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.

Hackerone

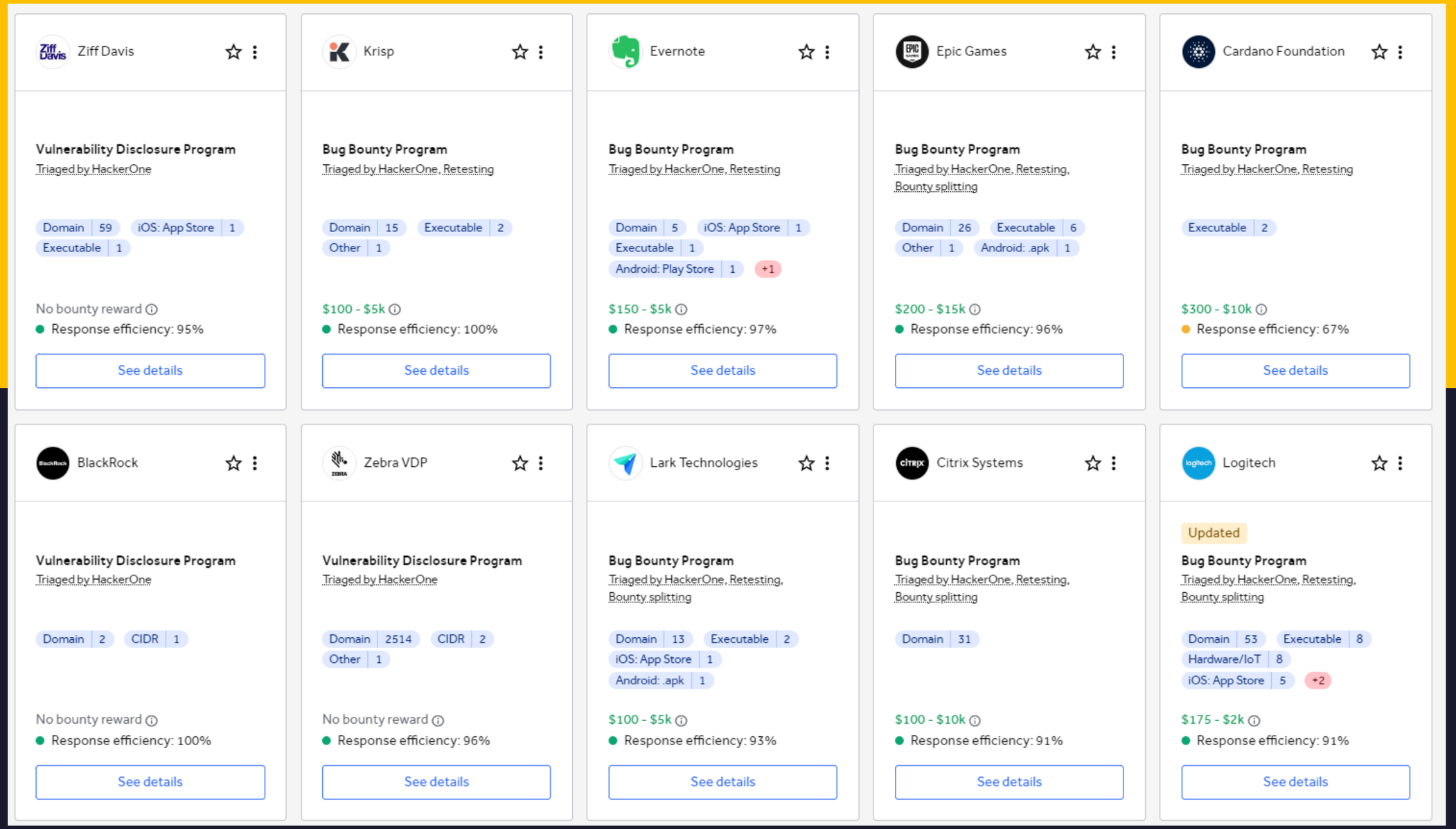
Intigriti

Bugcrowd

Synack

PLATEFORMES

Voici les 4 plateformes les plus connues et utilisées



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

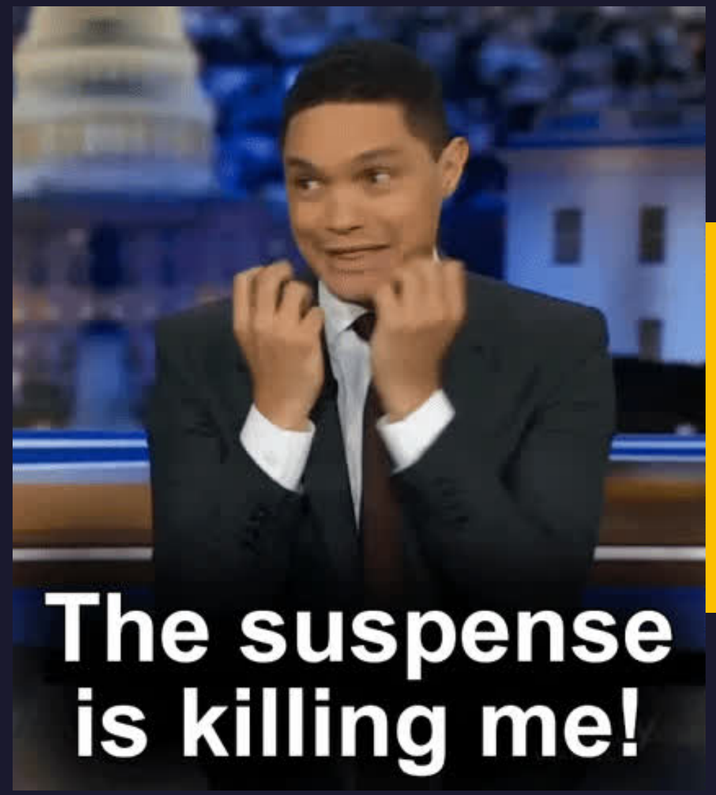
Certaines plateformes t'aident à le faire

Attendre

Ça peut être très long...

Recommencer

Et oui, c'est pas toujours gagné...



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 essayer ?

Hacker101

Plateforme d'apprentissage gratuite développée par HackerOne.

Intigriti

Lien vers plusieurs vidéos Youtube faites par Intigriti.

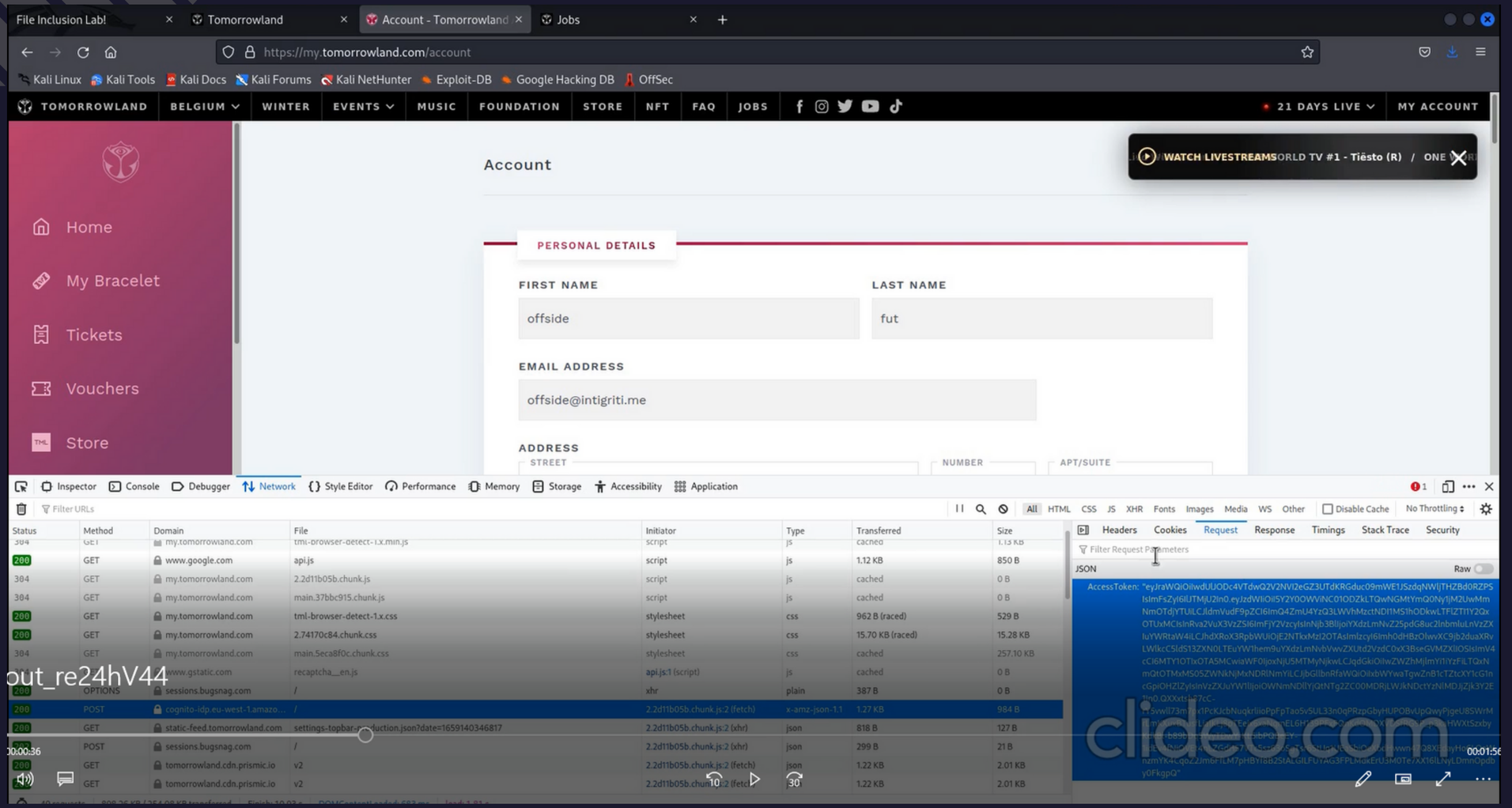
Bugcrowd University

Plusieurs articles disponibles, afin de vous aider à débuter

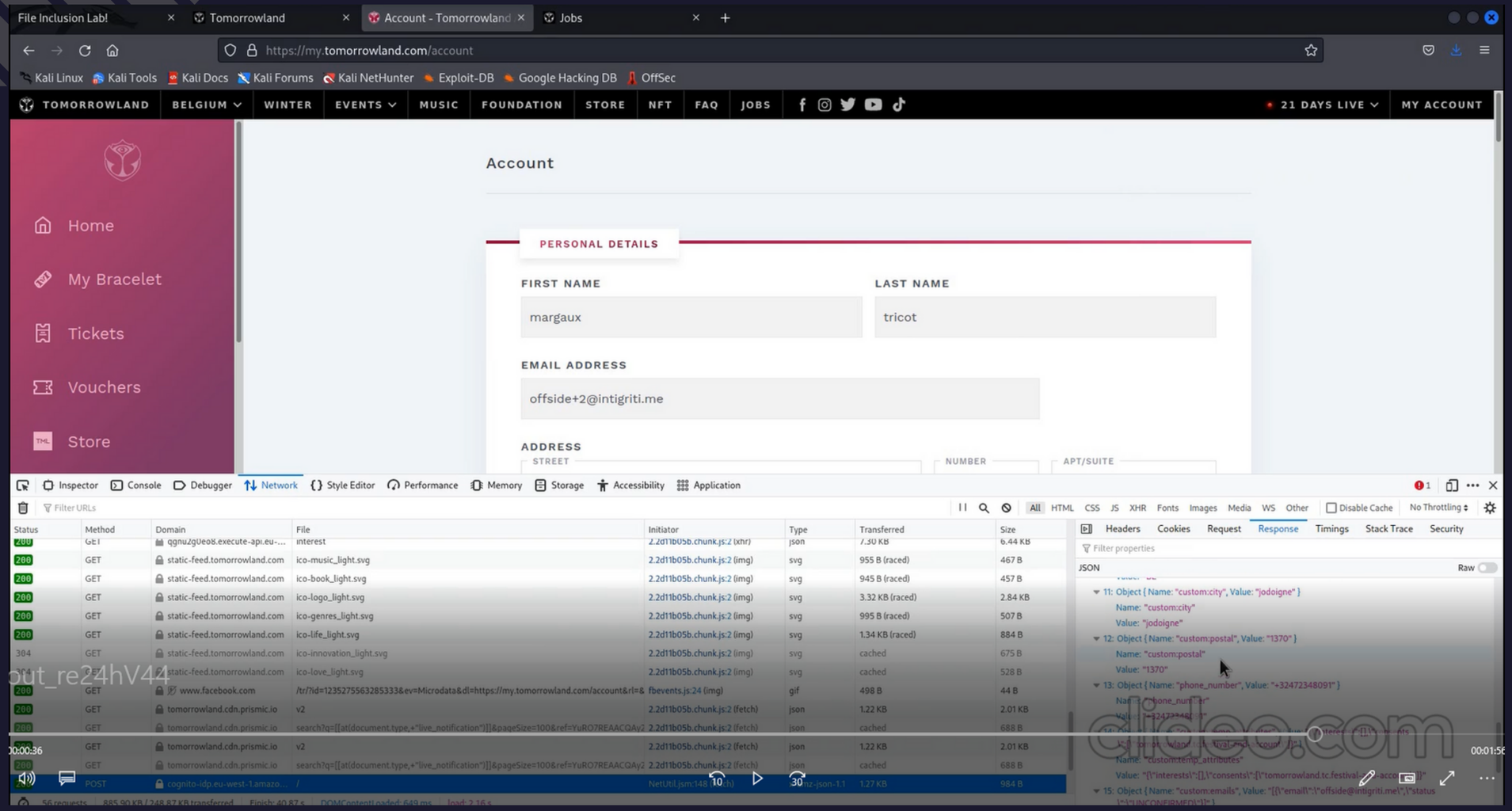
TryHackMe

Le bon vieux TryHackMe

Un exemple


File Inclusion Lab!
Tomorrowland
Account - Tomorrowland
Jobs
https://my.tomorrowland.com/account
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
TOMORROWLAND
BELGIUM
WINTER
EVENTS
MUSIC
FOUNDATION
STORE
NFT
FAQ
JOBS
21 DAYS LIVE
MY ACCOUNT
Home
My Bracelet
Tickets
Vouchers
Store
Account
WATCH LIVESTREAMS
PERSONAL DETAILS
FIRST NAME
offside
LAST NAME
fut
EMAIL ADDRESS
offside@intigriti.me
ADDRESS
STREET
NUMBER
APT/SUITE
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
Status
Method
Domain
File
Initiator
Type
Transferred
Size
Headers
Cookies
Request
Response
Timings
Stack Trace
Security
JSON
Raw
AccessToken:
out_re24hV44
clideo.com

Un exemple


File Inclusion Lab!
Tomorrowland
Account - Tomorrowland
Jobs
https://my.tomorrowland.com/account
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
TOMORROWLAND
BELGIUM
WINTER
EVENTS
MUSIC
FOUNDATION
STORE
NFT
FAQ
JOBS
21 DAYS LIVE
MY ACCOUNT
Home
My Bracelet
Tickets
Vouchers
Store
Account
PERSONAL DETAILS
FIRST NAME
margaux
LAST NAME
tricot
EMAIL ADDRESS
offside+2@intigriti.me
ADDRESS
STREET
NUMBER
APT/SUITE
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Status
Method
Domain
File
Initiator
Type
Transferred
Size
Headers
Cookies
Request
Response
Timings
Stack Trace
Security
JSON
Raw
00:00:36
00:01:56

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