{EPITECH}
LEARN DIFFERENT*

CIA

CONSOLIDATE, INVESTIGATE & ADMINISTRATE

* apprendre autrement

CIA

Welcome on board!

Our company is at a stake since our system administrator quit his position…
He left an insecure and partially broken infra which is very critical for us.
Many departments and services are paralysed without the hosted web platform.
We also fear a cyber-attack in the weeks to come.
Please take ownership of the infra, and fix it as soon as possible!

We absolutely need the web application to be functional in the shortest delay, with a complete inventory system (and not only users management).

I remind you of the constraints we have due to practical and security reasons, especially due to the fact that we work with third-party application:

1. the API **should not be in the same host as the web app** and **should not be moved** ;
2. the hosts computers have to stay neutral, that is why all of your sevices are **containerized** ;
3. all the containers must be launched with the user $service - web$.

Moreover, to make it sustainable, please put in place:

1. a **complete log system** of the API, and **test it extensively** ;
2. a **scripted integration and deployment system** with Gitlab as a versionning service ;
3. considering the unreliability of the hosts, we do not want the source code to be directly available on them. There should be an **artifact management software**. It would be interesting to have this software linked to the integration and deployment system.

Available intel

I must also apologize for the conditions in which I ask you to carry out this mission, since I only succeeded to gather partial information from the previous system administrator. As you can guess, he was not very professional, and I am not quite sure everything is useful nor fully reliable.

I share here, in bulk, all he gave me:

> **From:** John <john@unreliable_devops.ru>
> **To:** gina boss <gina@babaexpress.cn>
> **Date:** 01 Jun 2042 13:37
> **Subject:** Re: Re: Re: Re: Re: Re: [URGENT] need information
>
> Hi Gina,
>
> The website is hosted by 4 virtual machines, each of which containing a service: the web platform, the API, the database and the monitoring. The monitoring is managed by Portainer. It should be accessible with the credentials I sent you last week. I will try to search for files and more info about this project and will forward you what I find interesting.
>
> About the automation, nothing has been put in place so far. I planned to install a gitlab server but to be honest, I am not even sure the host could handle a gitlab charge.
>
> Please stop sending me emails on my private email address, I won't answer them. I left and it is for good.
>
> **— John —**

Terminal

```
T-NSA-810> cat babaexpress/web/inventory/API/routes.txt
// main route : /auth
router.post('/register', [validateEmpty], AuthController.register);
// main route : /user
// get all users
router.get('/', [checkJwt, checkRole(['ADMIN'])], UserController.listAll);
// edit 1 user
router.patch('/:username', [checkJwt, checkRole(['ADMIN'])], UserController.editUser);
// delete 1 user
router.delete('/:username', [checkJwt, checkRole(['ADMIN'])], UserController.deleteUser);
```

Details

Front

Features

- ✓ React (without jQuery etc.)
- ✓ TypeScript
- ✓ React Hooks
- ✓ Redux
- ✓ React-router-dom
- ✓ Bootstrap 4
- ✓ Authentication

Quick start without docker

1. Run `yarn install` to install dependencies.
2. `yarn start` to run the application on localhost.
3. Run `yarn run build` to build the production version of the app into the build folder.

Quick start with docker

1. `docker-compose up --build -d; cd back && docker-compose up --build -d` run the app on localhost:8080.

Back

Quick start without docker

1. `yarn install` installs the dependencies.
2. `yarn start` runs the application on port 3000 of localhost.
3. `yarn run build` builds the production version of the app into the build folder.

Quick start with docker

1. `docker-compose up --build -d; cd back && docker-compose up --build -d` runs the app on localhost:3000.

```
Terminal
T-NSA-810> cat babaexpress/web/inventory/.creds.txt
test:test
admin:admin
john:fJrUkjsh_0~E1&
john:john
baba:express
root:aSecurePasswordMustBeAtLeast128CharactersLongIncludingDifferentStuff
root:doNotCommunicate
no_rights:no_rights
toto:toto
titi:tata
user:password
```

If some credentials are missing, you are allowed to try to open by all means. You must exploit vertical vulnerabilities for privilege escalation and lateral vulnerabilities for pivoting.

Make a written report of the procedure used in order to identify the vulnerabilities by which you infiltrated the services. The clarity of the report and the duplicability of your steps are critical.

Obviously, you are expected to patch each vulnerability to secure the accesses (preferably without upgrading the technical stack); provide any recommandation / best practises for the hardening of those services in your report.

Last but not least, we will meet for the overall presentation of your work, with all concerned parties. Please prepare a demo of the functionnal web platfrom, connected to a database. I gave the creds `admin:admin` to Jeff, who will use them for the acceptance phase.

Furthermore, we need to access the services inside the containers, and it also would be nice to add an inventory management inside the web application.

Finally, I insist on the necessity to set up a rapid and efficient deployment of the services listed above. I will be very busy the next weeks, but will try to keep in touch if you have any question.

Kind regards. Gina, your manager.

You are not allowed to use the GRUB vulnerability to get root access, and you should use *dirty COW* instead.

v 1.3

* apprendre autrement