

Cyber Security Project Report, author kxkyllon.

The source code for the project can be found in <https://github.com/kxkyll/csecp>

The application is for enrolling people to some event. It stores participant name, address and phone numbers. One can also suggest links for other people to see prior the event.

Application lists participants and allows to search for them. The predefined username is ted and password is president.

The screenshot shows two browser tabs. The left tab, titled 'A template', displays a page with the URL 'localhost:8080'. The page content includes 'My security project' and a 'Login' link. The right tab, titled 'Participant form', displays the URL 'localhost:8080/form'. The page content includes 'My security project', a 'ted' username, a list of links ('Sign to our event', 'Search participants', 'Suggest links', 'Logout'), and a 'Sign to our event' section with input fields for Name, Address, and Phone, and a Submit button.

## A2-Broken authentication and session management

User can press logout link, but the application is missing all functionality. If a user goes back to some of the application pages he/she is still treated as a logged in user.

How to avoid? Use spring security logout handler (SecurityContextLogoutHandler) to manage logout functionality.

The screenshot shows a browser tab titled 'Participant form' with the URL 'localhost:8080/form'. The page content includes 'My security project', a 'ted' username, a list of links ('Sign to our event', 'Search participants', 'Suggest links', 'Logout'), and a 'Sign to our event' section with input fields for Name, Address, and Phone, and a Submit button.

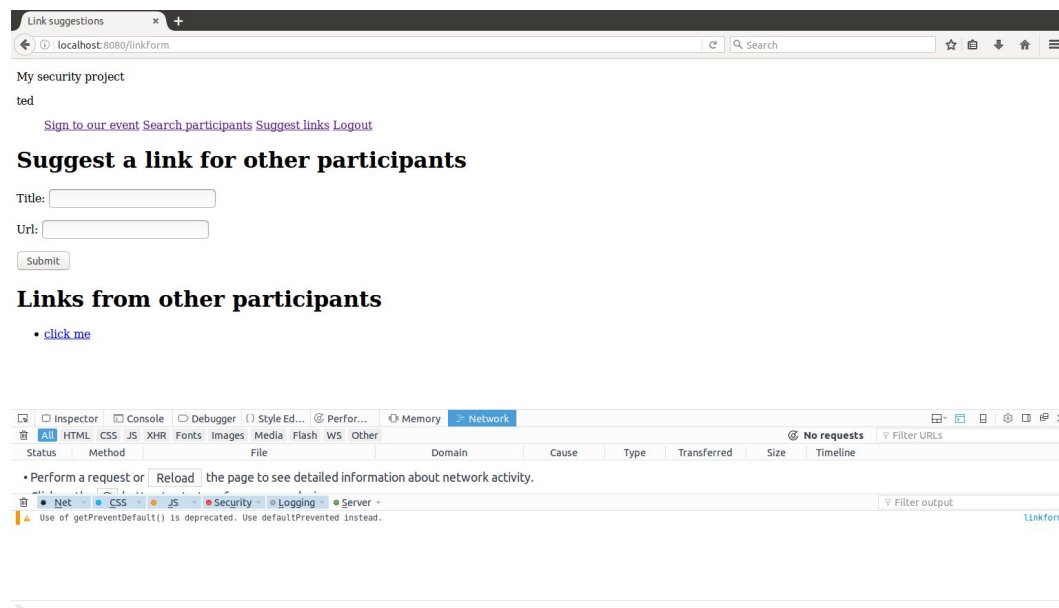
## A10-Unvalidated Redirects and Forwards

If target URL is included in parameter and not validated against a white list the app is vulnerable.

Go to to page <http://localhost:8080/link> and insert a link. The link is directly added to database without any validation or confirming with a whitelist and then listed to the user. After clicking some of the links a user is forwarded to that page.

How to avoid. Use validation in the client and in the server side. Use whitelists of accepted links. Or even better is not not to allow a user to insert a link at all. Instead provide yourself some links that might be useful. More thorough guide:

[https://www.owasp.org/index.php/Unvalidated\\_Redirects\\_and\\_Forwards\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Unvalidated_Redirects_and_Forwards_Cheat_Sheet)



## A7-Missing function level access control

The application is meant to work so that only the one's that have logged in can add participants to the event <http://localhost:8080/form> and send links via page <http://localhost:8080/link> but in reality anyone can go directly to these pages. Also participant data can be searched <http://localhost:8080/participant>

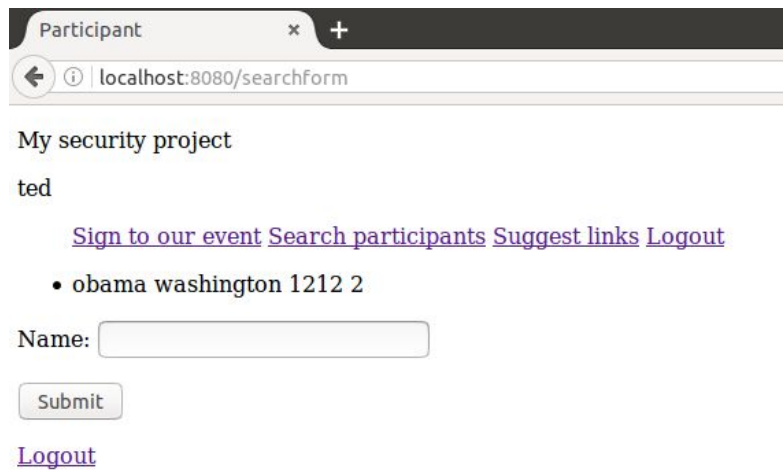
How to avoid? Confirm that only users that are logged in are authorized to go to these pages. Use spring security configuration to achieve that.

## A6-Sensitive data exposure

The enrollment form asks for phone number that is saved in clear text). Anybody (also users that have not logged in) can also query participants by name and then all participants matching this name will be shown with their phone numbers.

Phone numbers are considered here as sensitive data, could be as well credit card numbers etc.

How to avoid? Allow such a search to only ones with admin role using spring security.



Participant x +

localhost:8080/searchform

My security project

ted

[Sign to our event](#) [Search participants](#) [Suggest links](#) [Logout](#)

- obama washington 1212 2

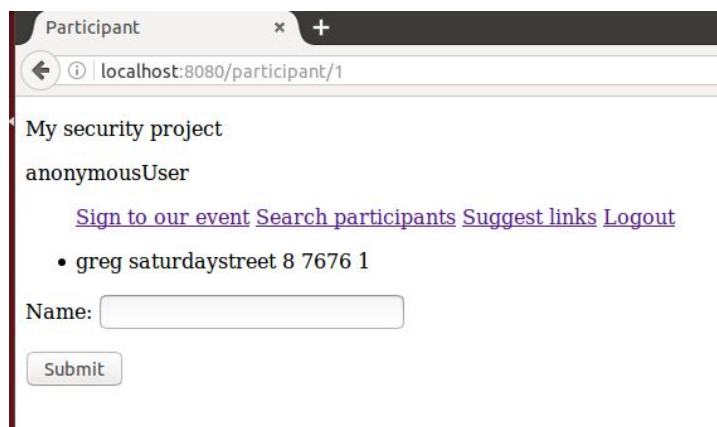
Name:

[Logout](#)

## A4-Insecure Direct Object References

In this application anyone can access directly a participant data by giving an participant id to page e.g. <http://localhost:8080/participant/1/>

How to avoid? Remove possibility from user to go directly to the participant page when an id is known or guessed by redirecting to login page when a user is not logged in or to enrolling new participants when a user is logged in.



Participant x +

localhost:8080/participant/1

My security project

anonymousUser

[Sign to our event](#) [Search participants](#) [Suggest links](#) [Logout](#)

- greg saturdaystreet 8 7676 1

Name: