XSS

- ***1.1: screenshot of a successful attack + the payload that you injected***
- ***1.2: payload that you injected***
- ***1.3: payload that you injected***
- ***1.4: description of the fix***

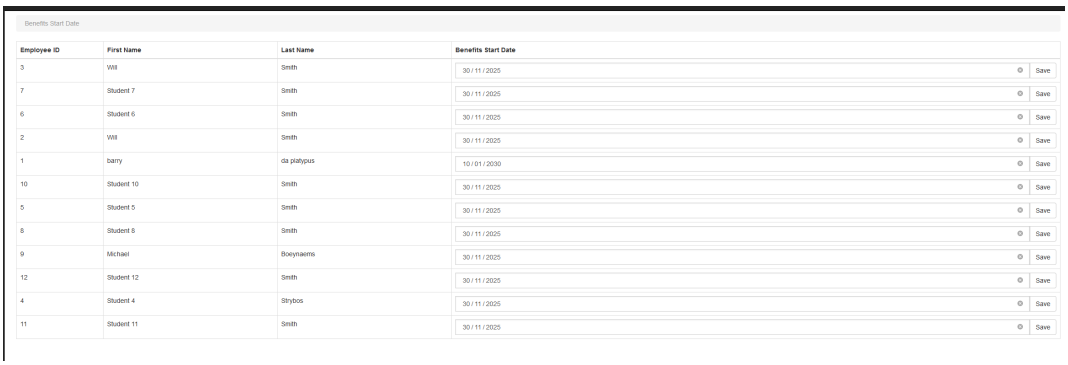
1.1 XSS attack

Execute an XSS attack against the search functionality of the Juiceshop application.

https://juiceshop-websec.herokuapp.com/#/search

1.2 XSS attack

The nodegoat application (https://nodegoat-websec.herokuapp.com/), where you have an account (ask the teacher if you do not remember it) is managed by an administrator. The administrator regularly reviews the list of registered users, which looks like this:



You are one of these users (the teacher has provided an account).

The profile pages and the page shown above is vulnerable to XSS. Can you execute a stored XSS attack which will also execute in the administrator's browser when he opens the list of all users?

Execute it. The teacher will open the administration page at the end of the exercises.

1.3 XSS advanced attack

The application hosted at https://todo-app-react-xss.herokuapp.com/ is an application that can be used to keep a list of todo's between a group of friends. However, one friend is a little bit bored and tries to hack the others through cross-site scripting. You are that friend, can you find and exploit the vulnerability?

HINT: if you can't find it, take a look at the next exercise which shows some of the source code of this application that may help you finding the vulnerability.

Note that this is a default React application. It has not been altered, or its security has not been deliberately reduced. Please remember this example and do not simply think "*I'm building my application in a framework that thousands of other people are using, I will be fine*". As a developer you always have to think about security, frameworks are only part of the solution.

1.4 XSS advanced attack fix

The source code for the page responsible for displaying the todolist is displayed below. Can you spot the problem and think of a possible fix?

```
import React from 'react';

const ListTodo = ({ todos, deleteTodo }) => {
  return (
    <div >
    <hr />
    <h2>Things to do</h2>
    <table className="table">
        <thead className="thead-dark">
            <tr>
                {/* <th scope="col">#</th> */}
                <th scope="col">Todo</th>
                <th scope="col">More information</th>
                <th scope="col">Remove from list</th>
            </tr>
        </thead>
        <tbody>
        {
            todos &&
            todos.length > 0 ?
                (
                todos.map(todo => {
                    return (
                        <tr key={todo._id}>
                            {/* <th scope="row">{todo._id}</th> */}
                            <td>
                                {todo.action}
                            </td>
                            <td>
                                 {!todo.infourl ? "/" :  <a  href={todo.in-
fourl}>More information</a>}

                            </td>
                            <td className="list-group-item-danger" style={{cur-
sor:'pointer'}} key={todo._id} onClick={() => deleteTodo(todo._id)}>
                                Delete
                            </td>
                        </tr>
                    )
                })
                )
                :
                (
                <tr className="list-group-item-success">
                    {/* <th scope="row"></th> */}
                    <td >
                        No todo's left
                    </td>
                    <td></td>
                    <td></td>
```