Laborator 5 – Securitatea Sistemelor Informatice

**Exercitiul 1** – *sample1.js*

Pentru interpretarea codului am folosit <https://replit.com/languages/nodejs>

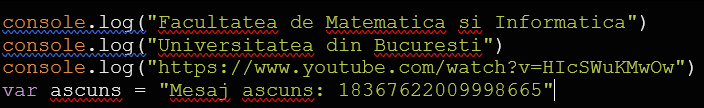
Textul rezultat este:

**Facultatea de Matematica si Informatica**

**Universitatea din Bucuresti**

**<https://www.youtube.com/watch?v=HIcSWuKMwOw>**

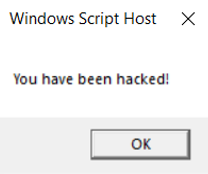
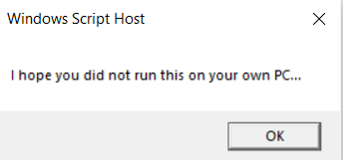
Pentru decode am folosit <https://lelinhtinh.github.io/de4js/> unde apare si mesajul ascuns

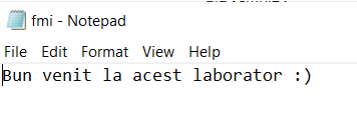
****

Este cod generat automat de un executabil, deoarece este inteligibil, iar un om ar scrie un cod mult mai curat.

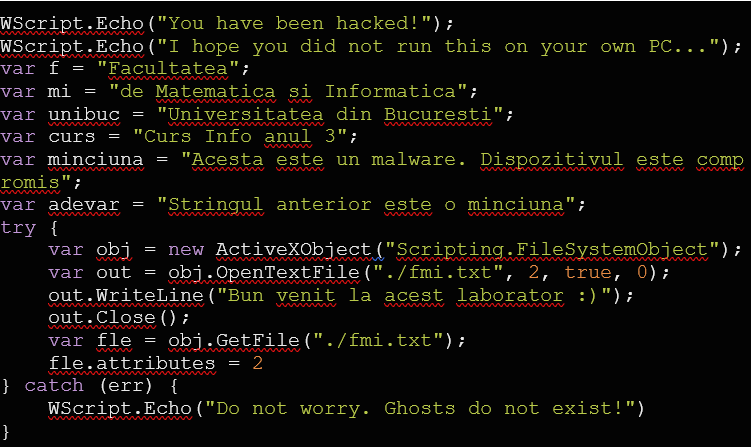
**Exercitiul 2** – *sample2.js*

La prima vedere pare mai inteligibil decat codul din *sample1.js*, insa ultima parte nu are niciun sens, deci si acest cod este generat automat de un executabil. De asemenea, creeaza un fisier ascuns denumit **fmi.txt** in folderul samples. Nu este malware pentru ca nu afecteaza functionalitatea sistemului in vreun fel.



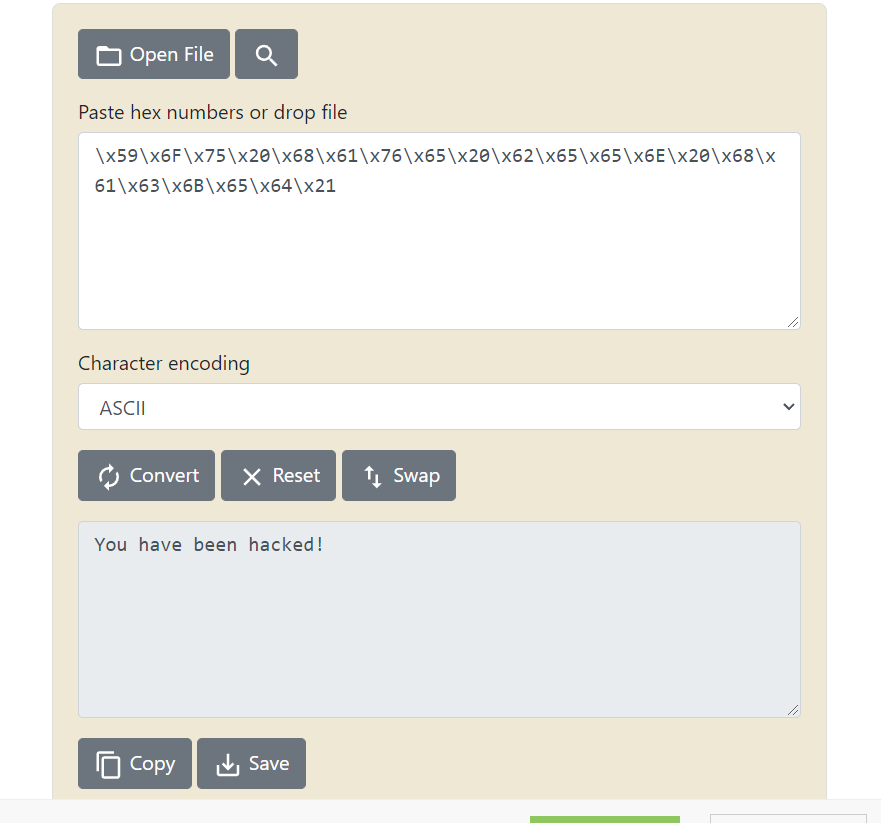
Prin deofuscare folosind <https://lelinhtinh.github.io/de4js/>, se poate vede si scriptul original:

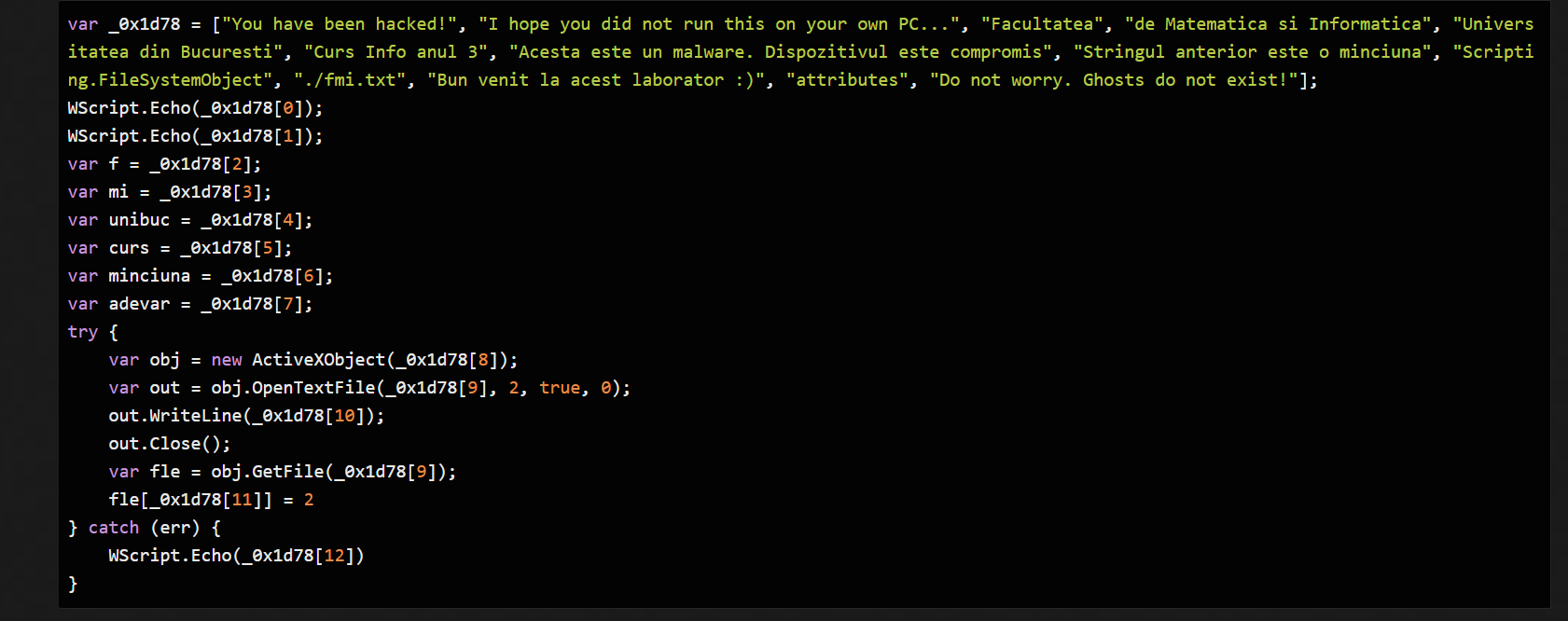


**Exercitiul 3** – *sample3.js*

Acelasi comportament ca *sample2.js* (deschide ferestre de popup).

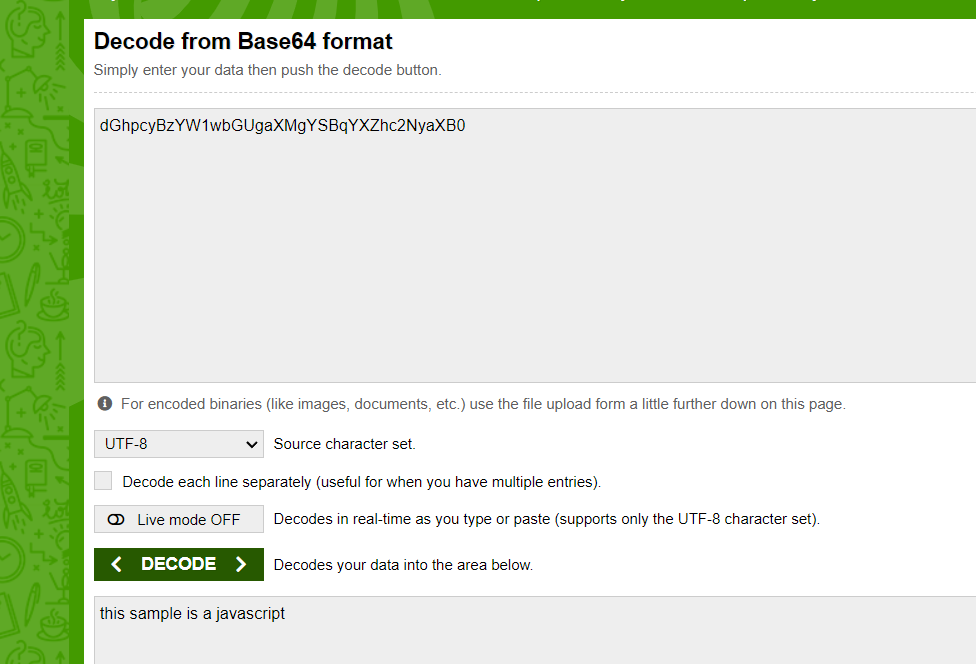
Folosind hex to ASCII converter (<https://www.rapidtables.com/convert/number/hex-to-ascii.html>), am trasnformat vectorul de la inceput care contine numere in hexa. Vectorul este format din mai multe stringuri de mesaje criptate in hexa:

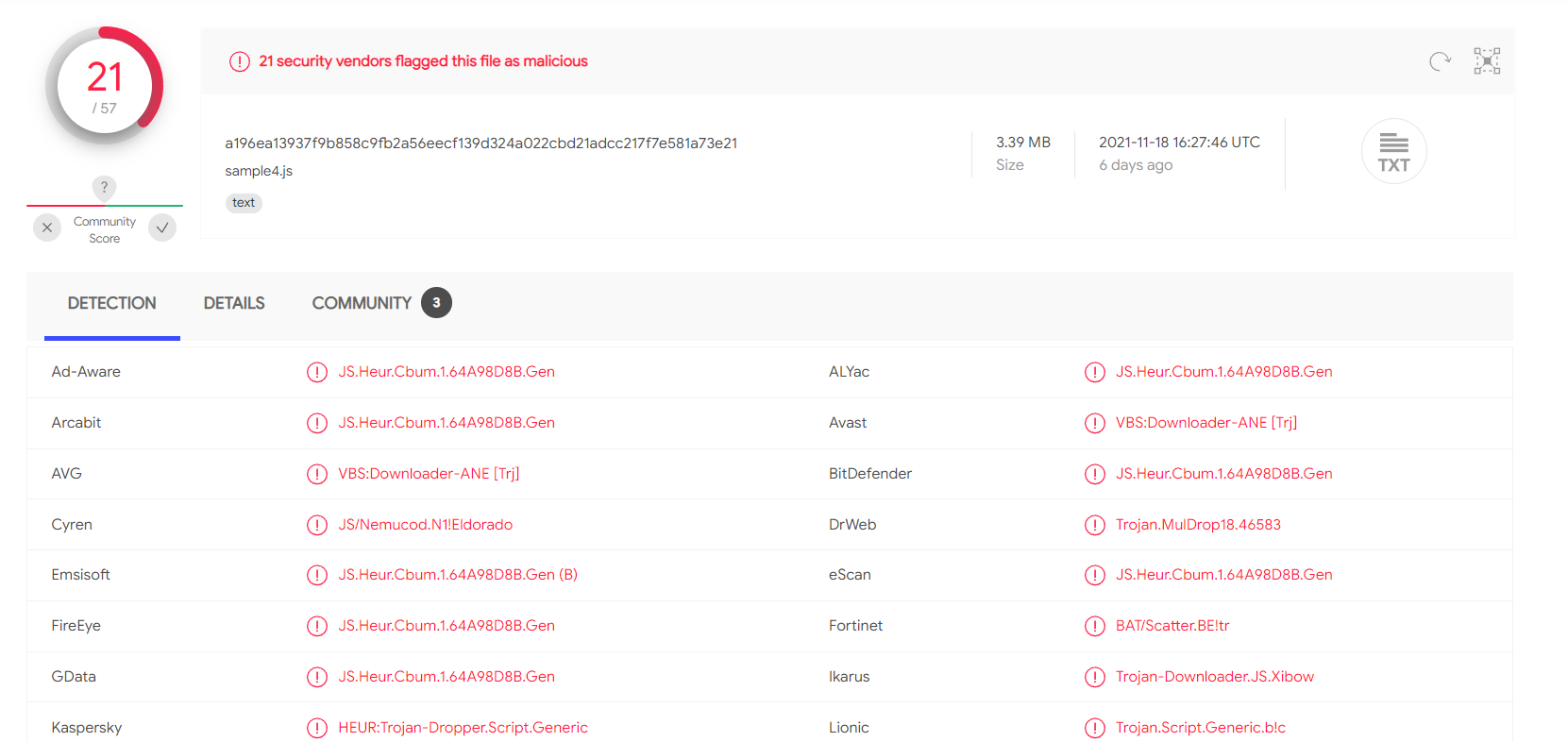


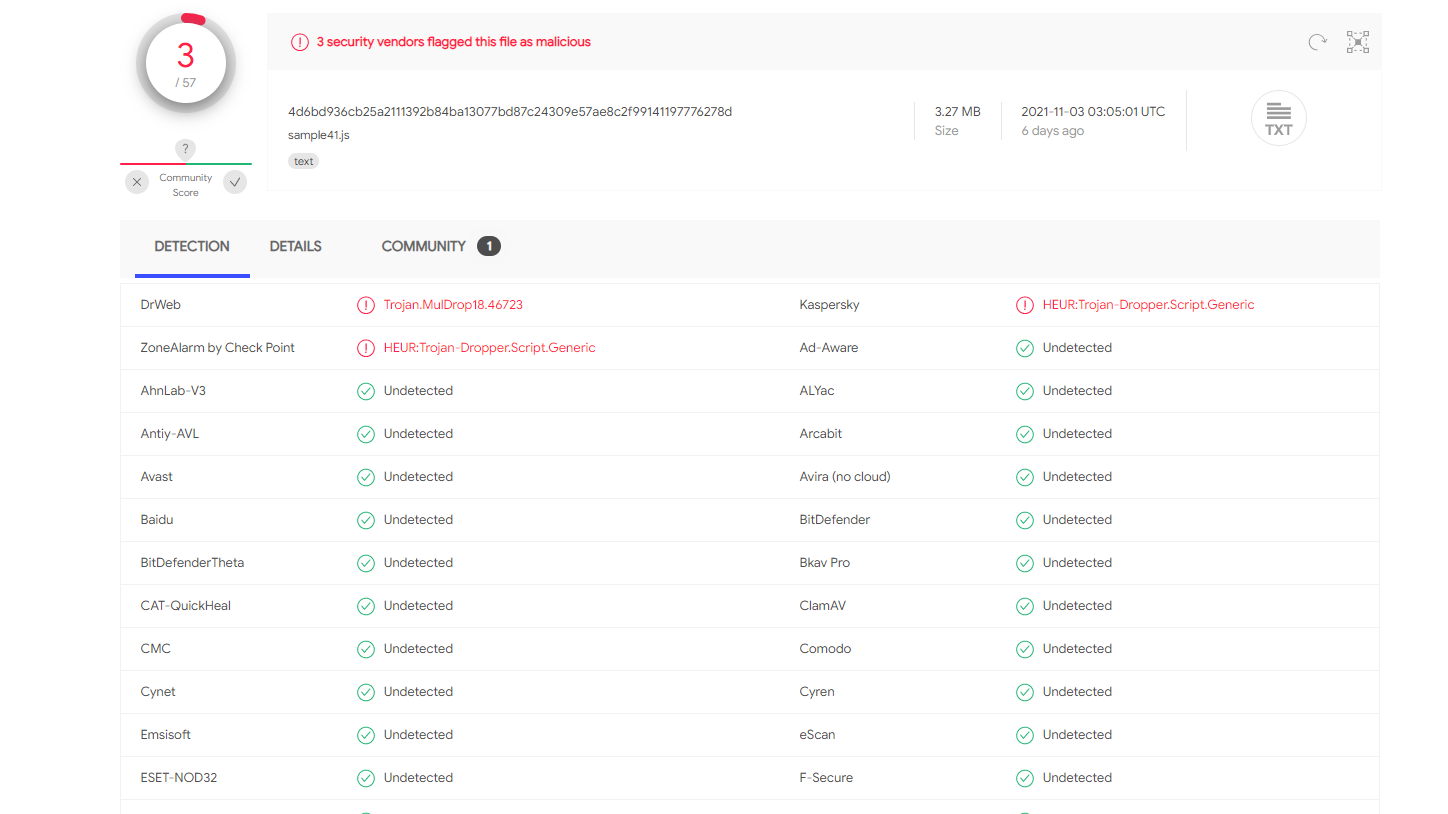
****

**Exercitiul 4** – *sample4.js*

Comentariile sunt in base64. Folosesc decoderul online pentru a le decoda. (<https://www.base64decode.org/>)

Este un virus, conform verfificarii cu Virus Total, insa nu este malitios deoarece nu afecteaza sistemul in vreun fel.

[Virus Total](https://www.virustotal.com/gui/file/a196ea13937f9b858c9fb2a56eecf139d324a022cbd21adcc217f7e581a73e21): Pentru scriptul original – *sample4.js*

Virus Total: Pentru scriptul obtinut dupa obfuscare - *sample4v2.js*