



LE BUG BOUNTY

Becode

ANTONIO DA SILVA

...••

BUG QUOI ?



Souvent traduit en français par “prime au bogue” ou “prime à la faille détectée”, le bug bounty est apparu dans les années 90 au sein de Netscape Communications Corporation.

Bien connu des grandes entreprises telles que Tesla ou Apple, ainsi que des GAFAM (Les géants du Web : Google, Apple, Facebook, Amazon, Microsoft), le bug bounty est une méthode accordant une récompense pécuniaire à toute personne qui trouvera une ou des failles de sécurité dans un programme informatique défini.

SURPRISE



Une plateforme de bug bounty

Une plateforme de bug bounty, facilite la création et la gestion de programmes de primes aux bugs. La plupart des chercheurs en sécurité choisissent de signaler une vulnérabilité par le biais d'une plateforme de bug bounty car elle fournit la meilleure infrastructure et le cadre légal pour qu'ils puissent le faire.

Les chercheurs en sécurité peuvent s'engager et communiquer avec une entreprise de manière sûre, structurée et fiable, tout en recevant en direct des mises à jour et des communications.

De même, les entreprises considèrent que les bug bounty sont l'un des moyens les plus fiables et les plus stables de mettre en place des programmes. Lorsque vous vous inscrivez sur une plateforme en tant que client, par exemple, un responsable client vous aidera à définir une portée claire pour votre programme et vous conseillera sur des aspects tels que la rémunération des chercheurs et la façon de gérer le flux Minotaure.



1

Hackerone



Intigriti

b

Bugcrowd



Synack®

PLATEFORMES

Voici les 4 plateformes les plus connues et utilisées

 Ziff Davis ☆ : Vulnerability Disclosure Program Triaged by HackerOne Domain 59 iOS: App Store 1 Executable 1 No bounty reward ⓘ ● Response efficiency: 95% See details	 Krisp ☆ : Bug Bounty Program Triaged by HackerOne, Retesting Domain 15 Executable 2 Other 1 \$100 - \$5k ⓘ ● Response efficiency: 100% See details	 Evernote ☆ : Bug Bounty Program Triaged by HackerOne, Retesting Domain 5 iOS: App Store 1 Executable 1 Android: Play Store 1 +1 \$150 - \$5k ⓘ ● Response efficiency: 97% See details	 Epic Games ☆ : Bug Bounty Program Triaged by HackerOne, Retesting, Bounty splitting Domain 26 Executable 6 Other 1 Android: .apk 1 \$200 - \$15k ⓘ ● Response efficiency: 96% See details	 Cardano Foundation ☆ : Bug Bounty Program Triaged by HackerOne, Retesting Executable 2 \$300 - \$10k ⓘ ● Response efficiency: 67% See details
 BlackRock ☆ : Vulnerability Disclosure Program Triaged by HackerOne Domain 2 CIDR 1 No bounty reward ⓘ ● Response efficiency: 100% See details	 Zebra VDP ☆ : Vulnerability Disclosure Program Triaged by HackerOne Domain 2514 CIDR 2 Other 1 No bounty reward ⓘ ● Response efficiency: 96% See details	 Lark Technologies ☆ : Bug Bounty Program Triaged by HackerOne, Retesting, Bounty splitting Domain 13 Executable 2 iOS: App Store 1 Android: .apk 1 \$100 - \$5k ⓘ ● Response efficiency: 93% See details	 Citrix Systems ☆ : Bug Bounty Program Triaged by HackerOne, Retesting, Bounty splitting Domain 31 \$100 - \$10k ⓘ ● Response efficiency: 91% See details	 Logitech ☆ : Updated Bug Bounty Program Triaged by HackerOne, Retesting, Bounty splitting Domain 53 Executable 8 Hardware/IoT 8 iOS: App Store 5 +2 \$175 - \$2k ⓘ ● Response efficiency: 91% See details

QUELQUES EXEMPLES

Pris du site HackerOne

Comment ça marche ?

Inscription



Sur l'une des plateforme citée, ou sur une plateforme de votre choix

Choix de la cible



Vous aurez une large gamme de choix d'entreprises qui proposent des bug bounty

Début du cauchemar



Essayez de ne pas devenir fou !
Une très bonne organisation vous aidera





ATTENTION !

Certains programmes de bug bounty ne sont disponibles que si vous avez déjà fait vos preuves, ce sont alors des programmes privés. Ceux-ci sont disponibles si vous avez déjà fait vos preuves sur la plateforme, et que celle-ci décide de vous inviter à participer à l'un d'entre-eux.



Je pense avoir trouvé



Ecrire un rapport

Certaines plateformes t'aident à le faire



Attendre

Ça peut être très long...



Recommencer

Et oui, c'est pas toujours gagné...





CANVA STORIES

23 ▶

CANVA STORIES

◀ 23

...

MAIS

Si jamais votre vulnérabilité est
valable...
C'est la richesse !!

Une vulnérabilité peut vous rapporter
gros, elle peut aller d'une centaine
d'Euros à plusieurs milliers

**2ÈME
SURPRISE**

Oui mais...

Comment faire si j'ai jamais essayé ?



Hacker101

Plateforme d'apprentissage gratuite développée par HackerOne.



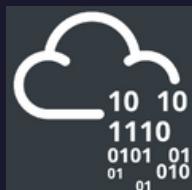
Intigriti

Lien vers plusieurs vidéos Youtube faites par Intigriti.



Bugcrowd University

Plusieurs articles disponibles, afin de vous aider à débuter



TryHackMe

Le bon vieux TryHackMe



Un exemple

The screenshot shows a web browser window with four tabs open:

- File Inclusion Lab!
- Tomorrowland
- Account - Tomorrowland
- Jobs

The main content area displays the Tomorrowland account page. On the left, there's a sidebar with links: Home, My Bracelet, Tickets, Vouchers, and Store. The main content area has tabs for PERSONAL DETAILS, ADDRESS, and SOCIAL. The PERSONAL DETAILS tab is active, showing fields for FIRST NAME (offside), LAST NAME (fut), and EMAIL ADDRESS (offside@intigriti.me). Above the form, a banner says "WATCH LIVESTREAMS WORLD TV #1 - Tiësto (R) / ONE X".

At the bottom of the browser window, the developer tools Network tab is open, showing a list of network requests. One request, "2.2d1b05b.chunk.js:2 (fetch)", is highlighted. The Request tab in the developer tools shows the URL: "https://my.tomorrowland.com/account". The Response tab shows a JSON object with a long AccessToken.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	my.tomorrowland.com	tml-browser-detect-1.x.min.js	script	js	cached	1.15 KB
200	GET	www.google.com	api.js	script	js	1.12 KB	850 B
304	GET	my.tomorrowland.com	2.2d1b05b.chunk.js	script	js	cached	0 B
304	GET	my.tomorrowland.com	main.37bbc915.chunk.js	script	js	cached	0 B
200	GET	my.tomorrowland.com	tml-browser-detect-1.x.css	stylesheet	css	962 B (raced)	529 B
200	GET	my.tomorrowland.com	2.74170c84.chunk.css	stylesheet	css	15.70 KB (raced)	15.28 KB
304	GET	my.tomorrowland.com	main.5eca8f0c.chunk.css	stylesheet	css	cached	257.10 KB
200	GET	www.gstatic.com	recaptcha_en.js	api.js:1 (script)	js	cached	0 B
200	OPTIONS	sessions.bugsnag.com	/	xhr	plain	387 B	0 B
200	POST	cognito-idp.eu-west-1.amazonaws.com	/	2.2d1b05b.chunk.js:2 (fetch)	x-amz-json-1.1	1.27 KB	984 B
200	GET	static-feed.tomorrowland.com	settings-topbar-production.json?date=1659140346817	2.2d1b05b.chunk.js:2 (xhr)	json	818 B	127 B
200	POST	sessions.bugsnag.com	/	2.2d1b05b.chunk.js:2 (xhr)	json	299 B	21 B
200	GET	tomorrowland.cdn.prismic.io	v2	2.2d1b05b.chunk.js:2 (fetch)	json	1.22 KB	2.01 KB
200	GET	tomorrowland.cdn.prismic.io	v2	2.2d1b05b.chunk.js:2 (fetch)	json	1.22 KB	2.01 KB

Request tab content:

```
AccessToken: "eyJraWQiOiwdUJODc4VTdwQ2V2NV1eGZ3UTdKGduc09mWE1JSzdqNWlJTHZBd0RZPSI..."
```

Response tab content (JSON):

```
{ "access_token": "eyJraWQiOiwdUJODc4VTdwQ2V2NV1eGZ3UTdKGduc09mWE1JSzdqNWlJTHZBd0RZPSI..."} 
```

Un exemple

The screenshot shows a web browser window with multiple tabs open. The main content area displays a user account page for 'Tomorrowland' at <https://my.tomorrowland.com/account>. The page includes a sidebar with links like Home, My Bracelet, Tickets, Vouchers, and Store. The main content area is titled 'Account' and shows 'PERSONAL DETAILS' with fields for FIRST NAME ('margaux') and LAST NAME ('tricot'). Below this is an 'EMAIL ADDRESS' field containing 'offside+2@intigriti.me'. Further down is an 'ADDRESS' section with fields for STREET, NUMBER, and APT/SUITE.

At the bottom of the browser window, the developer tools Network tab is open, showing a list of network requests. The table includes columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. Several requests are shown, including GET requests for static files like 'ico-music_light.svg' and 'ico-book_light.svg', and a POST request for 'cognito-idp.eu-west-1.amazonaws.com'.

The Network tab also features a detailed view of a selected JSON response. The JSON structure includes objects for 'custom:city' (value: "jodoigne"), 'custom:postal' (value: "1370"), 'phone_number' (value: "+32472348091"), and 'custom:temp_attributes' (value: "[{"interests":[], "consents": [{"tomorrowland.tc.festival": true}], "status": "UNCONFIRMED"}]").

Un exemple

 **offside** created the submission
30/07/2022 00:36:03

 **azerty [triage]**
01/08/2022 10:49:09

Hi offside!

Thanks for your submission!

We have reviewed your report, but unfortunately we do not consider this to be a valid security issue. That is because the AccessToken is used as a method of authorization. The token itself is pretty long and unrealistic to guess/brute force. The token is generated by amazon AWS, and the behaviour is intended. For these reasons, we decided to close your report as **not applicable**.

Best of luck with hunting!

Kind regards

azerty

 **azerty** changed the **status** from **Triage** to **Not applicable**
01/08/2022 10:49:20

THANKS
FOR WATCHING