x)

Vulnerabilities and Prevention

broken access controls: absent controls, bypassable or misconfigured exposing data or operations

- Access control vulnerability stems from changing the URL by bypassing access control check points or modifying API (application programming interface) requests
- Being a user or admin without being logged in
- Metadata manipulation, like elevating privileges using a hidden field to manipulate it
- Disabling web server directories to conserve data and creating backups
- Domain models should enforce unique application business limit compulsory demands
- Applying access control mechanisms, using them constantly during application and minimizing CORS (Cross-Origin Resource Sharing) usage
    - security mechanism that allows server to grant permission for resources to be accessed from another domain, implemented through web browsers

Vulnerabilities and Prevention

injection: injected malicious input into a program that doesn’t handle or sanitize data properly

- unvalidated, unfiltered, unsanitized users’ data by the app
- used hostile data inside ORM (Object Relational Mapping) to get sensitive records
- common injections: SQL, NoSQL, OS command, ORM and so on
- To detect if there are vulnerabilities, use source code review
- to prevent attacks, use a safe API
    - it gives a parametrized interface, migrates ORM tools

Vulnerabilities and Prevention

security misconfiguration

- unnecessary features (ports, services and privileges are unnecessary)

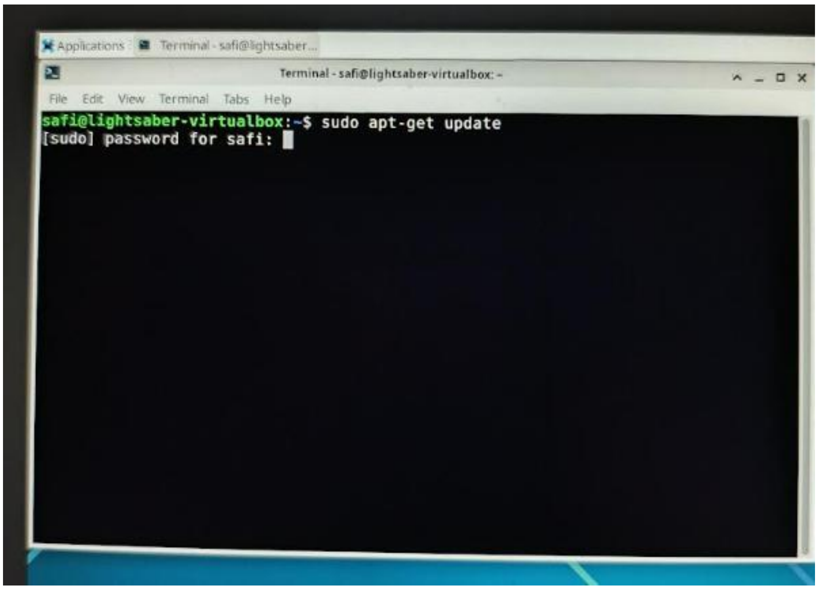
- unchanged details in default accounts such as passwords
- disabled security features for upgrades
- outdated or not updated software
- small platform without any extra features, components and documentation
- automated process to confirm efficiency configuration and settings in the environment

Vulnerabilities and Prevention

vulnerable and outdated components

- similar vulnerabilities to the other subjects, such as software being vulnerable, outdated or unsupported and if they are not constantly scanning and not updating framework,
- monitoring unmaintained libraries and components/ not create security patches for previous versions
- getting components from trustworthy links, preferably signed packages

I keep getting stuck on the commands in the VM. I had the same problem in my previous homework which is why there was barely anything on the pdf file.


Applications
Terminal - safi@lightsaber...
Terminal - safi@lightsaber-virtualbox: ~
File
Edit
View
Terminal
Tabs
Help

```
safi@lightsaber-virtualbox:~$ sudo apt-get update
[sudo] password for safi:
```