

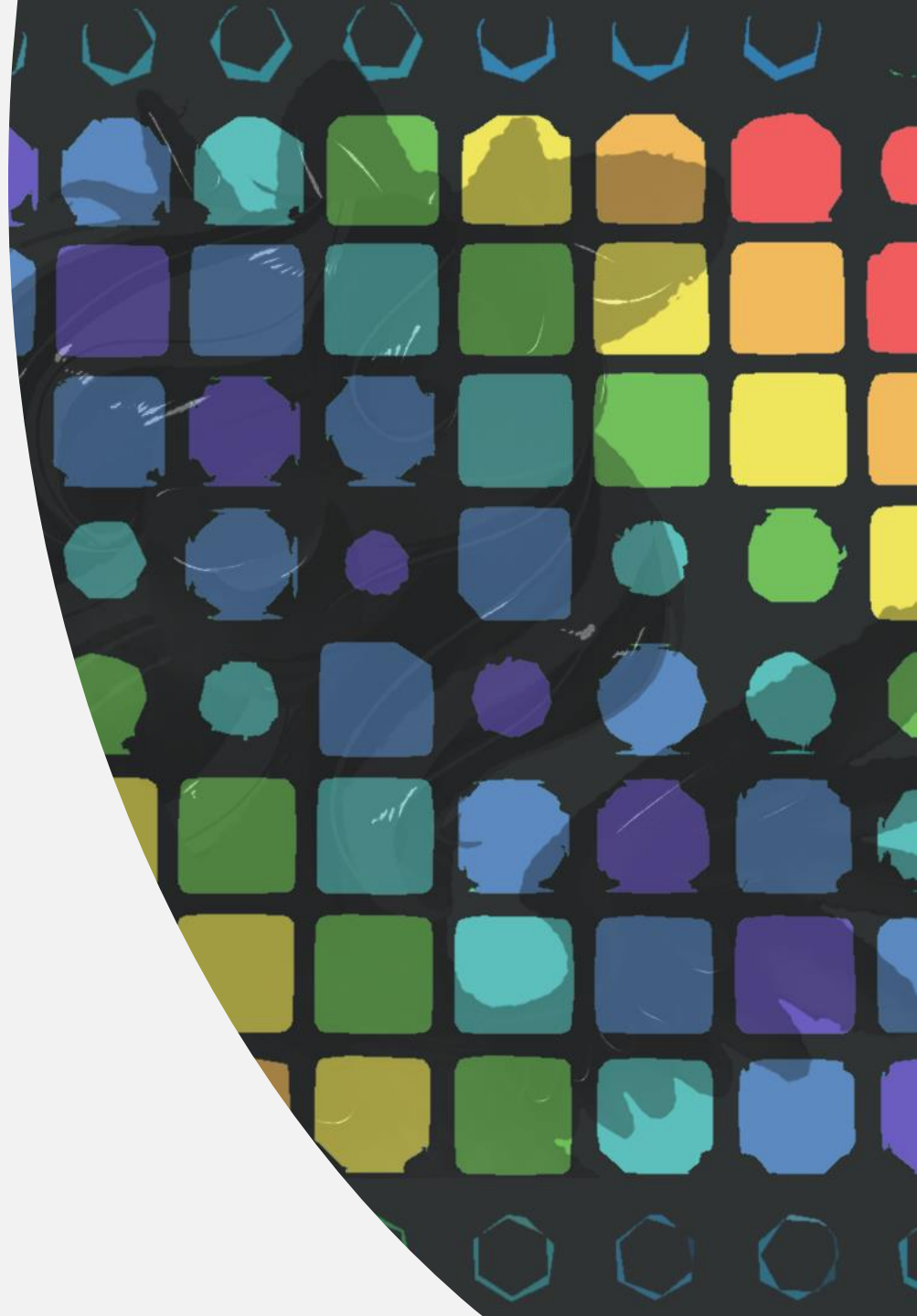


誤打誤撞的第一支 Bug Bounty

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



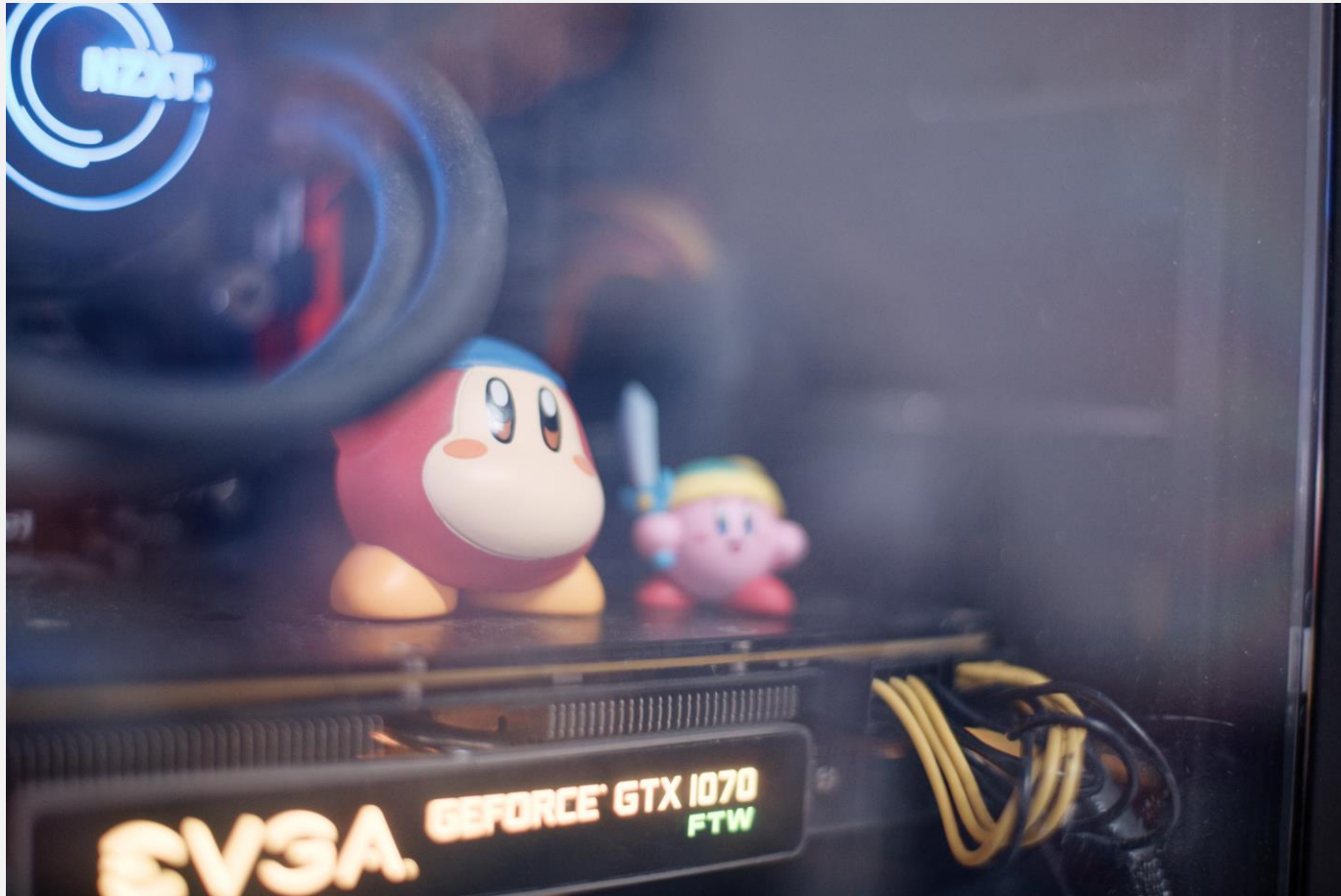
第一章

背景故事

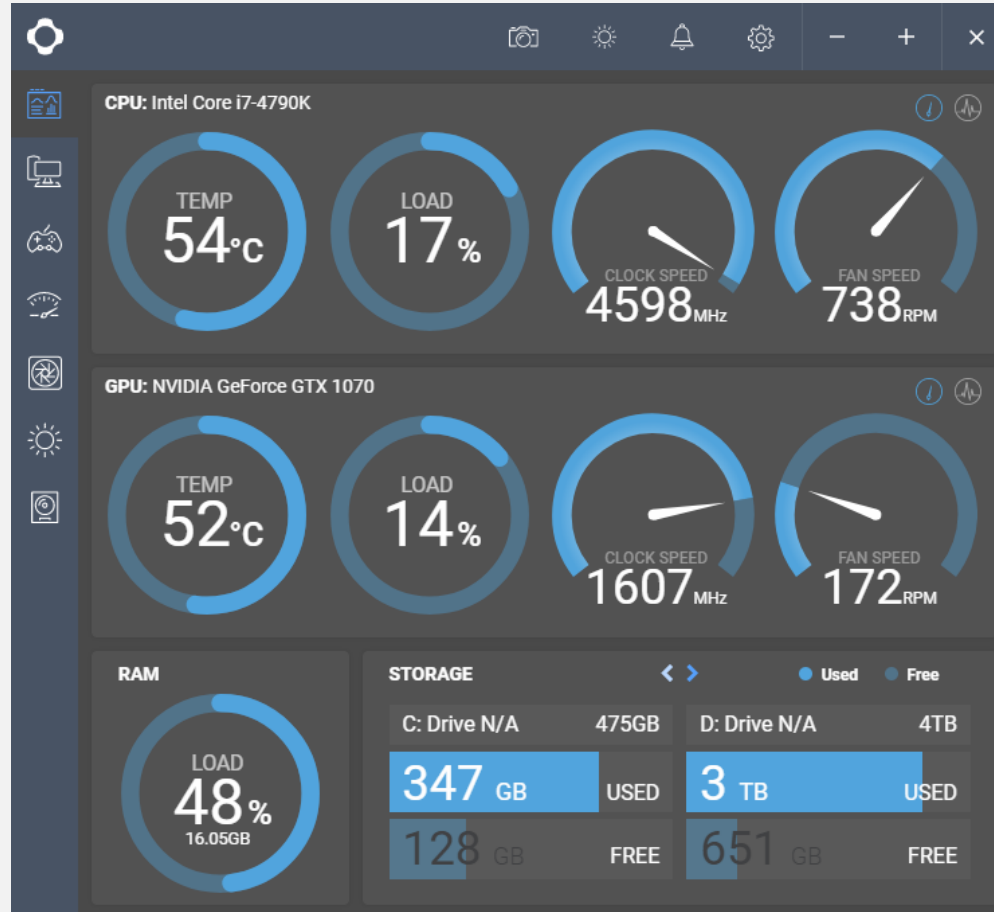
故事是這樣的...



故事是這樣的...



故事是這樣的...



A vibrant, cartoonish landscape featuring Kirby, a pink, round character with large eyes, standing in a field of green grass and colorful flowers. In the background, there are yellow arches and blue, cone-shaped structures. A large, colorful, insect-like creature with a striped body and pink wings is flying in the sky above Kirby. The text "NZXT CAM" is overlaid in the upper center, and "我寶貴的 CPU 資源" is overlaid on Kirby's body.

NZXT CAM

我寶貴的
CPU 資源

工程師精神發作

Fiddler

The screenshot displays the Fiddler Web Debugger interface. The top menu includes File, Edit, Rules, Tools, View, and Help. The main toolbar contains buttons for WinConfig, Replay, Stream, Decode, and various other functions. The central pane shows a list of HTTP requests with columns for #, Res., Result, Protocol, Host, URL, Body, Ca., Content-Type, Process, and Comments. The right pane shows the details of the selected request, including Request Headers, Client information, Entity, Transport, Response Headers, and Cache details.

#	Res...	Result	Protocol	Host	URL	Body	Ca.	Content-Type	Process	Comments
28	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...	curl:23212	
29	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
30	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
31	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
32	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
33	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
34	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
35	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
36	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
37	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
38	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
39	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
40	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
41	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
42	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
43	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
44	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
45	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		
46	OK	200	HTTP	example.com	/	1,256 ma...		text/html; c...		

Request Headers
POST / HTTP/1.1

Client
Accept: */*
User-Agent: curl/7.55.1

Entity
Content-Length: 16
Content-Type: application/x-www-form-urlencoded

Transport
Connection: Keep-Alive
Host: example.com

Response Headers
HTTP/1.1 200 OK

Cache
Cache-Control: max-age=604800
Date: Fri, 20 Mar 2020 18:27:30 GMT
Expires: Fri, 27 Mar 2020 18:27:30 GMT

Entity
Content-Length: 1256
Content-Type: text/html; charset=UTF-8
Etag: "3147526947"
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT

Miscellaneous
Accept-Ranges: bytes
Server: EOS (vny/0453)

Fiddler

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear

#	Res...	Result	Protocol	Host	URL	Body	Ca...	Content-Type	Process	Comments
28	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...	curl:23212	
29	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
30	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
31	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
32	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
33	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
34	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
35	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
36	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
37	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
38	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
39	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
40	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
41	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
42	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
43	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
44	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
45	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		
46	OK	200	HTTP	example.com	/	1,256	ma...	text/html; c...		

Fiddler

The screenshot displays the Fiddler web proxy tool interface. The top menu bar includes options like 'Get Started', 'Statistics', 'Inspectors', 'AutoResponder', 'Composer', 'Fiddler Orchestra Beta', 'FiddlerScript', 'Log', 'Filters', and 'Timeline'. Below the menu, there are tabs for 'Headers', 'TextView', 'SyntaxView', 'WebForms', 'HexView', 'Auth', 'Cookies', 'Raw', 'JSON', and 'XML'. The main content area is divided into two sections: 'Request Headers' and 'Response Headers'. The 'Request Headers' section shows a POST request to HTTP/1.1 with client information (Accept: */*, User-Agent: curl/7.55.1), entity information (Content-Length: 16, Content-Type: application/x-www-form-urlencoded), and transport information (Connection: Keep-Alive, Host: example.com). The 'Response Headers' section shows an HTTP/1.1 200 OK response with cache information (Cache-Control: max-age=604800, Date: Fri, 20 Mar 2020 18:27:30 GMT, Expires: Fri, 27 Mar 2020 18:27:30 GMT), entity information (Content-Length: 1256, Content-Type: text/html; charset=UTF-8, Etag: "3147526947", Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT), and miscellaneous information (Accept-Ranges: bytes, Server: EOS (vny/0453)).

Request Headers [Raw] [Header Definitions]
POST / HTTP/1.1

Client
Accept: */*
User-Agent: curl/7.55.1

Entity
Content-Length: 16
Content-Type: application/x-www-form-urlencoded

Transport
Connection: Keep-Alive
Host: example.com

Response Headers [Raw] [Header Definitions]
HTTP/1.1 200 OK

Cache
Cache-Control: max-age=604800
Date: Fri, 20 Mar 2020 18:27:30 GMT
Expires: Fri, 27 Mar 2020 18:27:30 GMT

Entity
Content-Length: 1256
Content-Type: text/html; charset=UTF-8
Etag: "3147526947"
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT

Miscellaneous
Accept-Ranges: bytes
Server: EOS (vny/0453)

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

The screenshot displays the Progress Telerik Fiddler Web Debugger interface. The left pane shows a list of 87 captured HTTP requests. The right pane shows the Fiddler dashboard with a 'RECENT' list of captured sessions.

#	Res...	Result	Protocol	Host	URL	Body	Ca...	Content-Type	Process	Comments
1	OK	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?...	880	pr...	text/plain; ...		
37	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:19640	[#49]
38	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:5024	[#47]
39	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:19640	[#48]
40	OK	200	HTTPS	apin.nzxt.com	/v1/auth	320	no...	application/...	cam_desktop:19640	[#163]
41	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:19640	[#608]
42	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:22364	[#988]
43	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:21340	[#990]
44	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:9696	[#1008]
45	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:21056	[#1013]
46	OK	200	HTTPS	apin.nzxt.com	/v1/auth	310		application/...	cam_desktop:21988	[#1069]
47	OK	200	HTTPS	apin.nzxt.com	/v1/blob/download	0		text/html; c...	cam_desktop:19640	[#164]
48	OK	200	HTTPS	apin.nzxt.com	/v1/blob/download	623		application/...	cam_desktop:19640	[#168]
49	OK	200	HTTPS	apin.nzxt.com	/v1/blob/download	0		text/html; c...	cam_desktop:19640	[#169]
50	OK	200	HTTPS	apin.nzxt.com	/v1/blob/download	1,429		application/...	cam_desktop:19640	[#176]
51	OK	200	HTTPS	apin.nzxt.com	/v1/blob/download	0		text/html; c...	cam_desktop:19640	[#179]
52	Un...	401	HTTPS	apin.nzxt.com	/v1/blob/download	57		application/...	cam_desktop:19640	[#181]
53	OK	200	HTTPS	apin.nzxt.com	/v1/blob/download	0		text/html; c...	cam_desktop:19640	[#182]
54	Un...	401	HTTPS	apin.nzxt.com	/v1/blob/download	57		application/...	cam_desktop:19640	[#183]
55	Un...	401	HTTPS	apin.nzxt.com	/v1/blob/download	57		application/...	cam_desktop:19640	[#184]
56	OK	200	HTTPS	apin.nzxt.com	/v1/blob/download	0		text/html; c...	cam_desktop:19640	[#196]
57	OK	200	HTTPS	apin.nzxt.com	/v1/blob/flst	6,406		application/...	cam_desktop:19640	[#174]
58	OK	200	HTTPS	apin.nzxt.com	/v1/blob/upload	80		application/...	cam_desktop:19640	[#173]
59	OK	200	HTTPS	apin.nzxt.com	/v1/blob/upload	85		application/...	cam_desktop:19640	[#197]
60	OK	200	HTTPS	apin.nzxt.com	/v1/checkappversion	220	no...	application/...	cam_desktop:19640	[#49]
61	OK	200	HTTPS	apin.nzxt.com	/v1/checkappversion	220	no...	application/...	cam_desktop:19640	[#52]
62	OK	200	HTTPS	apin.nzxt.com	/v1/checkappversion	220	no...	application/...	cam_desktop:19640	[#170]
63	OK	200	HTTPS	apin.nzxt.com	/v1/checkappversion	220	no...	application/...	cam_desktop:19640	[#616]
64	OK	200	HTTPS	apin.nzxt.com	/v1/feeds/1/promos	2	no...	application/...	vivaldi:19824	[#1064]
65	OK	200	HTTPS	apin.nzxt.com	/v1/feeds/1/promos	2	no...	application/...	vivaldi:19824	[#1113]
66	OK	200	HTTPS	apin.nzxt.com	/v1/table/insert	77		application/...	cam_desktop:19640	[#178]
67	OK	200	HTTPS	apin.nzxt.com	/v1/table/insert	69		application/...	cam_desktop:19640	[#180]
68	OK	200	HTTPS	apin.nzxt.com	/v1/table/insert	77		application/...	cam_desktop:19640	[#613]
69	Un...	401	HTTPS	apin.nzxt.com	/v1/table/insert	57		application/...	cam_desktop:19640	[#617]
70	Un...	401	HTTPS	apin.nzxt.com	/v1/table/query	57		application/...	cam_desktop:19640	[#12]
71	Un...	401	HTTPS	apin.nzxt.com	/v1/table/query	57		application/...	cam_desktop:19640	[#14]
72	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	37,591		application/...	cam_desktop:19640	[#15]
73	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	22,797		application/...	cam_desktop:19640	[#16]
74	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	179		application/...	cam_desktop:19640	[#17]
75	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	36,464		application/...	cam_desktop:19640	[#18]
76	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	2		application/...	cam_desktop:19640	[#54]
77	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	2		application/...	fiddler:7888	[#80]
78	Bad...	400	HTTPS	apin.nzxt.com	/v1/table/query	865		application/...	fiddler:7888	[#81]
79	Bad...	400	HTTPS	apin.nzxt.com	/v1/table/query	864		application/...	fiddler:7888	[#82]
80	Bad...	400	HTTPS	apin.nzxt.com	/v1/table/query	865		application/...	fiddler:7888	[#89]
81	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	1,262,430		application/...	fiddler:7888	[#90]
82	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	325		application/...	cam_desktop:19640	[#171]
83	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	2		application/...	cam_desktop:19640	[#175]
84	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	2		application/...	cam_desktop:19640	[#185]
85	Bad...	400	HTTPS	apin.nzxt.com	/v1/table/query	603		application/...	fiddler:7888	[#194]
86	OK	200	HTTPS	apin.nzxt.com	/v1/table/query	2		application/...	fiddler:7888	[#207]
87	Bad...	400	HTTPS	apin.nzxt.com	/v1/table/query	164		application/...	fiddler:7888	[#563]

The right pane shows the Fiddler dashboard with a 'RECENT' list of captured sessions:

- C:\Users\J4146\AppData\Local\Temp\{2008F0FA0D}\NZXT-2019-06-26.saz
- D:\NZXT-2019-06-26.saz
- K:\NewPlatform.saz
- C:\Users\J4146\Documents\lobeanalyzed.saz
- C:\Users\J4146\Documents\Fiddler2\Captures\input.saz

分析請求

登入

- POST v1/auth

下載關於用戶的
歷史資訊 (e.g. 超
頻設定、客戶端
設定)

- POST
v1/blob/download

上傳本地端設定

- POST
v1/blob/upload

插入用戶資訊

- POST
v1/table/insert

查詢資料庫資訊

- POST
v1/table/query

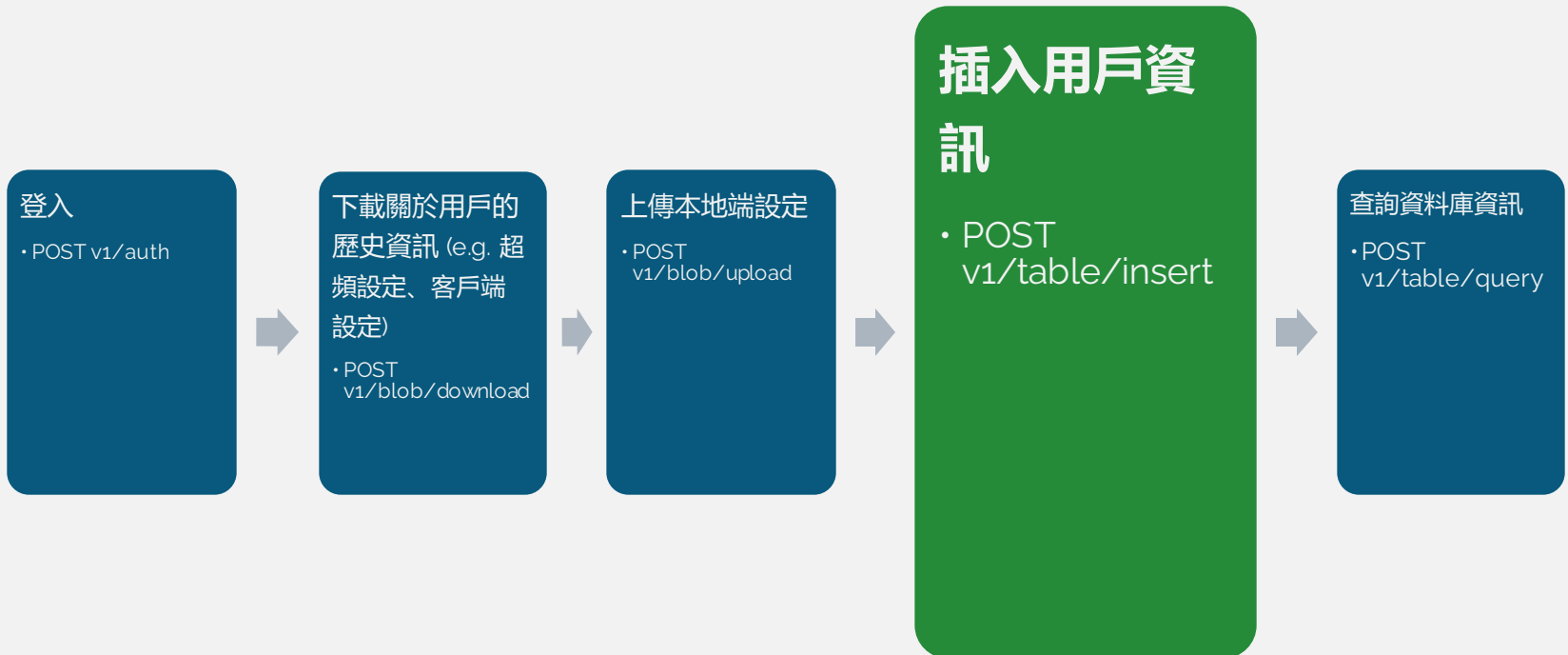
分析請求



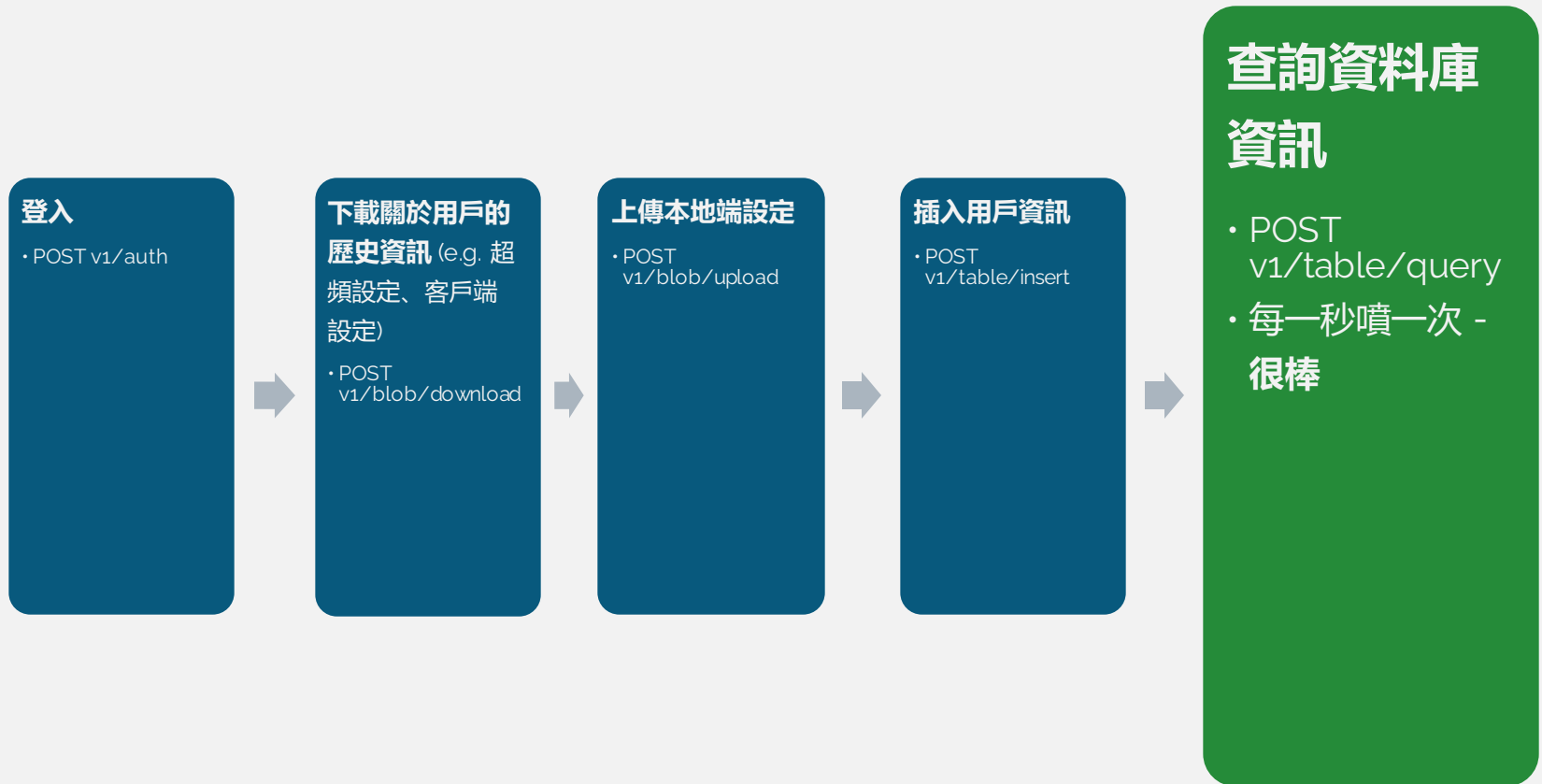
分析請求



分析請求



分析請求



登入請求

Body	
Name	Value
email	[REDACTED]
password	[REDACTED]

Transformer	Headers	TextView	SyntaxView	ImageView	HexView	WebView	Auth	Caching	Cookies	Raw	JSON	XML
-------------	---------	----------	------------	-----------	---------	---------	------	---------	---------	-----	------	-----

```
HTTP/1.1 200 OK
Access-Control-Allow-Methods: GET, POST, PUT, OPTIONS
Access-Control-Allow-Origin: *
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: application/json; charset=UTF-8
Date: Tue, 25 Jun 2019 17:17:12 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: nginx
Set-Cookie: PHPSESSID=1a71db985f37a37f929a727150296892; path=/
Content-Length: 320
Connection: keep-alive

{"id":50291,"cookies_id":50291,"token":"eyJ0[REDACTED]xw","time":"2019-06-25 17:17:12","expires":"2019-06-28 17:17:12","session_expires":3}
```

所有登入後的請求

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

Request Headers [\[Raw\]](#) [\[Header Definitions\]](#)

POST /v1/table/insert HTTP/1.1

Entity

- Content-Length: 2621
- Content-Type: application/x-www-form-urlencoded

Security

- Authorization: eyJ0

Transport

- Expect: 100-continue
- Host: apin.nzxt.com

開始亂翻請求

The screenshot displays a web proxy tool interface. The top section shows the request details, and the bottom section shows the transformed response.

Request Details:

- QueryString:**

Name	Value
- Body:**

Name	Value
storage	CAM_GPU_DB_USER
table	nvidiagpus
filter	

Transformed Response (JSON):

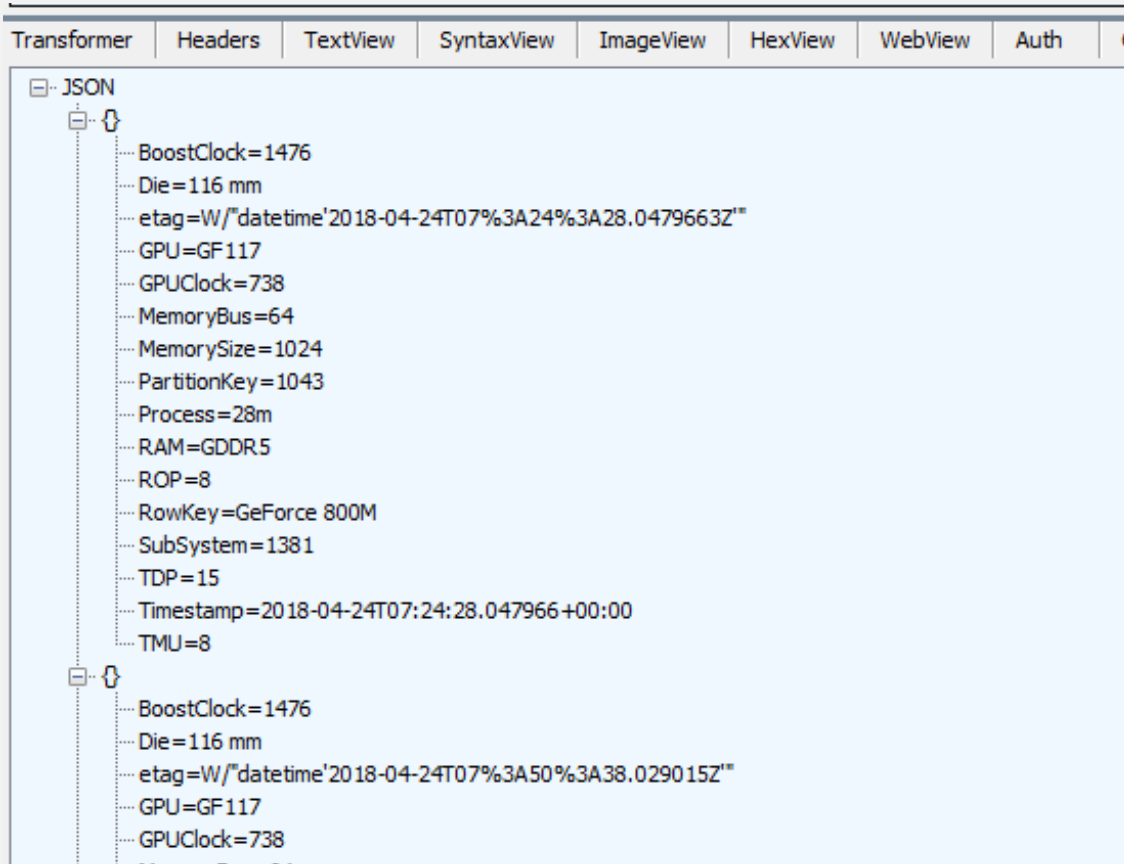
```
JSON
[
  {
    BoostClock=1476
    Die=116 mm
    etag=W/"datetime:2018-04-24T07%3A24%3A28.0479663Z"
    GPU=GF117
    GPUClock=738
    MemoryBus=64
    MemorySize=1024
    PartitionKey=1043
    Process=28m
    RAM=GDDR5
    ROP=8
    RowKey=GeForce 800M
    SubSystem=1381
    TDP=15
    Timestamp=2018-04-24T07:24:28.047966+00:00
    TMU=8
  },
  {
    BoostClock=1476
    Die=116 mm
    etag=W/"datetime:2018-04-24T07%3A50%3A38.029015Z"
    GPU=GF117
    GPUClock=738
  }
]
```

開始亂翻請求

QueryString	
Name	Value

Body	
Name	Value
storage	CAM_GPU_DB_USER
table	nvidiagpus
filter	

開始亂翻請求



The screenshot shows a network tool interface with a tabbed menu at the top containing: Transformer, Headers, TextView, SyntaxView, ImageView, HexView, WebView, Auth, and C. The main area displays a list of JSON objects under the heading 'JSON'. Each object is expanded to show its key-value pairs. The first object has the following properties:

- BoostClock=1476
- Die=116 mm
- etag=W/"datetime'2018-04-24T07%3A24%3A28.0479663Z"
- GPU=GF117
- GPUClock=738
- MemoryBus=64
- MemorySize=1024
- PartitionKey=1043
- Process=28m
- RAM=GDDR5
- ROP=8
- RowKey=GeForce 800M
- SubSystem=1381
- TDP=15
- Timestamp=2018-04-24T07:24:28.047966+00:00
- TMU=8

The second object in the list has the following properties:

- BoostClock=1476
- Die=116 mm
- etag=W/"datetime'2018-04-24T07%3A50%3A38.029015Z"
- GPU=GF117
- GPUClock=738

開始亂翻請求

The image shows a web browser's developer tools interface. The top section is titled 'QueryString' and contains a table with two columns: 'Name' and 'Value'. Below this is the 'Body' section, which also has a table with 'Name' and 'Value' columns. The 'Body' table contains three rows: 'storage' with value 'CAM_USER_TRACK', 'table' with value 'OfflineProfile', and 'filter' with value 'PartitionKey eq '3463188255' and RowKey eq 'LATEST_DATA''. The bottom section is titled 'Transformer' and shows a JSON object with various system properties.

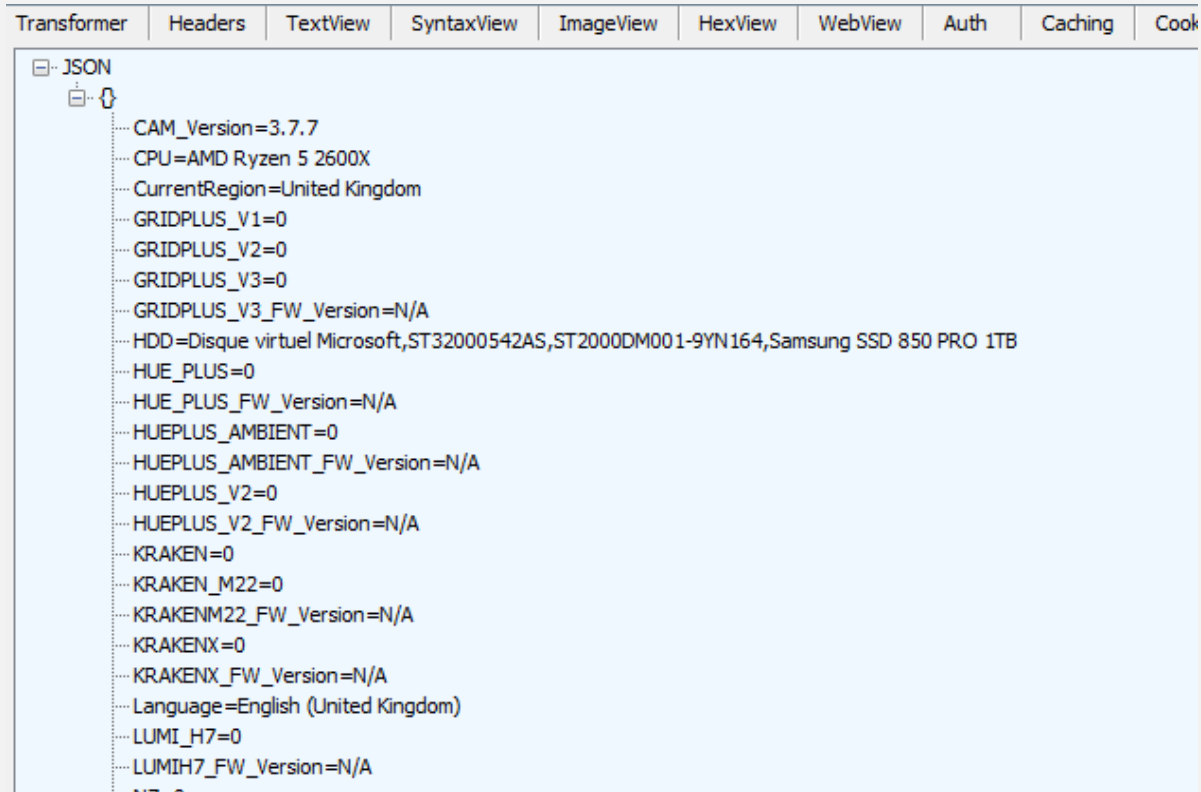
Name	Value
storage	CAM_USER_TRACK
table	OfflineProfile
filter	PartitionKey eq '3463188255' and RowKey eq 'LATEST_DATA'

```
JSON
{
  "CAM_Version": "3.7.7",
  "CPU": "AMD Ryzen 5 2600X",
  "CurrentRegion": "United Kingdom",
  "GRIDPLUS_V1": "0",
  "GRIDPLUS_V2": "0",
  "GRIDPLUS_V3": "0",
  "GRIDPLUS_V3_FW_Version": "N/A",
  "HDD": "Disque virtuel Microsoft,ST32000542AS,ST2000DM001-9YN164,Samsung SSD 850 PRO 1TB",
  "HUE_PLUS": "0",
  "HUE_PLUS_FW_Version": "N/A",
  "HUEPLUS_AMBIENT": "0",
  "HUEPLUS_AMBIENT_FW_Version": "N/A",
  "HUEPLUS_V2": "0",
  "HUEPLUS_V2_FW_Version": "N/A",
  "KRAKEN": "0",
  "KRAKEN_M22": "0",
  "KRAKENM22_FW_Version": "N/A",
  "KRAKENX": "0",
  "KRAKENX_FW_Version": "N/A",
  "Language": "English (United Kingdom)",
  "LUMI_H7": "0",
  "LUMIH7_FW_Version": "N/A",
  ...
}
```

開始亂翻請求

Headers	TextView	SyntaxView	WebForms	HexView	Auth	Cookies	Raw	JSON	XML
QueryString									
Name	Value								
Body									
Name	Value								
storage	CAM_USER_TRACK								
table	OfflineProfile								
filter	PartitionKey eq '3463188255' and RowKey eq 'LATEST_DATA'								

開始亂翻請求



The screenshot shows a web browser's developer tools interface. The top navigation bar includes tabs for Transformer, Headers, TextView, SyntaxView, ImageView, HexView, WebView, Auth, Caching, and Cook. The main content area displays a JSON object with the following properties:

```
JSON
{
  CAM_Version=3.7.7
  CPU=AMD Ryzen 5 2600X
  CurrentRegion=United Kingdom
  GRIDPLUS_V1=0
  GRIDPLUS_V2=0
  GRIDPLUS_V3=0
  GRIDPLUS_V3_FW_Version=N/A
  HDD=Disque virtuel Microsoft,ST32000542AS,ST2000DM001-9YN164,Samsung SSD 850 PRO 1TB
  HUE_PLUS=0
  HUE_PLUS_FW_Version=N/A
  HUEPLUS_AMBIENT=0
  HUEPLUS_AMBIENT_FW_Version=N/A
  HUEPLUS_V2=0
  HUEPLUS_V2_FW_Version=N/A
  KRAKEN=0
  KRAKEN_M22=0
  KRAKENM22_FW_Version=N/A
  KRAKENX=0
  KRAKENX_FW_Version=N/A
  Language=English (United Kingdom)
  LUMI_H7=0
  LUMIH7_FW_Version=N/A
}
```



修但積累

這不是我的電腦阿???

```
Transformer | Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cook
└─ JSON
  └─ {
    ...CAM_Version=3.7.7
    ...CPU=AMD Ryzen 5 2600X
    ...CurrentRegion=United Kingdom
    ...GRIDPLUS_V1=0
    ...GRIDPLUS_V2=0
    ...GRIDPLUS_V3=0
    ...GRIDPLUS_V3_FW_Version=N/A
    ...HDD=Disque virtuel Microsoft,ST32000542AS,ST2000DM001-9YN164,Samsung SSD 850 PRO 1TB
    ...HUE_PLUS=0
    ...HUE_PLUS_FW_Version=N/A
    ...HUEPLUS_AMBIENT=0
    ...HUEPLUS_AMBIENT_FW_Version=N/A
    ...HUEPLUS_V2=0
    ...HUEPLUS_V2_FW_Version=N/A
    ...KRAKEN=0
    ...KRAKEN_M22=0
    ...KRAKENM22_FW_Version=N/A
    ...KRAKENX=0
    ...KRAKENX_FW_Version=N/A
    ...Language=English (United Kingdom)
    ...LUMI_H7=0
    ...LUMIH7_FW_Version=N/A
    ...
  }
```

我把這串幹掉會怎麼樣？

QueryString	
Name	Value
Body	
Name	Value
storage	CAM_USER_TRACK
table	OfflineProfile
filter	PartitionKey eq '5463188255' and RowKey eq 'LATEST_DATA'

噴出一堆人的硬體資訊

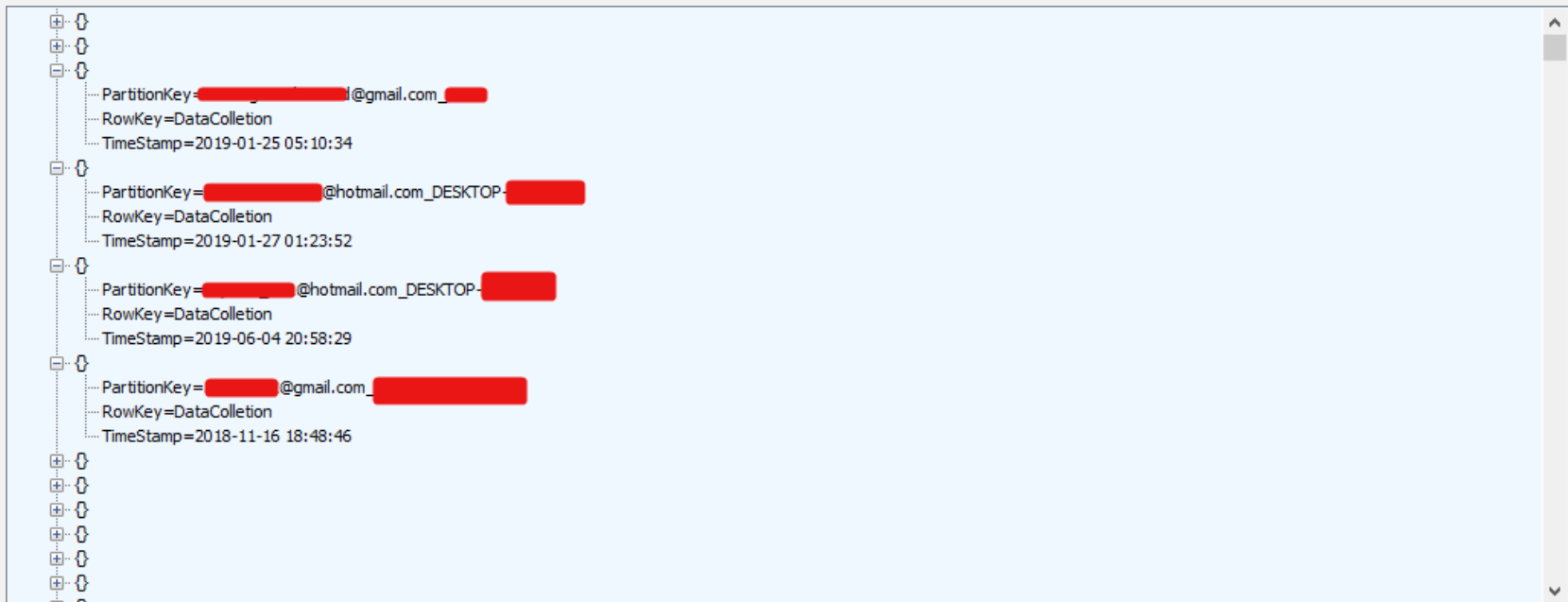
Body	
Name	Value
storage	CAM_TRACKER_USER
table	OfflineUserProfile

Transformer	Headers	TextView	SyntaxView	ImageView	HexView	WebView	Auth	Caching	Cookies	Raw	JSON	XML
<pre>[{"MotherBoard": "ASUS STRIX Z270H GAMING", "RowKey": "1438-11-19 10:22:46", "GridV1": "0", "GridV2": "0", "HostName": "DESKTOP-S17U8K9", "Cpu": "Intel Core i5-7600K", "Hdd": "WDC WD10EZEX-08WN4A0", "Language": "Arabic (Saudi Arabia)", "Gpu": "NVIDIA GeForce GTX 1070", "MonitorList": "\\\\.\\Generic PnP Monitor", "etag": "W\\\"\\\"datetime:2017-08-11T07:3A2Z%3A47.360437Z\"\"", "Aer": "0", "Kraken": "1", "OsVersion": "??Microsoft Windows 10 Pro", "LumiH7": "0", "Timestamp": "2017-08-11T07:22:47.360437+00:00", "CamVersion": "Version 3.3.5", "Hue": "0", "AudioInputList": "\\\\.\\Speakers (Wireless Stereo Headset)", "Realtek Digital Output (Realtek High Definition Audio)", "ZOWIE XL LCD-8 (NVIDIA High Definition Audio)", "KeyboardList": "\\\\.\\USB Input Device", "PartitionKey": "guest@nxt.com", "KrakenX": "0", "Ram": "Corsair.DDR4.8.2.Corsair", "MouseAndPointingList": "\\\\.\\USB Input Device", "MotherBoard": "MSI Z370 GAMING 3 (MS-7918)", "RowKey": "1438-11-19 11:05:30", "GridV1": "0", "GridV2": "0", "HostName": "DESKTOP-1HLOPCE", "Cpu": "Intel Core i7-7700K", "Hdd": "ST2000DM001-1CH164.ST31000528AS.WDC.WD10EADS-65L5B1.NVMe.Samsung.SSD.960", "Language": "English (United States)", "Gpu": "NVIDIA GeForce GTX 970", "MonitorList": "\\\\.\\Generic PnP Monitor", "etag": "W\\\"\\\"datetime:2017-08-11T08:3A05%3A29.2043324Z\"\"", "Aer": "0", "Kraken": "1", "OsVersion": "Microsoft Windows 10 Pro", "LumiH7": "0", "Timestamp": "2017-08-11T08:05:29.204332+00:00", "CamVersion": "Version 3.3.5", "Hue": "0", "AudioInputList": "\\\\.\\Speakers (Logitech G933 Gaming Headset)", "Digital Audio (S/PDIF) (High Definition Audio Device)", "U28D590-4 (NVIDIA High Definition Audio)", "KeyboardList": "\\\\.\\HID Keyboard Device", "HID Keyboard Device", "USB Input Device", "PartitionKey": "guest@nxt.com", "KrakenX": "0", "Ram": "G.Skill.DDR3.8.1", "MouseAndPointingList": "\\\\.\\USB Input Device", "HID-compliant mouse", "MotherBoard": "ASUS H170-PLUS D3", "RowKey": "1438-11-19 11:53:43", "GridV1": "0", "GridV2": "0", "HostName": "DESKTOP-DICU148", "Cpu": "Intel Core i5-7400", "Hdd": "WDC.WD10EARX-00N0YB0", "Language": "English (United Kingdom)", "Gpu": "NVIDIA GeForce GTX 560", "MonitorList": "\\\\.\\Generic PnP Monitor", "etag": "W\\\"\\\"datetime:2017-08-11T08:3A53%3A54.2114945Z\"\"", "Aer": "0", "Kraken": "0", "OsVersion": "Microsoft Windows 10 Pro", "LumiH7": "0", "Timestamp": "2017-08-11T08:53:54.211494+00:00", "CamVersion": "Version 3.3.5", "Hue": "0", "AudioInputList": "\\\\.\\SAMSUNG-14 (NVIDIA High Definition Audio)", "Realtek Digital Output (Realtek High Definition Audio)", "Speakers (Realtek High Definition Audio)", "KeyboardList": "\\\\.\\Razer Naga", "USB Input Device", "HID Keyboard Device", "HID Keyboard Device", "PartitionKey": "guest@nxt.com", "KrakenX": "0", "Ram": "Kingston.DDR3.4.2.Kingston", "MouseAndPointingList": "\\\\.\\USB Input Device", "MotherBoard": "ASUS H110M-K", "RowKey": "1438-11-19 12:45:51", "GridV1": "0", "GridV2": "0", "HostName": "DESKTOP-3R4EQ0", "Cpu": "Intel Core i5-7600", "Hdd": "WDC.WD10EZRX-00HTKB0", "Language": "Arabic (Saudi Arabia)", "Gpu": "NVIDIA GeForce GTX 1050 Ti", "MonitorList": "\\\\.\\Generic PnP Monitor", "etag": "W\\\"\\\"datetime:2017-08-11T09:3A45%3A56.2460919Z\"\"", "Aer": "0", "Kraken": "0", "OsVersion": "Microsoft Windows 10 Pro", "LumiH7": "0", "Timestamp": "2017-08-11T09:45:56.246091+00:00", "CamVersion": "Version 3.3.5", "Hue": "0", "AudioInputList": "\\\\.\\AAA-4 (NVIDIA High Definition Audio)", "Realtek Digital Output (Realtek High Definition Audio)", "KeyboardList": "\\\\.\\USB Input Device", "PartitionKey": "guest@nxt.com", "KrakenX": "0", "Ram": "Crucial Technology.DDR4.4.2.Crucial Technology", "MouseAndPointingList": "\\\\.\\USB Input Device", "MotherBoard": "MSI Z170A GAMING M7 (MS-7976)", "RowKey": "1438-11-19 14:16:13", "GridV1": "0", "GridV2": "0", "HostName": "XDHMAS", "Cpu": "Intel Core i7-6700K", "Hdd": "Samsung SSD 950 PRO 256GB.TOSHIBA.MQ01ABD075", "Language": "Arabic (Saudi Arabia)", "Gpu": "NVIDIA GeForce GTX 1080", "MonitorList": "\\\\.\\ZOWIE XL LCD (DisplayPort)", "etag": "W\\\"\\\"datetime:2017-08-11T11:3A16%3A14.5263538Z\"\"", "Aer": "0", "Kraken": "1", "OsVersion": "??Microsoft Windows 10 Pro", "LumiH7": "0", "Timestamp": "2017-08-11T11:16:14.526353+00:00", "CamVersion": "Version 3.3.5", "Hue": "0", "AudioInputList": "\\\\.\\Realtek HD Audio 2nd output (Realtek High Definition Audio)", "Realtek Digital Output (Realtek High Definition Audio)", "Speakers (2-Logitech G35 Headset)", "BenQ XL2430T-8 (NVIDIA High Definition Audio)", "KeyboardList": "\\\\.\\HID Keyboard Device", "USB Input Device", "HID Keyboard Device", "USB Input Device", "HID Keyboard Device", "PartitionKey": "guest@nxt.com", "KrakenX": "0", "Ram": "DDR4.8.2", "MouseAndPointingList": "\\\\.\\HID-compliant mouse", "HID-compliant mouse", "USB Input Device", "HID-compliant mouse", "MotherBoard": "Gigabyte Z170X-UD5-CF", "RowKey": "1438-11-19 14:46:16", "GridV1": "0", "GridV2": "0", "HostName": "DESKTOP-KC18M7J", "Cpu": "Intel Core i7-6700K", "Hdd": "SanDisk.Ultra.11.960GB.WDC.WD10EZRX-00HTKB0.SanDisk.SDSSDH1120G", "Language": "English (United Kingdom)", "Gpu": "NVIDIA GeForce GTX 1070", "MonitorList": "\\\\.\\Generic PnP Monitor", "etag": "W\\\"\\\"datetime:2017-08-11T11:3A46%3A21.162959Z\"\"", "Aer": "2", "Kraken": "0", "OsVersion": "Microsoft Windows 10</pre>												

好喔那我試試看這個

Name	Value
storage	CAM_APP_DATA_USER
table	UserConsents
filter	PartitionKey eq '...' and RowKey eq 'DataCollection'

噴出一堆人的Email + 電腦名稱



第三章

意外的轉折

通報去

https://www.nzxt.com/users/account#acc-submit-ticket

WELCOME, STILL

ACCOUNT INFORMATION	Region North America	Department General Support
ORDER HISTORY	Subject*	Product*
CREATE A TICKET	Description*	Attachment Choose a file:
TICKETS		
RETURN MANAGEMENT		

SUBMIT

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...



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

NZXT - Database Security Breach  Inbox x

意外的訊息

Thu, Jul 11, 2019, 12:00 PM

意外的訊息

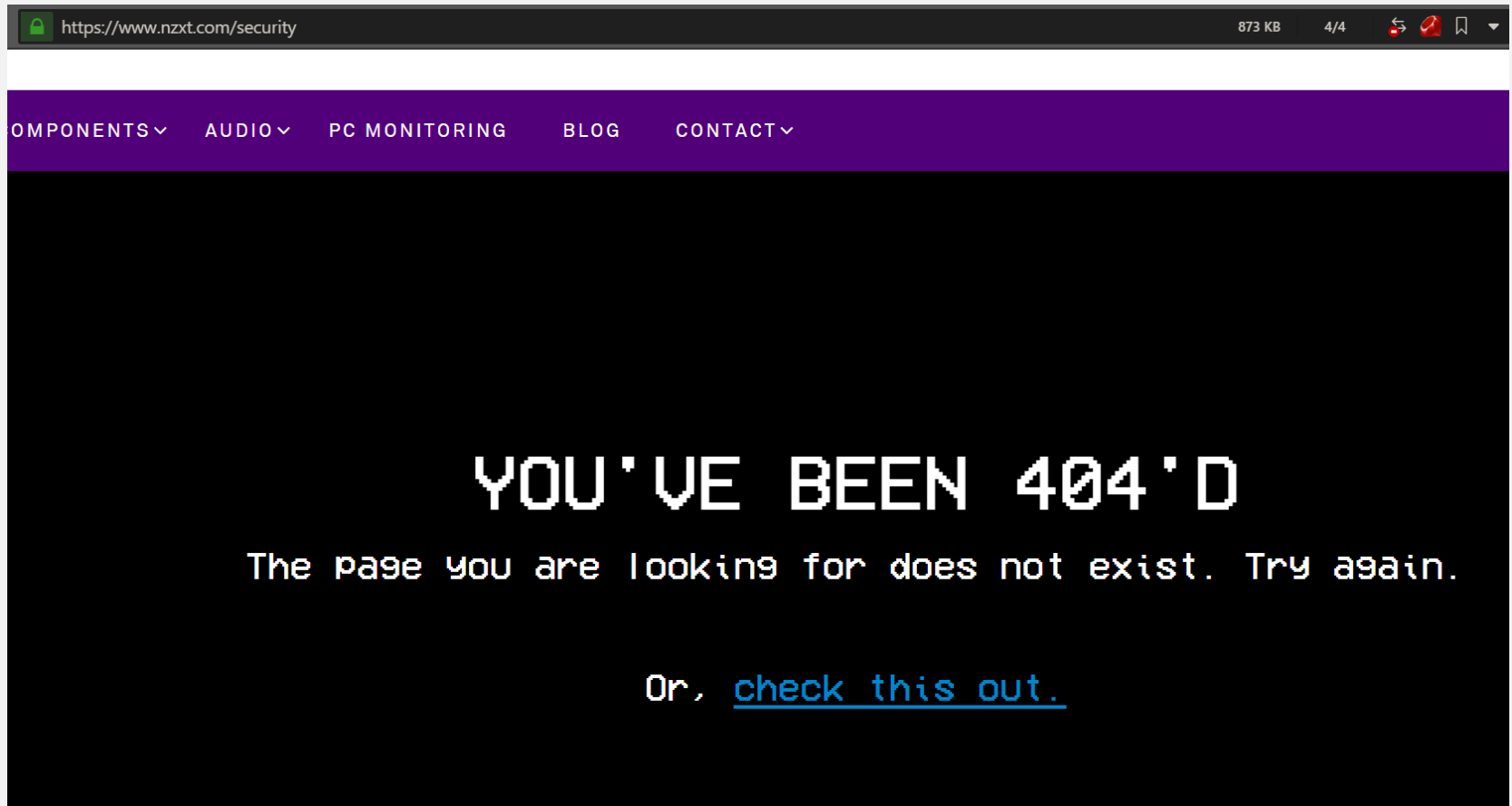
NZXT Rep Jul 11, 2019, 12:00 PM

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？

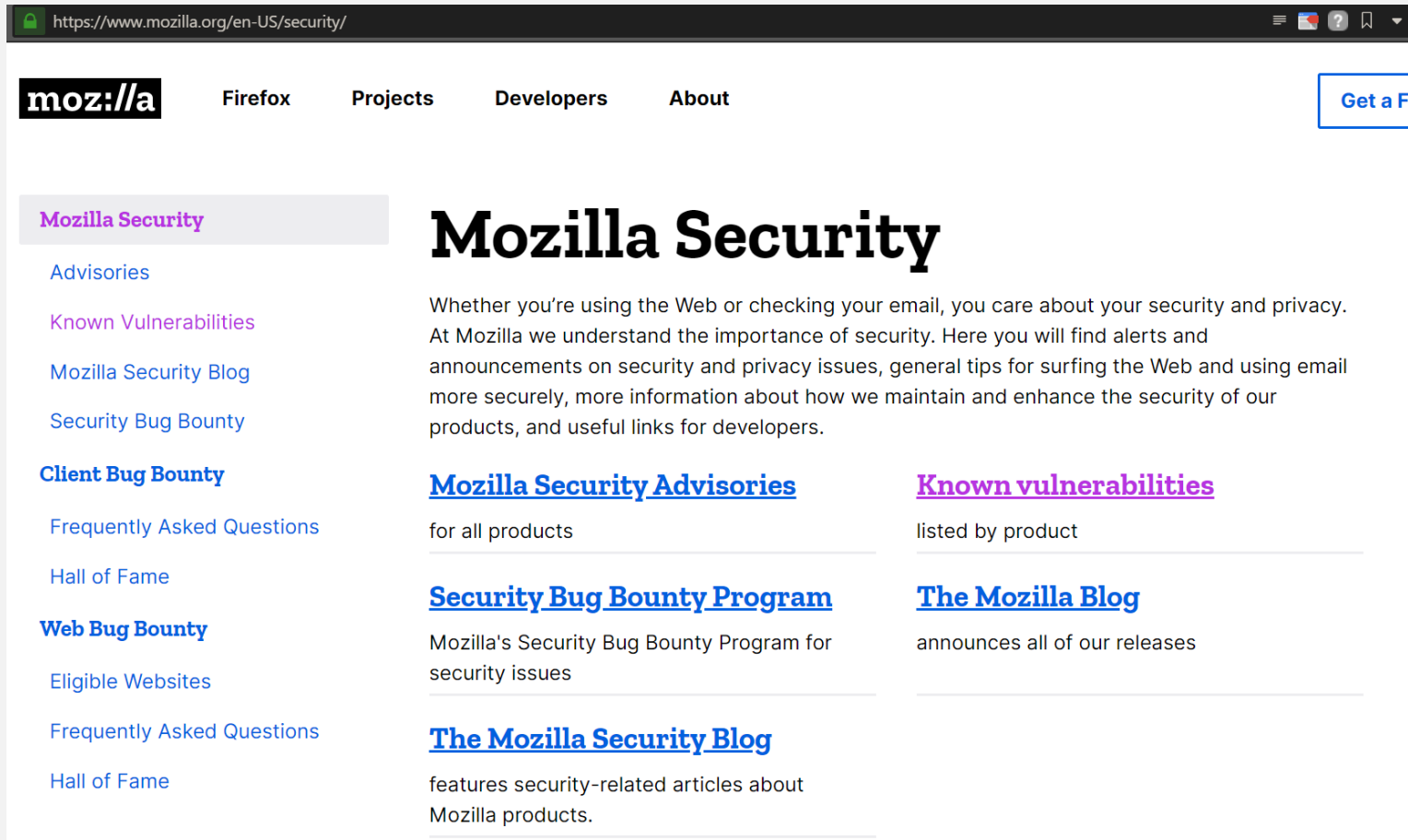
沒有VDP頁面



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



The image shows a screenshot of the Mozilla Security website. The browser's address bar displays the URL <https://www.mozilla.org/en-US/security/>. The page features the Mozilla logo and navigation links for Firefox, Projects, Developers, and About. A 'Get a Firefox' button is visible in the top right corner. The main content area is titled 'Mozilla Security' and includes a paragraph explaining the importance of security. Below this, there are four sections: 'Mozilla Security Advisories', 'Known vulnerabilities', 'Security Bug Bounty Program', and 'The Mozilla Security Blog'. A left sidebar contains links for 'Advisories', 'Known Vulnerabilities', 'Mozilla Security Blog', 'Security Bug Bounty', 'Client Bug Bounty', 'Frequently Asked Questions', 'Hall of Fame', 'Web Bug Bounty', 'Eligible Websites', 'Frequently Asked Questions', and 'Hall of Fame'.

<https://www.mozilla.org/en-US/security/>

moz://a [Firefox](#) [Projects](#) [Developers](#) [About](#) [Get a Firefox](#)

Mozilla Security

[Advisories](#)

[Known Vulnerabilities](#)

[Mozilla Security Blog](#)

[Security Bug Bounty](#)

Client Bug Bounty

[Frequently Asked Questions](#)

[Hall of Fame](#)

Web Bug Bounty

[Eligible Websites](#)

[Frequently Asked Questions](#)

[Hall of Fame](#)

Mozilla Security

Whether you're using the Web or checking your email, you care about your security and privacy. At Mozilla we understand the importance of security. Here you will find alerts and announcements on security and privacy issues, general tips for surfing the Web and using email more securely, more information about how we maintain and enhance the security of our products, and useful links for developers.

[Mozilla Security Advisories](#)
for all products

[Known vulnerabilities](#)
listed by product

[Security Bug Bounty Program](#)
Mozilla's Security Bug Bounty Program for security issues

[The Mozilla Blog](#)
announces all of our releases

[The Mozilla Security Blog](#)
features security-related articles about Mozilla products.



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

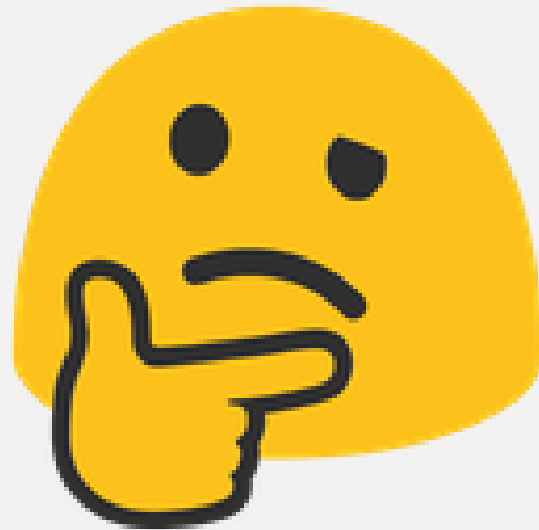
約五周之後...

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

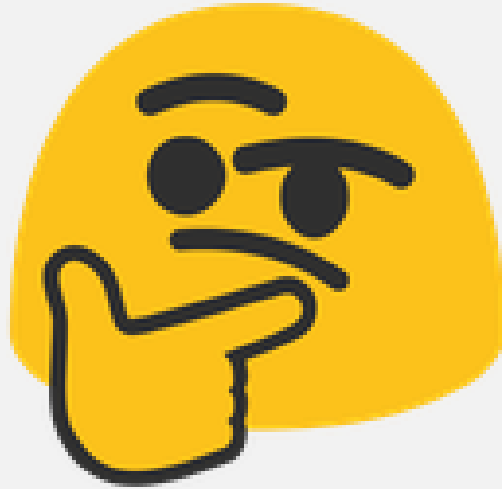
NZXT

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。

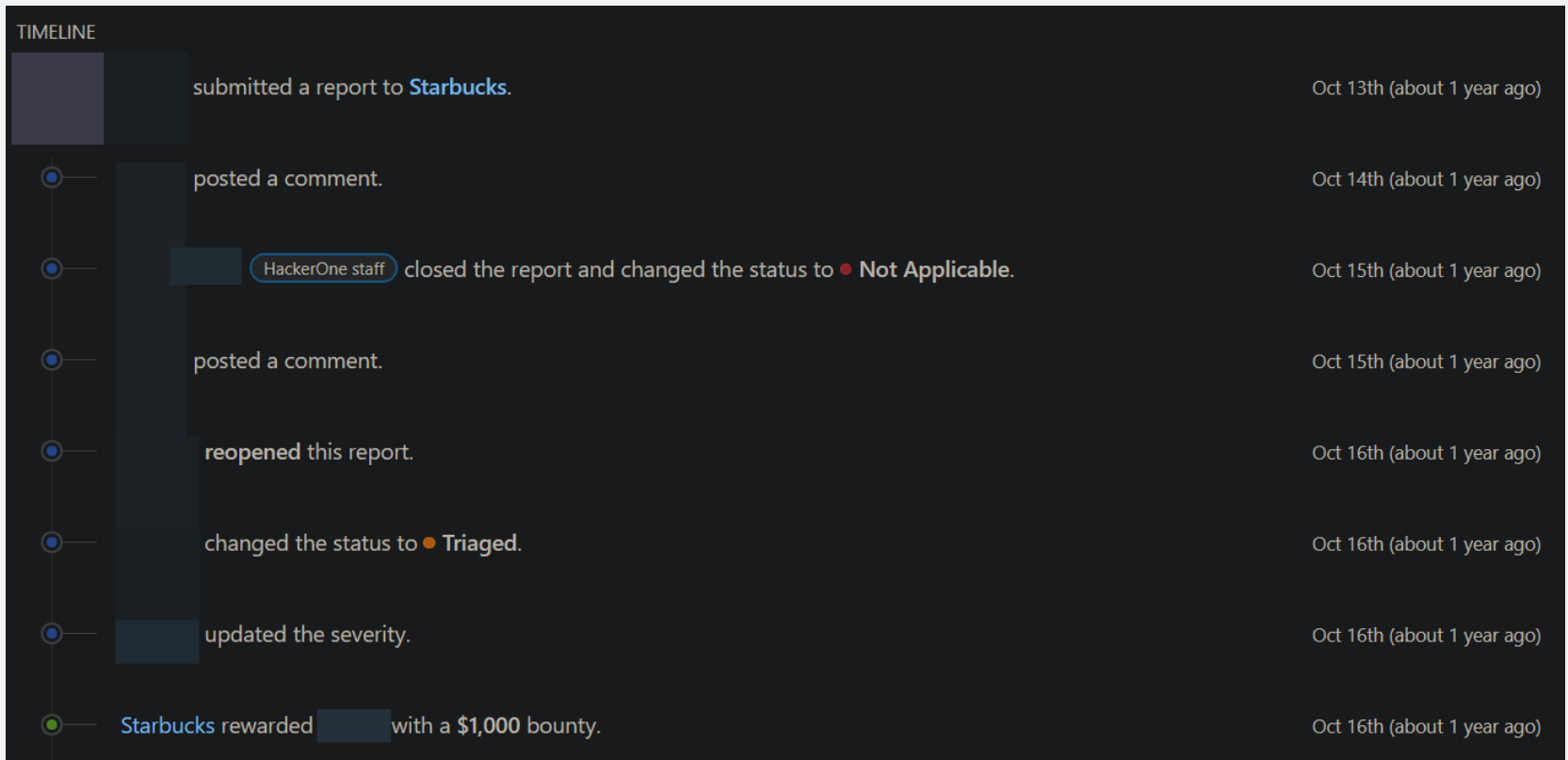
第四章

結論

時間線



HackerOne 隨便抓一個時間線



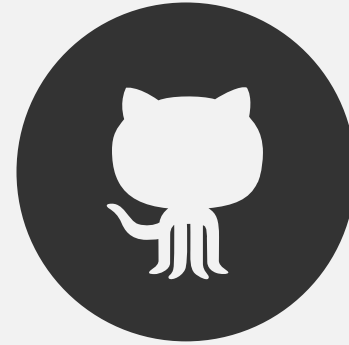
所以這讓我學到了什麼？

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](mailto:business@stillu.cc)