第一回　2023/3/7

A04:Insecure Design
不適切な入力検証

菅田大輔

Admin Registration

- 目的

  管理者権限を持つユーザーとして登録する

- 手段

  localhost:42000/api/UsersにPOSTリクエストを送る。
PostリクエストのBodyは、{“email” : ”admin” , “password” , “admin”, “body” : “admin”}とする。

- 考察

  なぜadminにすれば管理者権限が付与されてしまうのか分からない。形式さえ合っていれば、任意のユーザーからのリクエストを受け付けてしまうことが原因？

Payback Time

- 目的

　買い物カゴの商品の数量を負の値に変更し、決済を行うことで残高を増やす

- 手段

　買い物かごに商品を追加し、その時のNetworkを追跡する。数量をマイナスに書き換えたPUTリクエストを再度送信する。その後、ブラウザ上で決済を行う。

- 考察

　商品の個数が負の値になった場合も考慮すれば防げる。

Upload Size(未達成)

- 目的

  100kB以上のpdfをアップロードする

- 手段

  localhost:42000/file-uploadに、pdfを付与したPOSTリクエストを送る

  →リクエストにpdfを付与することができずに失敗

Deluxe Fraud(未達成)

- 目的

  お金を支払わず、Deluxe Membershipに登録する

- 手段

  残高が足りない場合、Membership購入画面にて開発者画面を開き、「購入不可」のボタンを押せるように変更する。そして、実際に購入を実行する。この時、ウォレットに資金が含まれていないというエラーが返ってくるが、paymentModeパラメータを空の文字列に変更し、再度リクエストを実行する（すなわち、支払いのリクエストを空のものに上書きし、購入だけ行う？？）