HackerOne

In this lesson, we'll look at how HackerOne works and see an example of a BBP.

We'll cover the following

- How BBP platforms work
  - Aggregation for researchers and organizations
  - Monetization model
- Example: Starbucks
  - Terms & conditions
  - Stats
  - Identifying target domains
  - Payouts
  - Reports

How BBP platforms work

BBP platforms like HackerOne provide organizations with tools to host an efficient program and offer the kind of network that allows organizations to attract researchers from the get-go.

Aggregation for researchers and organizations

These platforms are sort of an aggregator of BBP, so the number of researchers browsing the platform and looking for programs is higher than the number of researchers that would bump into your program organically. Researchers know that the platform hosts thousands of programs, so they can easily search through the platform's directory to find new targets. At the same time, organizations tend to join these platforms exactly because of the number of researchers lurking in them, granting broad exposure to their program.

Monetization model

The way these platforms survive is by charging organizations a fee for joining their service or taking a cut of each bounty awarded through their platform. This makes

service or taking a cut of each bounty awarded through their platform. This makes sure that everyone is a winner: researchers can access thousands of programs,

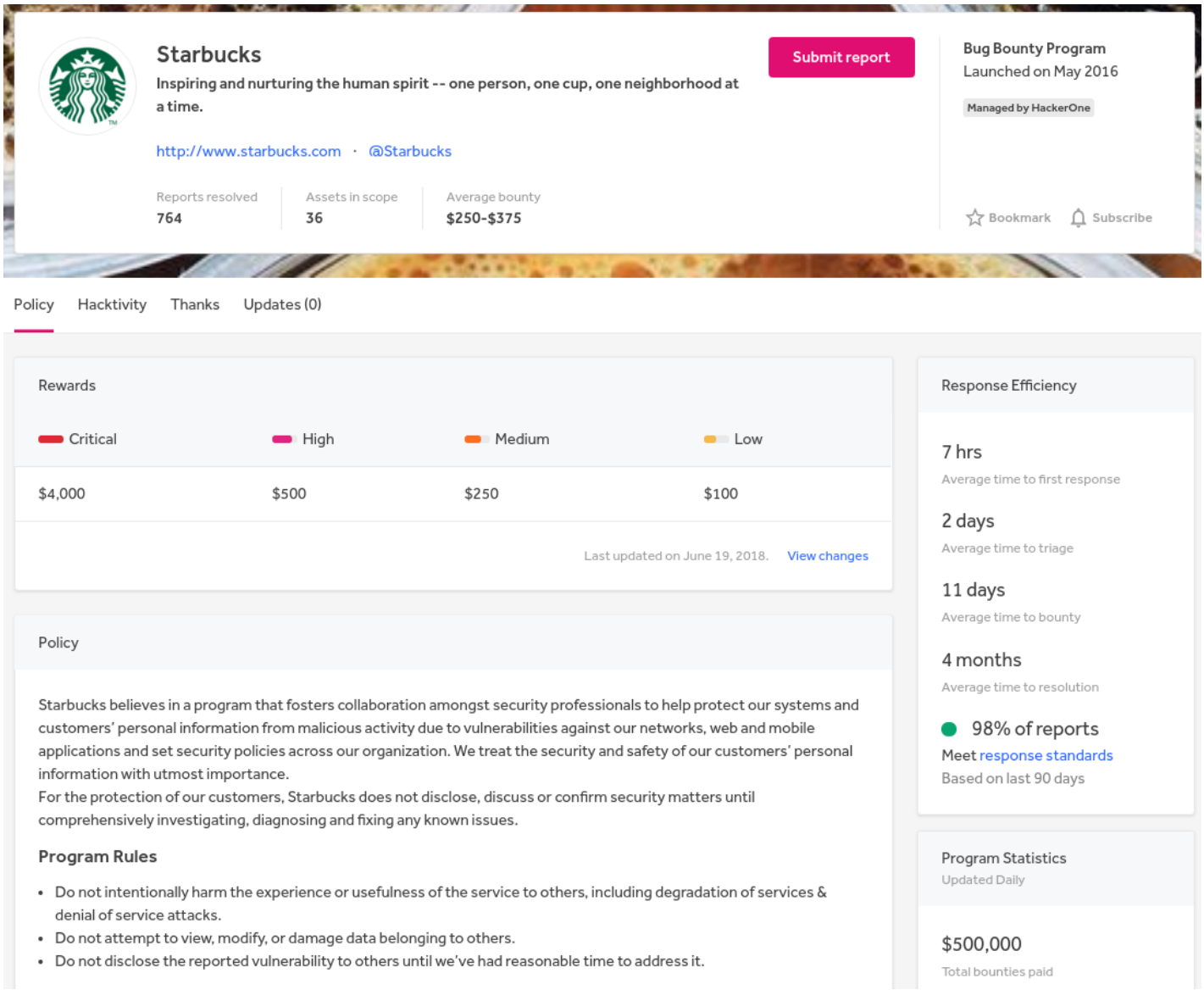
organizations are exposed to thousands of researchers, and the platform monetizes their mutual success by collecting fees in between.

Example: Starbucks

For a better understanding of how the platform works, we can take a look at the program published by Starbucks.

Terms & conditions

It all starts with the program's page, which states terms and conditions at hackerone.com/starbucks.



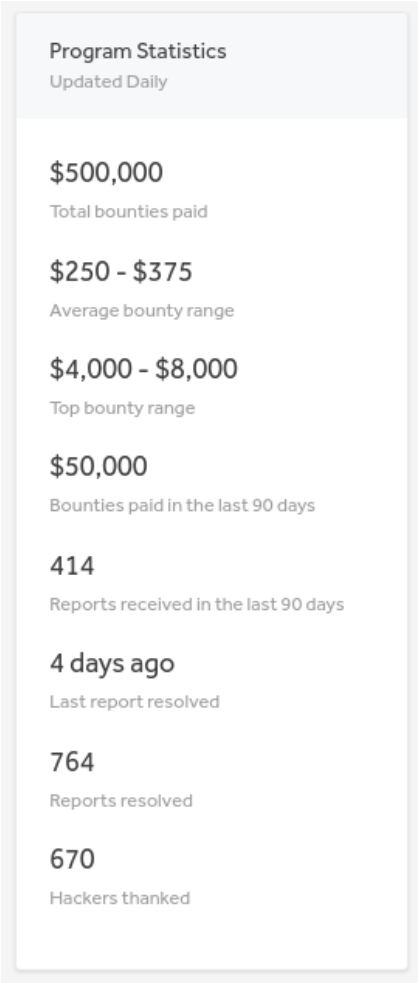
A screenshot of Starbucks' BBP. The program is much more extensive than what can be captured within a small screenshot

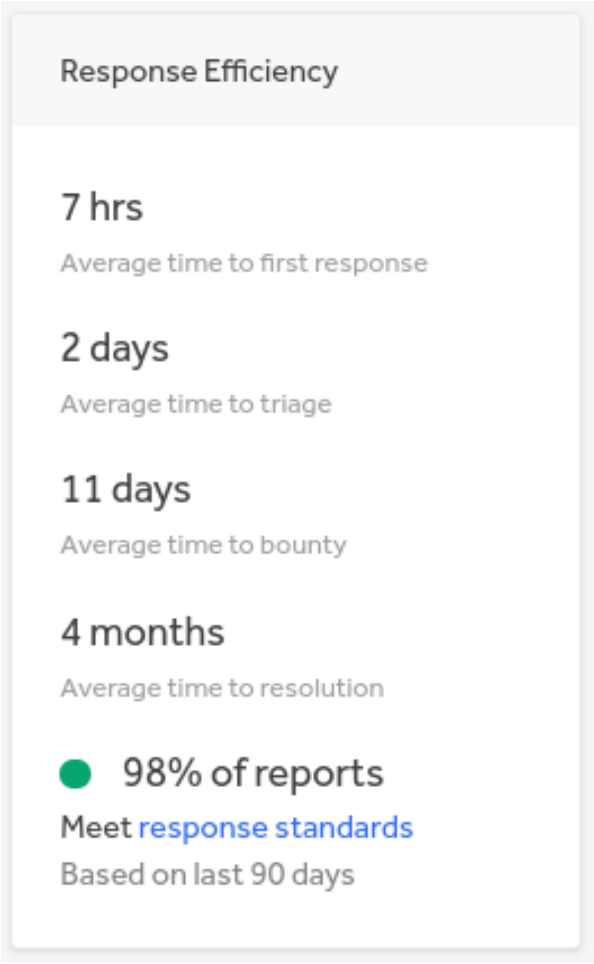
HackerOne has a neat user interface, and allows researchers to understand the

most important information about a program very easily.

Stats

There are sections with a recap of the most important stats of the program.





Identifying target domains

Ethical hackers can identify their targets very quickly thanks to the organization listing all the assets considered to be in scope for the program.

Scopes

In Scope

Domain	**www.starbucks.com** Starbucks US https://www.starbucks.com/	Critical	Eligible
Domain	**gift.starbucks.co.jp** Starbucks e-gift Japan https://gift.starbucks.co.jp/	Critical	Eligible
Domain	**www.starbucks.co.jp** Starbucks Japan https://www.starbucks.co.jp	Critical	Eligible
Domain	**www.starbucks.com.cn** Starbucks China https://www.starbucks.com.cn/	Critical	Eligible
Domain	**www.starbucks.de** Starbucks Germany https://www.starbucks.de/	Critical	Eligible
Domain	**www.starbucks.fr** Starbucks France https://www.starbucks.fr/	Critical	Eligible

All of Starbucks's domains are in the scope of the program

Payouts

More importantly, the payouts are clearly defined at the top of the program.

Rewards

Critical	High	Medium	Low
$4,000	$500	$250	$100

Last updated on June 19, 2018. View changes

Payouts are clearly laid out

Right from the start, it's clear that finding a critical vulnerability in Starbucks' BBP will net a researcher a few thousand dollars. Keep in mind these amounts may vary based on the specific vulnerability that's been reported.

Reports

In addition to the program's page, we can even take a peek at some of the reports researchers have submitted. An interesting report can be found at hackerone.com/reports/506646, where an arbitrary code execution vulnerability was reported. As you can see from the following screenshots, the reporter clearly states where the problem lies and starts collaborating with Starbucks' security team on resolving the issue.

TIMELINE · EXPORT

johnstone submitted a report to **Starbucks**. Mar 8th (9 months ago)

Summary:
OS Command Injection which can let the attacker who get more important information of the server,such as disclosures internal source code of the webapp,database data and invade the internal network.

Description:
I found that users can upload asp/aspx and other dynamic files via the avatar upload function when adding a space character behind the file type to bypass the upload file limit.The attacker can run malicious cmd on the server.

Steps To Reproduce:

1. Sign in the url(https://ecjobs.starbucks.com.cn) and direct to the resume endpoint.
2. Use burp suite tools to interupt the avatar upload request.
3. Replace the filename type `.jpg` to `asp` which have a space character behind and modify the content

After that you have uploaded malicious files on the server and run any os command on server you wanted.
Do some command like list all files on the server

```
curl -i -s -k  -X $'GET' \
    -H $'Host: ecjobs.starbucks.com.cn' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0
    -b $'_ga=GA1.3.779308870.1546486037; ASP.NET_SessionId=w2dbbzgyv3cu0hi1wkysnooo; ASPSESSIONIDSSSBQTQR=
    $'https://ecjobs.starbucks.com.cn/recruitjob/tempfiles/temp_uploaded_739175df-5949-4bba-9945-1c1720e8e
```

Recommendations for fix

*Strictly limit file upload types
*Only allow jpg/png/gif/jpeg file parsing on the uploaded fiels
*More safe code design

Thks!Looking forward to your reply.
With kind regards
John stone

Impact

disclosures the internal source code data and user's information,broken ring server,etc.

still HackerOne staff posted a comment. Mar 8th (9 months ago)
Thank you for reporting this potential issue,

Your report is currently being examined by the HackerOne triage team. You will receive further details, or questions, as soon as technically possible. Thanks for your patience.

Cheers,
@still

still HackerOne staff updated the severity from Critical to Critical (10.0). Mar 8th (9 months ago)

still HackerOne staff posted a comment. Mar 8th (9 months ago)
Hi @johnstone, thank you for your report.

This appears to be reproducible, but please note that your submission is not currently in scope, and the product team will rule whether this is an issue they intend to reward.

Thanks for your patience,
@still

johnstone posted a comment. Mar 8th (9 months ago)
Thks@still
Kind regards
john stone

johnstone posted a comment. Updated Mar 8th (9 months ago)
hi,@still, thank you so much to remind me,but in starbucks policy section of In Scope,they write

`Significant information disclosures such as internal source code, PII, credentials (excluding those identified in other/prior public breaches).`
Disclosures internal source code is eligibled for bounty,i hope my report is eligible for bounty and starbucks team can intend to reward.
Regardless of the results, the process of finding vulnerabilities is what every hackerone pursues.isn't it? :)
By the way,thks again! @still
Kind regards
john stone

coldbr3w posted a comment. Mar 13th (9 months ago)
Hi @johnstone,

The team is reporting back to us that this issue has been resolved. Can you please re-test and confirm that the issue has been fixed?

johnstone posted a comment. Updated Mar 14th (9 months ago)
Hi @coldbr3w ,I'm so happy that the vulnerability was fixed,but there have some potential risk on `/recruitjob/hxpublic_v6/hxdynamicpage6.aspx?_hxpage=hxsm_v6/hxsm_file_upload_process.hxpage.xhtml&max_file_size_kb=1024&allow_file_type_list=jpg;gif;png;` endpoint,
I found delete the `allow_file_type_list` parameter when i try to bypass upload limite that can be uploaded the docx/xls/csv files,the `hxsm_file_upload_process.hxpage.xhtml` endpoit did't checked if it is a picture.the docx/xls/csv can also cause the server to receive an attack via XXE.

Recommendations for fix

1. Change the upload files to base64
2. Transcode the base64 data on the server to picture
3. Check if it is a picture files

Thank you @coldbr3w
Kind regards
john stone

johnstone posted a comment. Mar 15th (8 months ago)
hi @coldbr3w .After a few days of testing, I found that the vulnerability seems to have been fixed.

johnstone posted a comment. Mar 16th (8 months ago)
Hi @coldbr3w.Can you change the reports statue to resolved?(XXE report and this one to Starbucks)thks
Kind regards
John stone

johnstone posted a comment. Mar 18th (8 months ago)
Any update in this report?

coldbr3w closed the report and changed the status to ● **Resolved**. Mar 20th (8 months ago)
Thank you for your patience @johnstone and confirming that a fix has been applied. We plan to award bounties for your recent submissions in the coming week and look forward to working with you again in the future.

It's important to note that the content of this report, as well as the ensuing conversation, are, by default, private between the two parties. Only when an organization decides to make the report public (usually sometime after the fix has been applied) will other users be able to access the report.

johnstone requested to disclose this report. Mar 29th (8 months ago)

Starbucks rewarded johnstone with a **$4,000** bounty. Apr 4th (8 months ago)

Hi @johnstone,

Although this asset is not explicitly included in the bounty program's scope, we award bounties for reports demonstrating "significant information disclosure" against other assets. The ability to remotely execute code on a system (RCE) generally allows significant information disclosure. As such, we have determined that this report is eligible for a bounty. In the meantime, we're working on updating the program scope to explicitly identify reports demonstrating RCE as bounty eligible.

Thanks again for the report!
@shadegrown

shadegrown cancelled the request to disclose this report. Apr 4th (8 months ago)

Also, we'd like to hold off on disclosing any reports for this site until our China team has a chance to fix all of the related issues and make sure the site is a little more stable. At that point, we'll be happy to work with you to disclose this report. Let's plan to check back in on this in 3 months and reevaluate whether the timing is right for disclosure.

Thanks!
@shadegrown

johnstone posted a comment. Apr 4th (8 months ago)

Thank you @shadegrown ,I was so glad for eligible bounty that gave me a lot of confidence,In the meantime， I also appreciate the attitude of the Starbucks Security Team in handling reports.So look forward to working with Starbucks again in the future.
Thanks!
@johnstone

johnstone requested to disclose this report. Oct 18th (about 1 month ago)

agedsumatra agreed to disclose this report. Nov 13th (12 days ago)

This report has been disclosed. Nov 13th (12 days ago)

After the researcher asked to disclose the report, the team at Starbucks requested to wait until the vulnerable asset had proven to be stable. Six months later, the report was disclosed to the public.

In the next lesson, we'll look at how to deal with ethical hackers.