How to Become a Rockstar: a Bug Bounty Hunter journey

HELLO!

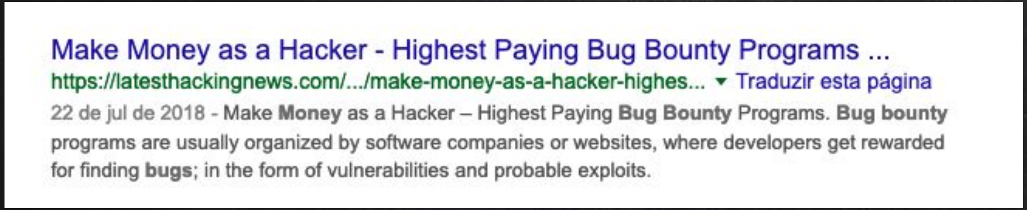
I am Heitor Gouvêa

Independent Security Consultant and part-time Bug Bounty Hunter

You can find me at @GouveaHeitor

1.

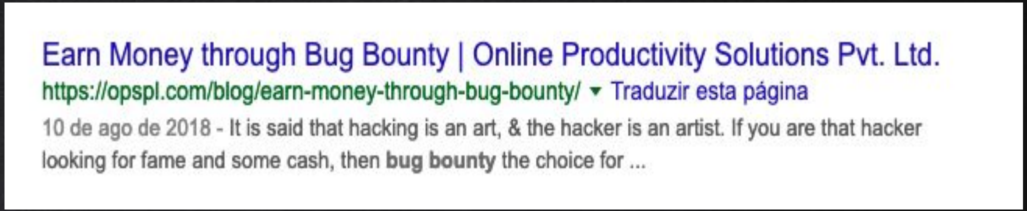
What is Bug Bounty Hunting?!



Make Money as a Hacker - Highest Paying Bug Bounty Programs ...

https://latesthackingnews.com/.../make-money-as-a-hacker-highes... ▾ Traduzir esta página

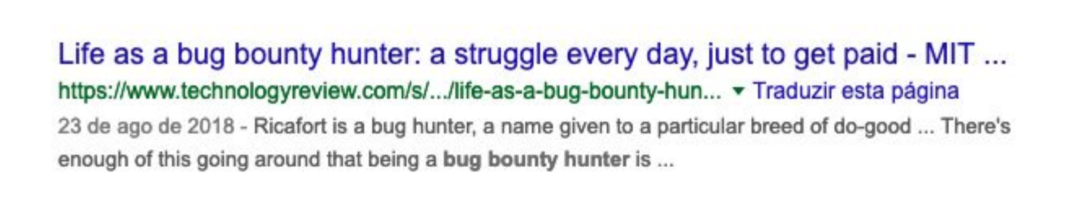
22 de jul de 2018 - Make **Money** as a Hacker – Highest Paying **Bug Bounty** Programs. **Bug bounty** programs are usually organized by software companies or websites, where developers get rewarded for finding **bugs**; in the form of vulnerabilities and probable exploits.



Earn Money through Bug Bounty | Online Productivity Solutions Pvt. Ltd.

https://opspl.com/blog/earn-money-through-bug-bounty/ ▾ Traduzir esta página

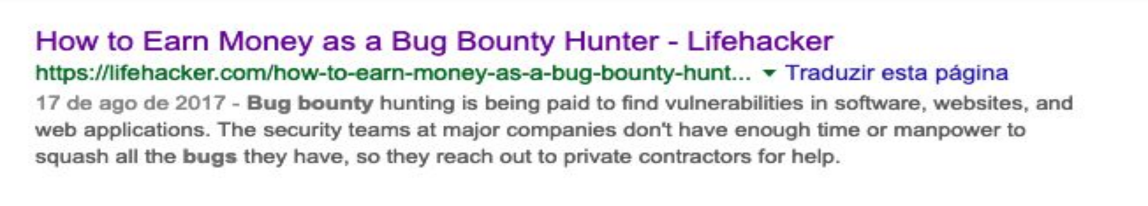
10 de ago de 2018 - It is said that hacking is an art, & the hacker is an artist. If you are that hacker looking for fame and some cash, then **bug bounty** the choice for ...



Life as a bug bounty hunter: a struggle every day, just to get paid - MIT ...

https://www.technologyreview.com/s/.../life-as-a-bug-bounty-hun... ▾ Traduzir esta página

23 de ago de 2018 - Ricafort is a bug hunter, a name given to a particular breed of do-good ... There's enough of this going around that being a **bug bounty hunter** is ...



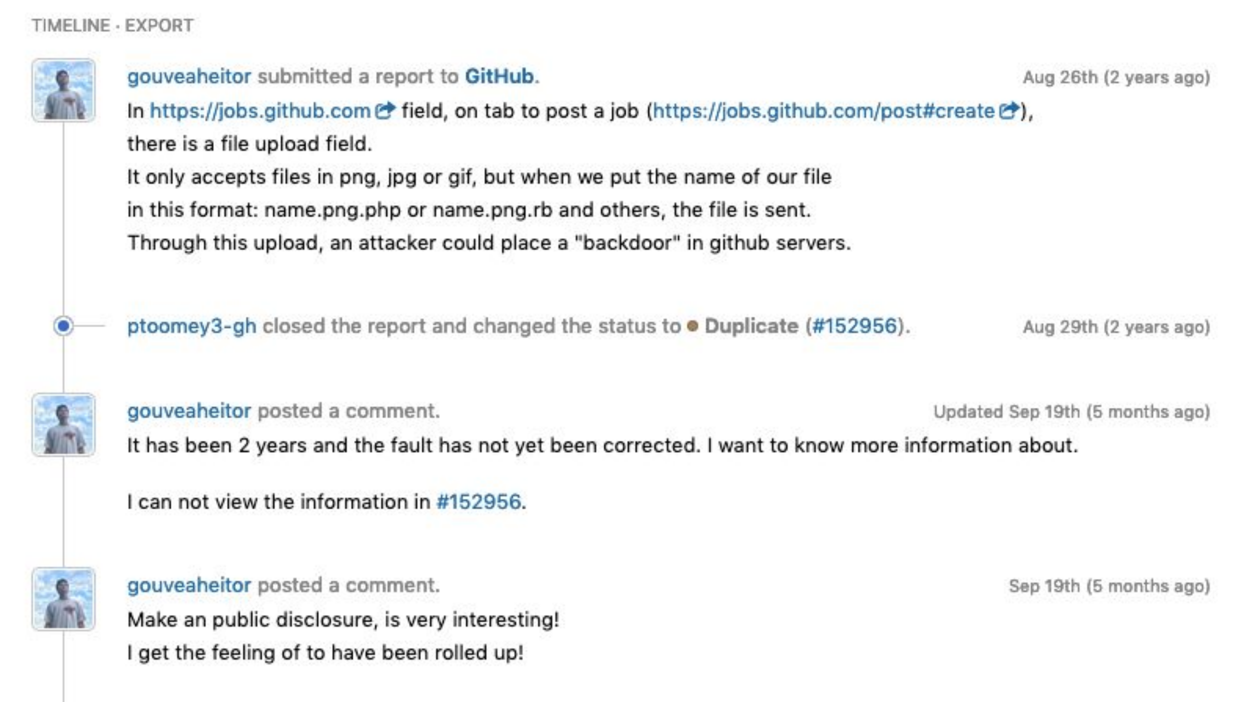
How to Earn Money as a Bug Bounty Hunter - Lifehacker

https://lifehacker.com/how-to-earn-money-as-a-bug-bounty-hunt... ▾ Traduzir esta página

17 de ago de 2017 - **Bug bounty** hunting is being paid to find vulnerabilities in software, websites, and web applications. The security teams at major companies don't have enough time or manpower to squash all the **bugs** they have, so they reach out to private contractors for help.

“Life as a bug bounty hunter: a ~~struggle~~ journey every day, just to ~~get paid~~ gain knowledge”

My first report:



TIMELINE · EXPORT

gouveaheitor submitted a report to GitHub. Aug 26th (2 years ago)

In https://jobs.github.com field, on tab to post a job (https://jobs.github.com/post#create),
there is a file upload field.
It only accepts files in png, jpg or gif, but when we put the name of our file
in this format: name.png.php or name.png.rb and others, the file is sent.
Through this upload, an attacker could place a "backdoor" in github servers.

ptoomey3-gh closed the report and changed the status to ● Duplicate (#152956). Aug 29th (2 years ago)

gouveaheitor posted a comment. Updated Sep 19th (5 months ago)

It has been 2 years and the fault has not yet been corrected. I want to know more information about.

I can not view the information in #152956.

gouveaheitor posted a comment. Sep 19th (5 months ago)

Make an public disclosure, is very interesting!
I get the feeling of to have been rolled up!

MOST FAMOUS PLATFORMS

HackerOne.com intigriti

Bugcrowd

Synack red team Vulnscope ltda

Cobalt.io HackenProof

* Zerodium *

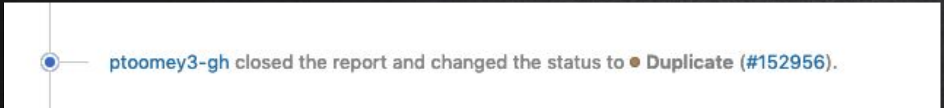
Hackaflag (brazilian platform)

REPORT STATUS

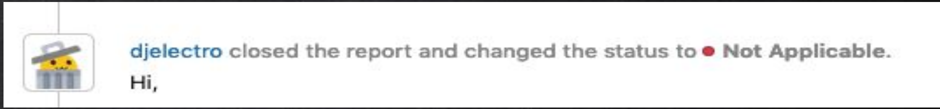
- Triaged
- Duplicate
- Informative
- Resolved
- Not Applicable
- Needs more info

I failed. A lot.

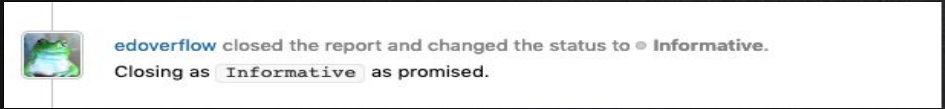
"Failures are finger posts on the road to achievement." – C.S. Lewis



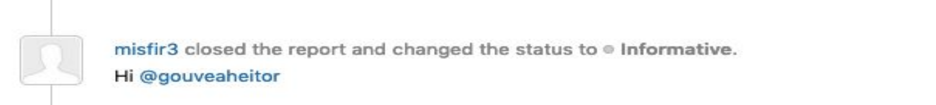
ptoomey3-gh closed the report and changed the status to ● Duplicate (#152956).



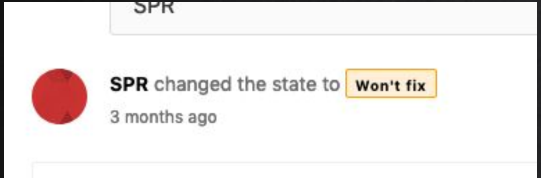
djelectro closed the report and changed the status to ● Not Applicable.
Hi,



edoverflow closed the report and changed the status to ● Informative.
Closing as `Informative` as promised.

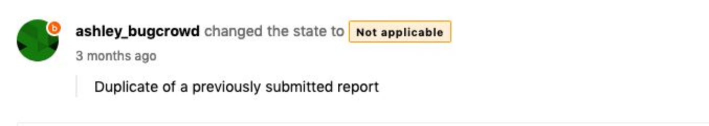


misfir3 closed the report and changed the status to ● Informative.
Hi @gouveaheitor



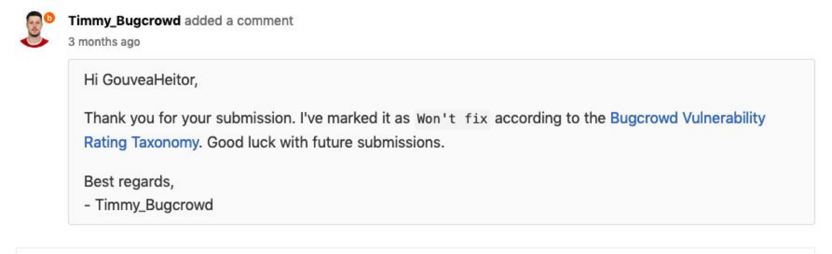
SPR

SPR changed the state to Won't fix
3 months ago



ashley_bugcrowd changed the state to Not applicable
3 months ago

Duplicate of a previously submitted report

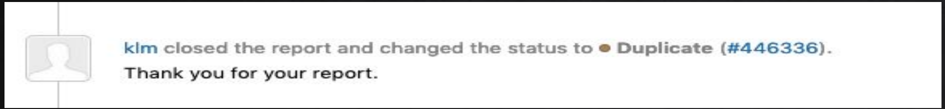


Timmy_Bugcrowd added a comment
3 months ago

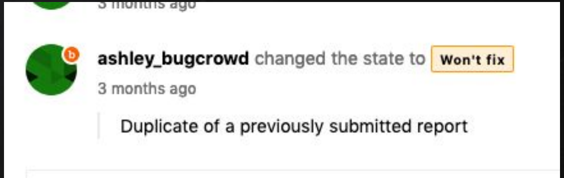
Hi GouveaHeitor,

Thank you for your submission. I've marked it as `Won't fix` according to the Bugcrowd Vulnerability Rating Taxonomy. Good luck with future submissions.

Best regards,
- Timmy_Bugcrowd



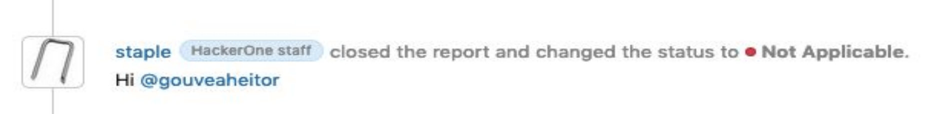
klm closed the report and changed the status to ● Duplicate (#446336).
Thank you for your report.



3 months ago

ashley_bugcrowd changed the state to Won't fix
3 months ago

Duplicate of a previously submitted report



staple HackerOne staff closed the report and changed the status to ● Not Applicable.
Hi @gouveaheitor

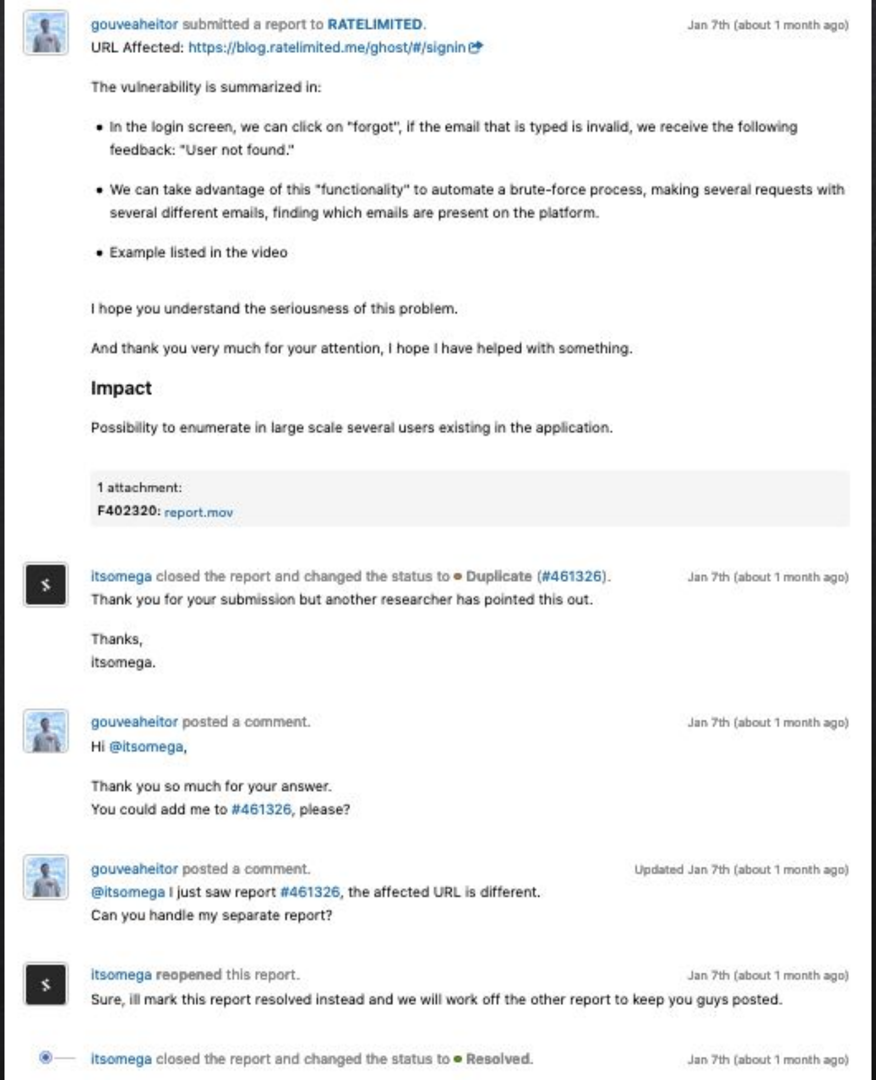
NOT EVERYTHING ARE ROSES

"Knowing your mistakes is the first step in correcting them"

I started reading the reports made by the community

I started to see Bug Bounty as something other than Pentesting

I focused on low vulnerabilities



gouveaheitor submitted a report to **RATELIMITED**. Jan 7th (about 1 month ago)
URL Affected: https://blog.ratelimited.me/ghost/#/signin

The vulnerability is summarized in:

- In the login screen, we can click on "forgot", if the email that is typed is invalid, we receive the following feedback: "User not found."
- We can take advantage of this "functionality" to automate a brute-force process, making several requests with several different emails, finding which emails are present on the platform.
- Example listed in the video

I hope you understand the seriousness of this problem.

And thank you very much for your attention, I hope I have helped with something.

Impact

Possibility to enumerate in large scale several users existing in the application.

1 attachment:
F402320: report.mov

itsomega closed the report and changed the status to ● **Duplicate** (#461326). Jan 7th (about 1 month ago)
Thank you for your submission but another researcher has pointed this out.

Thanks,
itsomega.

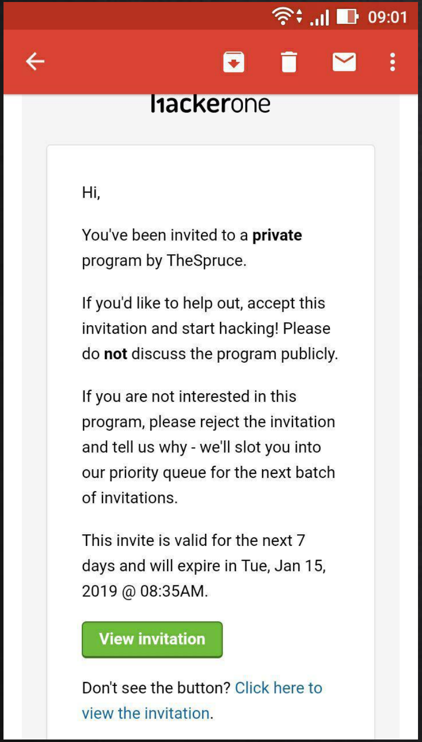
gouveaheitor posted a comment. Jan 7th (about 1 month ago)
Hi @itsomega,

Thank you so much for your answer.
You could add me to #461326, please?

gouveaheitor posted a comment. Updated Jan 7th (about 1 month ago)
@itsomega I just saw report #461326, the affected URL is different.
Can you handle my separate report?

itsomega **reopened** this report. Jan 7th (about 1 month ago)
Sure, ill mark this report resolved instead and we will work off the other report to keep you guys posted.

itsomega closed the report and changed the status to ● **Resolved**. Jan 7th (about 1 month ago)



Hi,

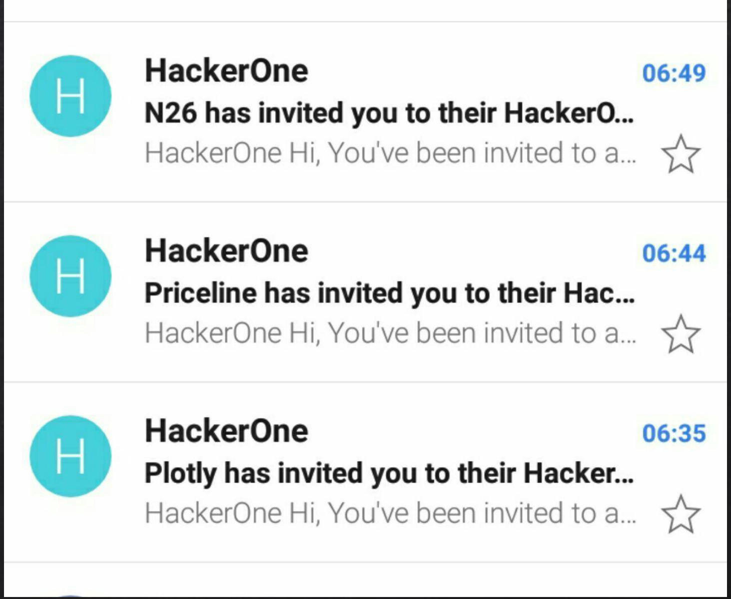
You've been invited to a **private** program by TheSpruce.

If you'd like to help out, accept this invitation and start hacking! Please do **not** discuss the program publicly.

If you are not interested in this program, please reject the invitation and tell us why - we'll slot you into our priority queue for the next batch of invitations.

This invite is valid for the next 7 days and will expire in Tue, Jan 15, 2019 @ 08:35AM.

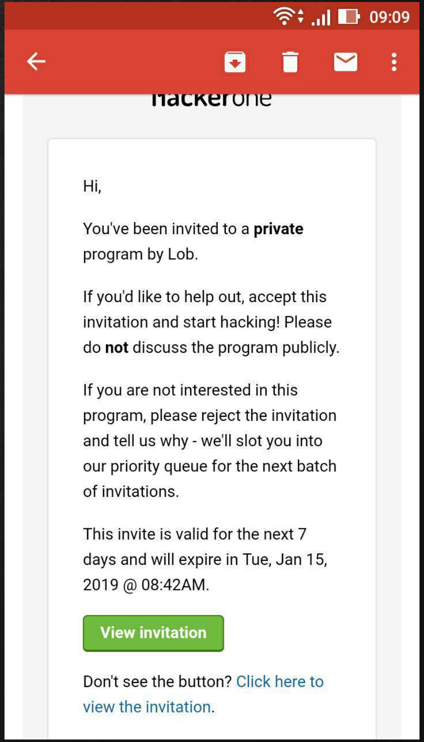
Don't see the button? Click here to view the invitation.



HackerOne 06:49
N26 has invited you to their HackerO...
HackerOne Hi, You've been invited to a...

HackerOne 06:44
Priceline has invited you to their Hac...
HackerOne Hi, You've been invited to a...

HackerOne 06:35
Plotly has invited you to their Hacker...
HackerOne Hi, You've been invited to a...



Hi,

You've been invited to a **private** program by Lob.

If you'd like to help out, accept this invitation and start hacking! Please do **not** discuss the program publicly.

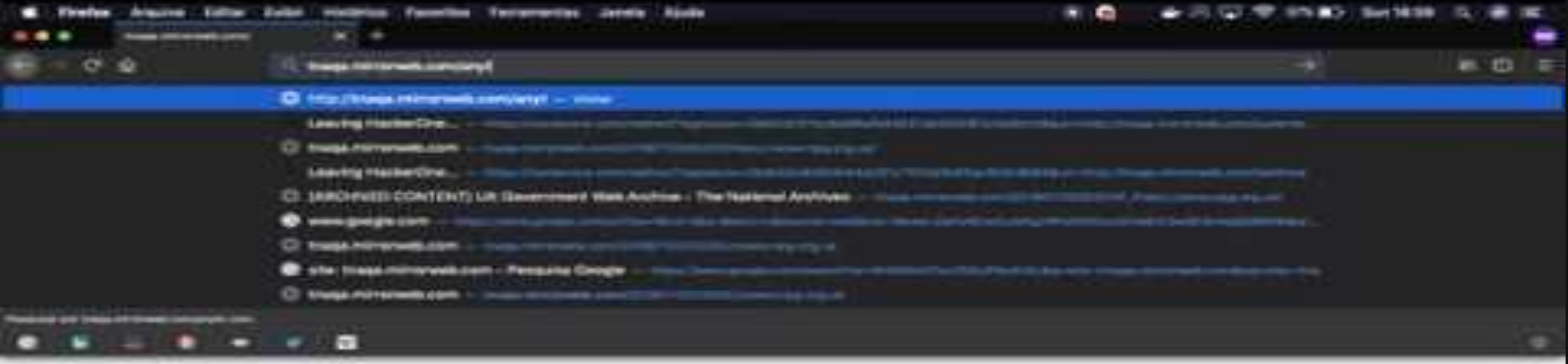
If you are not interested in this program, please reject the invitation and tell us why - we'll slot you into our priority queue for the next batch of invitations.

This invite is valid for the next 7 days and will expire in Tue, Jan 15, 2019 @ 08:42AM.

Don't see the button? Click here to view the invitation.

OH YEAH.

try harder



tnaqa.mirrorweb.com/amp!

http://tnaqa.mirrorweb.com/amp! — Visitar

Leaving HackerOne... — [illegible]

tnaqa.mirrorweb.com — [illegible]

Leaving HackerOne... — [illegible]

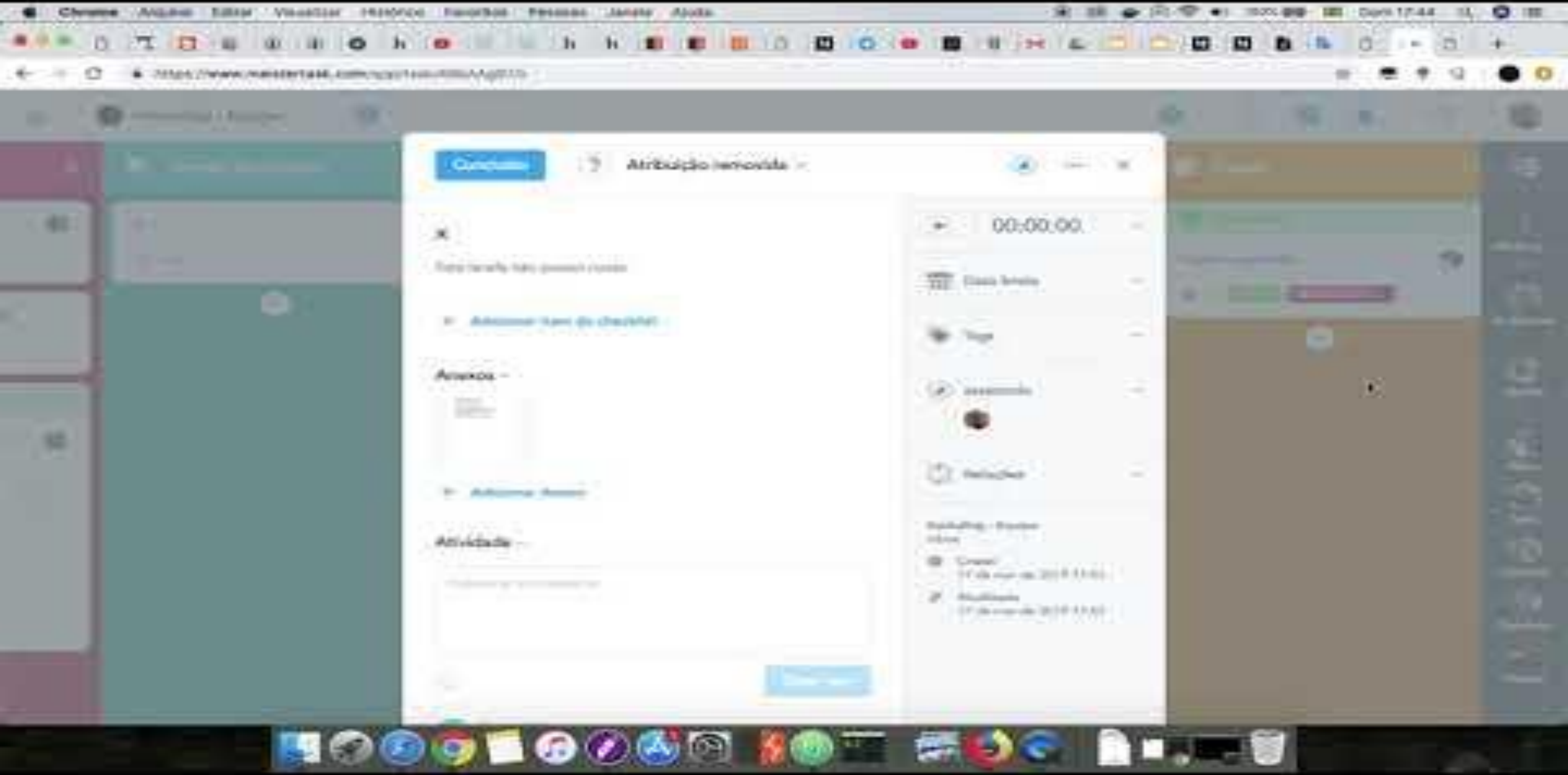
[ARCHIVED CONTENT] UK Government Web Archive - The National Archives — [illegible]

www.google.com — [illegible]

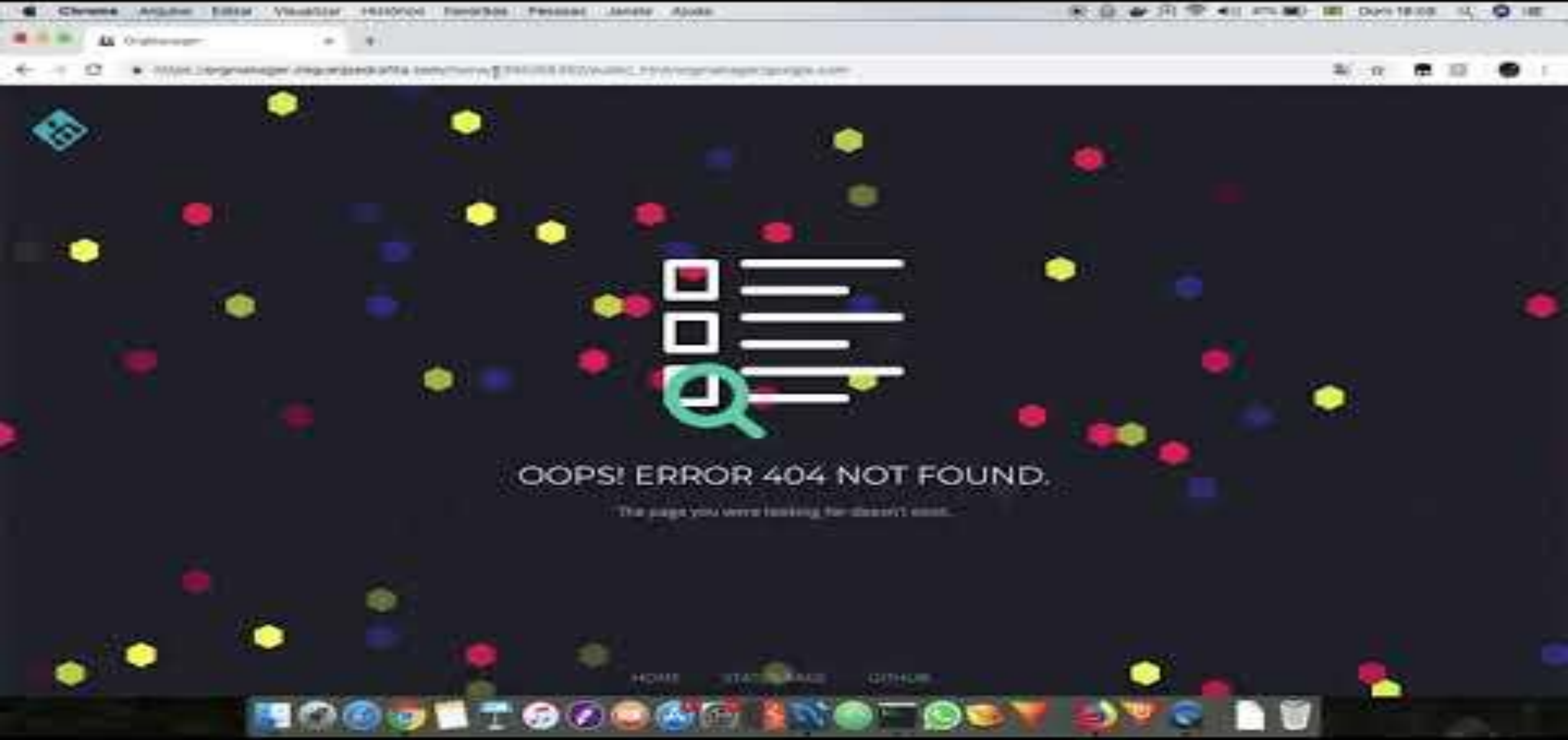
tnaqa.mirrorweb.com — [illegible]

site: tnaqa.mirrorweb.com - Pesquisa Google — [illegible]

tnaqa.mirrorweb.com — [illegible]

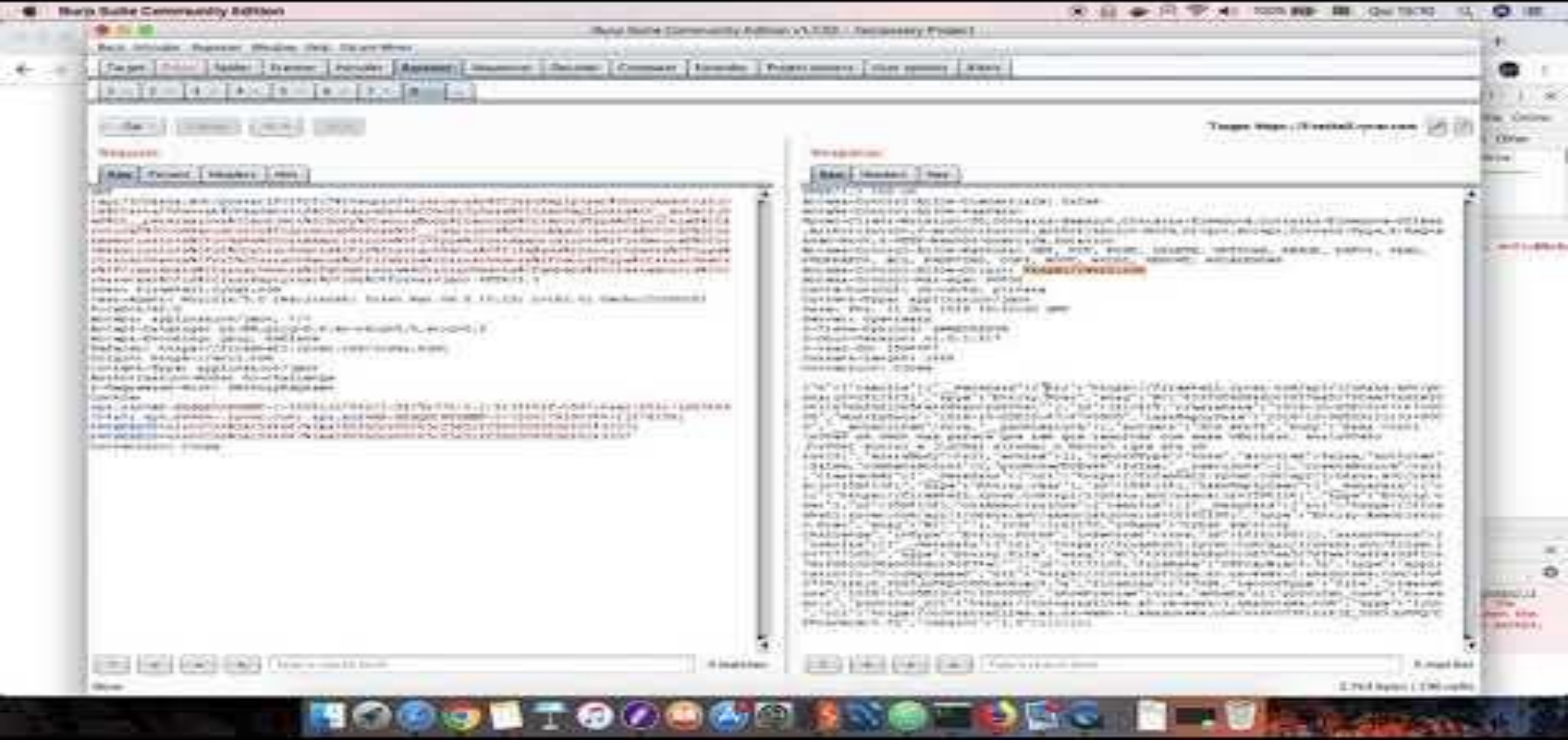


Chrome
Arquivo
Editar
Visualizar
Histórico
Favoritos
Pessoas
Janela
Ajuda
Concluído
Atribuição removida
00:00:00
Esta tarefa não possui notas
Adicionar item de checklist
Data limite
Tags
Anexos
Relações
Adicionar Anexo
Atividade
Criado
Modificado



OOPS! ERROR 404 NOT FOUND.

The page you were looking for doesn't exist.


Burp Suite Community Edition
Burp Suite Community Edition v1.7.33 - Temporary Project
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Go
Cancel
Request
Raw
Params
Headers
Hex
Response
Raw
Headers
Hex

"Hunting makes me a better pentester"

Find bugs more faster

Experience in diverses technologies applications

More attuned to emergent security trends

THANKS!

Any questions?

You can find me at:
@GouveaHeitor
hi@heitorgouvea.me