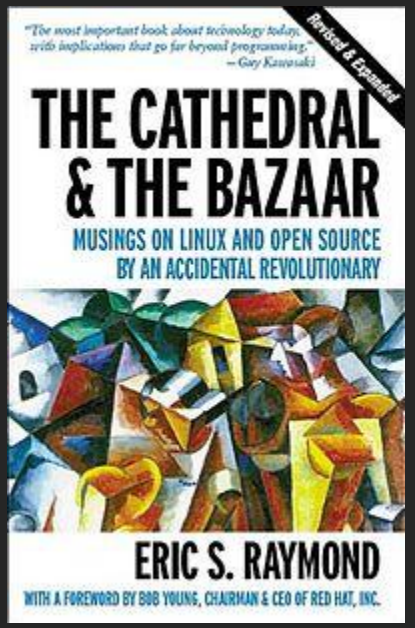
MohmmadAmin Kariman

Agenda

- Linus’s law
- Software Bug vs Vulnerability!
- What is Bug Bounty?
- History
- Bug Bounty Platform
- VDP
- IBB
- Open Bug Bounty
- RoadMap

Linus's law

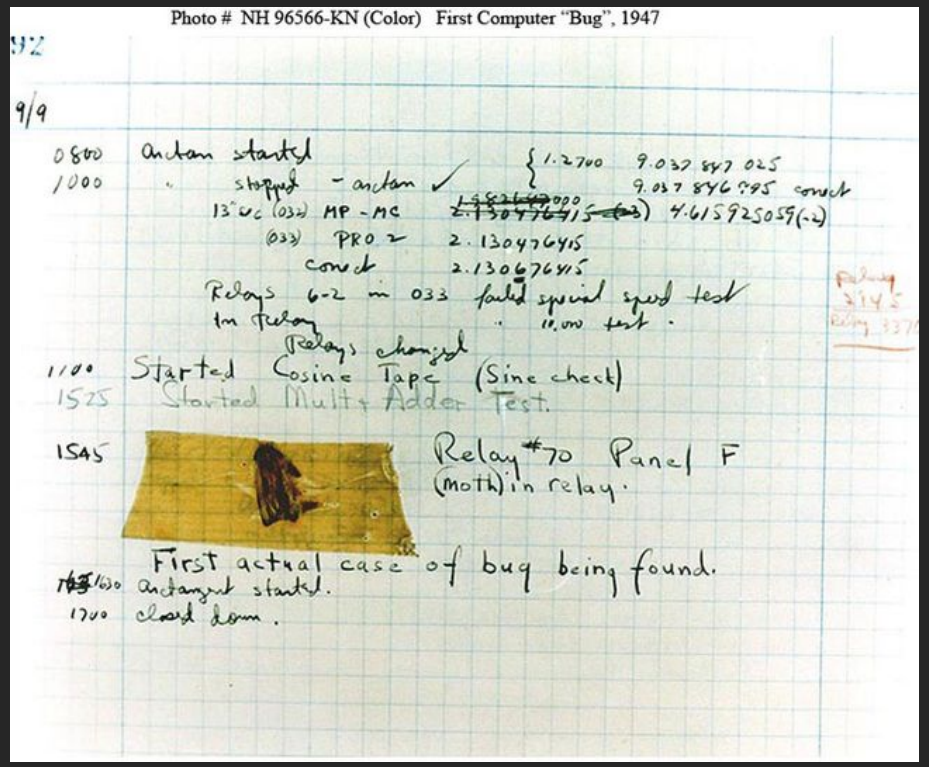
> “Given enough eyeballs, all bugs are shallow”.
>
> Eric S. Raymond, The Cathedral and the Bazaar



Software **Bug vs Vulnerability?**

A bug is *any* defect in a product.

Vulnerability is a subset of **bug**.

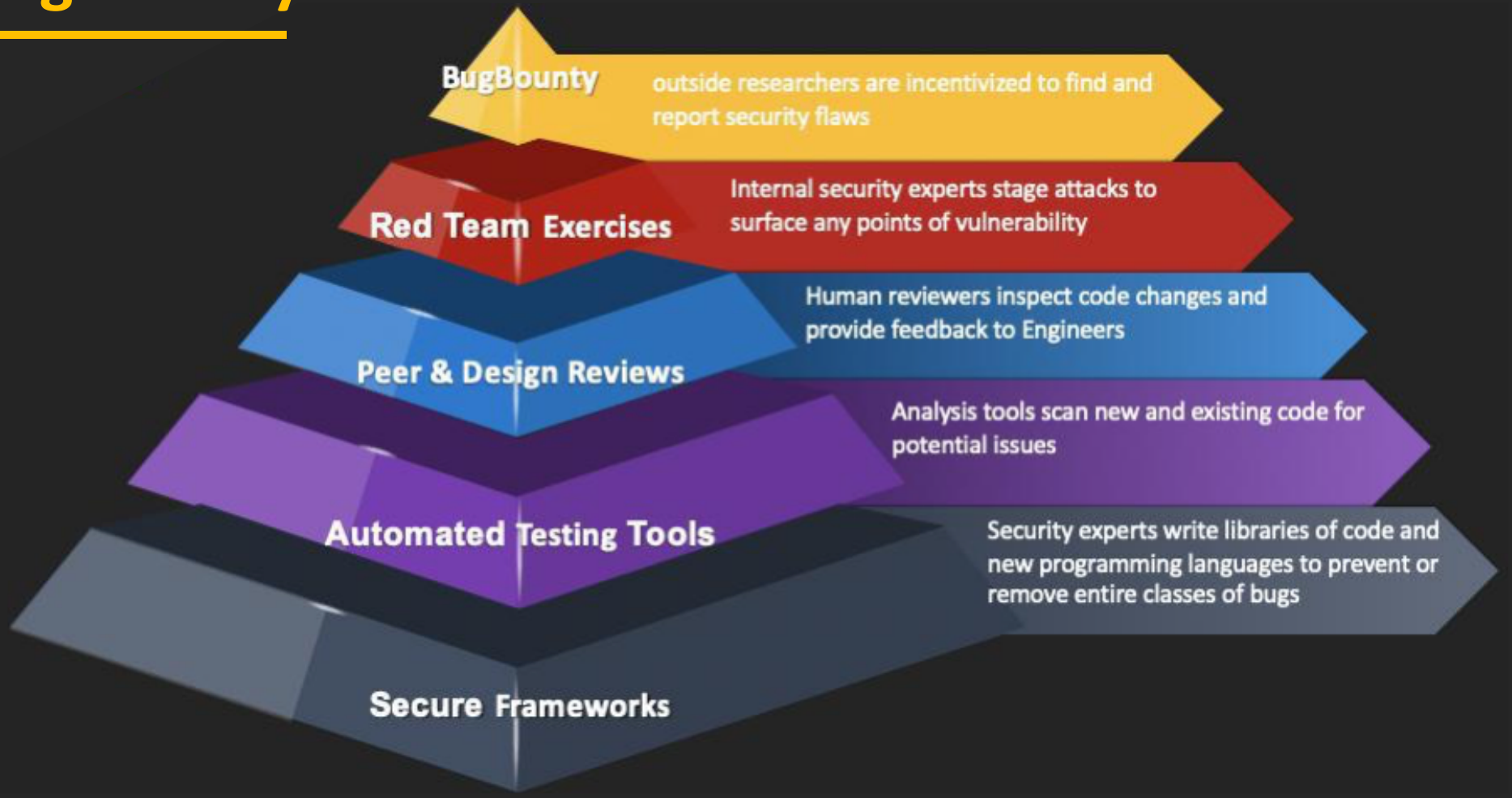


Software **Bug vs Vulnerability?**

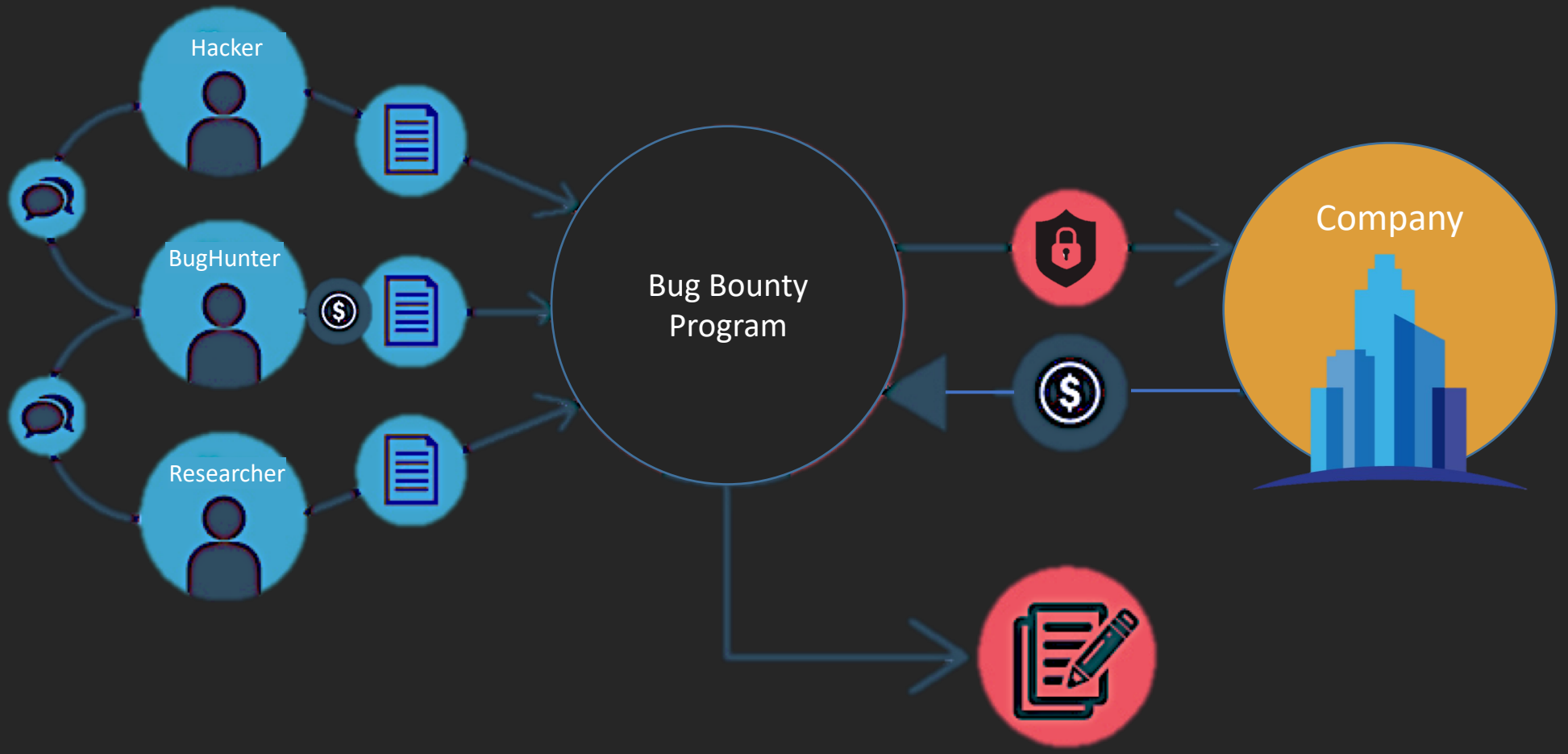
A bug is when a system isn't behaving as it's designed to behave.

A vulnerability is a way of abusing the system (most commonly in a security-related way) - whether that's due to a design fault or an implementation fault. In other words, something can have a vulnerability due to a defective design, even if the implementation of that design is perfect.

Bug Bounty?


BugBounty
outside researchers are incentivized to find and report security flaws
Red Team Exercises
Internal security experts stage attacks to surface any points of vulnerability
Peer & Design Reviews
Human reviewers inspect code changes and provide feedback to Engineers
Automated Testing Tools
Analysis tools scan new and existing code for potential issues
Secure Frameworks
Security experts write libraries of code and new programming languages to prevent or remove entire classes of bugs

Bug Bounty?



History?

۱۹۴۷ NetScape

۱۹۹۵

۲۰۰۴ Mozilla

۲۰۰۷ Google

۲۰۱۰

۲۰۱۱ HackerOne

۲۰۱۲

۲۰۱۴

۲۰۱۵ Open Bug Bounty

Hack The Pentagon,
24Day,138,$70,000
Hack the Army

۲۰۱۶

۲۰۱۷ synack

PWN2OWN

Facebook

BugCrowd

Microsoft

Bug Bounty Paltfrom?

bugcrowd

INTIGRITI
ETHICAL HACKING PLATFORM

hackerone

openbugbounty

YES WE HACK

safehats
Managed Bug Bounty

Bug Bounty Program?

https://www.google.com/about/appsecurity/reward-program/

https://www.intel.com/content/www/us/en/security-center/default.html

https://www.microsoft.com/en-us/msrc/bounty?rtc=1

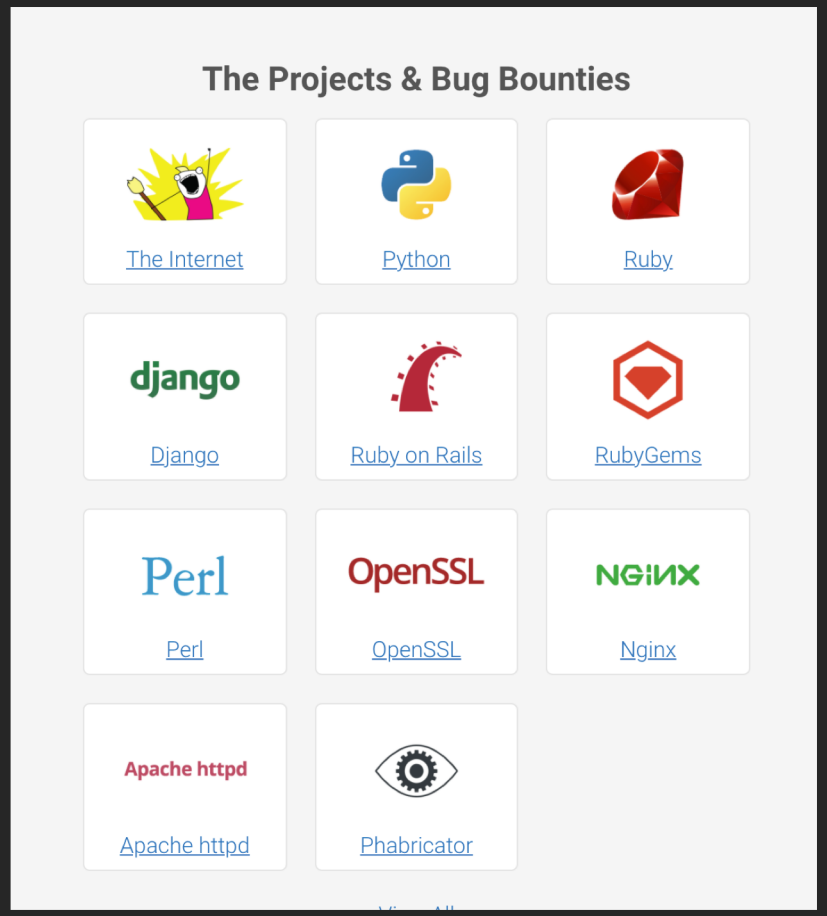
https://bounty.github.com/

https://www.facebook.com/whitehat

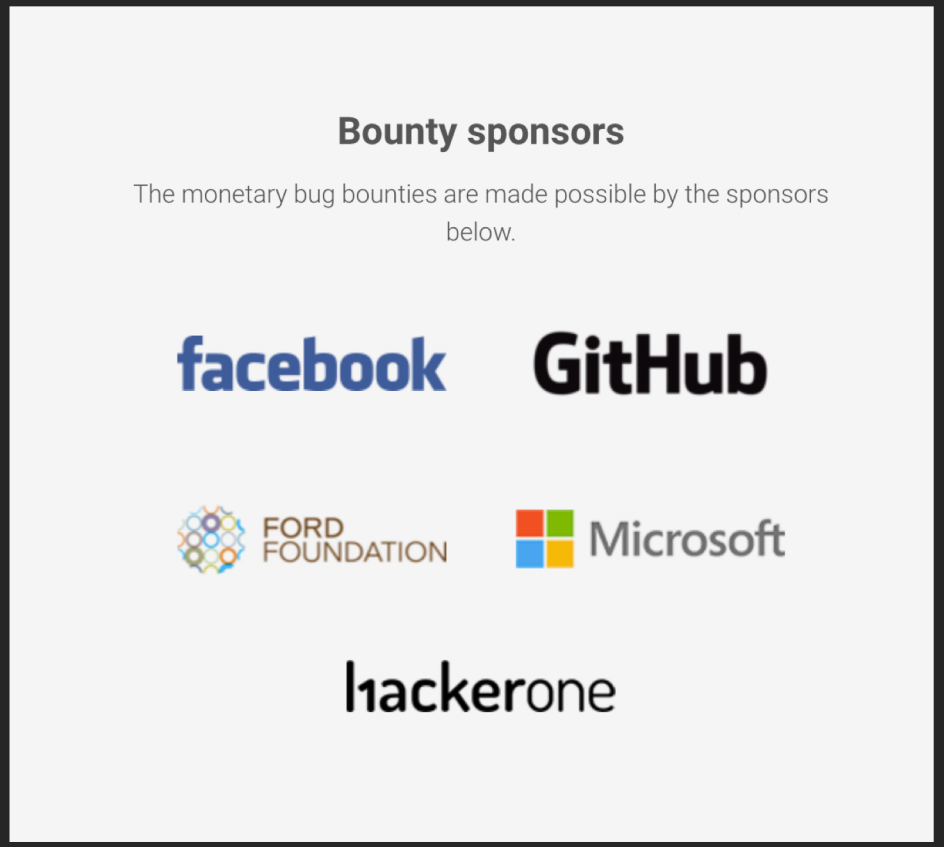
Internet Bug Bounty (IBB)

The Internet Bug Bounty has rewarded **788K+** in bounties to **245** friendly hackers for uncovering **923** flaws that have helped improve the security of the Internet:

ImageTragick ($7.5k)
Heartbleed ($15k)
Shellshock ($20k)



IBB Sponsors



Vulnerability Disclosure Policy (VDP)

a structured, easy and accessible way for anyone to report vulnerabilities

ISO 29147

Open Bug Bounty?

Open Bug Bounty is a non-profit platform designed to connect security researchers and website owners in a transparent, respectful and mutually valuable manner.

Our purpose is
to make the Web a safer place for everyone’s benefit.

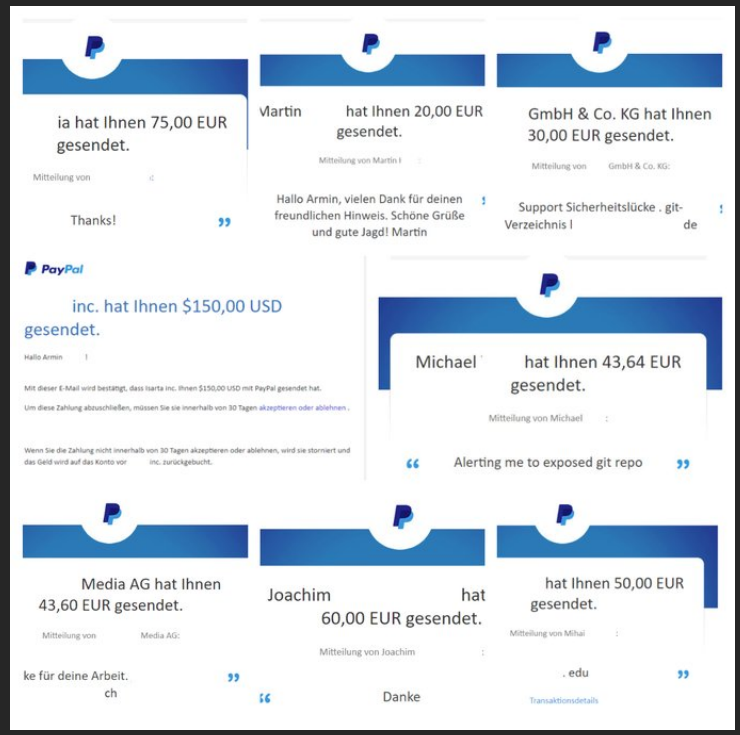
Open Bug Bounty?

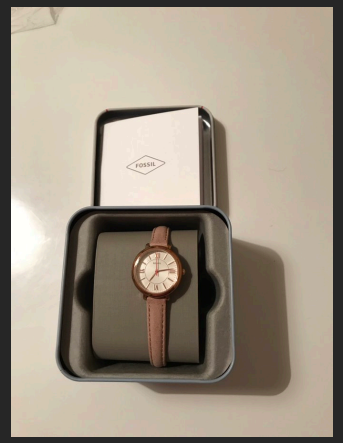
> We only accept Cross-Site Scripting, CSRF and some other vulnerabilities that figure among the most common web application vulnerabilities today

Open Bug Bounty?

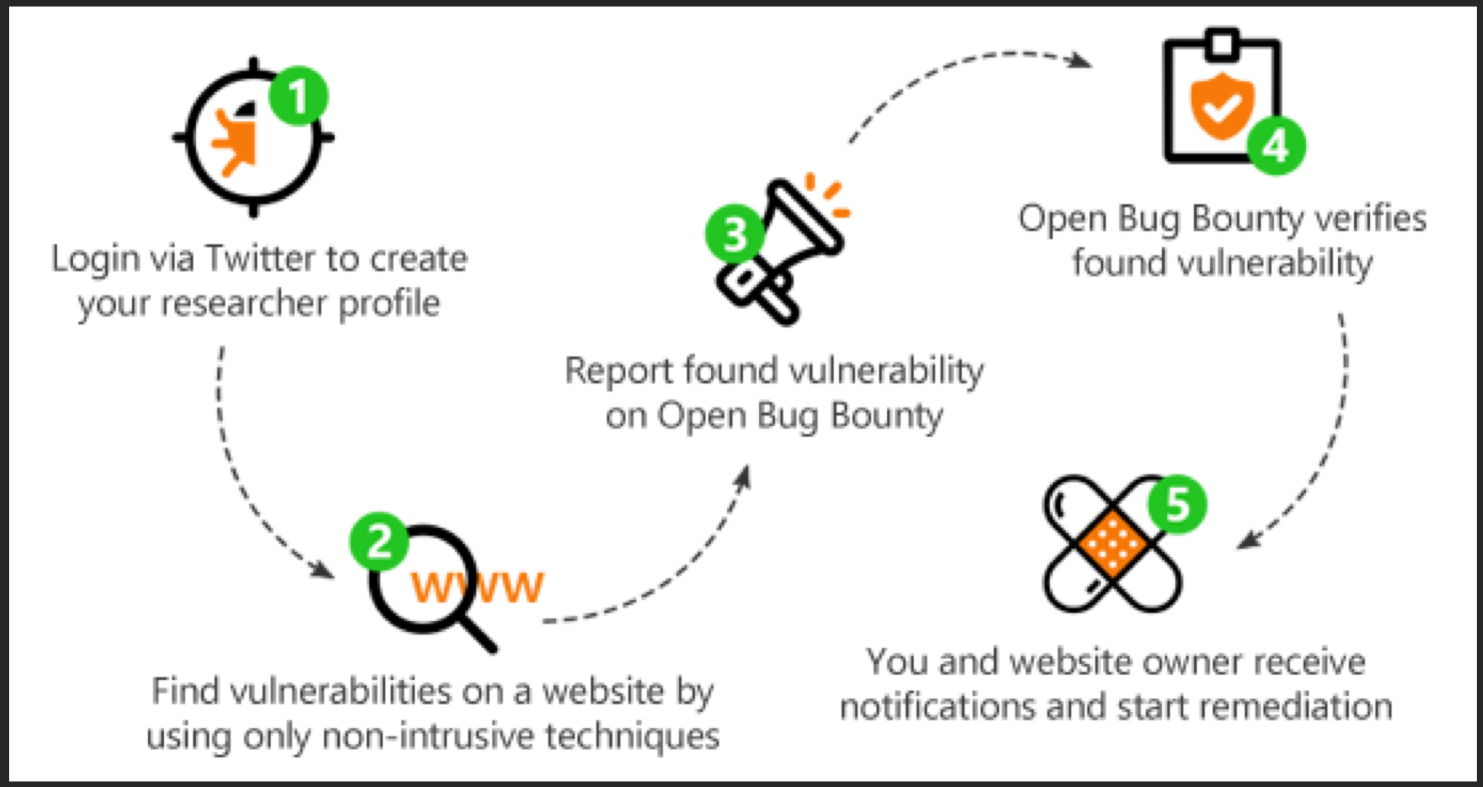
814,955 coordinated disclosures
462,133 fixed vulnerabilities
1273 bug bounties with 2,431 websites
21,581 researchers, 1276 honor badges

Open Bug Bounty Awards

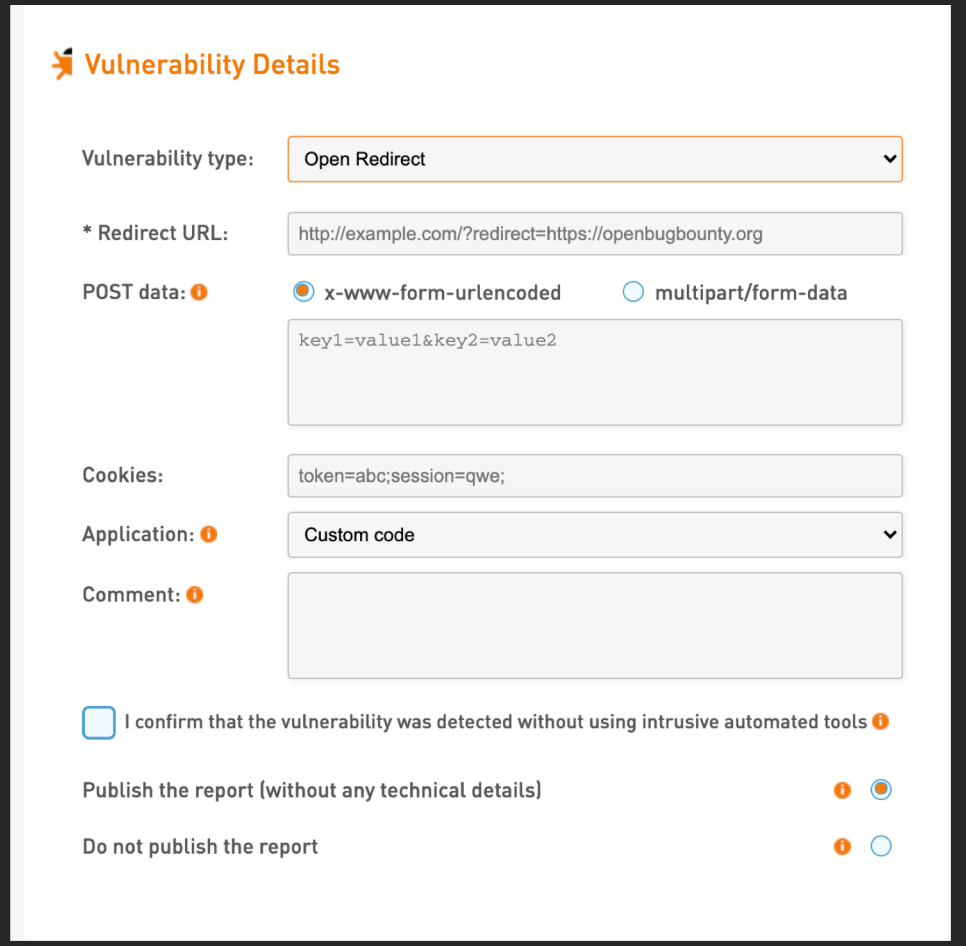




Open Bug Bounty for Security Researchers



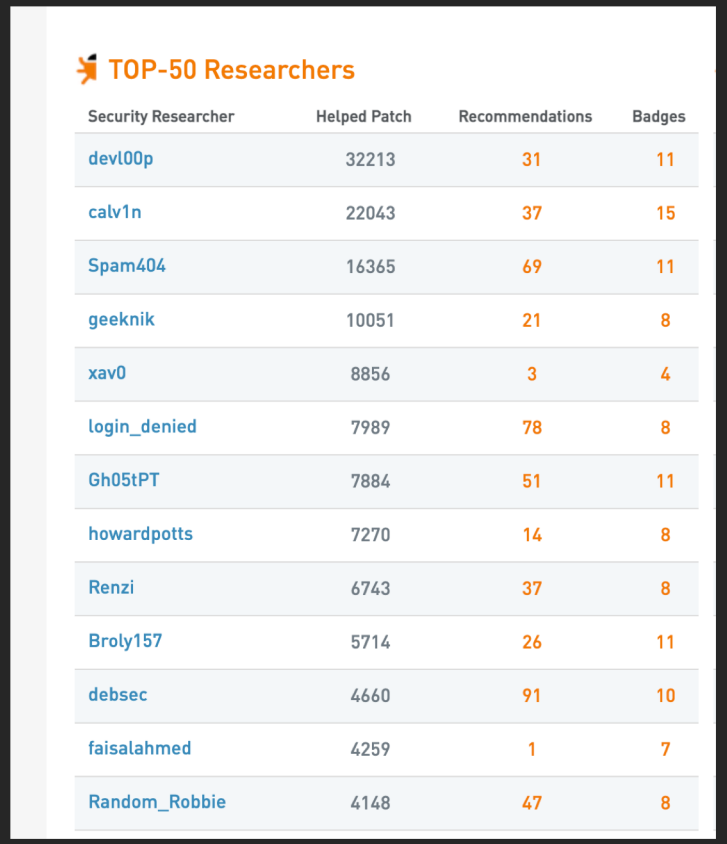
Open Bug Bounty for Security Researchers



Open Bug Bounty for Security Researchers

Affected Website:	ambrosia22.ascsa.edu.gr
Open Bug Bounty Program:	Not created yet
Vulnerable Application:	[hidden until disclosure]
Vulnerability Type:	XSS (Cross Site Scripting) / CWE-79
CVSSv3 Score:	[hidden until disclosure]
Disclosure Standard:	Coordinated Disclosure based on ISO 29147 guidelines
Discovered and Reported by:	devl00p
Remediation Guide:	OWASP XSS Prevention Cheat Sheet

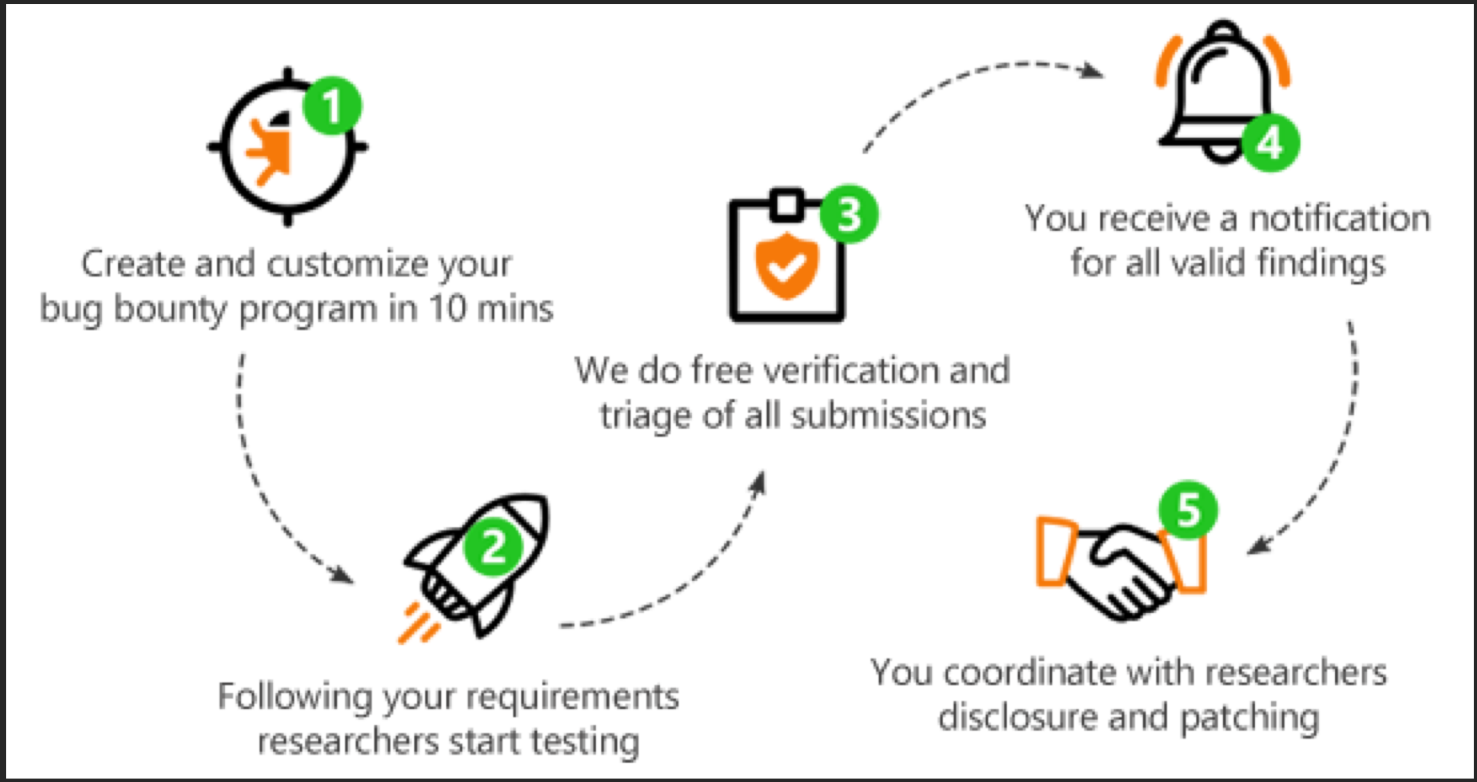
Open Bug Bounty for Security Researchers



TOP-50 Researchers

Security Researcher	Helped Patch	Recommendations	Badges
devl00p	32213	31	11
calv1n	22043	37	15
Spam404	16365	69	11
geeknik	10051	21	8
xav0	8856	3	4
login_denied	7989	78	8
Gh05tPT	7884	51	11
howardpotts	7270	14	8
Renzi	6743	37	8
Broly157	5714	26	11
debsec	4660	91	10
faisalahmed	4259	1	7
Random_Robbie	4148	47	8

Open Bug Bounty for Website Owners



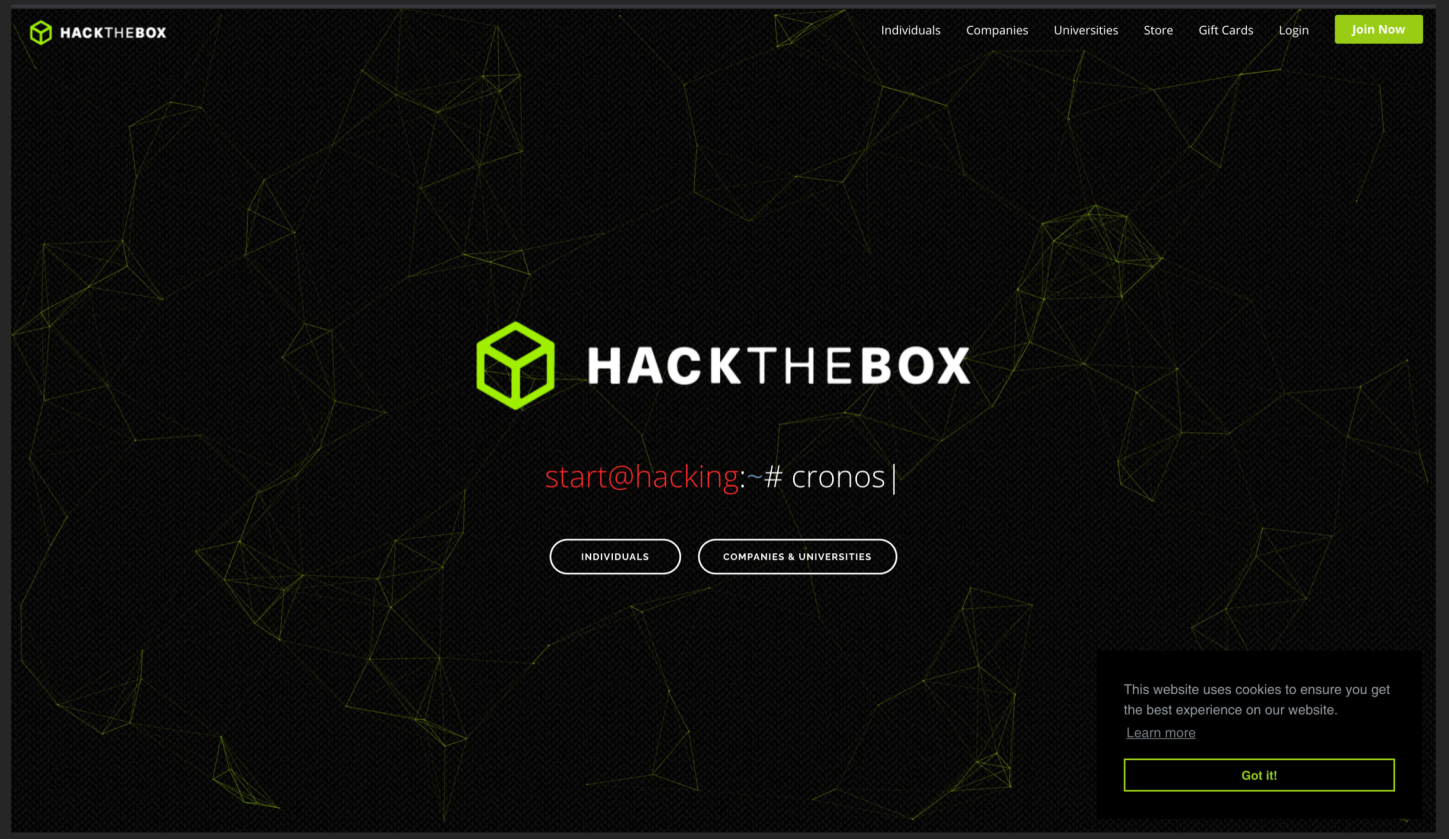
RoadMap

https://github.com/sundowndev/hacker-roadmap

RoadMap


Try Hack Me
Login
Join Now
Cyber Security Training
Making it easier to break into security, all through your browser.
Guides
Develop your skills by working through hands-on guided tasks and supporting videos.
0101
010
01
Challenges
Learn and test your skills with gamified, real-world cybersecurity challenges.

RoadMap


HACKTHEBOX
Individuals
Companies
Universities
Store
Gift Cards
Login
Join Now
HACKTHEBOX
start@hacking:~# cronos|
INDIVIDUALS
COMPANIES & UNIVERSITIES
This website uses cookies to ensure you get the best experience on our website.
Learn more
Got it!

Q ?