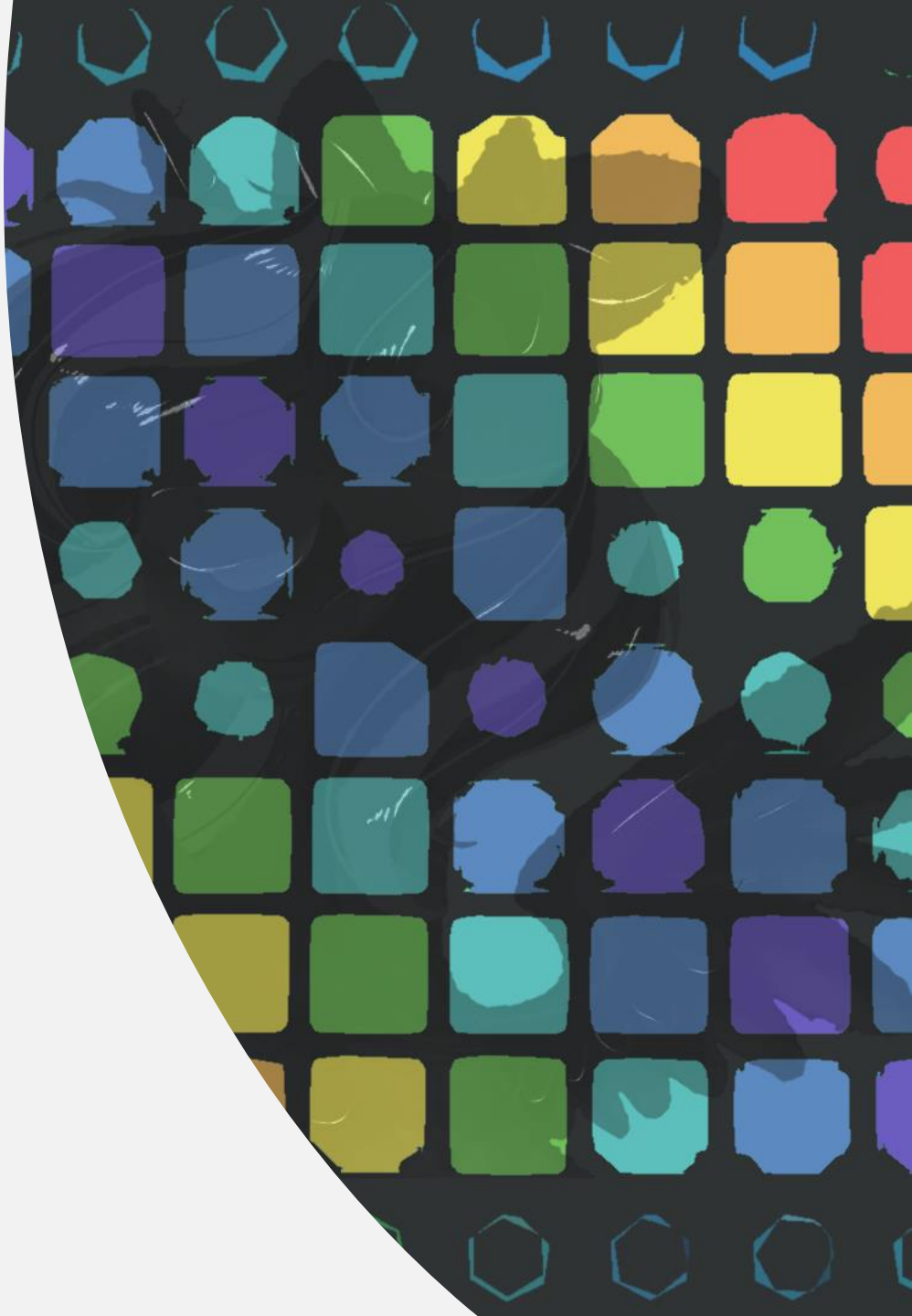
誤打誤撞的第一支 Bug Bounty

whoami



Still Hsu

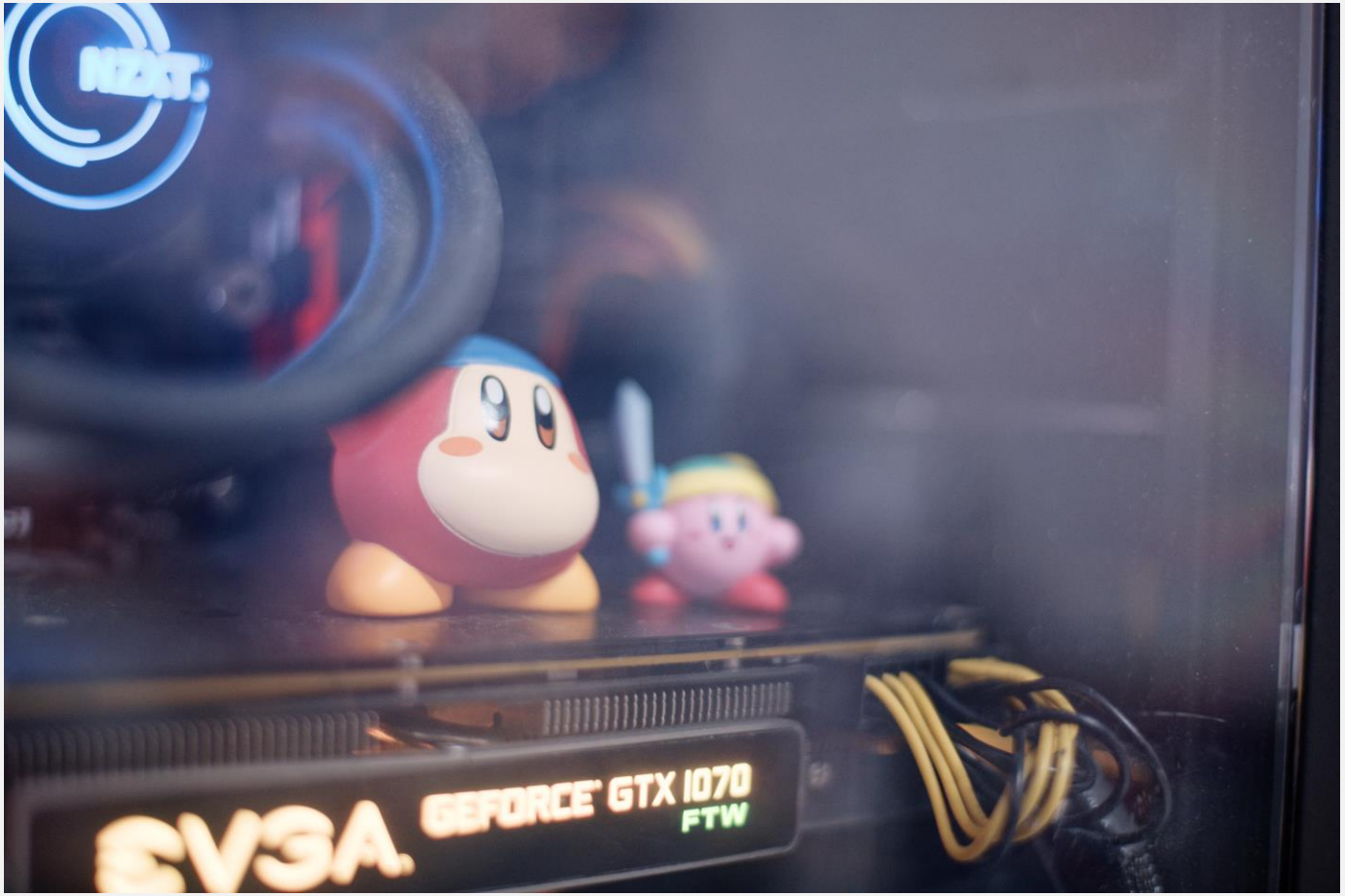
- Security researcher
  - Reverse engineering / websec / forensics
  - Windows-focused
- Developer
  - .NET / PowerShell (Core)
    - Discord.NET docs maintainer
  - Node.JS
- English major @ NPTU
  - Native English speaker
  - 2020 graduate

第一章

背景故事

故事是這樣的...

故事是這樣的...

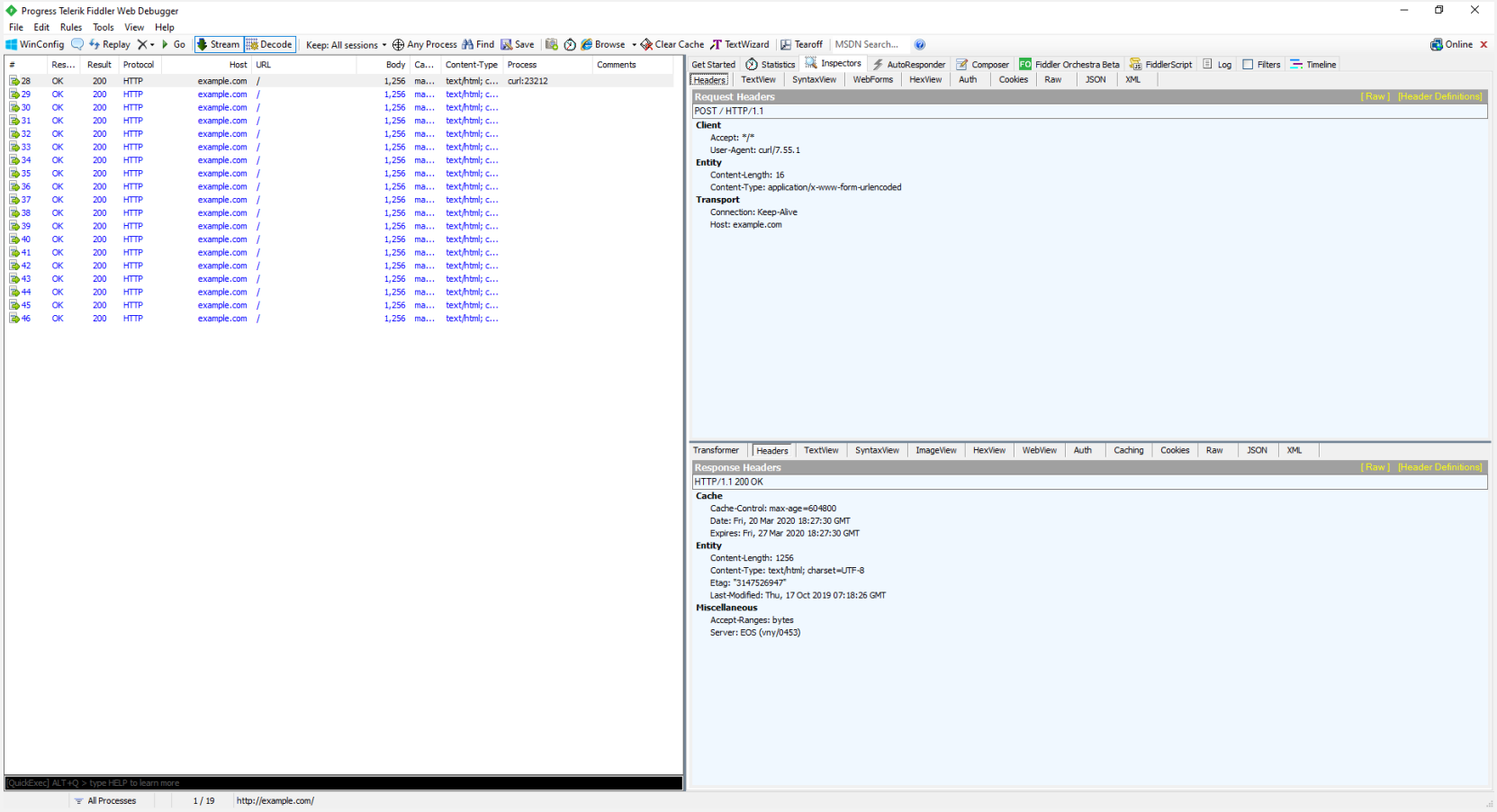


故事是這樣的...

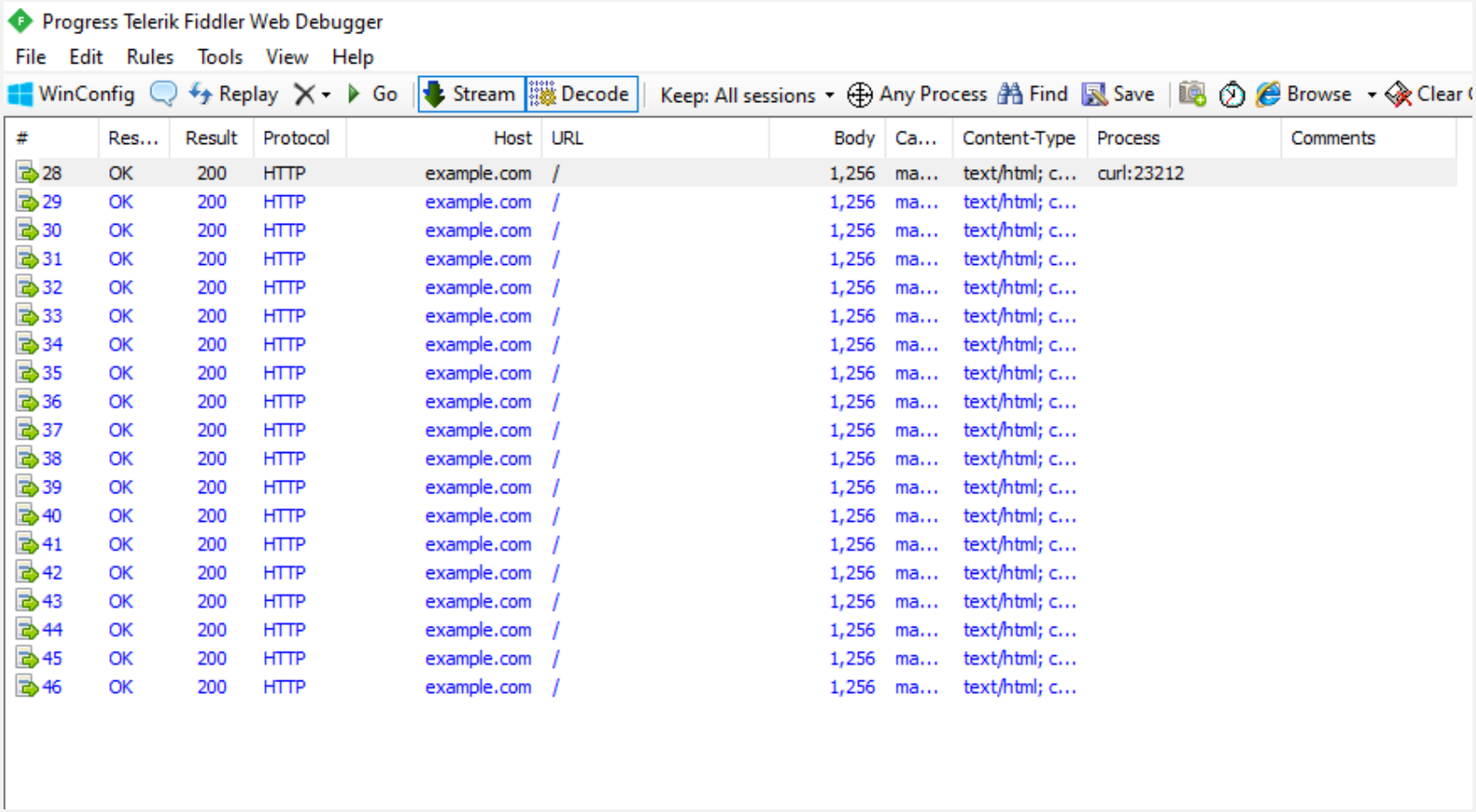

NZXT CAM
我寶貴的
CPU資源

工程師精神發作

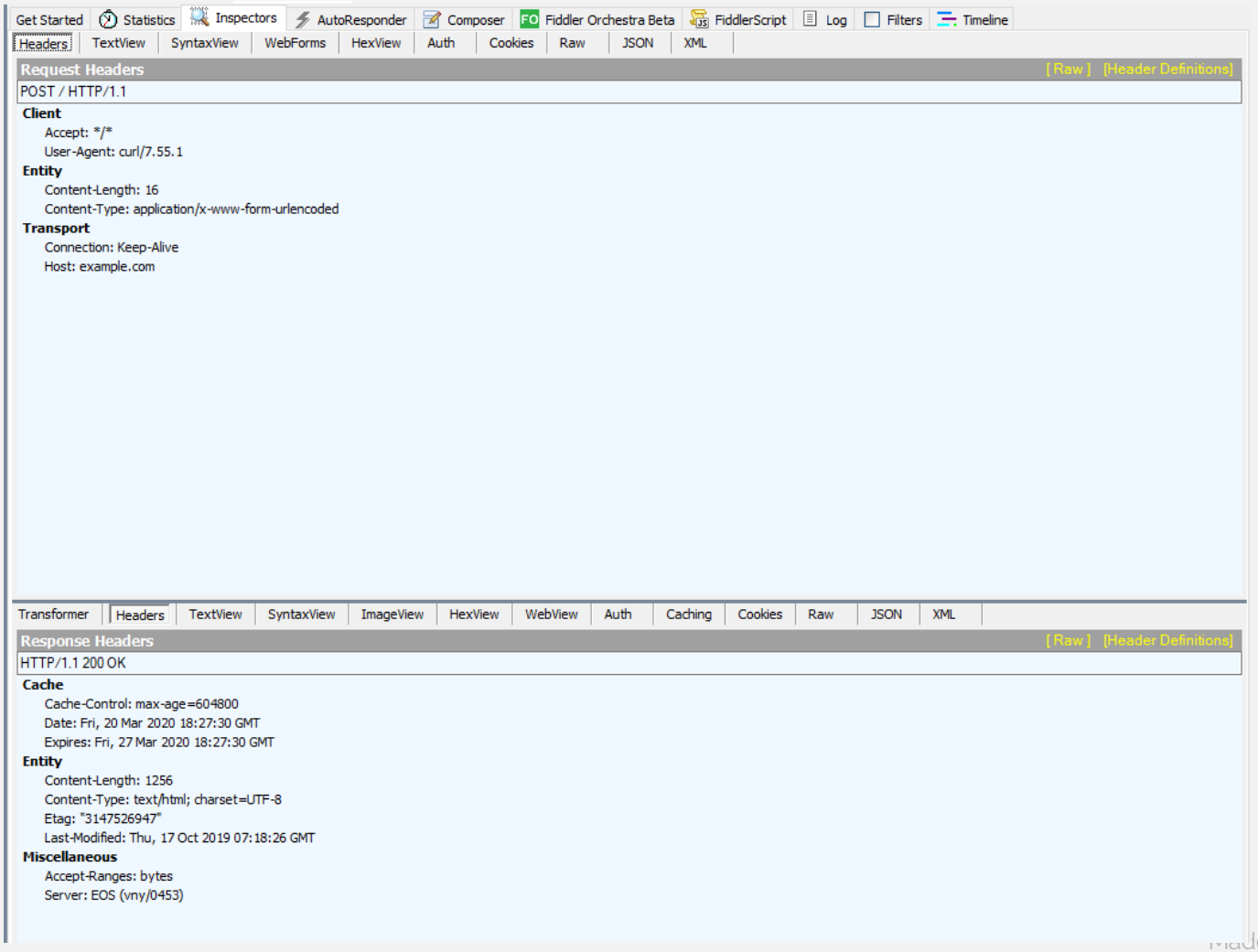
Fiddler



Fiddler



Fiddler



很快地解釋 Fiddler

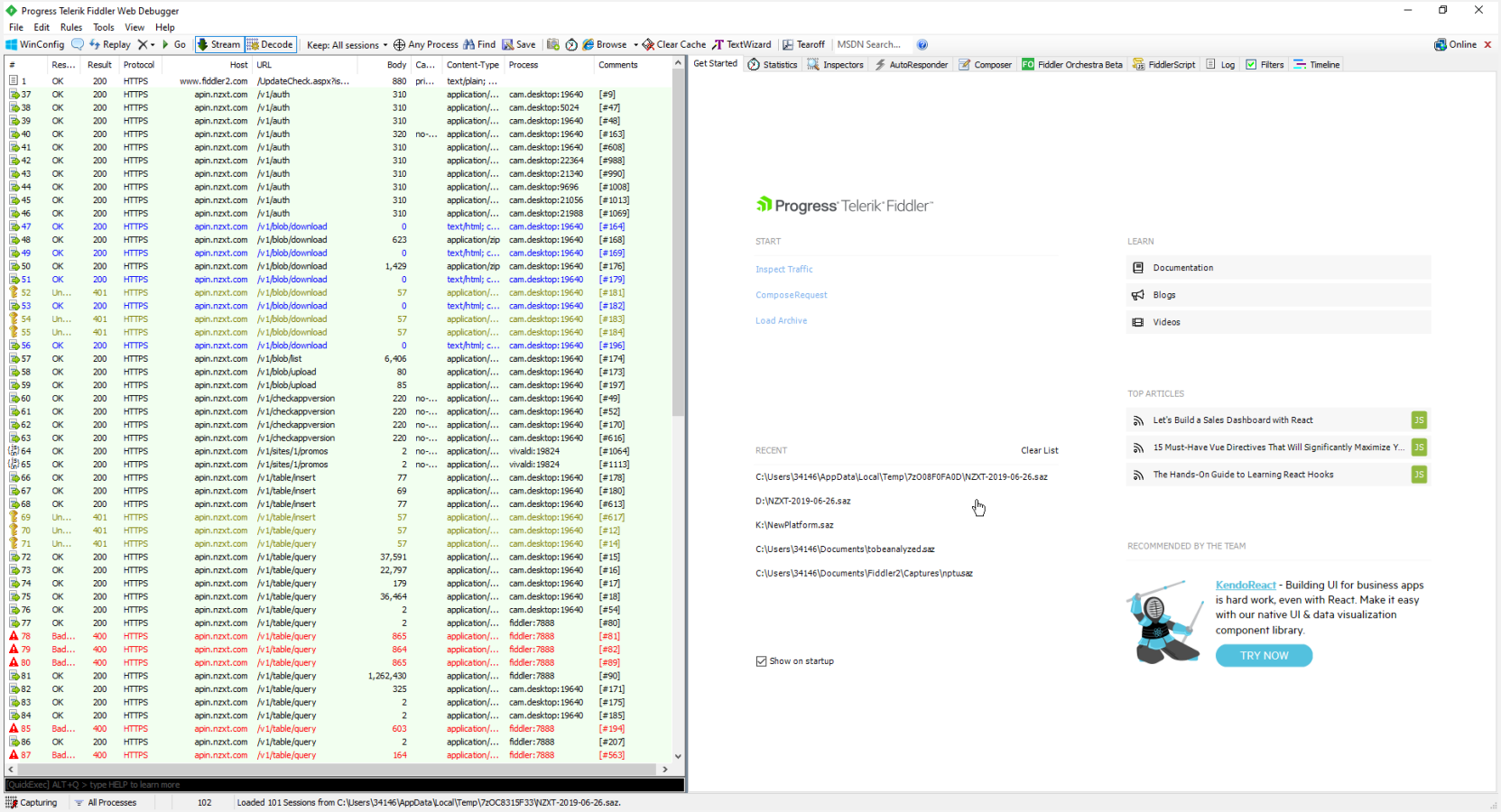
- Debug proxy
  - Intercept traffic
  - Decrypt HTTPS (CA Root)
  - MITM-attack analysis
  - Stress-test (send multiple requests)
  - Scriptable
- Windows-only (for now)
  - Fiddler Everywhere (Beta) for Mac/Linux
- Free
  - Unlike Burp which loves to put things under paywall

工程師精神發作

第二章

分析時間

所有 CAM 丟出的請求

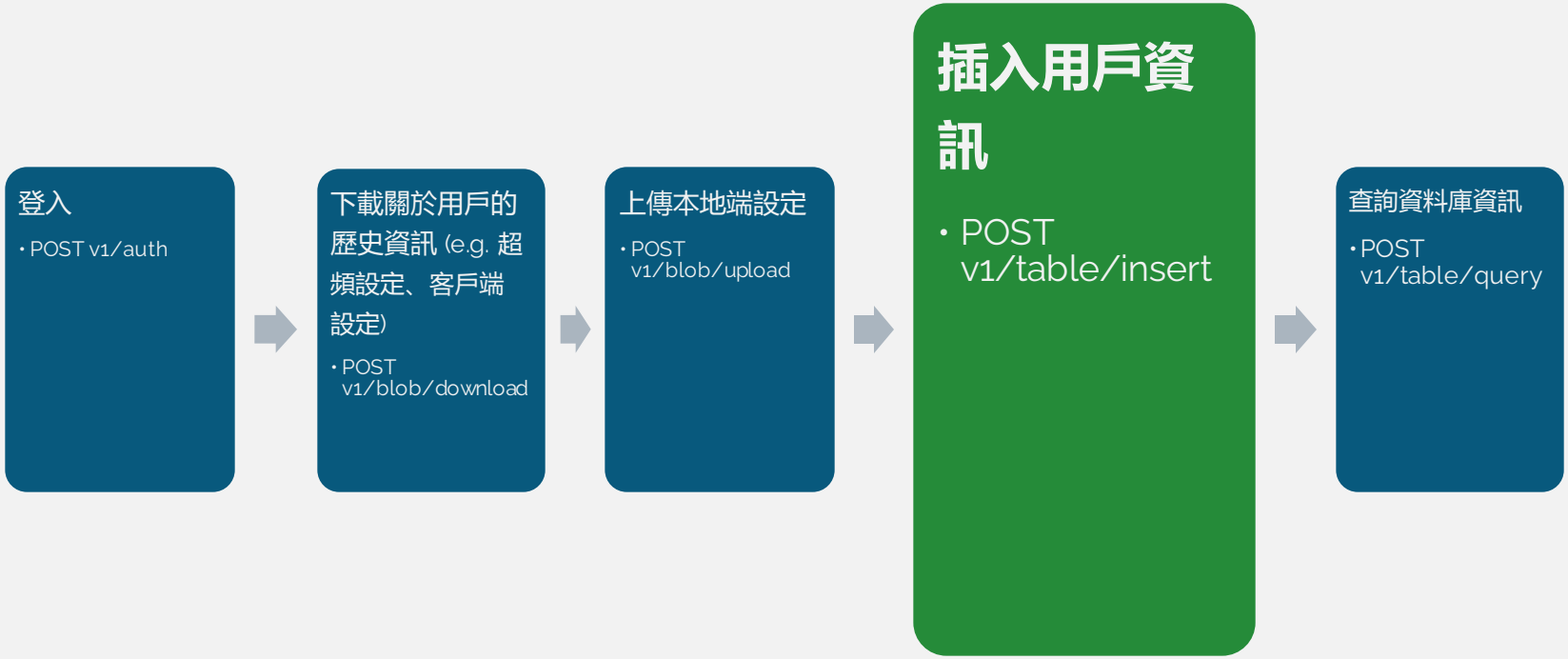


分析請求

分析請求

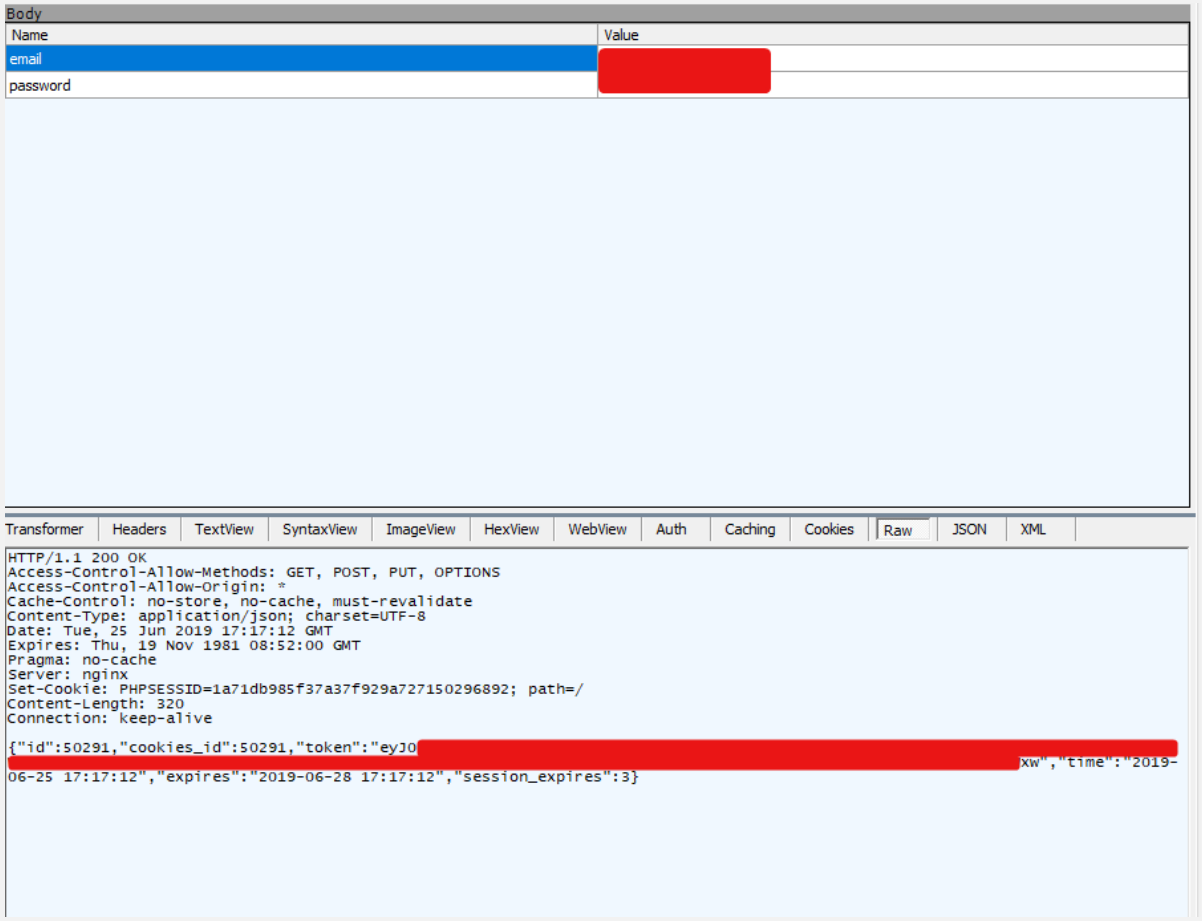
分析請求

分析請求

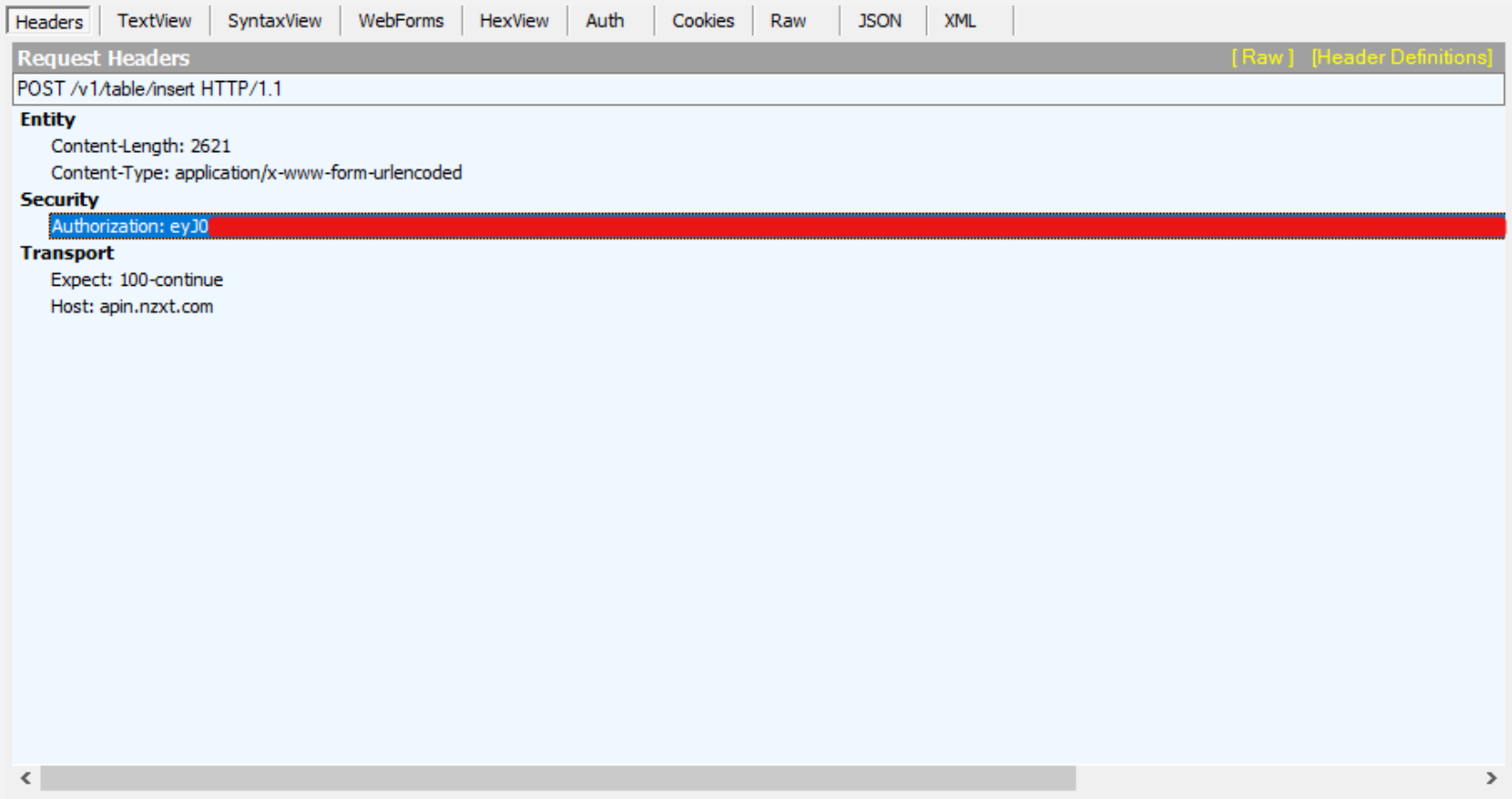


分析請求

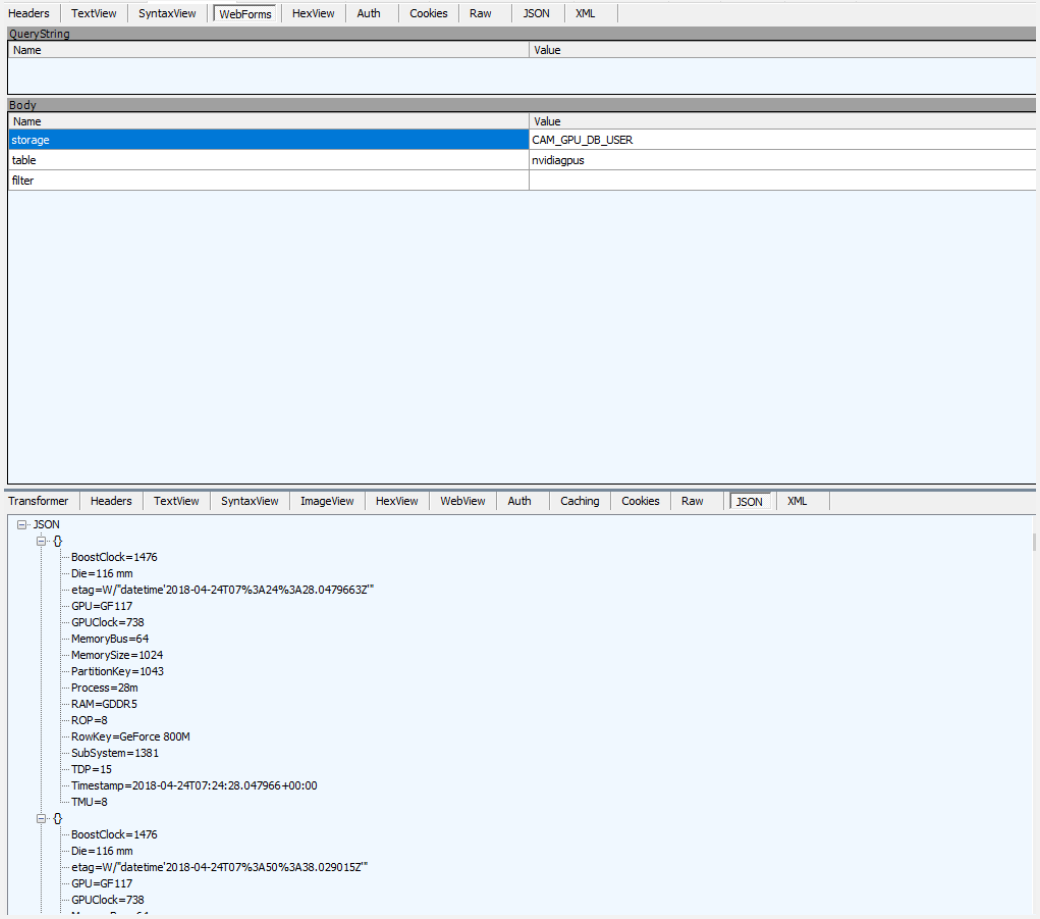
登入請求



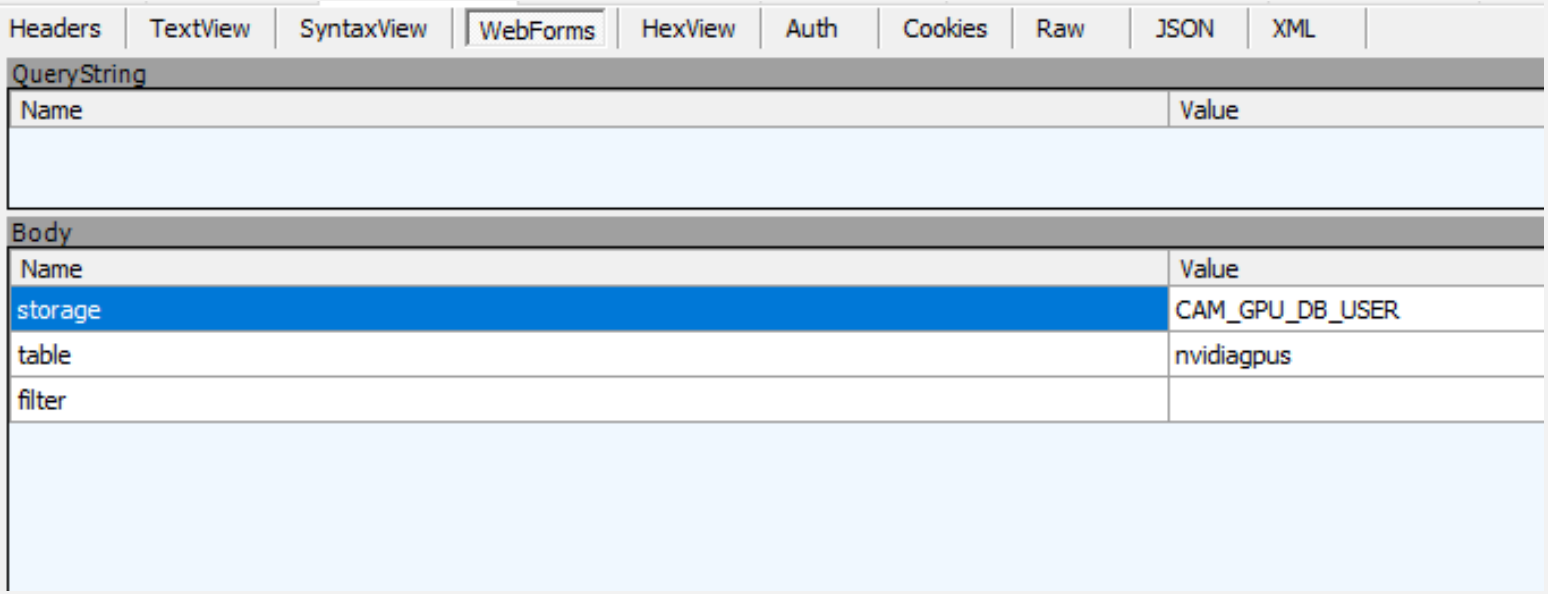
所有登入後的請求



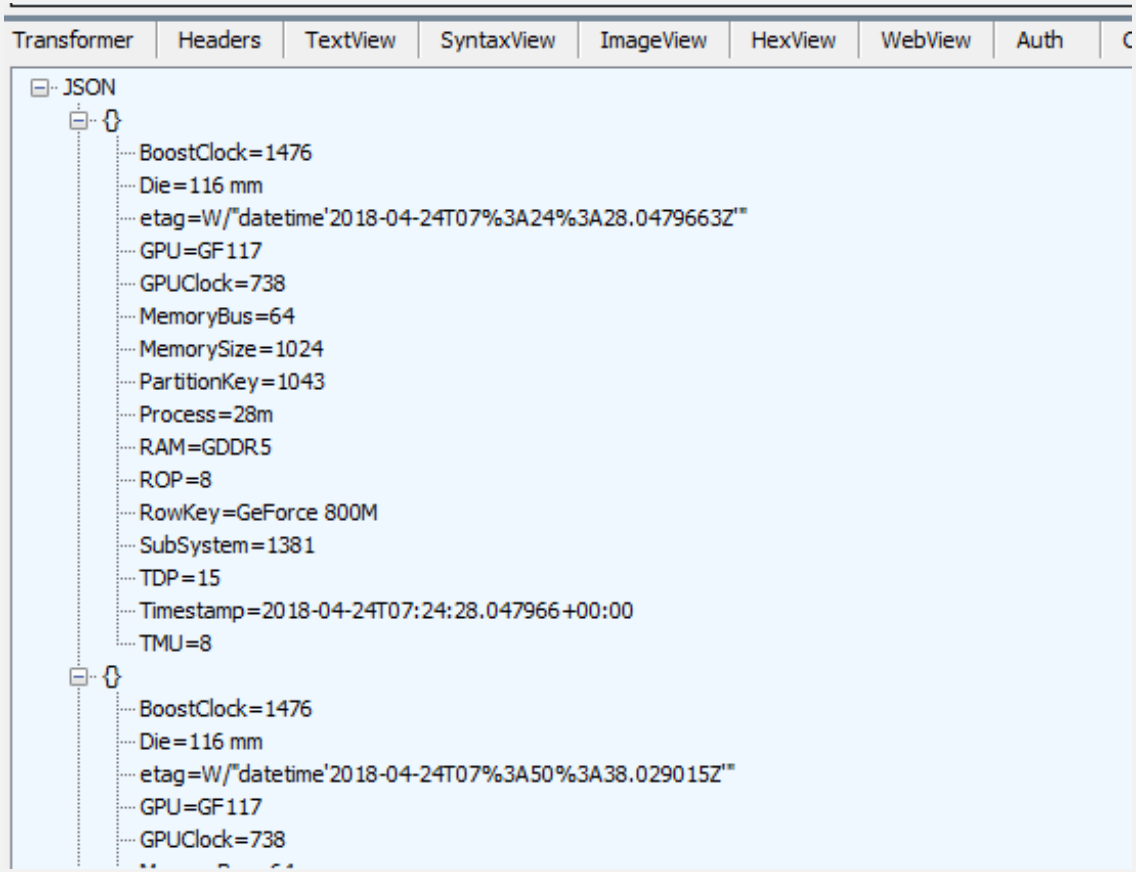
開始亂翻請求



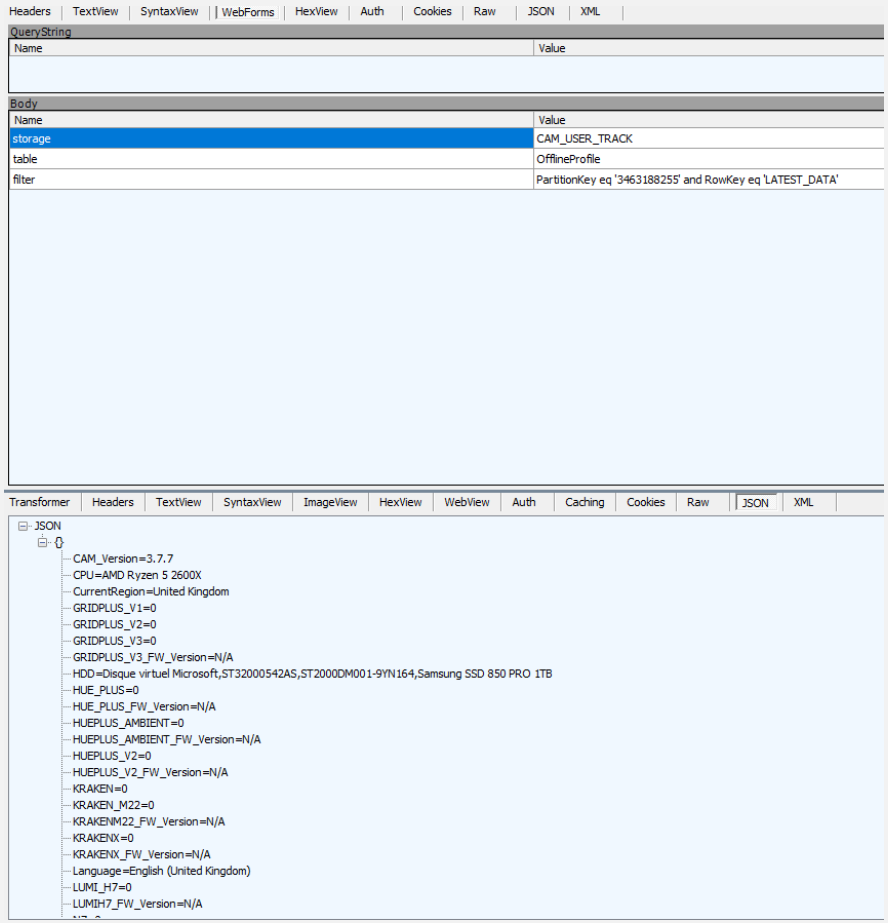
開始亂翻請求



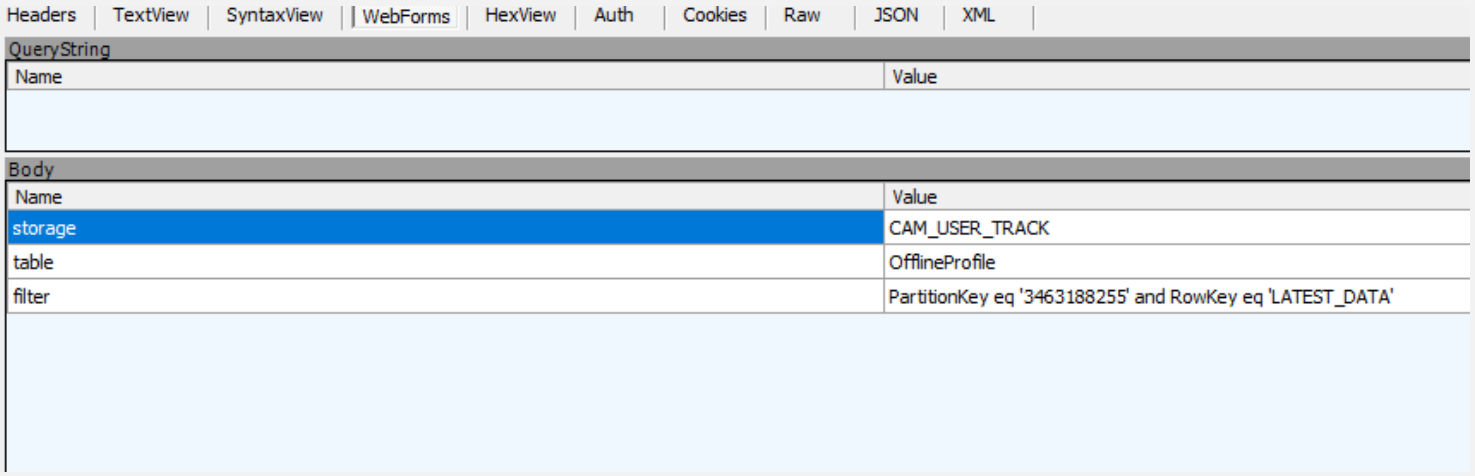
開始亂翻請求



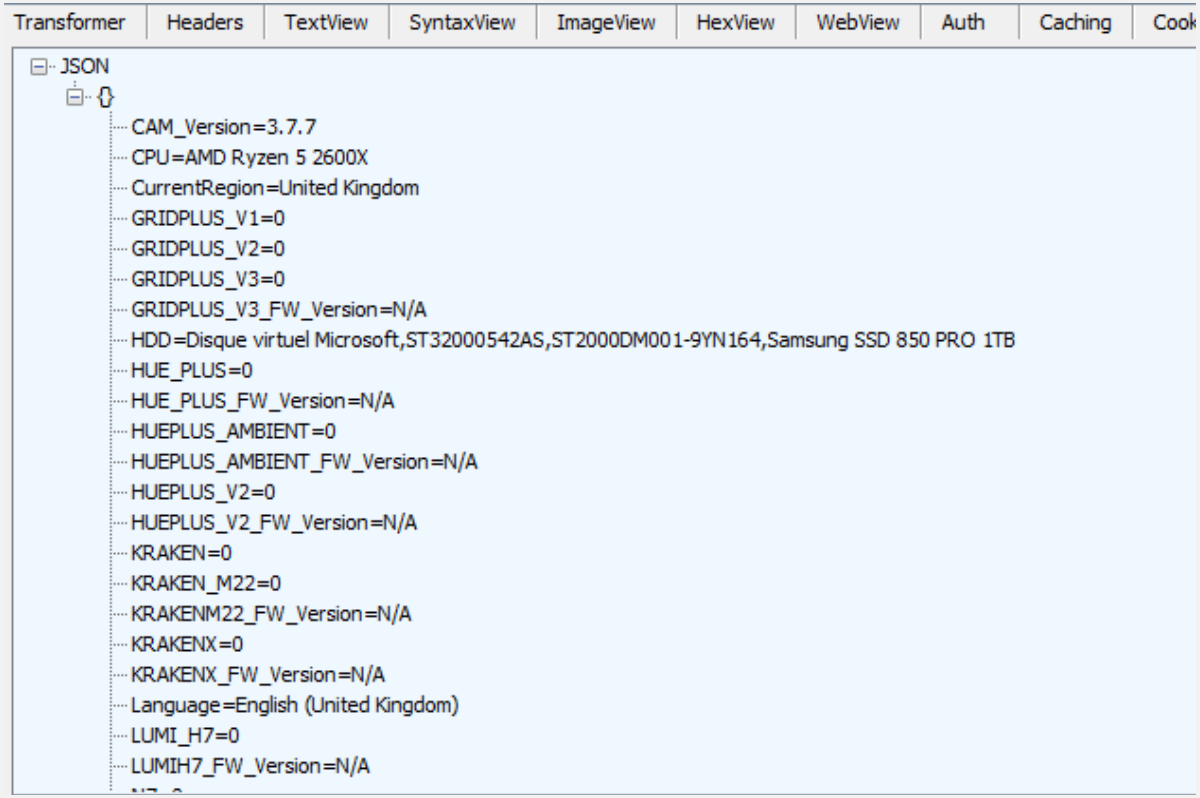
開始亂翻請求



開始亂翻請求

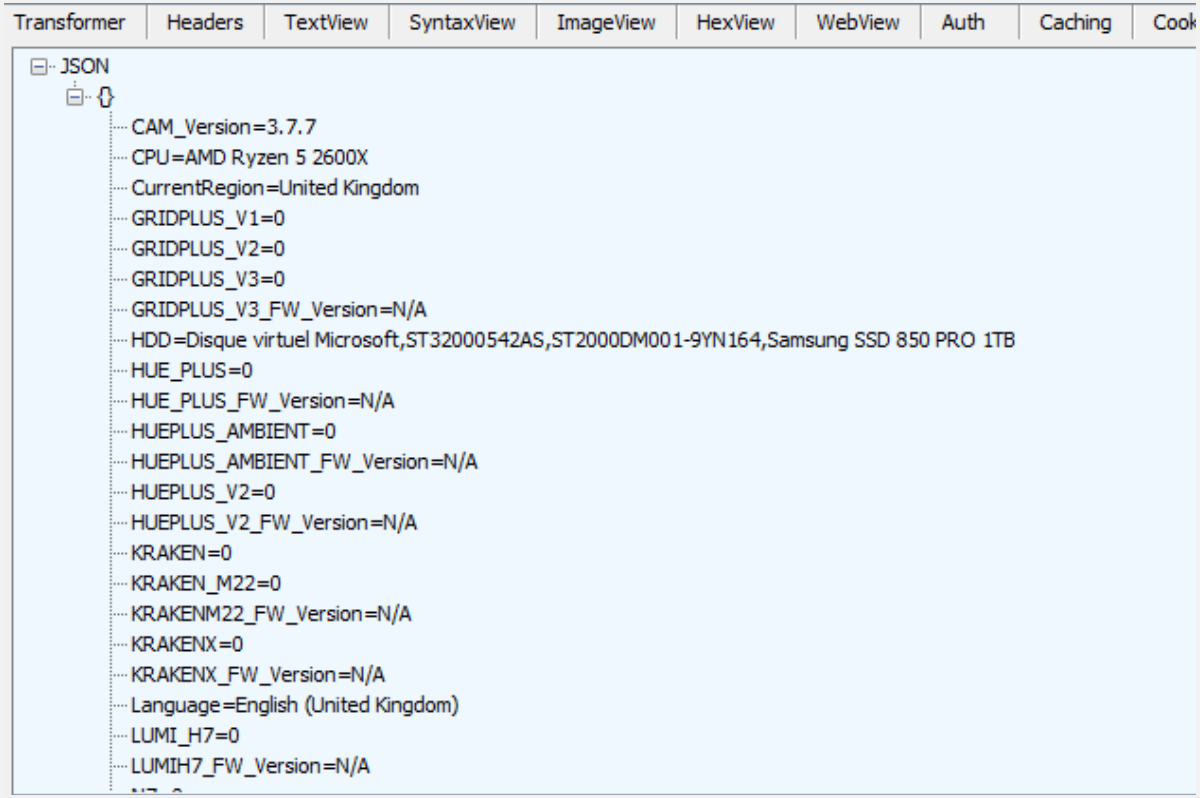


開始亂翻請求

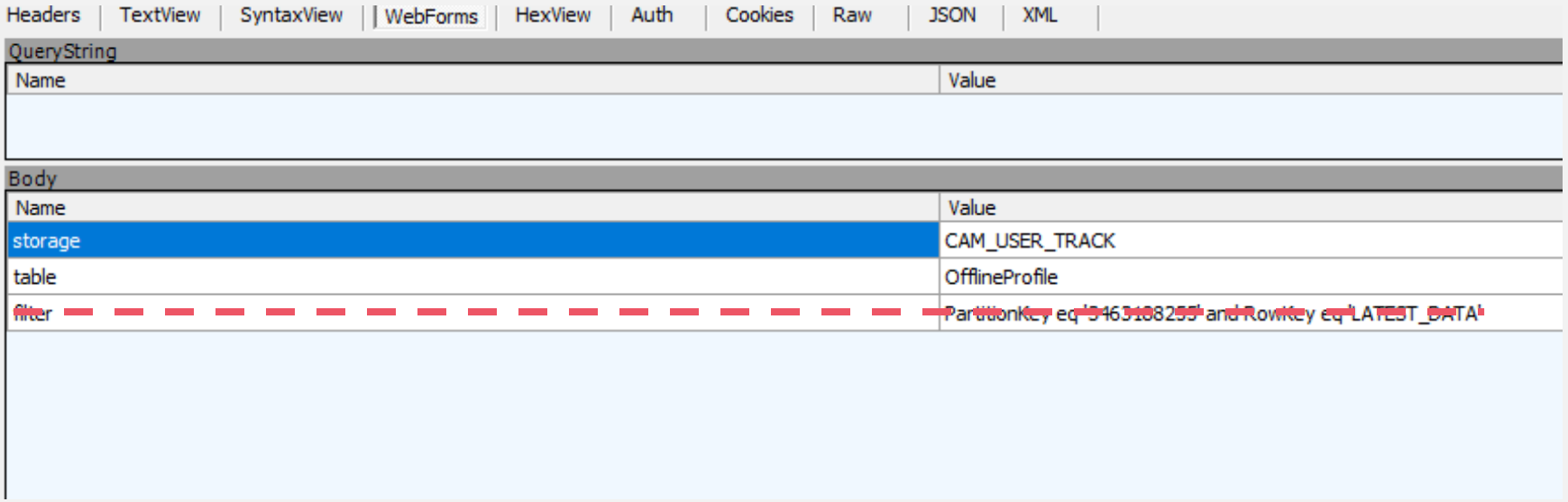



修但積累

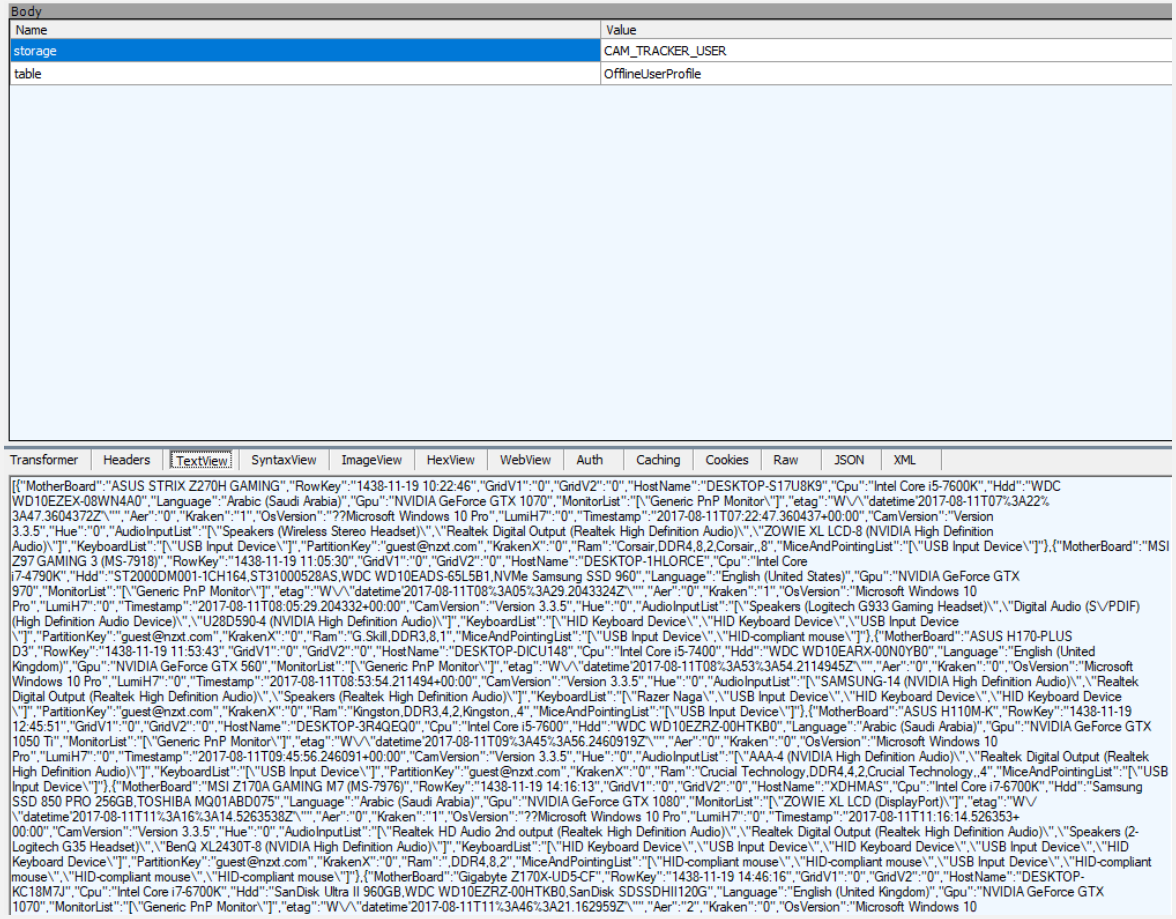
這不是我的電腦阿???



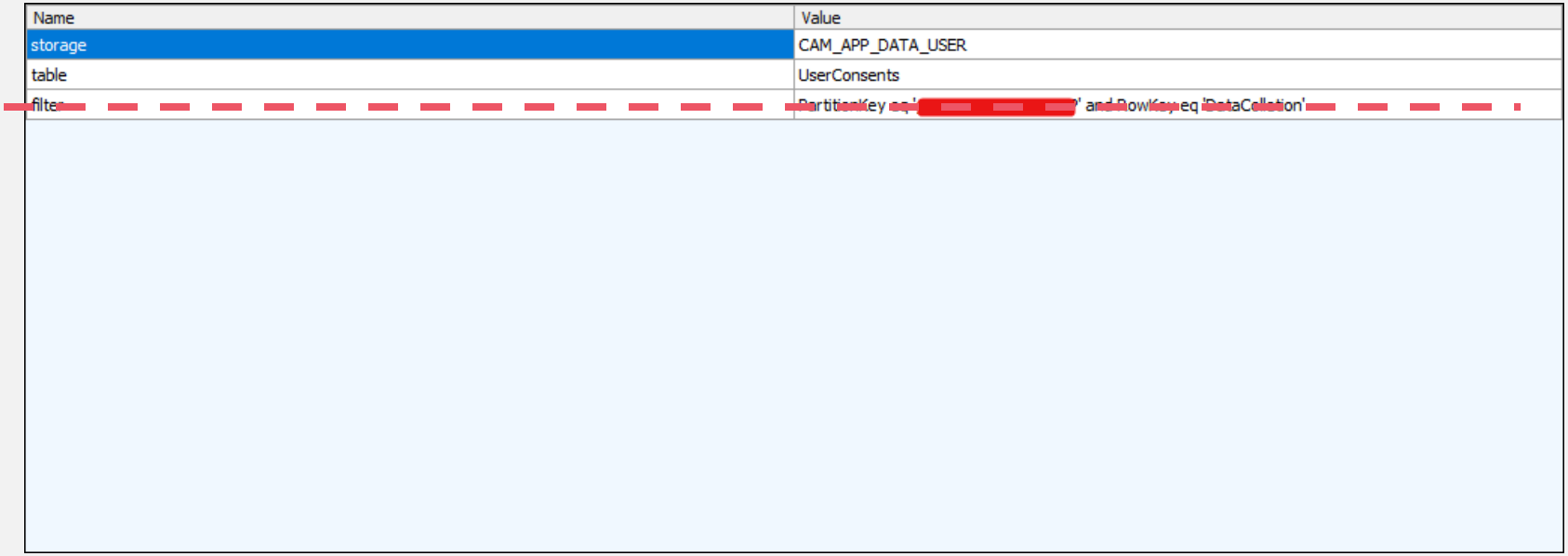
我把這串幹掉會怎麼樣?



噴出一堆人的硬體資訊



好喔那我試試看這個



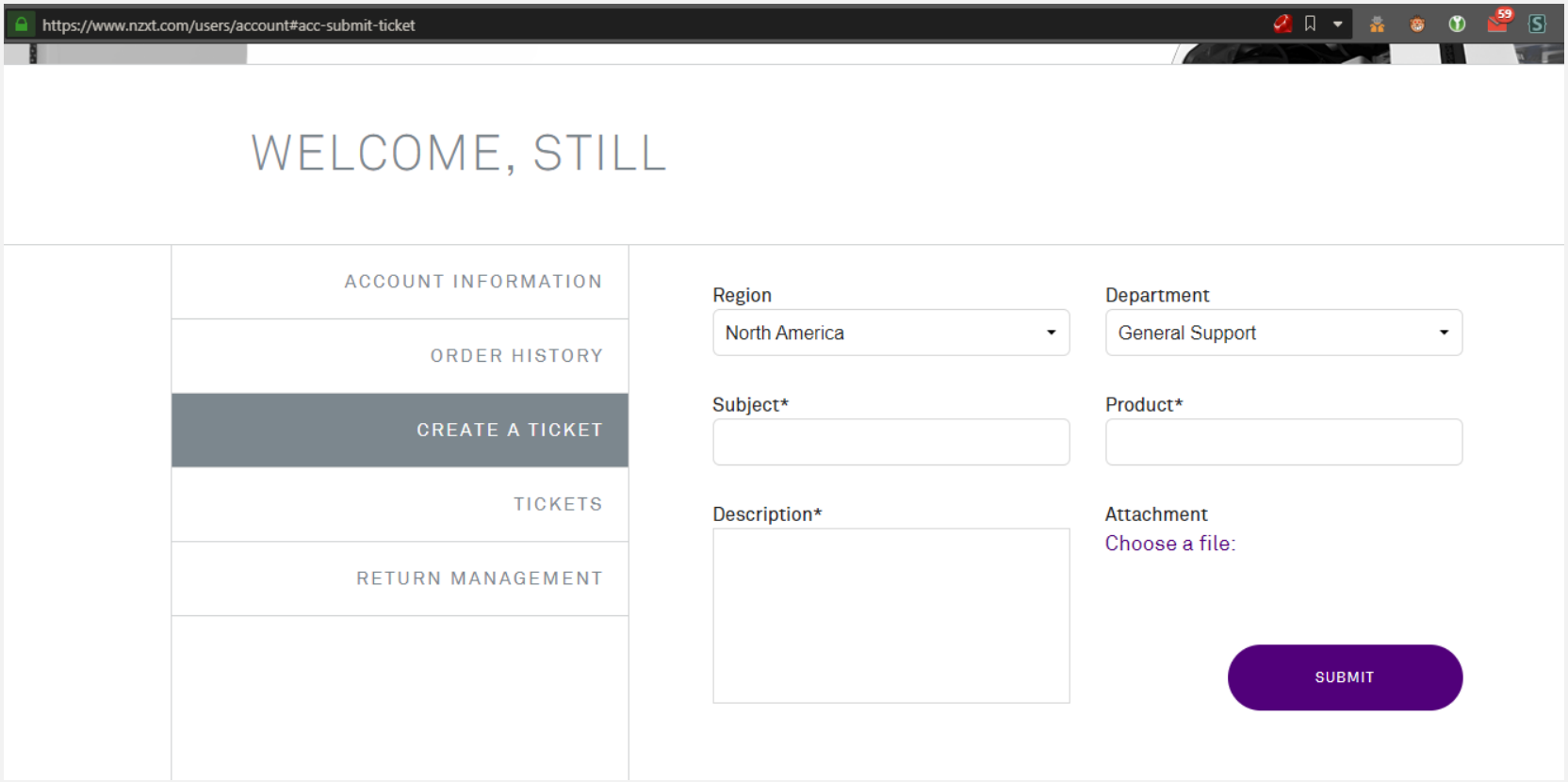
Name	Value
storage	CAM_APP_DATA_USER
table	UserConsents
filter	PartitionKey eq '[redacted]' and RowKey eq 'DataCollation'

噴出一堆人的Email + 電腦名稱

第三章

意外的轉折

通報去



初次通報 2019/06/26

Still
9 months

Hello,
I'm writing to inform the dev team that there may be a potential database leak from the NZXT API query. I noticed that CAM was sending API requests to apin.nzxt.com, and I was able to send a request using the guest token to query tables such as user data collection consent status, which contained unique user information such as the user's email and Windows identifier.

While I only tested the UserConsents table, shouldn't the database be locked behind a more secure authentication?

- 2019-06-26_01-34-12-(Fiddler).png (190 KB)

同一天...

NZXT

Dominic Fragoso

9 months

Hey there,

Thank you very much for bringing this to our attention. We really appreciate it.
We have sent this info over to our engineers so they can look into it.
Dominic Fragoso
CAM by NZXT
camwebapp.com

隔天 06/27/2019

Dominic Fragoso
9 months

Hey there,

Again, thank you for the info on this.
The engineers/dev team have located the issue and are working on this.

Look out for an email from them saying thank you for all of this.

Please feel free to contact us at any time and have a good one, take care!
Dominic Fragoso
CAM by NZXT
camwebapp.com

好了收工回家

等等不就這樣而已嗎

等等不就這樣而已嗎
你說還有是什麼意思

意外的訊息

意外的訊息

Thu, Jul 11, 2019, 12:00 PM

意外的訊息

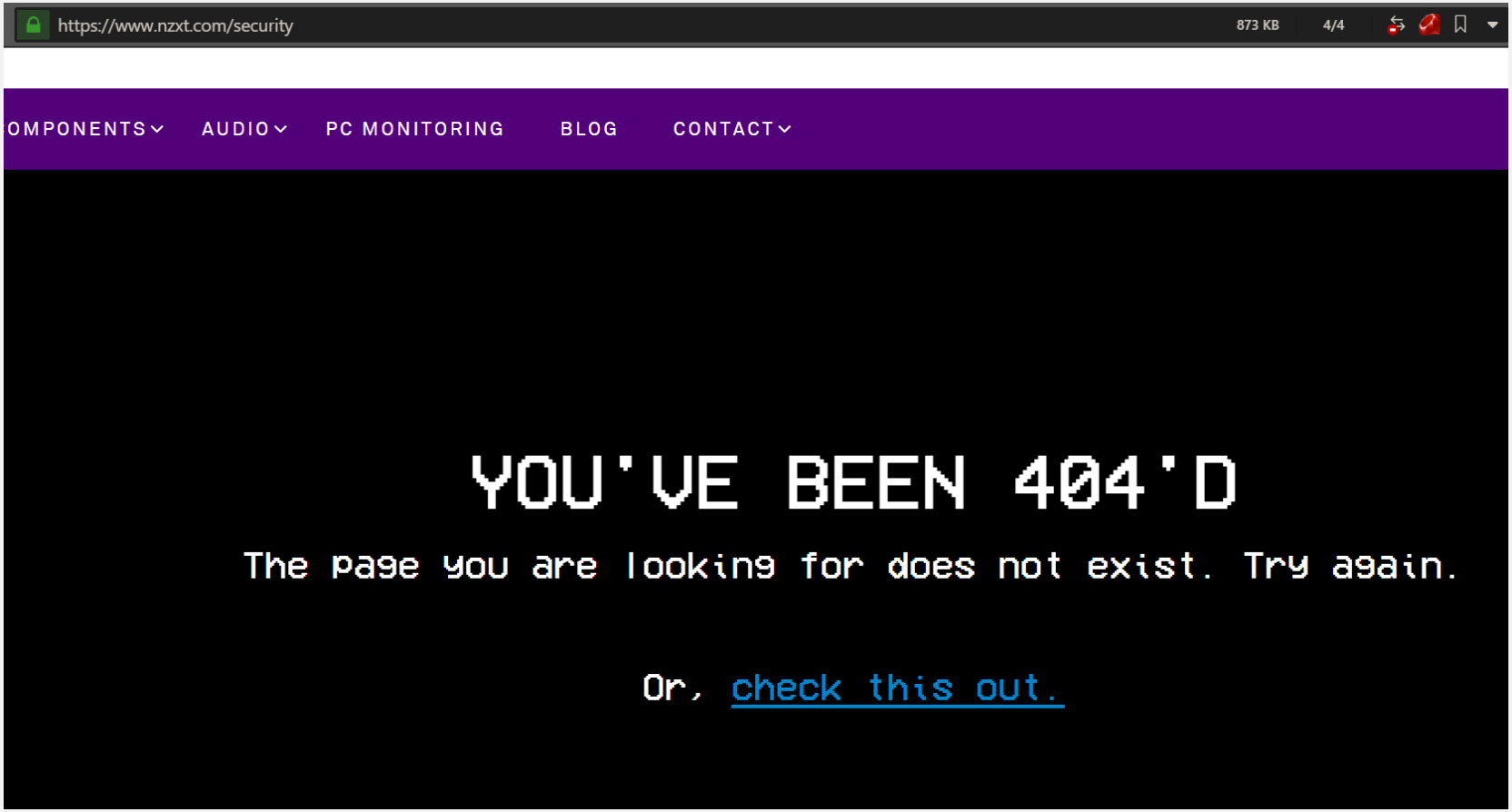
NZXT Rep Jul 11, 2019, 12:00 PM

Hi, just wanted to say thanks for pointing out the security issue and I would like to reward you with some bounty money or NZXT part let me know how to reach you

Thanks

為什麼我很意外?

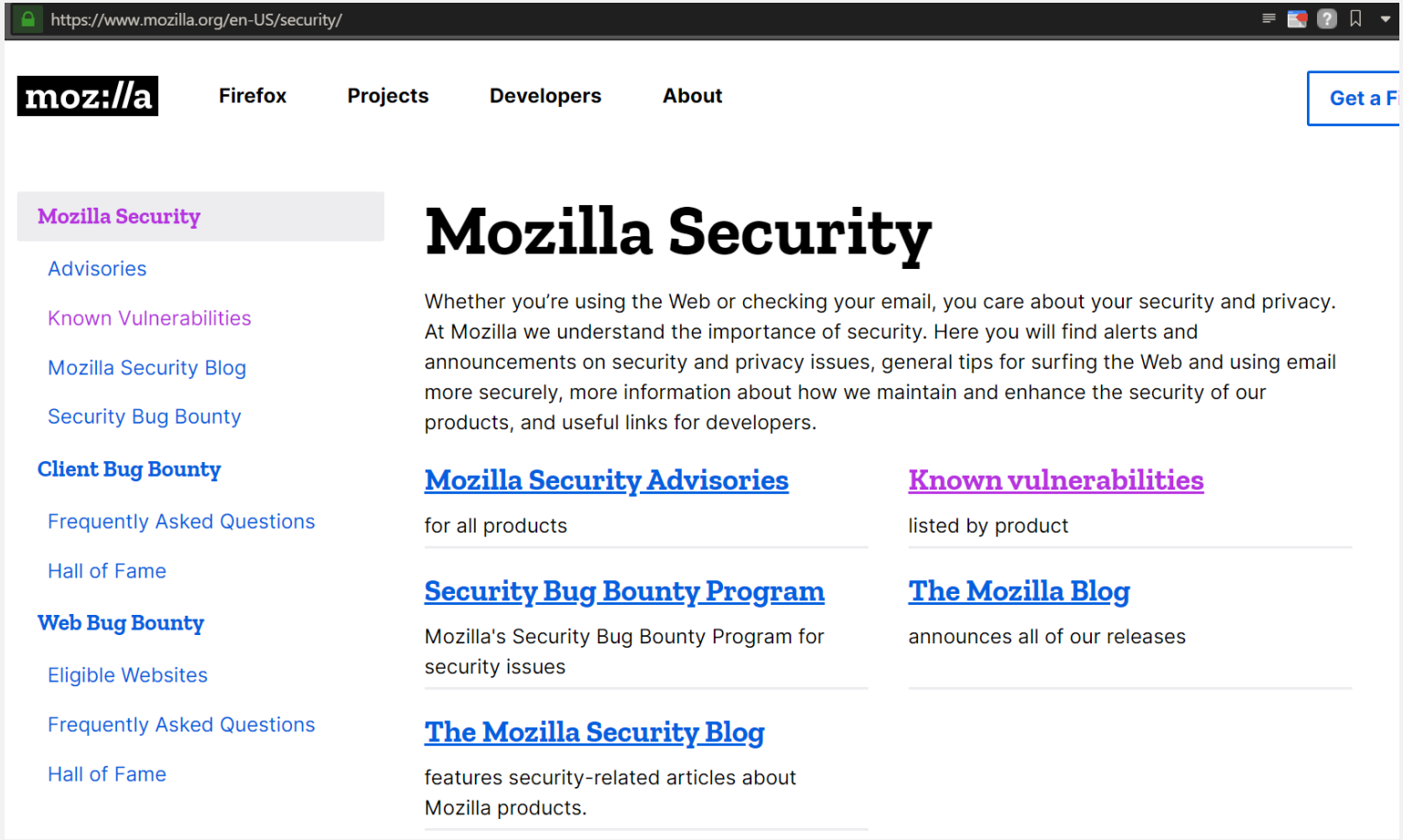
沒有VDP頁面



Vulnerability Disclosure Policy

- VDP 是公司用來跟白帽/灰帽講...
  - 不要亂搞我們系統
    - 你只能在我們指定的區域內亂搞
  - 找到問題先回報
  - 給我們X天的時間維修
  - 你只要違反...
    - 「我們有權告你」

大部分公司都有VDP Guideline



Still Hsu Jul 11, 2019, 1:56 PM

Hi,

Good to hear that the vuln has been fixed! I actually was not expecting to be rewarded for that. However, I'm actually from Taiwan so I'm not too sure how this would work out. Regardless, here is some of my contact information.

Name: Still Hsu

PayPal: [REDACTED]

Tel: +886-[REDACTED]

Add: [REDACTED], Taiwan (R.O.C.)

哦哦看來有希望?

NZXT Rep Jul 17, 2019, 12:09 PM

HI Still,

I'll talk to our Taiwan team to check how can we proceed

Thanks ;)

Still Hsu Wed, Jul 17, 2019, 1:32 PM

No problem. Thanks!

約兩周之後...

NZXT Rep Jul 30, 2019, 5:52 PM

Hi Still, I'll let you know when I have update on this

Thanks

NZXT

沒關係，跨國溝通嘛
可能需要一點時間

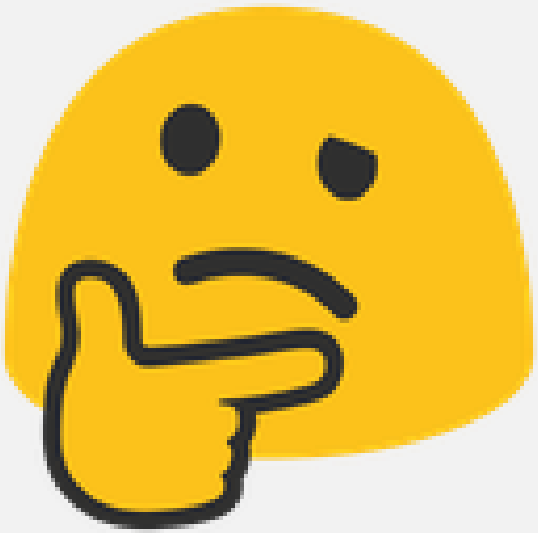
約五周之後...

Still Hsu Sep 7, 2019, 4:40 AM

Hey there,

Has there been any update on the TW branch? Just checking in since it's been a while.

Thanks!



NZXT Rep Sep 7, 2019, 5:46 AM

Hi Still, let me check if not I'll handle it next week

Sorry for the delay :(

NZXT Rep Sep 10, 2019, 8:56 PM

Hi Still, can you receive money from paypal or something similar or do you prefer some NZXT Parts?

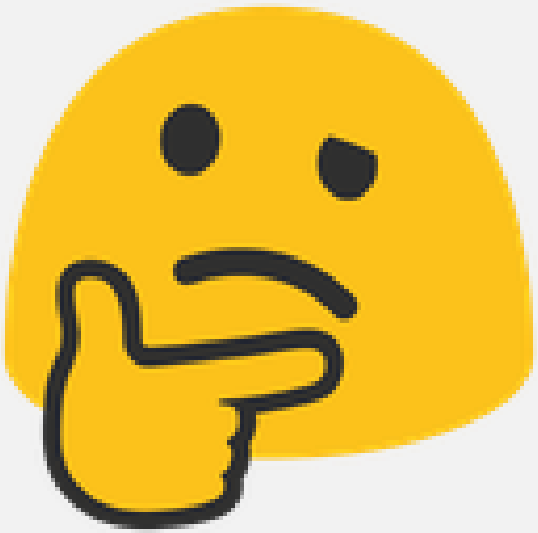
Thanks

NZXT

Still Hsu Wed, Sep 11, 2019, 1:00 AM

I can via PayPal, [REDACTED], same as this email.

Thanks!



NZXT Rep Sep 13, 2019, 9:16 PM

Hi Still , I'll be sending US $250.00 next week , hope that helps ;)

NZXT

Still Hsu Fri, Sep 13, 2019, 9:25 PM

Awesome! Appreciate it! By the way, just curious, do you guys plan on disclosing a bug bounty program? I walked into this not expecting a bounty since I didn't find any page like that on your company's website.

Thanks again!

NZXT Rep Sep 13, 2019, 9:27 PM

Hi Still, as of this moment we do not, we do plan on talking about this for our plan for 2020. But right now we dont ;)

Thanks

NZXT

約一周之後...

NZXT Rep Sep 23, 2019, 9:27 PM

Hi Still, still waiting for this to be process, will keep you posted , should be done this week . Sorry for the delay

NZXT

約一周之後...

Still Hsu Sun, Sep 29, 2019, 10:50 AM

Hi,

Thanks for the update, but it's been almost another week. Could I get another status update on what's going on? It is getting a little bit unbearable at this point.

NZXT Rep Sep 29, 2019, 10:57 AM

Hi Still, really sorry you haven't gotten the payment. I'll handle it ASAP. I'll add another 50 for the delay.

I'll send you the money personally this week

Thanks and truly sorry again

NZXT

Still Hsu Sep 29, 2019, 11:07 AM

Hi,

Thanks for the quick response. While it's not *that* big of a deal for me, I would certainly love to get the transaction done as soon as possible. I'm sure it's not straightforward on your side either, so I appreciate the responses.

Thanks.

NZXT Rep Sep 29, 2019, 11:09 AM

No pro I understand. I'll get this resolved ASAP for you

Again sorry for the delays

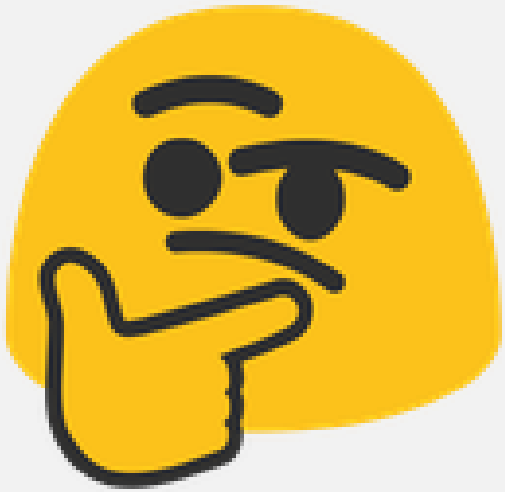
NZXT

又過了一周之後...

Still Hsu Sat, Oct 5, 2019, 2:54 AM

Requesting another status update. May I ask what the trouble is? Is it PayPal or...?

Thanks



NZXT Rep Oct 5, 2019, 3:10 AM

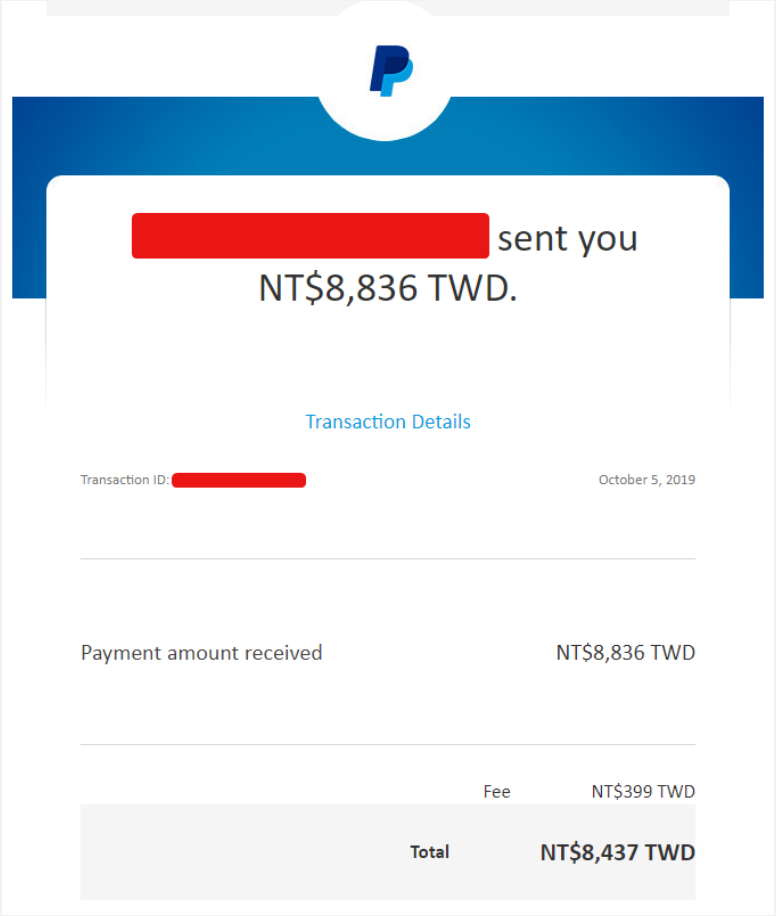
Nop, you will get your payment today ;)

All is on time

Thanks

NZXT

圓滿收場


[redacted] sent you
NT$8,836 TWD.

Transaction Details

Transaction ID: [redacted] October 5, 2019

Payment amount received	NT$8,836 TWD
Fee	NT$399 TWD
Total	**NT$8,437 TWD**

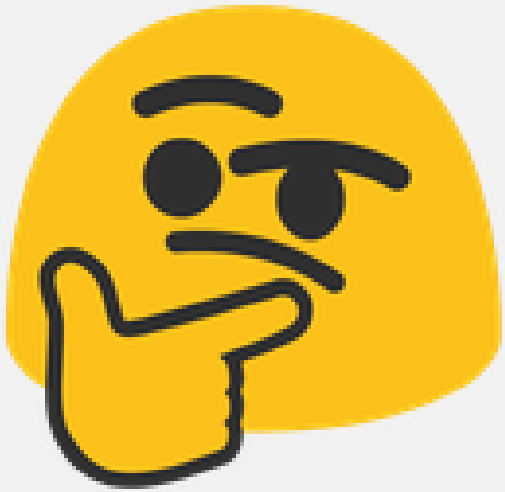
圓滿收場...?

Still Hsu Sat, Oct 5, 2019, 6:58 PM

Received about $285, was the fee deducted by PayPal? If so, then that's correct, thanks.

Still Hsu Sat, Oct 5, 2019, 10:51 PM

Actually, no, upon further inspection, PayPal deducted yet another 13 dollars, so I'm only receiving about $272.



NZXT Rep Oct 5, 2019, 11:07 PM

-_- , sorry for that reduction I'll later send the rest :(

Thanks

NZXT

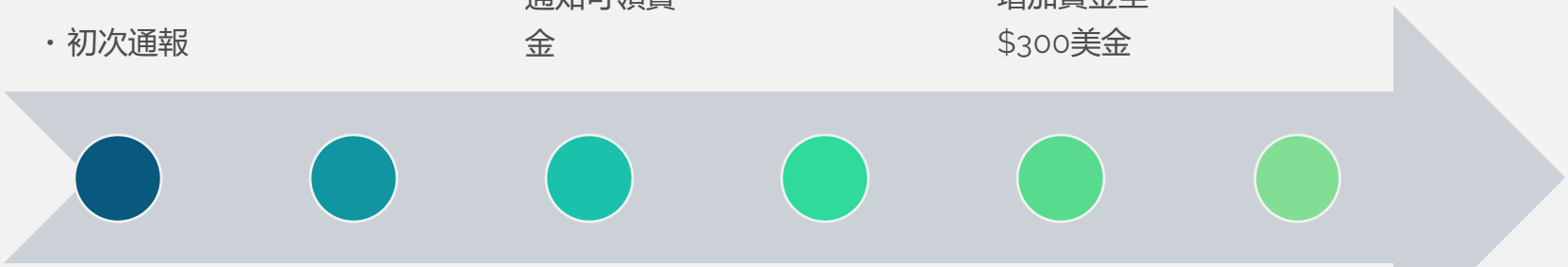
然後...

沒下文。

第四章

結論

時間線



06/26
- 初次通報

06/27
- 收到通報，已報修

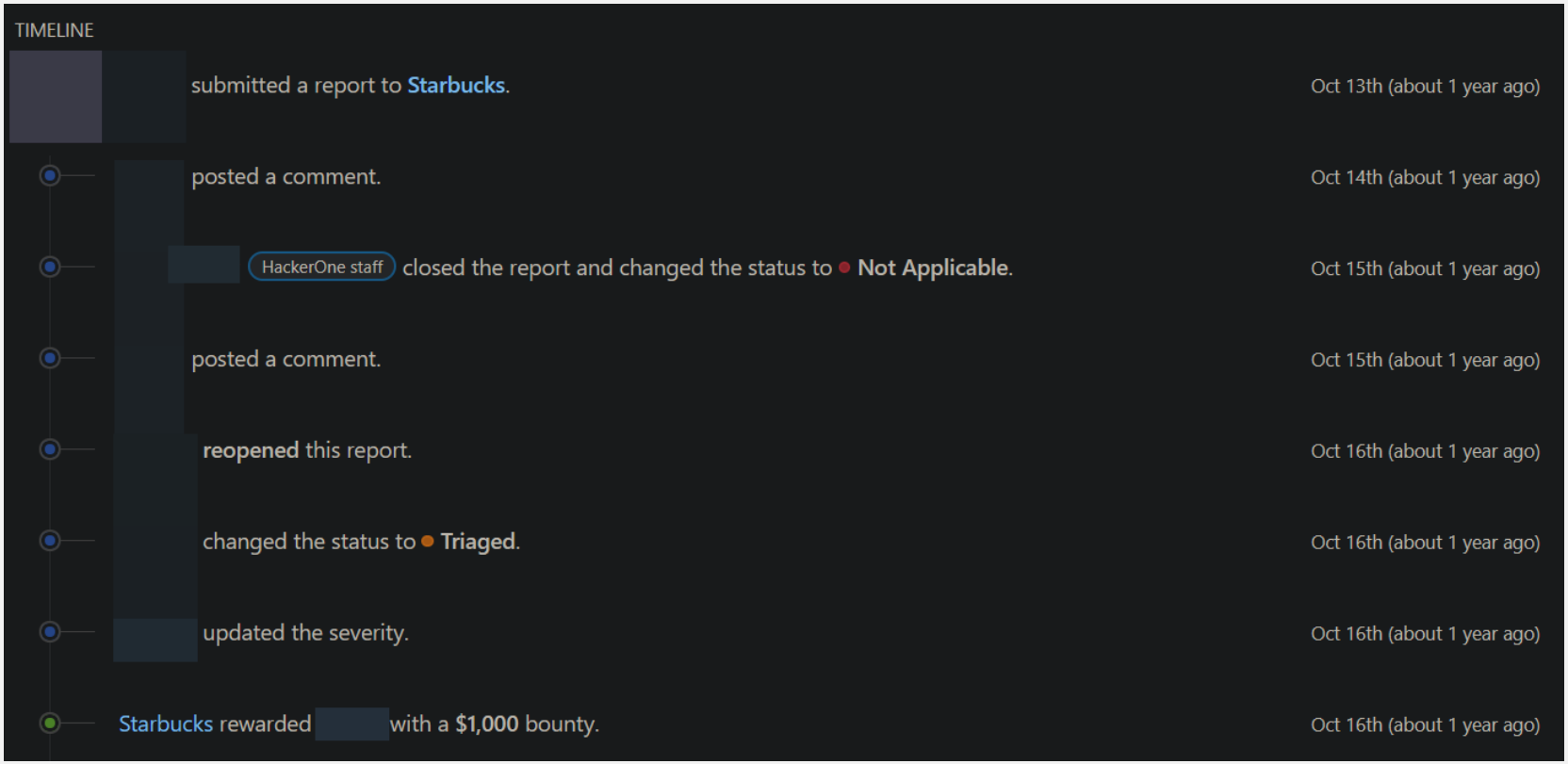
07/11
- 通知已修正
- 通知可領賞金

09/13
- 通知將透過PayPal發送$250美金

09/29
- 增加賞金至$300美金

10/05
- 收到PayPal約$272美金

HackerOne 隨便抓一個時間線



所以這讓我學到了什麼?

其實我也不知道

其實我也不知道

- 回報Bug並沒有要拿賞金的念頭
- 對方…
  - 問題處理迅速
  - 但賞金部分持續出槌
  - 是因為第一次處理類似事情嗎?
- 未來到底該注意些什麼?
  - 沒提供VDP
    - 回報Bug如果有賞金，*對方慢/金額不對該當正常嗎?*
  - 有提供VDP
    - 回報Bug如果有賞金，*我是不是該靠HackerOne?*

建議/問答

Email: business @ stillu.cc