**DOT framework research**

**Student:** Jorn Kersten

**Student number:** 483331

**Class:** DB-S3-DB03

Tabel of contents

[DOT framework 3](#_Toc124427490)

[What is the DOT framework 3](#_Toc124427491)

[The “What” 3](#_Toc124427492)

[The “Why” 3](#_Toc124427493)

[The “How” 4](#_Toc124427494)

[Library (Top right of figure 1) 4](#_Toc124427495)

[Field (Top left of figure 1) 4](#_Toc124427496)

[Lab (Bottom left of figure 1) 4](#_Toc124427497)

[Showroom (Bottom right of figure 1) 4](#_Toc124427498)

[Workshop (middle of figure 1) 4](#_Toc124427499)

[Source 4](#_Toc124427500)

[OWASP A07:2021-Identification and Authentication Failures 5](#_Toc124427501)

[Main question 5](#_Toc124427502)

[Chosen research method 5](#_Toc124427503)

[Execution 5](#_Toc124427504)

[Possible Loophole in Authentication Workflow 5](#_Toc124427505)

[The Problem 5](#_Toc124427506)

[Client-Side Vulnerabilities 5](#_Toc124427507)

[Browser Storage 5](#_Toc124427508)

[Solution according to Angular docs 6](#_Toc124427509)

[Sources 6](#_Toc124427510)

[Results 6](#_Toc124427511)

# DOT framework

## What is the DOT framework

The DOT framework is a research framework that helps answer ICT-related questions. The DOT framework helps to structure the research. The structure goes as follows: first comes the "What" of the research, then comes the "Why" of the research then follows the "How of the research". Below, I explain what these three parts mean.

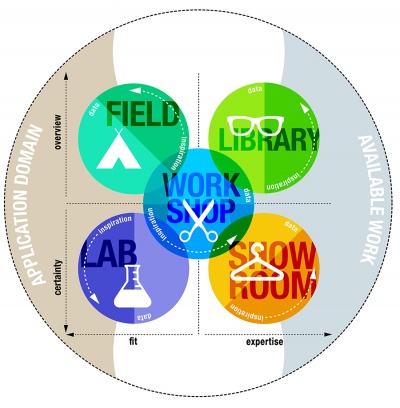


Figure 1

## The “What”

There are two different studies that can be done. One is the specific application context of the project and the other is a more general knowledge available that can help with a project. Both forms of research help and are necessary to create your own "innovation", your first new product or report. This can be expressed using three domains. The first domain is the "application domain". This is the domain of the specific context in which the ICT project takes place. The second domain is that of the "Available work". This uses all accessible theories, models and other artefacts that can be used from all currently available work. The third domain is the "Innovation domain". This is where the actual innovation takes place and all the under is done.

## The “Why”

It starts with getting on paper what you would like to research. This helps with creating a better structure to your research. If you are researching the context of your application, then the reason for your research is probably to obtain a product that is relevant to the stakeholders in the project. You are trying to optimize the **fit** between your product and the application context. Sometimes you want your product to conform to quality standards, in this case you are trying to make use of as much **expertise** available in the creation of your project. In both topics you use the "available work" domain (Figure 1, right column). You often use both research methods in these types of projects.

Similarly, there is a trade-off between optimizing **overview** and **certainty**. Often, mostly in the beginning you want to gain a good overview about what is needed or what is available. At other times you want to test specific aspects of your work, making sure it works. In these cases you try to configure your research to optimize "certainty" about your hypotheses or goals.

## The “How”

During the project, the aim is to learn as much as possible about the context of available work, the application context and the innovation space. The DOT framework has 5 methods for this:

### Library (Top right of figure 1)

Library research is done to explore what is already done and what guidelines and theories exist that could help you further your design. Since the advent of the internet library research is also called desk research.

### Field (Top left of figure 1)

Field research is done to explore the application context. You apply a field strategy to get to know your end users, their needs, desires and limitations as organizational and physical contexts in which they will use your product.

### Lab (Bottom left of figure 1)

Lab research is done to test parts or concepts of your product, of the final product. You use lab research to learn if things work out the way you intended them, or to test different scenarios.

### Showroom (Bottom right of figure 1)

Showroom research is done to test your ideas in relation to existing work. Showing your prototype to experts can be a form of showroom research or spelling out how your product is different from the competition. Also testing your product to general guidelines is a form of showroom research.

### Workshop (middle of figure 1)

Workshop research is done to explore opportunities. Prototyping, designing and co-creation activities are all ways to gain insights in what is possible and how things could work.

## Source

<https://ictresearchmethods.nl/The_DOT_Framework>

# OWASP A07:2021-Identification and Authentication Failures

## Main question

The main question of this research is as follows: I would like to know how to prevent identification and authentication failures within my project.

## Chosen research method

I’m going to be using the [Community](https://ictresearchmethods.nl/Community_research) (library) research and the [Document analysis](https://ictresearchmethods.nl/Document_analysis) (field) research to reach my goal.

## Execution

### Possible Loophole in Authentication Workflow

The server is responsible for generating the session ID or auth-token. The client, on the other hand, is responsible for storing it securely. If this auth-token or session ID is intercepted, it can create a loophole in the authentication workflow. If it is intercepted, someone from outside can use the token to access the application.

### The Problem

The problem is that the URL contains the auth-token or the session ID. If a hacker manages to get hold of the URL when the client logs into the website, the hacker can snip the token or session ID from the URL. Then, on the server, the hacker can impersonate the user and retrieve all kinds of data from the user or from the server.

If you don't pay attention to how you send the auth token or session ID, you probably put it in the URL. Then the hacker can access the token. It can also happen that someone forgets to log out on a public PC, if the session ID is then visible, it can also be used.

### Client-Side Vulnerabilities

Most of your client-side code is available in the browser. So, it's vital that you structure your system in a way that it will still be intact if your global variables of the source code are exposed.

One of the best practices you should follow is ensuring that session IDs are not easily visible or accessible to anyone. As a first step, you should never store or append the authentication token or session ID in your front-end URL.

You should implement session management in your front end that keeps the session ID away from the UI. For this, you can store the session ID inside browser storage instead of route parameters.

Let's see how we can achieve the above implementation in an Angular application. The result is that we should have some defences against Angular broken authentication.

### Browser Storage

The solution to this problem is to use browser storage. Instead of passing the session ID in the front-end route, we can put it in browser storage, such as local storage or session storage. Instead of the server passing the session ID or auth token along in the URL, the token is passed along through the body and stored as a value. Because it is an HTTPS request, this value cannot be read. However, the front-end can then use the session ID or auth-token, and so it is safe again.

### Solution according to Angular docs

As indicated in the previous sections, it can be seen that the auth-token or session ID should not be given along with the URL. Angular uses a router for this purpose. With the router, it is possible to track a resource and specify a new URL location, in addition, parameters can also be passed along to the next URL. As a result, the auth-token or session ID is not visible in the URL or anywhere else on the page, but can still be used on the website.

### Sources

<https://cyolo.io/blog/identification-and-authentication-failures-and-how-to-prevent-them/>

<https://www.stackhawk.com/blog/angular-broken-authentication-guide-examples-and-prevention/>

<https://angular.io/guide/security>

<https://angular.io/guide/accessibility>

## Results

To avoid identification and authentication failures, it is important that no auth-tokens or session IDs are leaked to a visual section on a web page. This could be in the URL or somewhere on a page. If this does happen, a lot of harm can be done. The solution to this is to send it to browser storage, this can easily be done in Angular using a router, for example. This ensures that parameters are easily forwarded to another page without being leaked.