

# Nyertem egy hajszárítót?

Instagramon jött az értesítés, hogy meg lettem említve egy posztban, és nyertem egy hajszárítót.

Ehhez mindössze annyit kell tennem, hogy a megadott instagram profil "bio"-jában lévő linkre kattintok.

A megadott profilok elég rövid életűek, mert folyamatosan jelentik és törlik őket, de sikerült elcsípnem egy ilyen linket, hogy mögénézzek, tényleg nyertem-e hajszárítót.

Na nem azért, mert annyira érdekel az ajándék hajszárító, az én hajamnak elég egy kis törölköző is, inkább a szakmai kíváncsiság miatt.

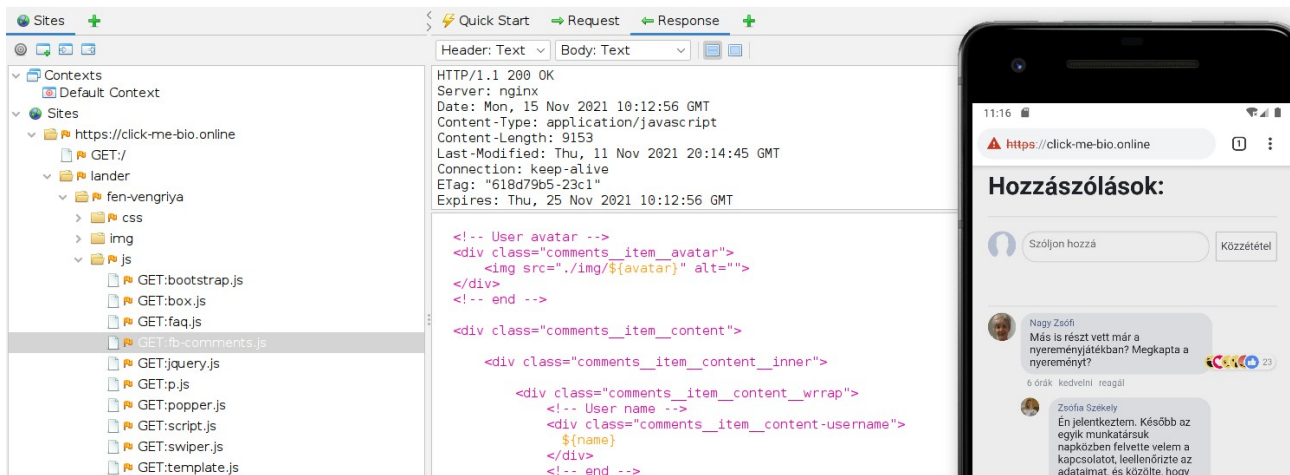
Szóval bedurrantotam az android-emulátort és irány a megadott link:

[https://click-me-bio\[.\]online](https://click-me-bio[.]online)

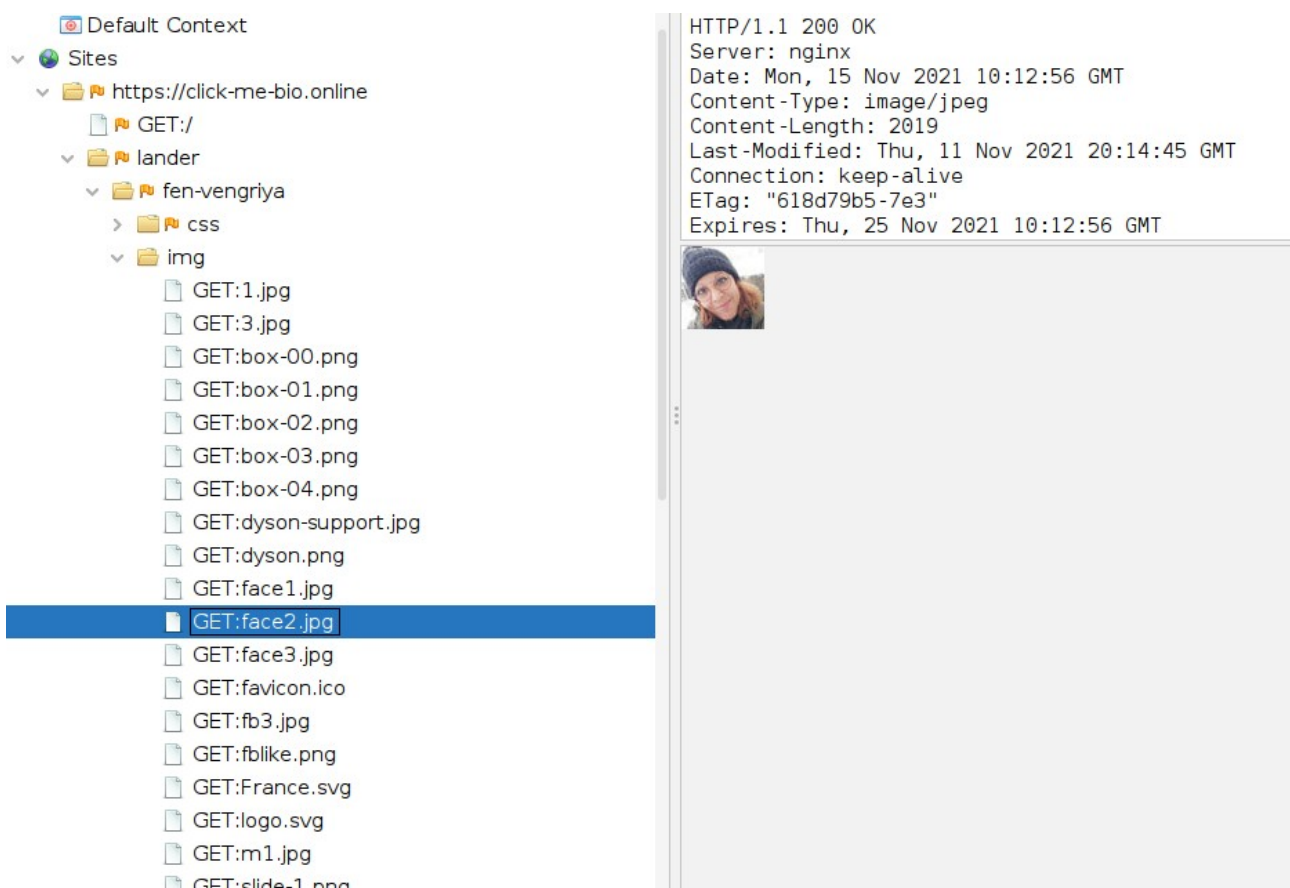
Azzal, hogy a https nem secure, most ne törődjünk, egy intercepting proxyt vezettem keresztül a forgalmat, hogy bele tudjak nézni, ami nyilván eltöri az SSL-t.



Ami viszont sokkal érdekesebb az a komment szekció, ahol mindenki boldogan újságolja, hogy megnyerte és megkapta és mennyire szereti az új hajszárítóját:

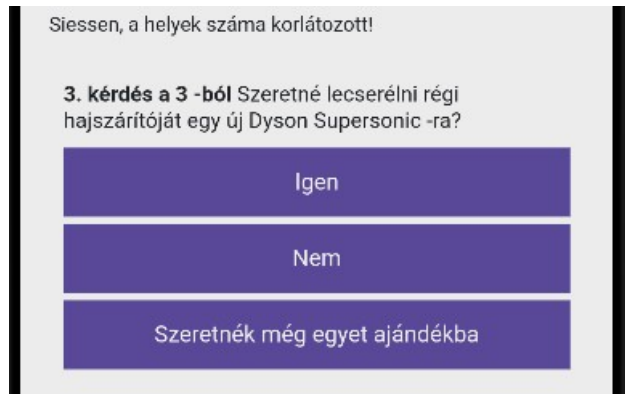
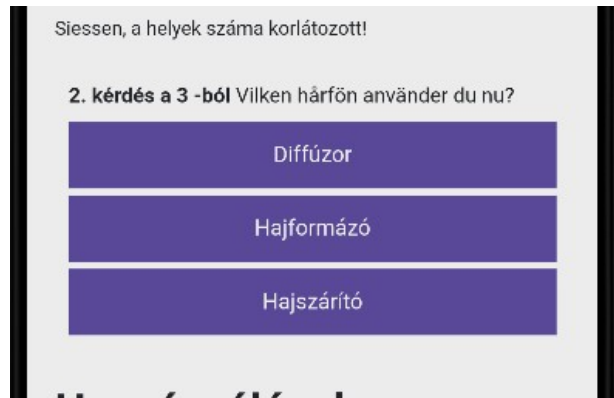
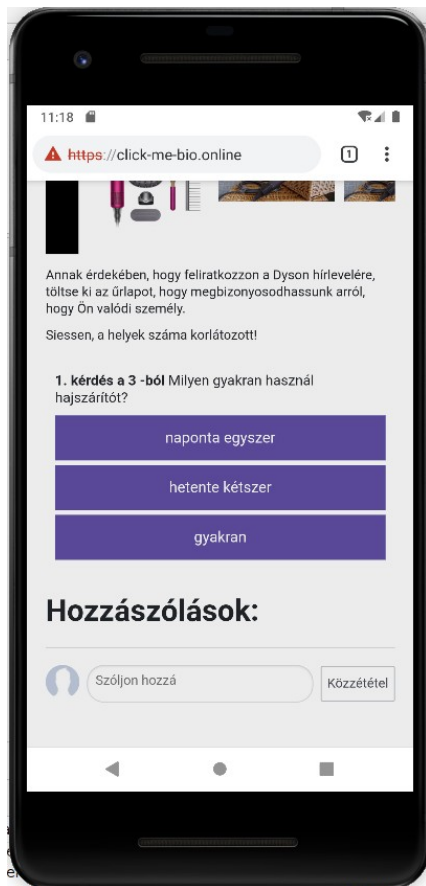


Ahogy a proxy logokban is látszik, ezek nem igazi kommentek nem az igazi facebookról, hanem a szerveren helyben eltárolt és a fb-comments.js szkript által összeállított hozzászólások. Még a profilképek is le vannak mentve:

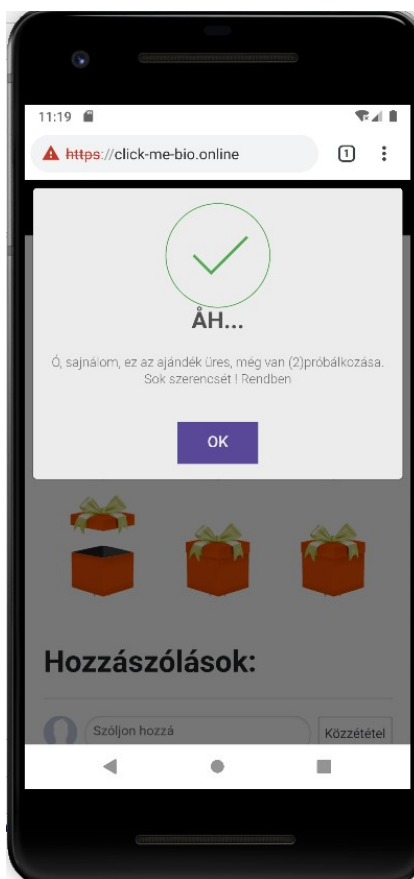
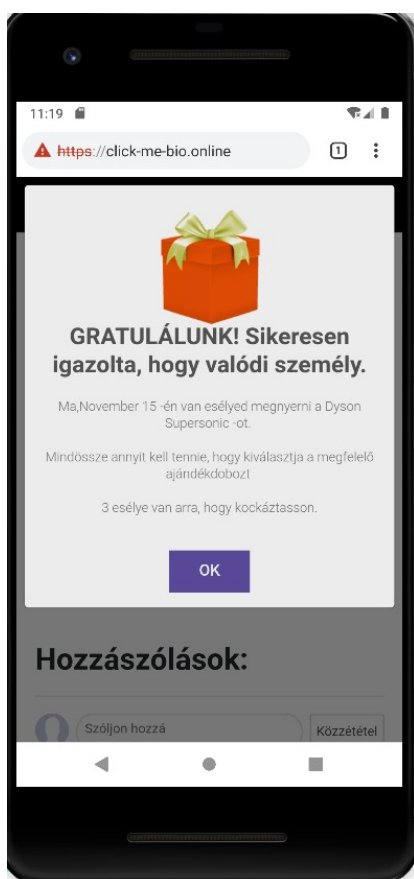


Na de ne ragadjunk le a komment szekciónál, nézzük, hogy mit kell tennünk a hajszárító megszerzéséért. Először is kérdésekre kell válaszolni.

A kedvencem a második kérdés, ami így hangzik: “Vilken hárfön använder du nu?” Szerencsére itt nincs rossz válasz. :)



Ha mindhárom kérdést megválasztottuk (sietve, hiszen a helyek száma korlátozott!), akkor:



A már jól ismert három próbálkozásból találd meg a nyertes csomagot séma töltődik be. Természetesen másodikra meg is lett a nyereményem, ami – nem meglepő módon – egy Dyson Supersonic hajszárító! Szinte már érzem, ahogy a forró levegő borzolja a sörényem.

Menjünk tovább! Az OK gombbal egy másik URL-re ugrunk, ahol egy űrlapot kell kitölteni:

The image shows two smartphone screens displaying a contest registration page. The left screen shows the contest details, including the text "Fedezze fel az új Dyson Supersonic Hairdryer-t!" and a price tag of "Az Ön ára 700 Ft". The right screen shows the registration form with fields for "Hakker", "Hugo", "Hakkoló utca 1337.", "1337", "Budapest", "Hungary", "+36 313374444", and "haxor@haxory.hu". A green "Folytatás" button is at the bottom.

Folytatás?? Naná, hogy folytatás, hiszen egy Hajszárító a tét!

A Folytatás gombra kattintva történik az első POST request:

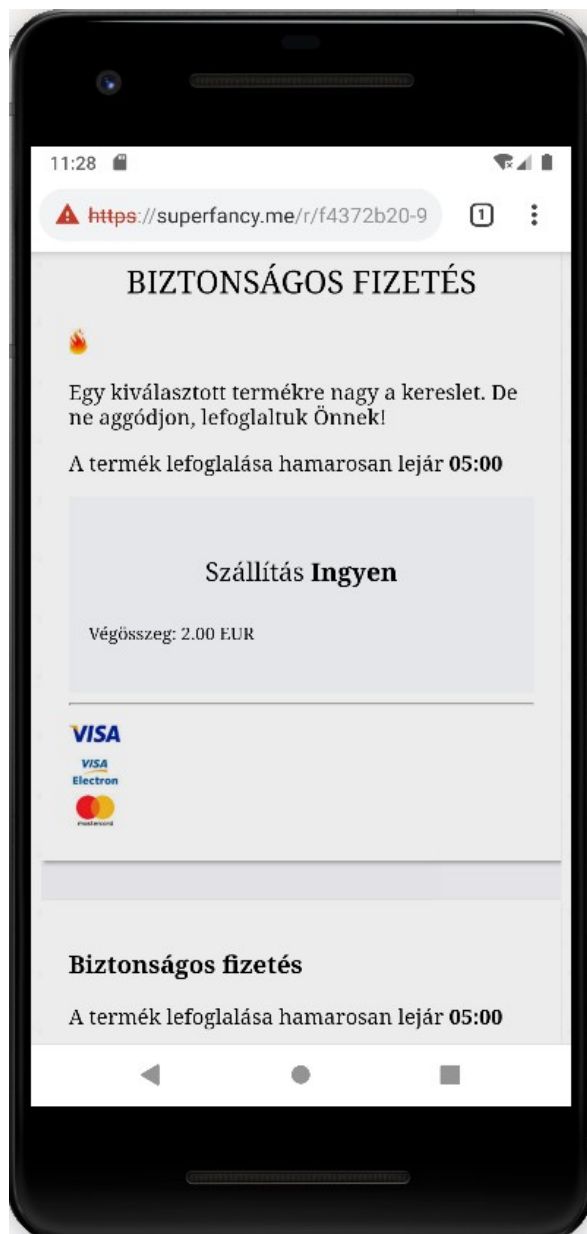
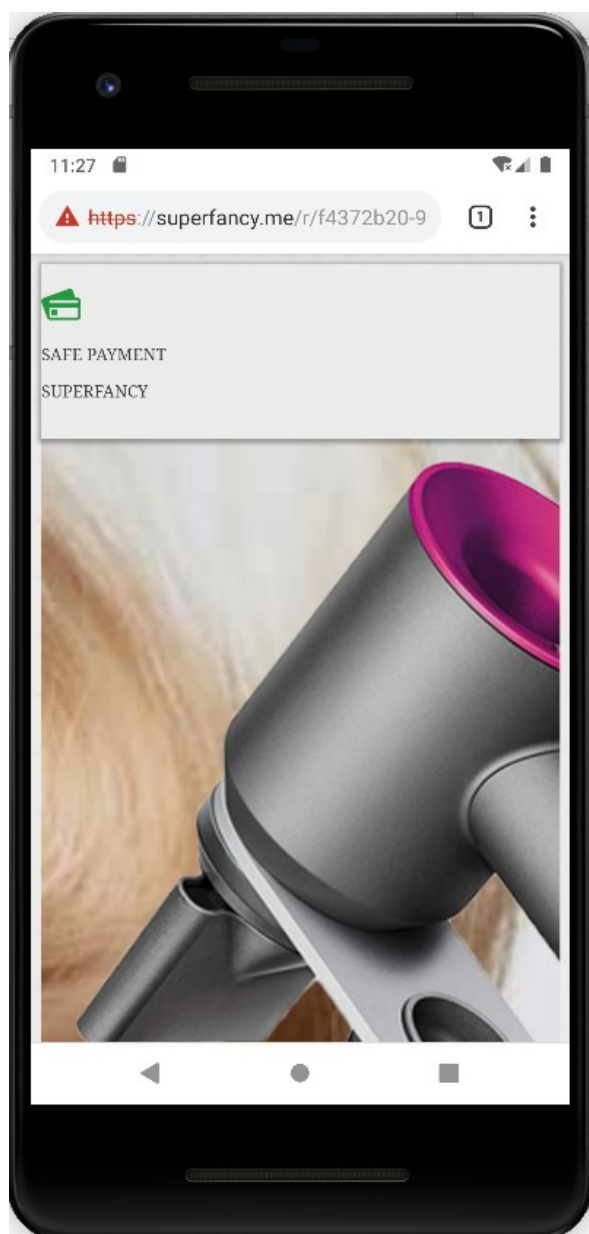
```
POST https://go-deal.club/c/dyson-supersonic-hairdryer/register?_luuid=88eade34-2cdd-4c85-a1b7-301c1bb6c66b HTTP/1.1
Host: go-deal.club
Connection: keep-alive
Content-Length: 580
Cache-Control: max-age=0
Origin: https://go-deal.club
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Linux; Android 9; Android SDK built for x86_64 Build/PSR1.180720.122) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Referer: https://go-deal.club/c/dyson-supersonic-hairdryer/register?_luuid=88eade34-2cdd-4c85-a1b7-301c1bb6c66b
_token=WUtbhBR3oM6QF7vj22ZpaE1S3WRfTdS1125LEsiz&landing=64765&tracking=ho&aff_id=1040&req_id=102bbba17e1ec9e72a217ce3954f0f&sub_id=1769&newsletter=on
&product_name=17.500-Ft+AJ%C3%81ND%C3%89KK%C3%81RTYA&product_image_path=
%2Fstorage%2Ffd3ddc8a-7c97-42eb-a7f4-94803b95e93b%2FGift-Card-mini-apple.jpg%3Fv%3D53beac7a7bf0bbdb6b16d9b2afe265b86674d39&product_color=0ne+color&
product_size=0ne+size&first_name=Hakker&last_name=Hugo&line_1=Hakkol%C3%83+utca+1337.&zip_or_postcode=1337&city=Budapest&country_code=HU&intl-phone=
%2B36313374444&phone=313374444&email=haxor%40haxory.hu&terms=on
```

A válaszban látható néhány hardcoded azonosító is:

```
Header: Text Body: Text
HTTP/1.1 302 Found
Date: Mon, 15 Nov 2021 10:27:10 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
cache-control: no-cache, private
location:
https://superfancy.me/r/f4372b20-9de6-4cc9-988e-365d97945599/6344de96-211d-4dba-88b4-9156f373882d/payment?token=eyJpdiI6Im02a3N2RisrTWlpeUpGaEM3SkxC
SKE9PSIsInZhbnVlIjoRGJPb2NaNTJtYjliNGJTYLdnhb29LRDQraH42Z3QWVMBUxjWlhpPeGEzMD0iLCJtYmM1O1JJYTdhYmRhYjIyMWNKODNjMzYxYTgxN2U2M2I2Mzc3NDlmMjM1Nzc3NjIy
OWYlZmNmN2VjZmU0M2YyMzB1TGZlIiwidGFnIjoIn0%3D&_luuid=88eede34-2cdd-4c85-a1b7-301c1bb6c66b

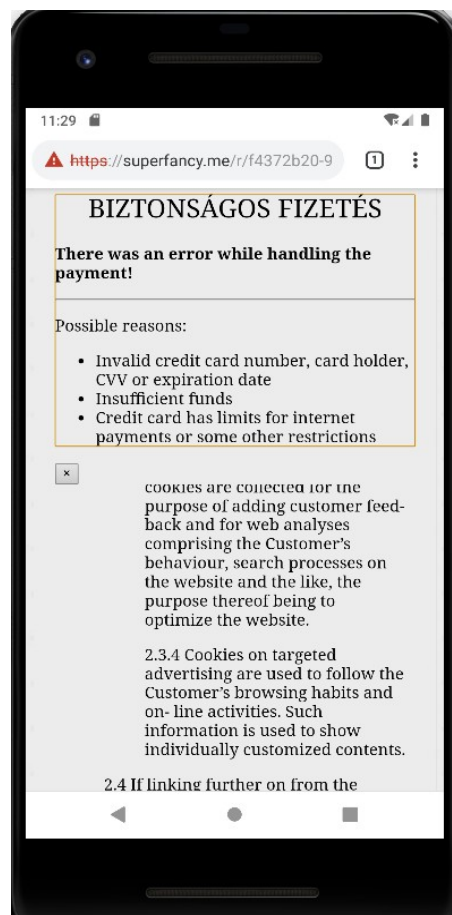
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" /><script type="text/javascript">(window.NREUM||(NREUM={})).init={ajax:{deny_list:["bam.eu01.nr-data.net"]}};(window.
NREUM||(NREUM={})).loader_config={licenseKey:"NRJS-84f38501d7c636516a5",applicationID:"26538562"};window.NREUM||(NREUM={}))._nr_require=function(t,e
,n){function r(n){if(!e[n]){var i=e[n]={exports:{}};t[n][0].call(i,exports,function(e){var i=t[n][1][e];return r(i|e)},i,i,exports)}return e[n]
}.exports;if("function"===typeof __nr_require)return __nr_require;for(var i=0;i<n.length;i++)r(n[i]);return r}({1:{function(t,e,n){function r(){}
function i(t,e,n,r){return function(){}return s.recordSupportability("API/"+e+"/called"),o(t+e,{u.now()}).concat(c(arguments)),n?null:this,r),n?void 0
:this}}var o=t("handle"),a=t(10),c=t(11),f=t("ee").get("tracer"),u=t("loader"),s=t(4),d=NREUM,"undefined"===typeof window.newRelic66(newRelic=d);var
p=["setPageViewName","setCustomAttribute","setErrorHandler","finished","addToTrace","inlineHit","addRelease"],l="api-",v="l+ixn-";a(p,function(t,e){
d[e]=i(l,e,!0,"api")},d.addAction=i(l,"addAction",!0),d.setCurrentRouteName=i(l,"routeName",!0),e.exports=newRelic,d.interaction=function()
{return(new r).get();var m=r.prototype={createTracer:function(t,e){var n={},r=this,i="function"===typeof e;return o(v+"tracer",[u.now(),t,n],r),
function(){if(f.emit(i?"":"no-")+"fn-start",[u.now(),r,i],n).i){try{return e.apply(this,arguments)}catch(t){throw f.emit("fn-err",f.arguments,this.tl
function(){}if(f.emit(i?"":"no-")+"fn-start",[u.now(),r,i],n).i){try{return e.apply(this,arguments)}catch(t){throw f.emit("fn-err",f.arguments,this.tl
```

A HTTP 302 response header átdob minket a superfancy[.]me URL-re, ahol már biztonságos fizetés is a rendelkezésünkre áll:





Mivel az emulátoron az SSL certificate érvénytelen, ezért a kártyás fizetési oldal nem jelent meg, helyette egy hibaüzenet fogadott:



Belenézve a forgalomba látható, hogy egyébként hova menne a fizetés:

[https://go-deal\[.\]club/c/dyson-supersonic-hairdryer/register?\\_luuid=88eede34-2cdd-4c85-a1b7-301c1bb6c66b](https://go-deal[.]club/c/dyson-supersonic-hairdryer/register?_luuid=88eede34-2cdd-4c85-a1b7-301c1bb6c66b):

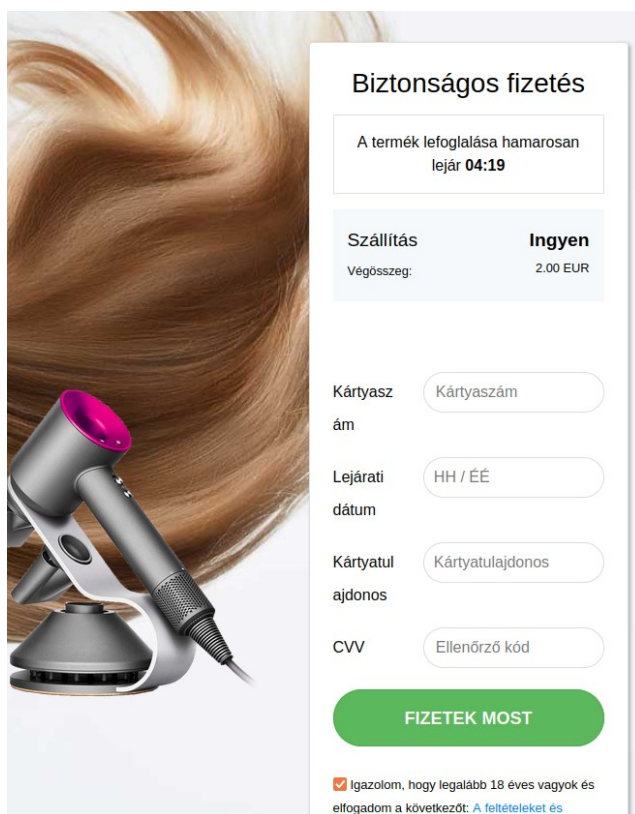
```
        window.preValidate = function (e) {
            if (!validateHolder(e)) {
                return false;
            }
            var result = true;

            globalData.card_holder = $('.wpwl-control-cardHolder').val();
            globalData.card_expiry_month = $("input[name='card.expiryMonth']").val();
            globalData.card_expiry_year = $("input[name='card.expiryYear']").val();
            globalData.token = $('meta[name="csrf-token"]').attr('content');
            globalData.kount_id = window.ka && window.ka.sessionId;

            $.ajax({
                type: 'POST',
                url: 'https://fancy2go.com/preflight/dbc90e6d-57b6-4a51-a3e9-a2c70013de47/tri-yyRp08Q8EKWKznc',
                data: globalData,
                dataType: 'json',
                async: false
            }).done(function (data) {
```

A fancy2go[.]com felé küldi a kártyaadatokat.

Nem hagyott nyugodni a dolog, ezért átvittem a sessiont egy desktop böngészőbe, ami már elfogadja a beavatkozó proxym által megpiszkált HTTPS kapcsolatot is, és egyből lehetőségem nyílt fizetni:



**Biztonságos fizetés**

A termék lefoglalása hamarosan lejár **04:19**

<b>Szállítás</b>	<b>Ingyen</b>
Végösszeg:	2.00 EUR

Kártyaszám

Lejárat dátum

Kártyatulajdonos

CVV

**FIZETEK MOST**

☒ Igazolom, hogy legalább 18 éves vagyok és elfogadom a következőt: [A feltételeket és](#)

Generált kártyaadatokkal viszont elutasította a fizetést, tehát valószínűleg egy valós bankkártyás fizetési tranzakció történt volna..

Akkor hol itt a csalás, kérdezem én, mert hát nyertem is, csak 2 eurót kérnek tőlem, valószínűleg valós kártyás tranzakció zajlik le...

Szóval jobban belenézve az apróbetűs részekbe ez szúrt szemet:

Minden új vásárló 50 Ft értékű ajándékkártyában részesül. Az ajándékkártya e-mailben lesz elküldve. Kattintson a linkre, hogy beváltsa és 50 kredit azonnal bekerül a fiókjába. Ekkor el kezdhet vásárolni. Ehhez a különleges ajánlathoz tartozik egy partneri előfizetési szolgáltatás 5 -napos kipróbálása, amelyet követően az előfizetési díj (havi €38.95 ) automatikusan levonásra kerül a bankkártyájáról. Ha bármilyen okból nem elégedett a szolgáltatással, a fiókját 5 napon belül megszüntetheti. A szolgáltatás hónaponként megújításra kerül, míg meg nem szünteti vagy átugorja a hónapot.

Nehéz középben nem észrevenni a havi 38.95 Euro (kb. 15 000 Ft) előfizetési díjat, ami innentől kezdve automatikusan vonódik a kártyáról.

Tehát összefoglalva:

- előfizettetnek velem egy havi 15000 Ft-os VIP tagságra valahol,
- kapok 50 Ft (!!)
- értékű ajándékkártyát,
- kapok 50 kreditet is,
- megkapják a bankkkártya-adataimat,
- a személyes adataimat,
- és nagy valószínűséggel hajszárítót sem kapok, tekintettel a kamu kommentekre...

Nekem ez nem tűnik jó üzletnek.