

Forum: [Hack Forums](#)

Thread: [An Introduction to Bug Bounties.](#)

illuminati? - June 2, 2024, 8:01 pm

An Introduction to Bug Bounties

What is a Bug Bounty?:

A bug bounty is a reward offered by organizations/companies to individuals/teams who identify and report security vulnerabilities in their software or systems, which helps companies/organizations with keeping their security update to date. It's a proactive approach to discovering and fixing flaws before malicious actors can exploit them.

Why do companies offer/have bug bounty programs?:

They offer/have these bug bounties for a different variety of reasons, some may include;Enhancing Security: By utilizing the community of ethical hackers, and security researchers, this allows companies to identify and fix vulnerabilities that were potentially missed by their internal team(s).

Cost: Offering bug bounties can be extremely cost effective for companies, where people can submit exploits/vulnerabilities, instead of the company having to hire full-time security "Experts" or sub-contracting it out to security firms. You would be paying per exploit, rather than full time salaries.

Continuous testing: Rather than doing periodic security audits, bounties allow for continuous testing, ensuring anything exploit/vulnerability wise can be identified and addressed rather quickly, opposed to random audits (that could happen quarterly, bi-annual, etc.).

Engagement within the community: These programs can help build engagement within the

Cyber-community, and it helps demonstrate that they have a commitment to their security, and these can in theory lead to increased trust from the community and, future customers/partners.

Standards/Compliance: A vast majority of industries have standards and regulations, that may require regular security testing, and with more companies being hacked, and exploited, these requirements are going to continue to get more strict. Bug bounty programs can help companies meet their requirements for these standards/regulations.

Access to diverse skill sets: Things like bug bounty programs attract a lot of talent. These talents can be a different wide range of skills & perspectives, that could potentially be something that the company doesn't have within their internal team. Which in theory could be a way for them to discover future potential employees.

Early Detection: Programs like these allows for the potential of exploits/vulnerabilities being found earlier, allowing for early fixes/patches/preventative maintenance. Which can help with reducing the risk of data breaches, financial losses, and damage to a companies reputation.

Improvement/Innovation: Bug Bounty programs usually allow for feedback from the community, and this can help with providing insights into improvements/innovative practice(s) that a company may not have considered/thought of.

Marketing/Public Relations: Running a bug bounty program, allows you to address vulnerabilities with transparency which can help enhance a companies reputation/image, and it shows that they are taking security/customer data protection seriously.

How do Bug Bounties Work?:

Generally speaking, companies will set-up Bug Bounty Programs on their website, or another site (example: [HackerOne](#), where they will specify certain things such as; Scope: Which of their system(s)/software(s)/platform(s) that they deem are eligible for the program.

Rules: This will be the companies guidelines for reporting bugs.

Rewards: This can/will be payment, or recognition for reports they deem are valid.

Any other information that may be applicable.

Different Type(s) of Bug Bounty Programs:
Public: Public Bug Bounty programs are open to anyone. Public programs attract larger numbers of researchers/ethical hackers, and can end up with potentially more reports.

Private: Private Bug Bount Programs, are Invite only programs. These are smaller programs, and are generally only trusted researchers/ethical hackers, and are in a more "controlled" testing

environment.

List of Popular Bug Bounty Platforms: [HackerOne](#)

[Bugcrowd](#)

[Synack](#)

[Open Bug Bounty](#)

What are the benefits of participating in Bug Bounties?:

For Ethical Hackers & Security Researchers: Financial Incentives/Compensation

Professional/Community Recognition

The possibility for Skills development

Opportunity for networking

Etc.

For Companies: Patch/fix/acknowledge vulnerabilities at a faster rate.

The ability to discover more severe vulnerabilities/exploits.

Networking (the ability to find potential new-hires for inhouse)

The list goes on and on.

List of Common Vulnerabilities Discovered:(XSS) - Cross-Site Scripting: A Vulnerability that allows attackers to inject malicious scripts into various webpages.

SQL Injection: Exploits vulnerabilities in databases.

(RCE) - Remote Code Execution: Allowing attackers to execute arbitrary code on a server.

Broken Authentication: Enables/allows attackers to impersonate other users.

General challenges of running/participating in Bug Bounties:

Here is a small list of the general challenges of running and/or participating in Bug bounties; Quality of Reports: More often than not, trying to filter high quality submissions/reports can be extremely time-consuming. Keeping this in mind, not all of the reports that companies/organizations get are useful, which can lead to delays.

Scope: Basically, defining and maintaining a clear scope is essential to help avoid unmanageable workloads.

Legal Related Issues: Ethical Hackers/Security Researchers need to ensure that they operating within legal boundaries, and that they are respecting the rules of the program.

The list can go on and on.

How to get started as a "Bug Hunter:"

List below is a general idea of how to get started: You need to learn the basics: You will need to have an understanding of common vulnerabilities and web security principles.

Practice is key: Using platforms such as; [HackTheBox](#), [Hacker101 - CTF](#), [TryHackMe](#), and other CTF Competitions to help you hone your abilities/craft.

Join different programs: Obviously you're not going to start with the harder programs right away, so you're gonna want to start with the easier programs, (i.e. Public programs, find a mentor, or a team that'll help you build your skills), this will help you build some experience, potentially learn some new skills, and some credibility.

Networking: This can be a big help when you're first trying to get started. You can try engaging with the Cyber-security community through the use of forums, social media, and various events that are held throughout the world.

The list can go on and on.

Here's a list of resources for Bug Hunters: [TryHackMe](#): A good place to start for people who are interesting in learning.

[HackTheBox](#): Another amazing place to get started.

[Hacker101 - CTF](#) Another good place to start with.

[OWASP - Open Web Application Security Project](#): Offers Guidelines, tools, and information related to Web-Security.

[PortSwigger's: Web Security Academy](#): Offers Free online training and resources related to Web-Security.

Will continue to update the list.

List of Bug Bounty Sites: [HackerOne](#)

[Bugcrowd](#)

[Synack - Red Team](#)

[Detectify](#)

[Open Bug Bounty](#)

[Zero Copter](#)

[Yes We Hack](#)

[HackenProof - Crypto](#)

[Vulnerability Lab](#)

[Fire Bounty](#)

[Bug Bounty \(JP\)](#)

[Intigriti](#)

[safehats](#)

[Redstorm](#)

[CyberArmy \(IND\)](#)

[Bug Bounty - Switzerland](#)

[Apple - Bug Bounty](#)

[Google - Bug Hunter](#)

[Xbox - Bug Bounty Program \(Microsoft\)](#)

[Microsoft - Bounty Program](#)

Comment below with links;

Thanks for reading.

If you feel like this thread is missing something, or if you have relevant information that could help others, please comment below (I will update it, and credit you).

V?rt - June 2, 2024, 8:15 pm

What a great informational thread. Love the list of bounty websites you've compiled.

Pentatonix - June 2, 2024, 8:25 pm

Great thread, it's nice seeing all the sites laid out like that.

Absence - June 2, 2024, 8:38 pm

Thank you for the info on Bug Bounties!

Bastille - June 2, 2024, 11:21 pm

Thanks for this amazing thread, learned a lot.

I'm not into bug bounties but thought that the vulnerabilities discovered would be more advanced, didn't expect that the most discovered would be the most easy to discover such as SQLi, RCE, XSS. Thought that the dev/programmers would have some security guys during the development to check, at least, the common vulnerabilities.

I also heard that some companies struggles to pay, and for some of them when a critical vulnerability is discovered they usually under evaluate the rank of the vulnerability to pay less (as, if I remember well, the reward is usually indexed on the criticality of the vulnerability)

illuminati? - June 3, 2024, 12:24 pm

(Jun 2, 2024 08:15 PM)V?rt Wrote: [\[CITE\]](#) What a great informational thread. Love the list of bounty

websites you've compiled.
Thank you :).

(Jun 2, 2024 08:25 PM)Pentatonix Wrote: [\[CITE\]](#) Great thread, it's nice seeing all the sites laid out like that.

Yeah, it should help others navigate a bit better

(Jun 2, 2024 08:38 PM)Absence Wrote: [\[CITE\]](#) Thank you for the info on Bug Bounties!
No worries pal!

(Jun 2, 2024 11:21 PM)Yseurk Wrote: [\[CITE\]](#) Thanks for this amazing thread, learned a lot.

I'm not into bug bounties but thought that the vulnerabilities discovered would be more advanced, didn't expect that the most discovered would be the most easy to discover such as SQLi, RCE, XSS. Thought that the dev/programmers would have some security guys during the development to check, at least, the common vulnerabilities.

I also heard that some companies struggles to pay, and for some of them when a critical vulnerability is discovered they usually under evaluate the rank of the vulnerability to pay less (as, if I remember well, the reward is usually indexed on the criticality of the vulnerability)

Well those the more common bugs that are found apparently. I'm sure there is tons of more complex bugs, but chances of it being the same category is probably on the lower side.

I haven't really heard much about payouts, I would think they'd want to see the severity before making a big payout. If you look at the most recent hacking event that took place in Vancouver, there was some insanely priced bugs that were hunted successfully. One feller took over a 6 figure payday.

Perfect - June 3, 2024, 1:40 pm

(Jun 2, 2024 08:01 PM)illuminati? Wrote: [\[CITE\]](#)

An Introduction to Bug Bounties

What is a Bug Bounty?:

A bug bounty is a reward offered by organizations/companies to individuals/teams who identify and report security vulnerabilities in their software or systems, which helps companies/organizations with keeping their security update to date. It's a proactive approach to discovering and fixing flaws before malicious actors can exploit them.

Why do companies offer/have bug bounty programs?:

They offer/have these bug bounties for a different variety of reasons, some may include;

Enhancing Security: By utilizing the community of ethical hackers, and security researchers, this allows companies to identify and fix vulnerabilities that were potentially missed by their internal team(s).

Cost: Offering bug bounties can be extremely cost effective for companies, where people can submit exploits/vulnerabilities, instead of the company having to hire full-time security "Experts" or sub-contracting it out to security firms. You would be paying per exploit, rather than full time salaries.

Continuous testing: Rather than doing periodic security audits, bounties allow for continuous testing, ensuring anything exploit/vulnerability wise can be identified and addressed rather quickly, opposed to random audits (that could happen quarterly, bi-annual, etc.).

Engagement within the community: These programs can help build engagement within the Cyber-community, and it helps demonstrate that they have a commitment to their security, and these can in theory lead to increased trust from the community and, future customers/partners.

Standards/Compliance: A vast majority of industries have standards and regulations, that may require regular security testing, and with more companies being hacked, and exploited, these requirements are going to continue to get more strict. Bug bounty programs can help companies meet their requirements for these standards/regulations.

Access to diverse skill sets: Things like bug bounty programs attract a lot of talent. These talents can be a different wide range of skills & perspectives, that could potentially be something that the company doesn't have within their internal team. Which in theory could be a way for them to discover future potential employees.

Early Detection: Programs like these allows for the potential of exploits/vulnerabilities being found earlier, allowing for early fixes/patches/preventative maintenance. Which can help with reducing the risk of data breaches, financial loses, and damage to a companies reputation.

Improvement/Innovation: Bug Bounty programs usually allow for feedback from the community, and this can help with providing insights into improvements/innovative practice(s) that a company may not have considered/thought of.

Marketing/Public Relations: Running a bug bounty program, allows you to address vulnerabilities with transparency which can help enhance a companies reputation/image, and it shows that they are taking security/customer data protection seriously.

How do Bug Bounties Work?:

Generally speaking, companies will set-up Bug Bounty Programs on their website, or another site (example: [HackerOne](#), where they will specify certain things such as; Scope: Which of their system(s)/software(s)/platform(s) that they deem are eligible for the program.

Rules: This will be the companies guidelines for reporting bugs.

Rewards: This can/will be payment, or recognition for reports they deem are valid.

Any other information that may be applicable.

Different Type(s) of Bug Bounty Programs:Public: Public Bug Bounty programs are open to anyone. Public programs attract larger numbers of researchers/ethical hackers, and can end up with potentially more reports.

Private: Private Bug Bount Programs, are Invite only programs. These are smaller programs, and are generally only trusted researchers/ethical hackers, and are in a more "controlled" testing environment.

List of Popular Bug Bounty Platforms:[HackerOne](#)

[Bugcrowd](#)

[Synack](#)

[Open Bug Bounty](#)

What are the benefits of participating in Bug Bounties?:

For Ethical Hackers & Security Researchers: Financial Incentives/Compensation

Professional/Community Recognition

The possibility for Skills development

Opportunity for networking

Etc.

For Companies: Patch/fix/acknowledge vulnerabilities at a faster rate.

The ability to discover more severe vulnerabilities/exploits.

Networking (the ability to find potential new-hires for inhouse)

The list goes on and on.

List of Common Vulnerabilities Discovered:(XSS) - Cross-Site Scripting: A Vulnerability that allows attackers to inject malicious scripts into various webpages.

SQL Injection: Exploits vulnerabilities in databases.

(RCE) - Remote Code Execution: Allowing attackers to execute arbitrary code on a server.

Broken Authentication: Enables/allows attackers to impersonate other users.

General challenges of running/participating in Bug Bounties:

Here is a small list of the general challenges of running and/or participating in Bug bounties; Quality of Reports: More often than not, trying to filter high quality submissions/reports can be extremely time-consuming. Keeping this in mind, not all of the reports that companies/organizations get are useful, which can lead to delays.

Scope: Basically, defining and maintaining a clear scope is essential to help avoid unmanageable workloads.

Legal Related Issues: Ethical Hackers/Security Researchers need to ensure that they operating within legal boundaries, and that they are respecting the rules of the program.

The list can go on and on.

How to get started as a "Bug Hunter:"

List below is a general idea of how to get started: You need to learn the basics: You will need to have an understanding of common vulnerabilities and web security principles.

Practice is key: Using platforms such as; [HackTheBox](#), [Hacker101 - CTF](#), [TryHackMe](#), and other CTF Competitions to help you hone your abilities/craft.

Join different programs: Obviously you're not going to start with the harder programs right away, so you're gonna want to start with the easier programs, (i.e. Public programs, find a mentor, or a team that'll help you build your skills), this will help you build some experience, potentially learn some new skills, and some credibility.

Networking: This can be a big help when you're first trying to get started. You can try engaging with the Cyber-security community through the use of forums, social media, and various events that are held throughout the world.

The list can go on and on.

Here's a list of resources for Bug Hunters: [TryHackMe](#): A good place to start for people who are interesting in learning.

[HackTheBox](#): Another amazing place to get started.

[Hacker101 - CTF](#) Another good place to start with.

[OWASP - Open Web Application Security Project](#): Offers Guidelines, tools, and information related to Web-Security.

[PortSwigger's: Web Security Academy](#): Offers Free online training and resources related to Web-Security.

Will continue to update the list.

List of Bug Bounty Sites: [HackerOne](#)

[Bugcrowd](#)

[Synack - Red Team](#)

[Detectify](#)

[Open Bug Bounty](#)

[Zero Copter](#)

[Yes We Hack](#)

[HackenProof - Crypto](#)

[Vulnerability Lab](#)

[Fire Bounty](#)

[Bug Bounty \(JP\)](#)

[Intigriti](#)

[safehats](#)

[Redstorm](#)

[CyberArmy \(IND\)](#)

[Bug Bounty - Switzerland](#)

[Apple - Bug Bounty](#)

[Google - Bug Hunter](#)

[Xbox - Bug Bounty Program \(Microsoft\)](#)

[Microsoft - Bounty Program](#)

Comment below with links;

Thanks for reading.

If you feel like this thread is missing something, or if you have relevant information that could help others, please comment below (I will update it, and credit you).

Love the design on it bro <3
Great tutorial

Loaded Lux - June 3, 2024, 2:43 pm

Thank you for the detailed write-up. It will definitely help newcomers like me understand more and head in the right direction for bug bounty hunting.

Dialgan - June 11, 2024, 9:58 am

Thank you for this. Quality post with important and useful information/links

illuminati? - June 11, 2024, 10:24 am

(Jun 11, 2024 09:58 AM)Dialgan Wrote: [\[CITE\]](#) Thank you for this. Quality post with important and useful information/links

Thanks for the kind words friend!

DottVenkman - June 19, 2024, 12:29 pm

i love the fuzzing ? [warn]

BlackRock - June 19, 2024, 12:48 pm

Super helpful, quality information, thank you so much for sharing this.

0x1buf0n - September 29, 2024, 3:22 pm

Excellent information, thank you very much!

ItzClydeFrog - September 29, 2024, 3:40 pm

Thanks for the resources! Commenting to circle back to it

source - October 4, 2024, 2:45 pm

I love seeing threads like this to help guide beginners in a proper direction.