# D5.5 - Cyber Security Knowledge base v1

## WP5– Analysis and Decision Making

**Version: 1.00**

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

## Disclaimer



## Copyright message



## Document information

| Grant Agreement Number | 826183 | Acronym | SPHINX |
|---|---|---|---|
| **Full Title** | A Universal Cyber Security Toolkit for Health-Care Industry | | |
| **Topic** | SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures | | |
| **Funding scheme** | RIA - Research and Innovation action | | |
| **Start Date** | 1st January 2019 | **Duration** | 36 months |
| **Project URL** | http://sphinx-project.eu/ | | |
| **EU Project Officer** | Reza RAZAVI (CNECT/H/03) | | |
| **Project Coordinator** | Dimitris Askounis, National Technical University of Athens - NTUA | | |
| **Deliverable** | D5.5. Cyber security knowledge base v1 | | |
| **Work Package** | WP5 – Analysis and Decision Making | | |
| **Date of Delivery** | **Contractual** M22 | **Actual** | |
| **Nature** | R – Report | **Dissemination Level** | P - Public |
| **Lead Beneficiary** | FINT | | |
| **Responsible Author** | Argiris Sideris | **Email** | asideris@f-in.eu |
| | | **Phone** | |
| **Reviewer(s):** | Ilias Trochidis (ViLabs), George Doukas [NTUA] | | |
| **Keywords** | Knowledge base | | |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

*Document History*

| Version | Issue Date | Stage | Changes | Contributor |
|---|---|---|---|---|
| 0.10 | 15/09/2020 | Draft | ToC | Anargyros Sideris (FINT) |
| 0.50 | 15/10/2020 | Draft | First consolidated version | Dimitris Apostolakis (FINT), Yiannis Nikoloudakis (HMU) |
| 0.50 | 21/10/2020 | Draft | Internal Review | George Doukas (NTUA), Ilias Trochidis (ViLabs) |
| 0.9 | 28/10/2020 | Pre-Final | Second consolidated version | Dimitris Apostolakis, Argiris Sideris (FINT), Yiannis Nikoloudakis (HMU) |
| 0.91 | 28/10/2020 | Pre-Final | Quality Control | George Doukas (NTUA) |
| 1.00 | 29/10/2020 | Final | Final | Christos Ntanos (NTUA) |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Executive Summary

Deliverable D5.5 reports on the implementation status of the SPHINX Cyber security knowledge base repository (KBR) and Common cyber security toolbox (CCST) components. In this context, the document first provides a general overview of the Cyber security knowledge base concept. Further to that, it discusses the design of the Knowledge base repository and the common cyber security toolbox in the SPHINX ecosystem along with their internal structure and interfaces. In addition, a performance evaluation of the implemented Knowledge base API, through which other SPHINX entities are able to access the stored information about the collected cyber threat intelligence, is presented. Moreover, the Knowledge Base dashboard, from which the end users have access to the stored information regarding cyber threats, is presented. It is noted that this deliverable reports on the results of the first iteration (M13-M22) of the associated task (T5.5). The next iteration's (M26-M34) outcomes, concerning the final implemented system, will be included in the final version of this deliverable D5.10 (M34).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Contents



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Table of Figures



# Table of Tables



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Table of Abbreviations

| ABBREVIATION | EXPLANATION |
|---|---|
| **AI** | Artificial Intelligence |
| **API** | Application Programming Interface |
| **KBR** | Knowledge base repository |
| **CAPEC** | Common Attack Pattern Enumeration and Classification |
| **CCST** | Common cyber security toolbox |
| **DB** | Database |
| **MLID** | Machine Learning Intrusion Detection |
| **STIX** | Structured Threat Information eXpression |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# 1 Introduction

## 1.1 Purpose & Scope

The purpose of this document is to present the work results regarding the design and implementation of both the SPHINX KBR and CCST components. The scope of the current deliverable focusses on discussing:

- The various types and categories of Knowledge base repositories
- The design and implementation of interfaces allowing access to the Knowledgebase repository collected data
- The design and implementation of Common Cyber security toolkit
- The knowledge representation model used for exchanging threat information inside SPHINX components

## 1.2 Structure of the deliverable

This document is structured as follow: section 2 presents a survey about Knowledge Base Repositories; section 3 presents the design of the SPHINX KBR and its relative interfaces. Section 4 describes the design and the implementation of the CCST; section 5 contains a performance evaluation of the SPHINX KBR API. Finally, section 6 contains the conclusions regarding the current status of SPHINX KBR and CCST components' implementation.

## 1.3 Relation to other WPs & Tasks

SPHINX KBR is directly linked to WP3, WP4, and WP5 work packages as the SPHINX components (e.g. Vulnerability assessment as a Service-VAaaS) developed there may retrieve or store threat intelligence information. In order for SPHINX components to be able to retrieve the stored information, a REST API with specific endpoints will be designed:

- An endpoint for retrieving existing threat intelligence information (e.g. attack patterns) stored in the KBR
- An endpoint for creating and storing threat intelligence information (e.g. a new attack pattern) in the KBR

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# 2 Knowledge Base Survey

## 2.1 Survey overview

As an initial point of this survey, what a Knowledge Base is should be clarified. A Knowledge Base (KB) is a centralized repository where information is stored, organized into various categories in order to be easily queried and retrieved [1]. According to their visibility, KBs fall into two major categories, the Internal KBs and the External KBs. External are these KBs that are public and accessible by everyone. Such Knowledge Bases, for instance, are companies' support Knowledge Bases where customers can search and find all the information about companies' services and products. Internal on the contrary are those KBs that are only accessible by a selected type of users. A representative example of Internal KBs are KBs accessible only within the company's intranet which facilitates the collaboration of employees and the distribution of the important knowledge of the company internally.

## 2.2 Survey results

A knowledge-capture process requires a place to store what is collected. A repository is such a place, designed to be easy to use for storing and retrieving content. It can take the form of a database, a list or document library within a tool such as a Knowledge Base, or a collection of files within an intranet site, team space, or portal.

A KB is a repository typically used to store answers to questions or solutions to problems. It enables tasks such as rapid search, retrieval, and reuse, either performed by the help desk personnel, or directly by anyone who needs customer/technical support or information about a product of a company.

In addition, apart from browsing and searching capabilities, repositories are also useful in conjunction with threaded discussions. When a community member asks if a specific type of content is available, another member can reply with links to instances within existing repositories. This is an example of combining collection with connection; content has been collected and stored in a repository, and a connection is made between people to take advantage of that content at the time of need [2].

KBs are very important in the Cyber Security spectrum. Security data, based on events and behaviors, can create various security patterns. These patterns can be seen in systems rather than the operation of the single system alone. By aggregating these patterns, we can easily identify various attacks (like the formation of a knowledge base). The role of a Cyber Security Knowledge Base is to identify and categories these patterns against a huge set of common incidents, attacks and vulnerabilities. Likewise, it also provides a set of rules and inference capabilities, which facilitate matching and identification of threats based on a combination of indicators. These inference capabilities endow the security system with advanced characteristics that substantially enhance the intelligence of a security system. There are a lot of Open Source and Commercial KBs. One of the most important Open Source repository is the CVE (Common Vulnerabilities and Exposures) database, which is sponsored by the United States Department of Homeland Security. CVEs include two types of security threats, vulnerabilities and exposures. When multiple references of vulnerability are available, they are presented in the following order: First the initial announcement of the vulnerability, and next to the response team advisory followed by the vendor's acknowledgment and all other public sources where the vulnerability is referenced. In order for the CVEs to be stored and categorized efficiently, a database has been made by NIST. This database is named National Vulnerability Database (NVD). The NVD itself is a superset of the CVE system with some additional tools like analytics and search engines. Following the analytical tools of the NVD, a tool for calculating a vulnerability score for given threats has been made, which is called CVSS (Common Vulnerability Scoring System). Security vendors and integrators wishing to take advantage of the NVD are provided with access through XML and JSON data feeds, which comprise the augmented CVE information. They can also download and process the entire NVD information. Moreover, data and tools for using the CVSS scoring system are

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

provided. Overall, access to NVD data provides the means for an open and simple implementation of a security knowledge base. [3]

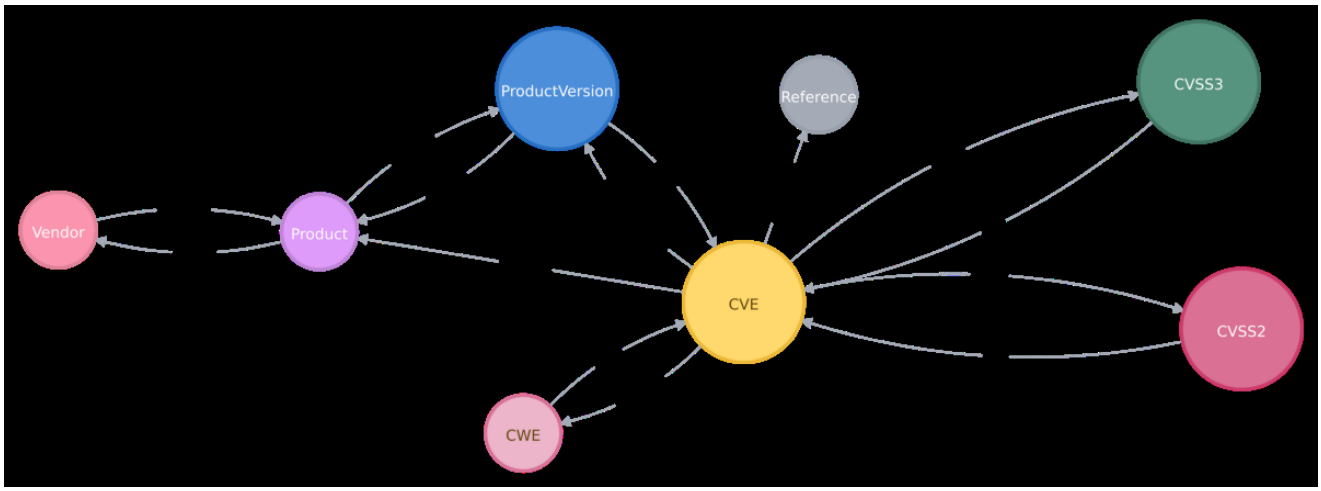


***Figure 1 Discovery and Visualization of a Security Vulnerability by CVE***

A similar standard to CVE is the STIX standard. STIX is the acronym for Structured Threat Information eXpression. The name is explicit: it is a standard for expressing information about computer threats in a structured and unambiguous way. Based on JSON, it has the potential to allow automatic information exchange between the many tools used to ensure the security of an organization [4]. STIX 2.0, standardized in July 2017, defines two categories of STIX objects: STIX Domain Objects (SDO) and STIX Relationship Objects (SRO).

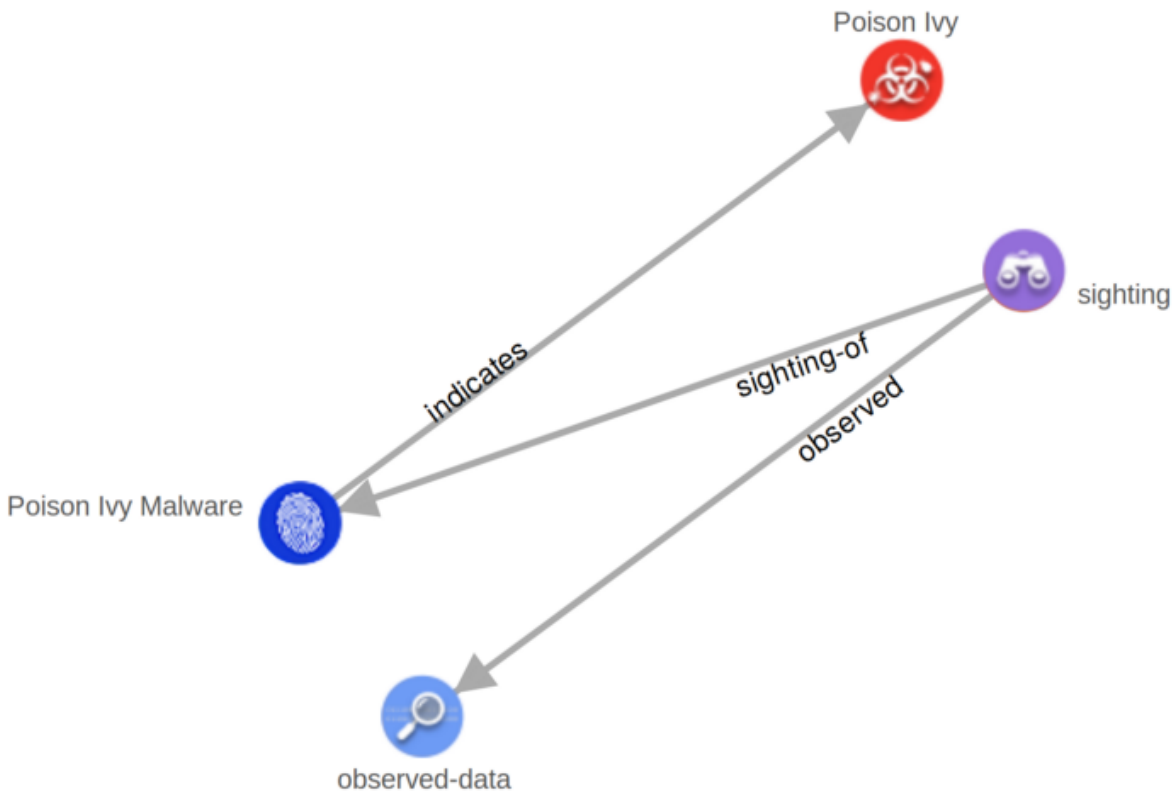


***Figure 2 Example of a STIX Object visualized***

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

The STIX items are distributed using the TAXII standard protocol. TAXII, or Trusted Automated Exchange of Intelligence Information, is an intelligence exchange protocol over HTTPS. The standard defines a set of requirements for clients/servers and a REST API to interact with two types of services: collection, an interface to a server-provided repository of objects that allows a producer to serve consumers in a request-response template and channel, that allows the exchange of information according to a publish-subscribe model. In reality, the channel service is not yet standardized and the term is only reserved for the moment. [5]

Medical devices are very fragile devices, by their nature, that need to work without interruption. However, there are a lot of vulnerabilities targeting medical devices. That is why these devices should be protected by using a security system with intelligent characteristics, with a self-improving Knowledge Base able to combine all the needed information.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# 3 SPHINX Knowledge Base Repository - KBR

## 3.1 SPHINX KBR overview

The KBR is an important part of SPHINX Toolkit. Its purpose is to combine information regarding attacks and vulnerabilities and to incorporate it into a large repository associated with possible solutions and links to other vulnerabilities. KBR draws information from reputable repositories using its Knowledge Extractor which can be enhanced by authorized personnel. In the next iteration phase, a new API will be created that will allow other SPHINX Components to share Threat Intelligence information with the KBR in machine-readable form. KBR is implemented with user friendliness in mind and that is why it has a functional and easy Dashboard that allows users to review and edit the information available. KBR can also distribute its information to other SPHINX Components as well as draw information from them, that is why it provides a powerful REST API.

## 3.2 SPHINX KBR design

### 3.2.1 SPHINX KBR functional design

The following figure (Figure 3), depicts the KBR component UML diagram, describing the entities and their relationships in the SPHINX KBR system. Component diagrams are the most appropriate way to model implementation details and ensure that every aspect of the system's required function is covered.

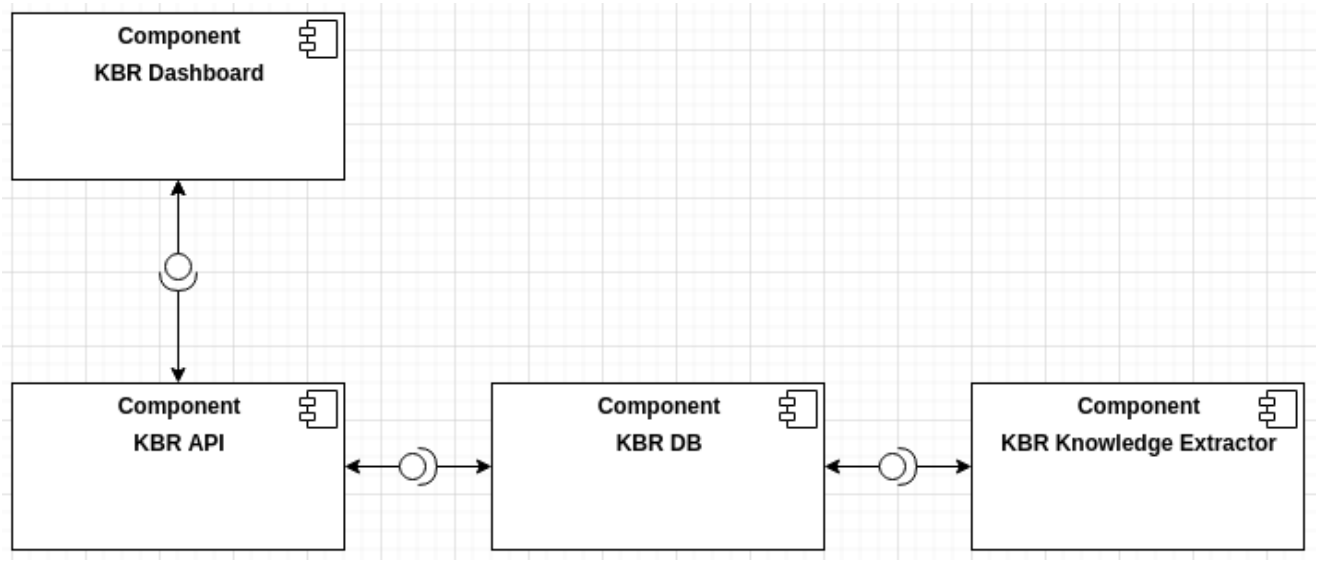


***Figure 3 SPHINX KBR Component diagram***

As can be seen from Figure 3, KBR consists of the following components:

- KBR DB
- KBR API
- KBR Knowledge Extractor
- KBR Dashboard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table 1 presents in a more detailed way the above-mentioned KBR Components

| KBR - Component | Description |
|---|---|
| **KBR Dashboard** | KBR Dashboard is a dashboard allowing users to search for existing knowledge or ad a new piece of knowledge. It contains user authentication and management |
| **KBR API** | KBR Api is used for retrieving pieces of knowledge created by users of the KBR Dashboard and pieces of knowledge generated by other SPHINX components |
| **KBR Knowledge extractor** | This component is responsible for extracting knowledge about security threats from external threat repositories |
| **KBR DB** | KBR DB is used to store information about attacks, data gathered from external threat repositories and other SPHINX components |

***Table 1 Component Description***

### 3.2.2 SPHINX KBR knowledge representation model

SPHINX KBR uses the CAPEC format to exchange threat information. CAPEC is a format that extends the STIX specification, that is used for exchanging cyber threat information between components. Below you will find some of the fields contained in the CAPEC schema[1]:

- ExecutionFlowType – A detailed step by step by step flow of an attack pattern
- ExternalReferenceType - A collection of elements that provide a pointer to where more information and deeper insight can be obtained
- PrerequisitesType - The PrerequisitesType complex type indicates one or more prerequisites for an attack and is used to provide a description of the conditions that must exist in order for an attack of this type to succeed.
- SeverityEnumeration - The SeverityEnumeration simple type contains a list of values corresponding to different severities

## 3.3 SPHINX KBR implementation and communication interfaces

#### *3.3.1.1 KBR backend*

SPHINX KBR uses NodeJS for the KBR Dashboard and API. The KBR Knowledge extractor is implemented in Golang. SPHINX KBR uses MongoDB as its database for storing articles and knowledge generated by SPHINX components. MongoDB is used as the selected database for the SPHINX KBR for the following reasons:

- MongoDB is ideal for storing raw data that their schema may change
- It uses JavaScript as query language
- It is Open Source
- It has support for TTL keys

[1] https://capec.mitre.org/documents/schema/index.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

### 3.3.1.2 KBR Dashboard

SPHINX KBR provides users with a responsive dashboard. Using dashboard, users are able to see articles created by other users or other SPHINX components and can also create their own articles. SPHINX KBR uses a set of predefined roles to provide accountability for any performed action. In Figure 4 the main screen of the dashboard is presented, after a user has logged in.

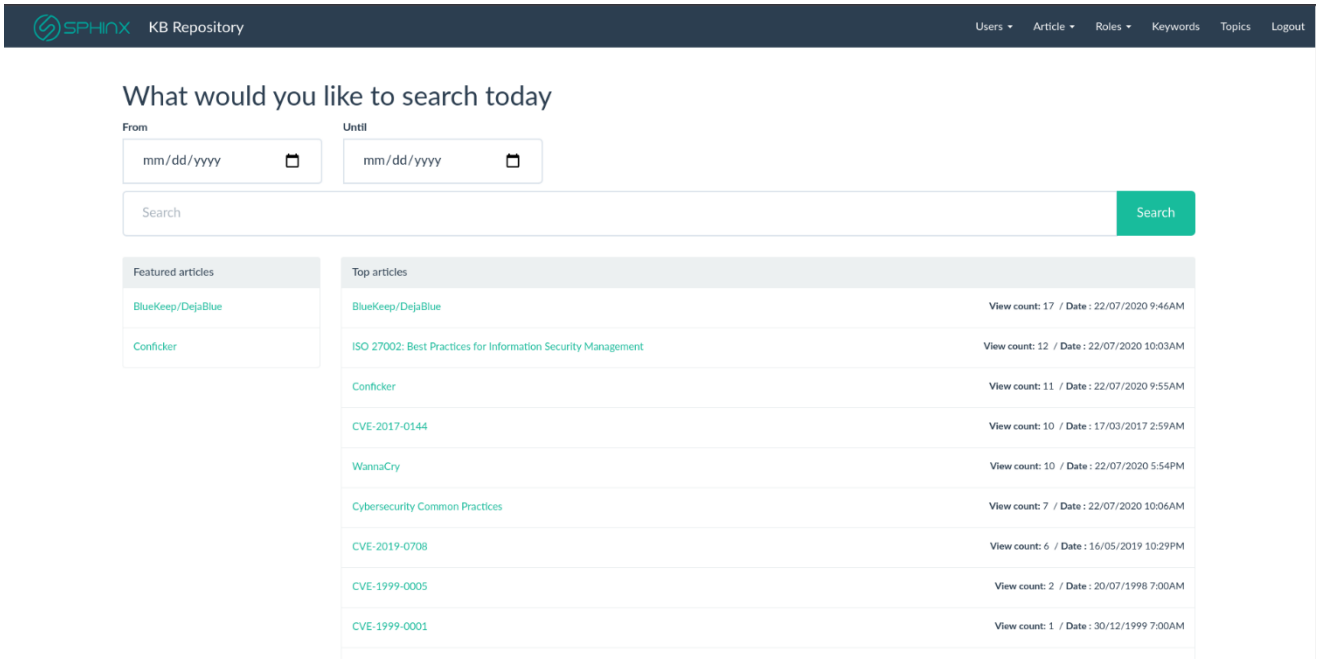


***Figure 4 SPHINX KBR Dashboard main screen***

In this screen the user can see a list of Top articles at the center of the screen and also a list of featured articles on the sidebar on the left. He/she can also use the search bar to search for articles based on title, keywords and a date range.

Figure 5 presents what a user sees when clicking on an article.

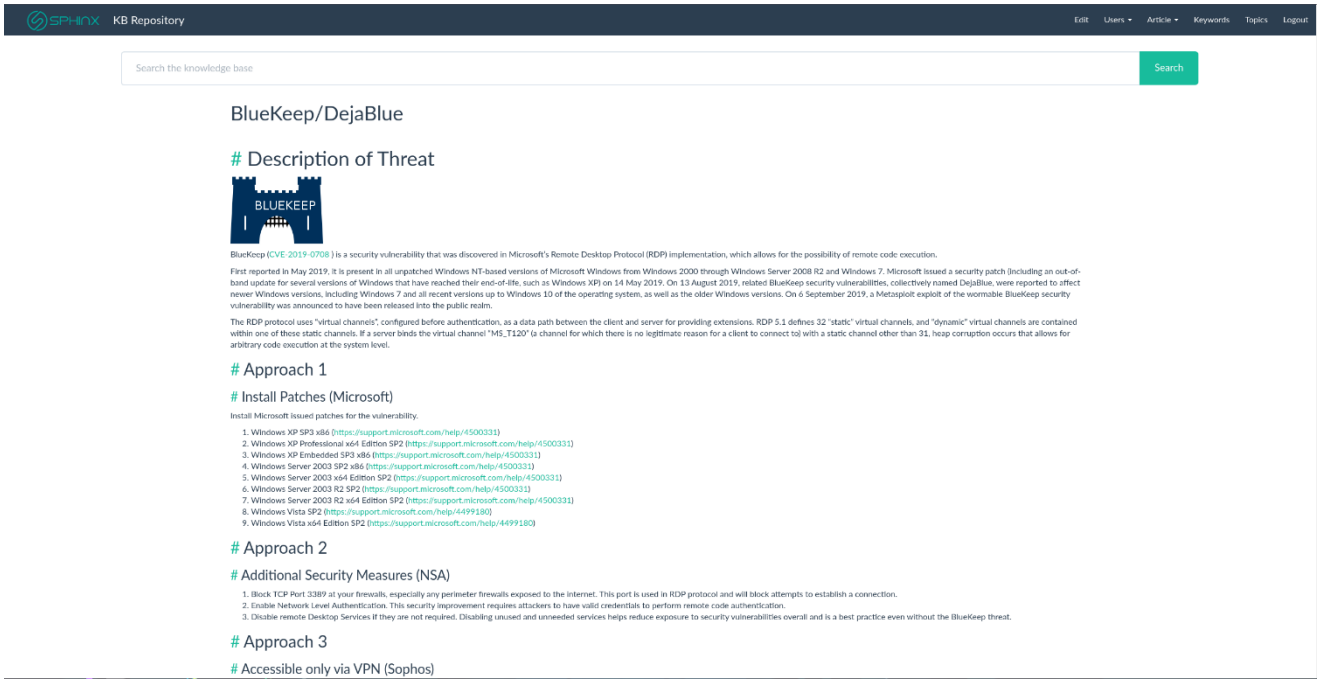


***Figure 5 Article View***

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

KBR Dashboards provides users with Topics. A topic is a collection of articles with a common theme. Here is the Topics view:

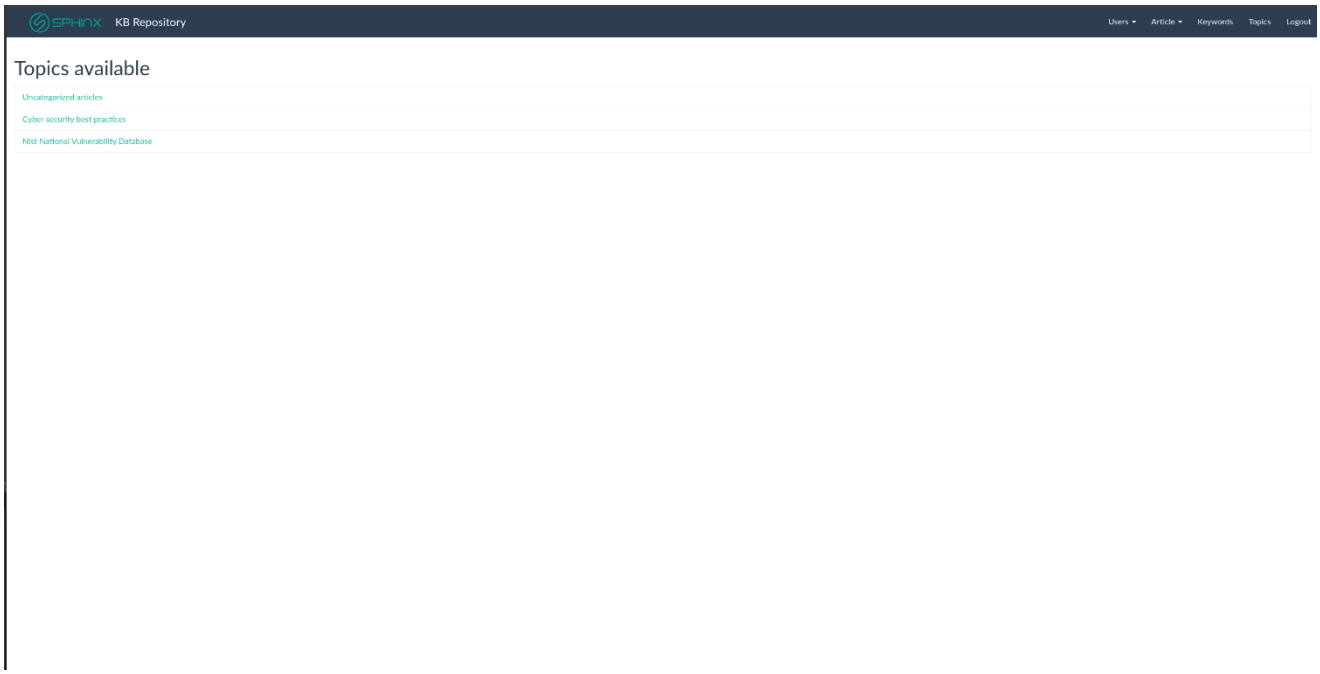


***Figure 6 Available topics***

Users can also create articles. Articles can be written with the help of a WYSIWYG editor that accepts plain text as well as markdown. They can also assign the article to a specific topic and set a password to limit access to specific users. After a user creates an article, it is automatically put in a queue to be reviewed and approved by users with the appropriate access. Once this article is approved it will be visible to all other users

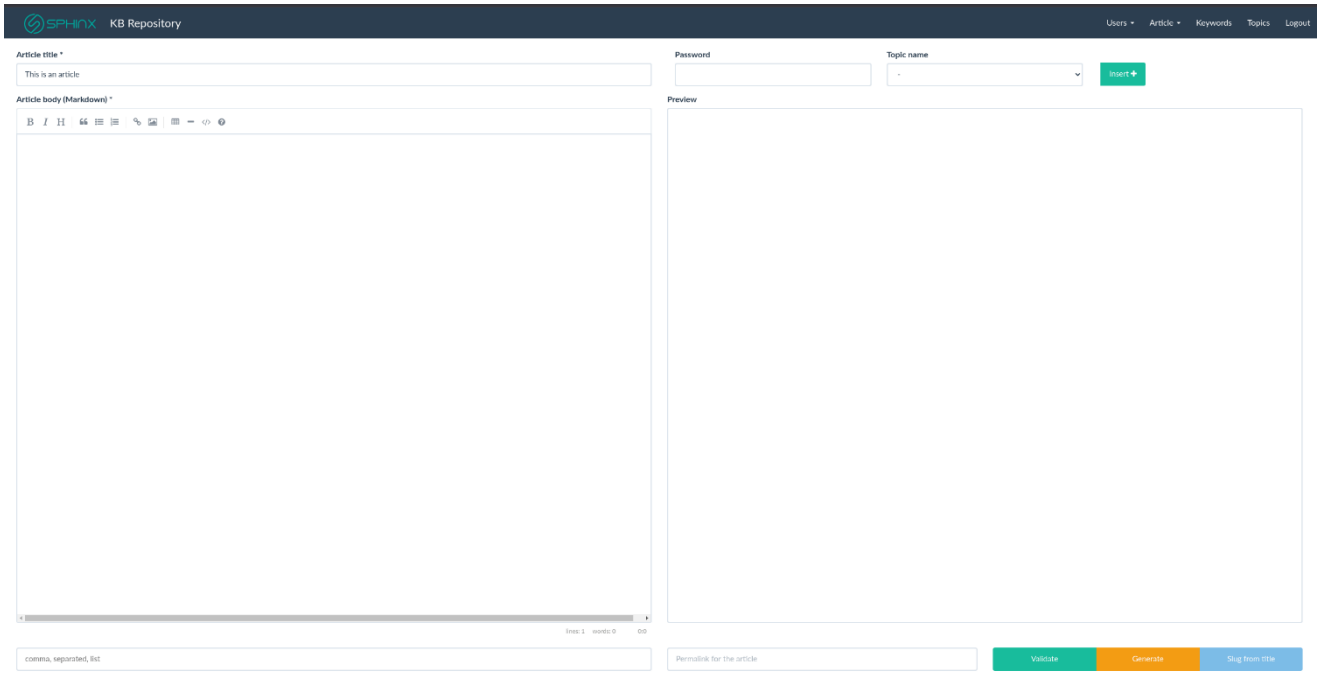


***Figure 7 Article creation area***

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

In the last picture we can see the articles that are pending for approval. This section is accessible to admin users. In this page admins can preview these articles and approve or reject these articles.

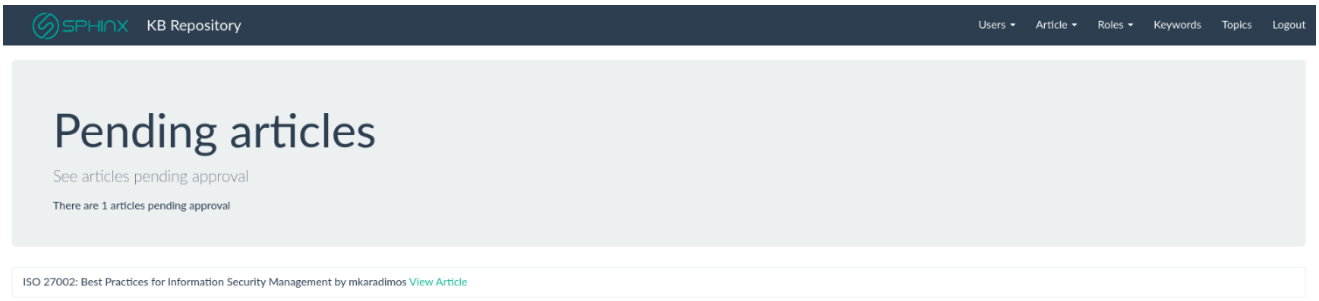


***Figure 8 Pending Articles***

#### *3.3.1.3 KBR API*

SPHINX KBR exposes a REST API allowing other SPHINX components to consume generated knowledge from articles created by KBR Dashboard users or other components. The list of the available API endpoints includes:

**Login**

By using this endpoint, users of the KBR dashboard can get authorized and get access to the KBR API.

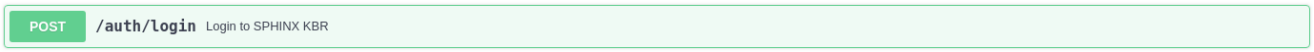


***Figure 9 Login to SPHINX KBR system***

**Register**

Admin users can use this endpoint to create a new user for the KBR dashboard. The new users can access the KBR dashboard and the functionalities provided with it.

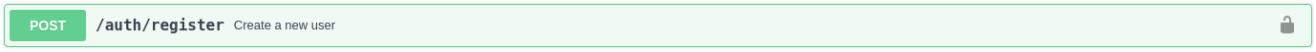


***Figure 10 Retrieve list of extracted keywords from articles***

**Keywords**

This endpoint provides the user with a list of keywords extracted from articles, available through the KBR dashboard.

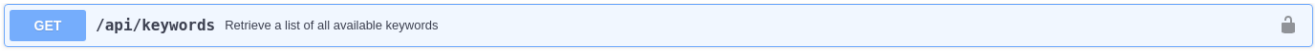


***Figure 11 Retrieve a list of keywords extracted from all articles***

**Get article**

In order to retrieve an article, you need to provide its kb_id and a password (if one is set) in the request body.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

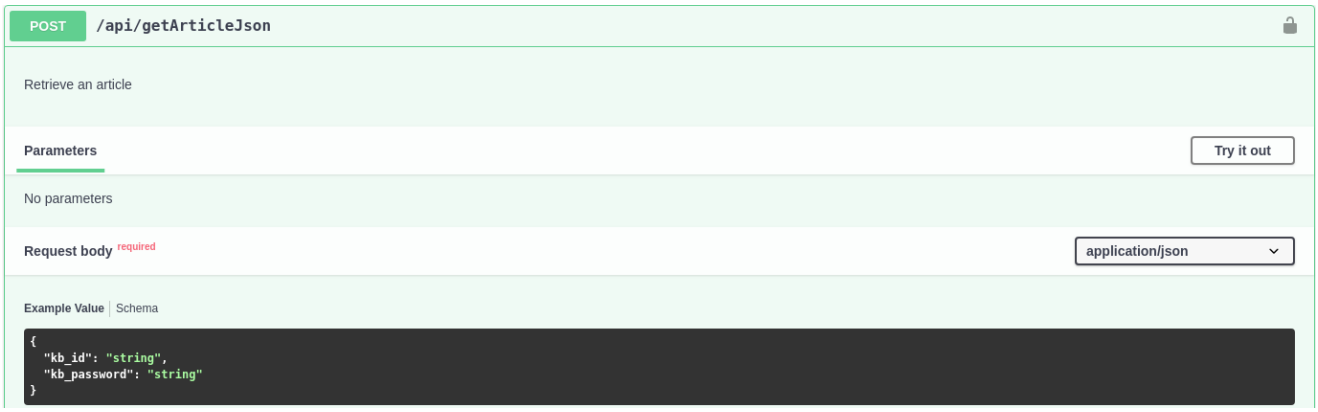


***Figure 12 Retrieve a specific article***

## Get articles

This endpoint allows users to retrieve articles that are saved in the KBR system. These articles have been created either by KBR users or by other SPHINX components.

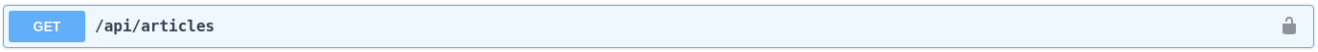


***Figure 13 Retrieve a list of available KBR articles***

## Create article

Creates a new article with a given title and body. Fields of request body marked with an asterisk are mandatory.

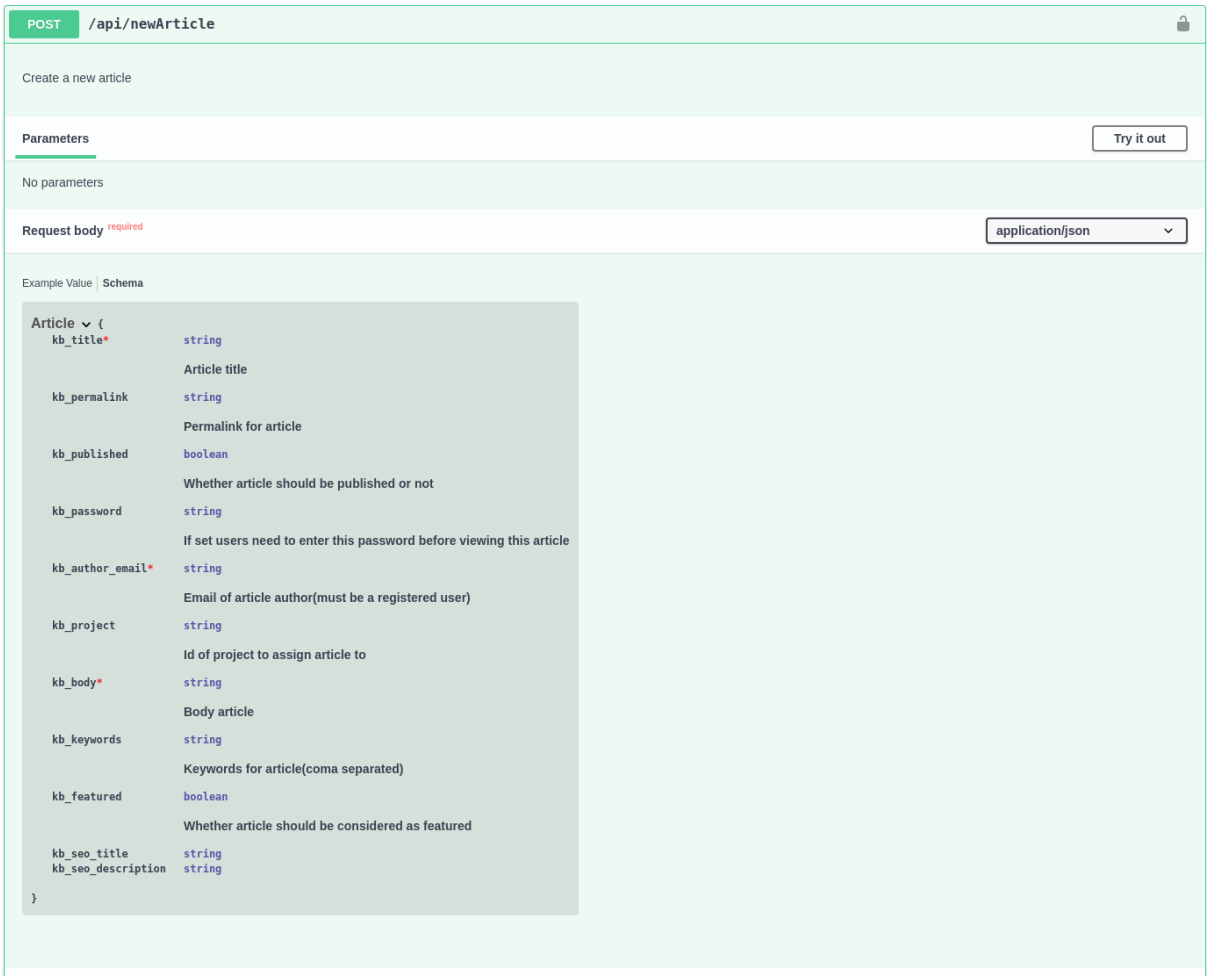


***Figure 14 Create a new Article***

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

### Delete article

This endpoint allows for the deletion of a specific article. In order for someone to delete an article they must be either the article creator or an admin.


*Figure 15 Delete an article by its id*

### Approve article

Approves an article by its id. User performing approval must have the appropriate rights.

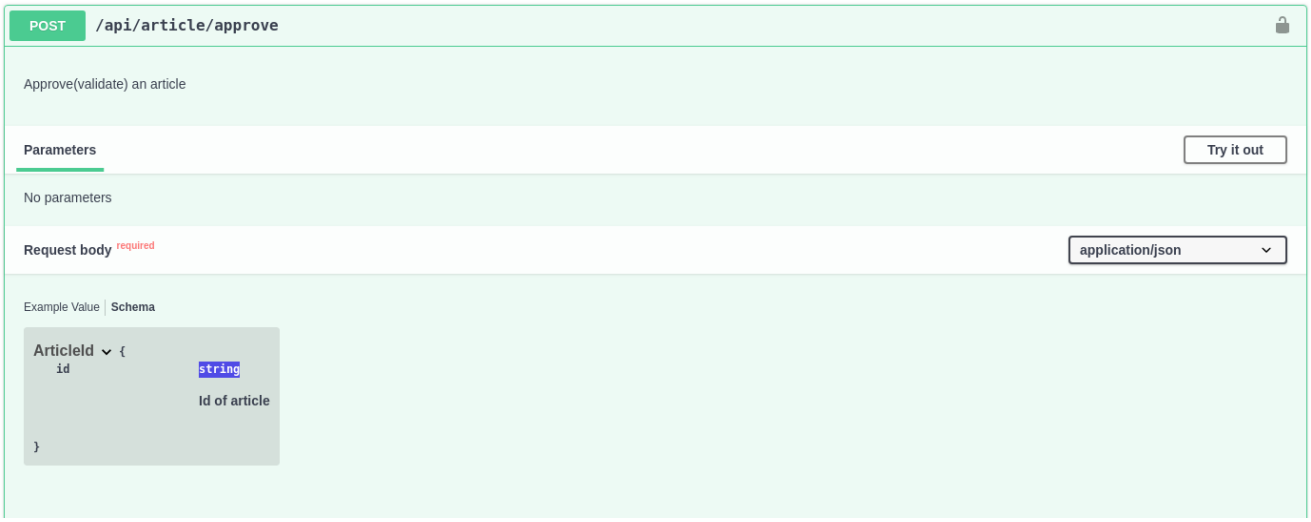


*Figure 16 Approve specific article*

### Reject article

Reject a pending article. Rejecting an article results in its deletions from SPHINX KBR. Only users with appropriate rights can reject an article

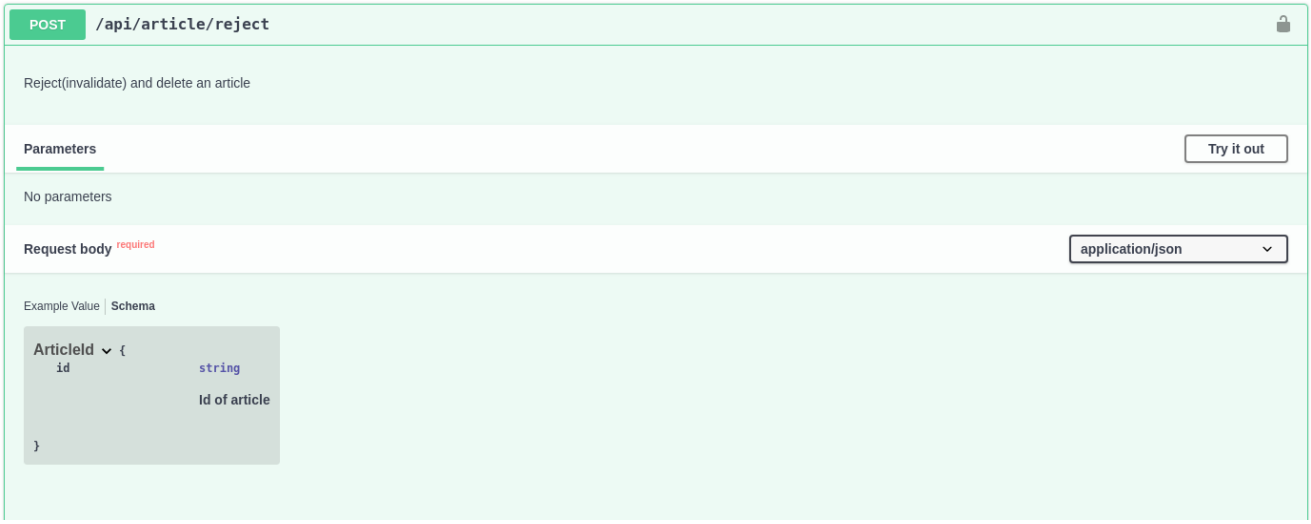


*Figure 17 Reject and delete article*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

#### 3.3.1.4 SPHINX KBR integration with external threat intelligence repositories

SPHINX KBR uses the KBR Knowledge extractor to retrieve information component to retrieve information from external threat intelligence repositories. It retrieves information from the following repositories:

- NIST
- MITRE

NIST is the National Institute of Standards and Technology. KBR Knowledge extractor retrieves a full list of CVEs. It also monitors the NIST database and updates its local repository when necessary.

KBR Knowledge extractor uses MITRE to retrieve the latest attack patterns provided. An attack pattern is a description of the common attributes and approaches employed by adversaries to exploit known software and hardware weaknesses [6].

For the next iteration phase (D5.10) we are planning on creating an additional and internal API for the SPHINX KBR so that other SPHINX Components will be able to share Treat Intelligence Information directly with the SPHINX KBR. By using the '/attack-patterns/create' a SPHINX Component will be able to create an Attack Pattern with the KBR and by using the '/attack-patterns/retrieve' a SPHINX Component will be able to retrieve the list of all the Attack Patterns stored in the SPHINX KBR. All the information send and received by the SPHINX KBR will follow the CAPEC Model [7] that uses the STIX protocol [5].


***Figure 18 Attack Pattern Creation by SPHINX Components***

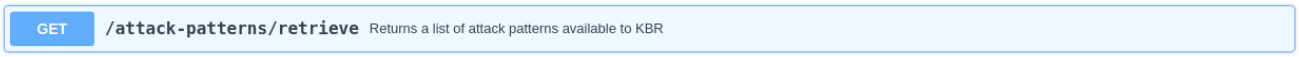


***Figure 19 Attack Pattern Retrieval by SPHINX Components***

In the following figure we can see an example of the response return from the API above

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
[
    {
        "type": "bundle",
        "id": "bundle--1341a9cf-5d7d-4df5-a055-8e14698c8d06",
        "spec_version": "2.0",
        "flag": "",
        "objects": [
            {
                "external_references": [
                    {
                        "source_name": "capec",
                        "url": "https://capec.mitre.org/data/definitions/87.html",
                        "external_id": "CAPEC-87",
                        "description": ""
                    },
                    {
                        "source_name": "cwe",
                        "url": "http://cwe.mitre.org/data/definitions/425.html",
                        "external_id": "CWE-425",
                        "description": ""
                    },
                    {
                        "source_name": "cwe",
                        "url": "http://cwe.mitre.org/data/definitions/285.html",
                        "external_id": "CWE-285",
                        "description": ""
                    },
                    {
                        "source_name": "cwe",
                        "url": "http://cwe.mitre.org/data/definitions/693.html",
                        "external_id": "CWE-693",
                        "description": ""
                    }
                ],
                "type": "attack-pattern",
                "id": "attack-pattern--00268a75-3243-477d-9166-8c78fddf6df6",
                "created": "2014-06-23T00:00:00.000Z",
                "created_by_ref": "identity--e50ab59c-5c4f-4d40-bf6a-d58418d89bcd",
                "modified": "2020-07-30T00:00:00.000Z",
                "name": "Forceful Browsing",
                "description": "An attacker employs forceful browsing to access portions of a website that are otherwise unreachable through direct URL entry. Usually, a front controller or similar design pattern is employed to protect access to portions of a web application. Forceful browsing enables an attacker to access information, perform privileged operations and otherwise reach sections of the web application that have been improperly protected.",
                "object_marking_refs": [
                    "marking-definition--17d82bb2-eeeb-4898-bda5-3ddbcd2b799d"
                ],
                "x_capec_abstraction": "Standard",
                "x_capec_prerequisites": [
                    "The forcibly browseable pages or accessible resources must be discoverable and improperly protected."
                ],
                "x_capec_resources_required": [
                    "None: No specialized resources are required to execute this type of attack. A directory listing is helpful, but not a requirement."
                ],
                "x_capec_status": "Draft",
                "x_capec_typical_severity": "High",
                "x_capec_version": "3.3",
                "x_capec_consequences": {
                    "Access_Control": [
                        "Bypass Protection Mechanism"
                    ],
                    "Accountability": null,
                    "Authentication": null,
                    "Authorization": null,
                    "Availability": null,
                    "Confidentiality": [
                        "Read Data",
                        "Bypass Protection Mechanism"
                    ],
                    "Integrity": null,
                    "Non_Repudiation": null,
                    "default": null
                },
                "x_capec_likelihood_of_attack": "High",
                "x_capec_execution_flow": "<h2> Execution Flow </h2><div><h3>Explore</h3><ol><li> <p> <b>Spider: </b>Using an automated tool, an attacker follows all public links on a web site. They record all the links they find.</p></li><table><tbody><tr><th>Techniques</th></tr><tr><td>Use a spidering tool to follow and record all links.</td></tr><tr><td>Use a proxy tool to record all links visited during a manual traversal of the web application.</td></tr></tbody></table></ol></div><div><h3>Experiment</h3><ol><li> <p> <b>Attempt well-known or guessable resource locations: </b>Using an automated tool, an attacker requests a variety of well-known URLs that correspond to administrative, debugging, or other useful internal actions. They record all the positive responses from the server.</p></li><table><tbody><tr><th>Techniques</th></tr><tr><td>Use a spidering tool to follow and record attempts on well-known URLs.</td></tr><tr><td>Use a proxy tool to record all links visited during a manual traversal of attempts on well-known URLs.</td></tr></tbody></table></ol></",
                "x_capec_example_instances": [
                    "\n                <xhtml:p>A bulletin board application provides an administrative interface at admin.aspx when the user logging in belongs to the administrators group.</xhtml:p>\n                <xhtml:p>An attacker can access the admin.aspx interface by making a direct request to the page. Not having access to the interface appropriately protected allows the attacker to perform administrative functions without having to authenticate themself in that role.</xhtml:p>\n            "
                ],
                "x_capec_skills_required": {
                    "Low": "Forcibly browseable pages can be discovered by using a number of automated tools. Doing the same manually is tedious but by no means difficult.",
                    "medium": "",
                    "High": ""
                }
            }
        ]
    }
]
```


***Figure 20 Example array of attack patterns returned***

The last 2 figures show an example POST body required for creating a new attack pattern and the response for successful attack pattern creation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
{
    "type": "bundle",
    "id": "bundle--0ecd8123-90d5-46e0-9cd4-65d4999b3a2e",
    "objects": [
        {
            "type": "attack-pattern",
            "spec_version": "2.1",
            "id": "attack-pattern--8ac90ff3-ecf8-4835-95b8-6aea6a623df5",
            "created": "2015-05-07T14:22:14.760Z",
            "modified": "2015-05-07T14:22:14.760Z",
            "name": "Phishing",
            "description": "Spear phishing used as a delivery mechanism for malware.",
            "kill_chain_phases": [
                {
                    "kill_chain_name": "mandiant-attack-lifecycle-model",
                    "phase_name": "initial-compromise"
                }
            ],
            "external_references": [
                {
                    "source_name": "capec",
                    "description": "phishing",
                    "url": "https://capec.mitre.org/data/definitions/98.html",
                    "external_id": "CAPEC-98"
                }
            ]
        }
    ]
}
```


***Figure 21 Attack pattern create body***


```
{
    "status": 200,
    "message": "attack pattern created"
}
```


***Figure 22 Attack pattern create response***

The schema of the internal API can be found in the Annex section (Annex III: , page 30)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# 4 Common Cyber Security Toolkit – CCST

The SPHINX cybersecurity toolkit is a rather wide constellation of digital interconnected, or standalone services that provide functionalities concerning the preservation and overall reinforcement of systems' security. Nonetheless, not all digital solutions are relevant to all organizations/institutes. Thus, one cannot predetermine which services, out of the rich collection within SPHINX's arsenal, should be pre-installed. Following this notion, a tool that will allow relevant stakeholders to selectively deploy any service that fits their use case and system requirements is required.

## 4.1 CCST Description

The Common Cyber Security Toolbox, as referred in the DoA, is a web portal through which relevant users can browse, list and select a digital solution that meets their requirements, and deploy it on their SPHINX deployment platform. Each digital solution can either be a standalone service, or a group of services that interactively provide a unified functionality (e.g. firewall, SIEM, Vulnerability Assessment, etc.). As one might understand, these services might require some initial configuration settings. Thus, the CCST module allows users to preconfigure those services, prior to deployment. Afterwards, users can deploy the selected services on the SPHINX platform. Consequently, they can monitor and control the services' lifecycle (start/stop/delete) through the CCST's dashboard. Moreover, users can place requests for services with specific characteristics/functionalities/requirements, and CCST can either propose any of the available services that match those characteristics or inform the relevant stakeholders of those requests.

## 4.2 Relevance to Other Components

The CCST component is closely related to WP2 and more specifically to tasks T2.2 (Basis of Legal and Ethical Requirements), T2.3 (Stakeholders' Requirements) and T2.5 (SPHINX Architecture and Detailed Technical Specifications). Moreover, the component has an inevitable relation to WP6, and more specifically tasks T6.1, T6.2, T6.4 and T6.5. This is a result of the direct interfacing of the component with components deriving from WP6, such as Service Manager (SM) and Continuous Integration Platform (CIT). Additionally, the CCST component is envisioned to interface with the Knowledgebase (current task – Wp5:T5.5), along with the Third-Party API component (WP3:T3.6).

## 4.3 CCST design

Following the modern approach for software development, for the design and development of the CCST component we have followed the Software Development Life Cycle (SDLC) principles, as presented in D6.1. The CCST component is a standalone service that offers a web-based dashboard for users to perform specific functionalities. The Angular2 web development framework and the Model-View-Controller (MVC) approach were utilized for the development of this web application.

### 4.3.1 Requirements' Fulfilment

The CCST component, as described in D2.6, has 5 distinct initial functional requirements (CST-F-010, CST-F-020, CST-F-030, CST-F-040, CST-F-050). Through these requirements, several stakeholder requirements are also fulfilled. Table 2 illustrates the stakeholders' requirements fulfilment in conjunction with the component's functional requirements.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

*Table 2 CCST stakeholder requirements*

| | | |
|---|---|---|
| **CST-F-010** | **STA-F-090**<br>**STA-U-040** | **Cyber security toolkit**<br>**Manage cybersecurity from a single location** |
| **CST-F-020** | STA-F-090<br>STA-U-040 | Cyber security toolkit<br>Manage cybersecurity from a single location |
| **CST-F-030** | STA-F-090<br>STA-U-040 | Cyber security toolkit<br>Manage cybersecurity from a single location |
| **CST-F-040** | STA-F-090<br>STA-U-040 | Cyber security toolkit<br>Manage cybersecurity from a single location |
| **CST-F-050** | STA-F-090<br>STA-U-040 | Cyber security toolkit<br>Manage cybersecurity from a single location |

### 4.3.2 Technical Details

The CCST component was developed utilizing the Angular2 web development framework, which is a client-side implementation. The abstract component diagram in Figure 23, presents the component's interfaces with other SPHINX components, illustrating the formal interface notations, as described in D2.6.

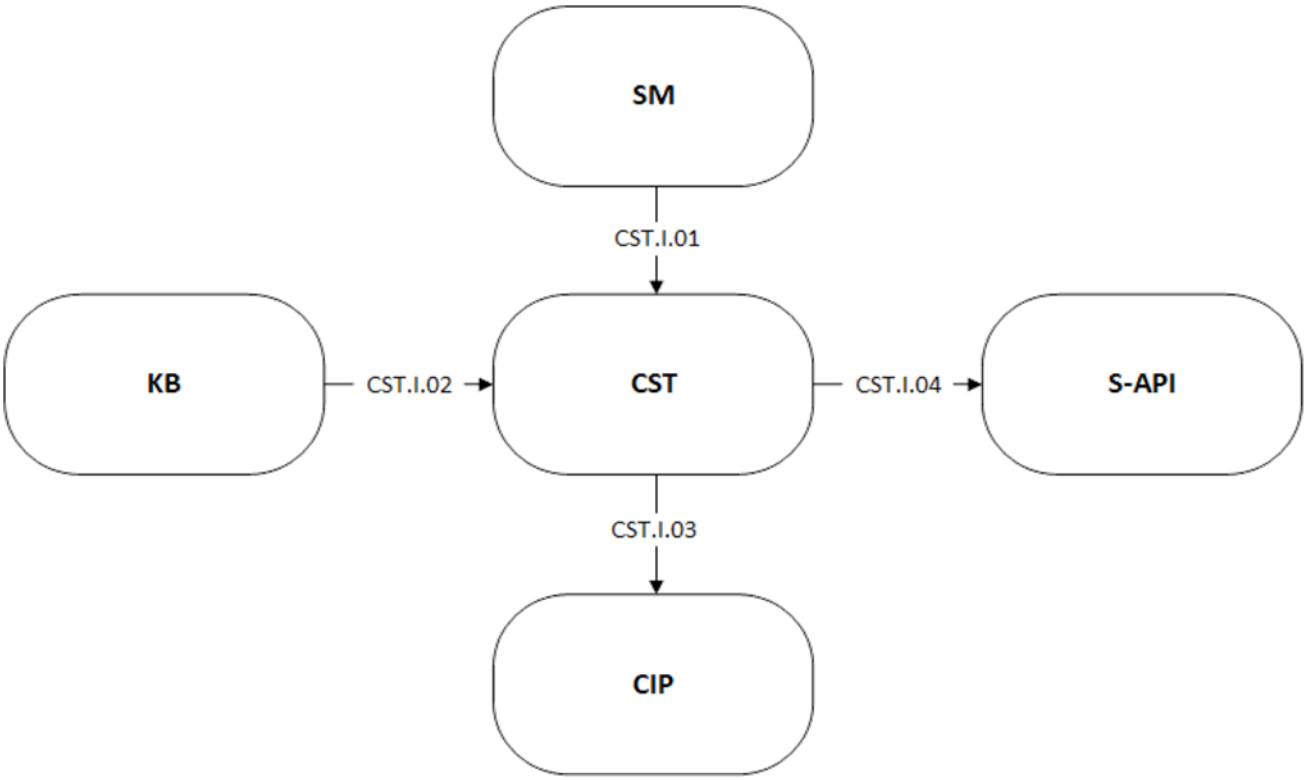


*Figure 23 CCST component diagram*

## 4.4 CCST Implementation

Due to the component's high dependence on several SPHINX components, such as Service Manager, Common Integration Platform, etc., the integration of which is rather delicate and must follow certain pre-defined rules, such as data models, communication channels, etc., some of the functionalities have not yet been developed. Currently, the user interface has been developed, and the interaction with the Service Manager and the Kafka messaging service has been integrated. The following image (Figure 23) presents the look and feel of the CCST

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

component. All the envisioned functionalities will be implemented as all relevant SPHINX components increase in maturity and will be reported in the final deliverable D5.10 - Cyber security knowledge base v2.

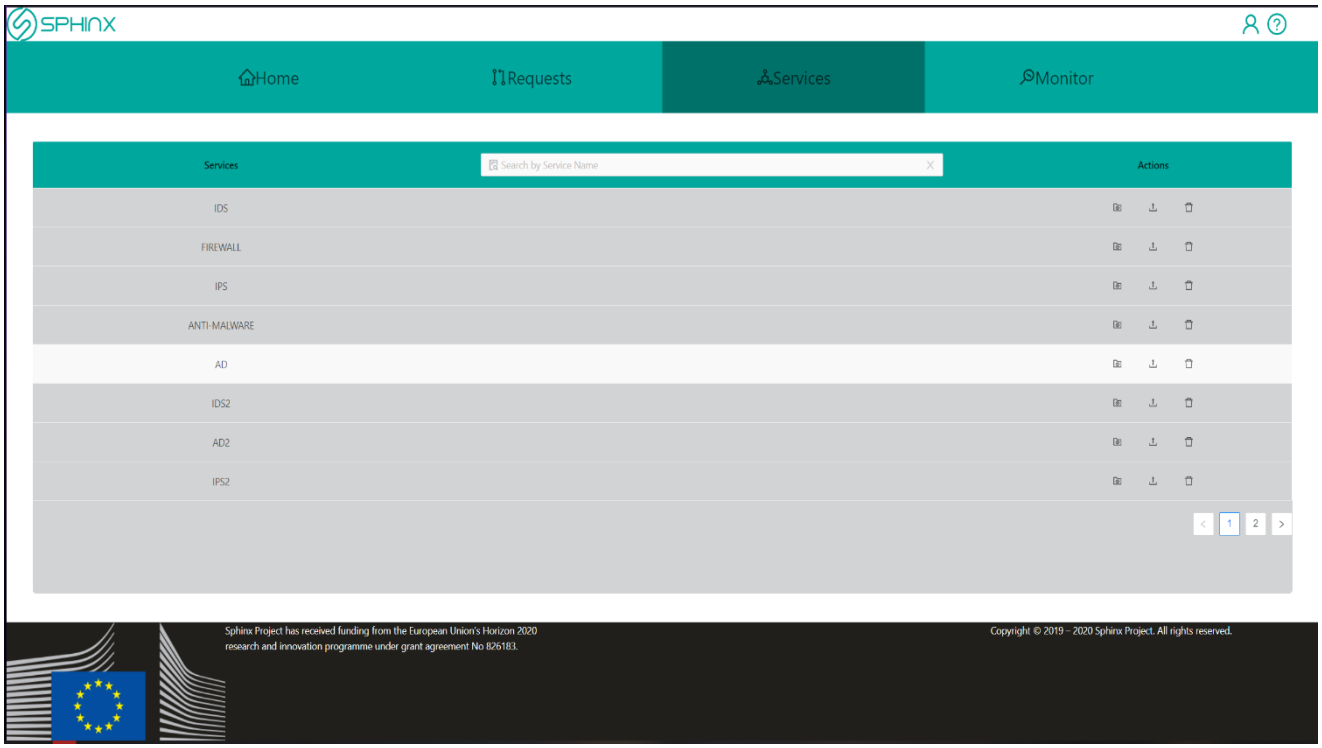


***Figure 24 CCST web interface***

# 5 Performance Evaluation

## 5.1 Evaluation methodology

In order to perform a more complete and thorough evaluation of the KBR API, the JMeter tool [8], depicted in Figure 25, was used.

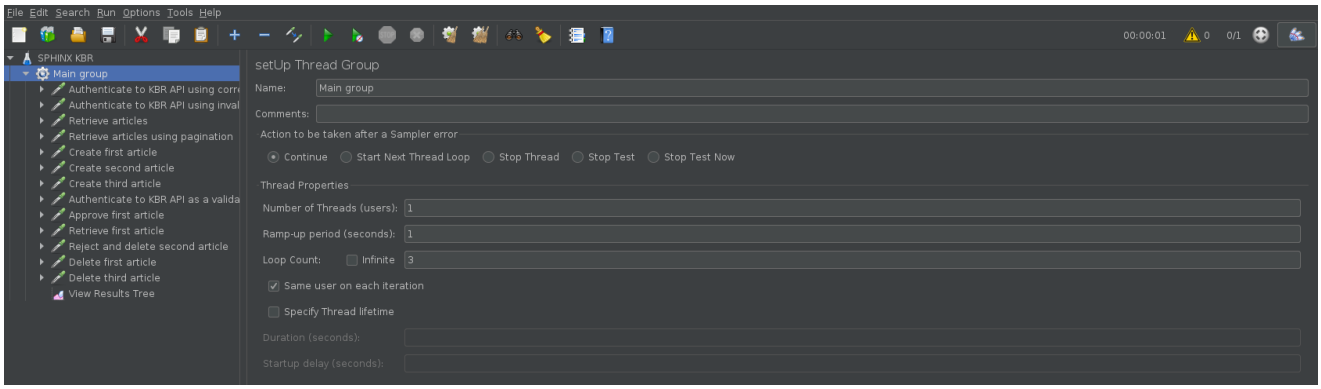


***Figure 25 Apache JMeter Main screen***

The Apache JMeter™ is an open source, 100% pure Java software application that offers an easy way to validate the implemented API in terms of availability, output validity (response conforming to the applications interfaces out-put specifications) and input invalidity (request data not conforming to the interface input specifications) [8]. To this end, we defined, for each HTTP API endpoint contained in Table 3, several test requests emulating the HTTP requests to the KBR API. As an example, Figure 26, demonstrates a request to the endpoint for retrieving available articles , while Figure 27 depicts the assertion received for this request indicating with a code 200 the success of the operation. It is noted that the endpoints were tested for both valid and invalid (erroneous) input.


***Figure 26 Retrieving articles***

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

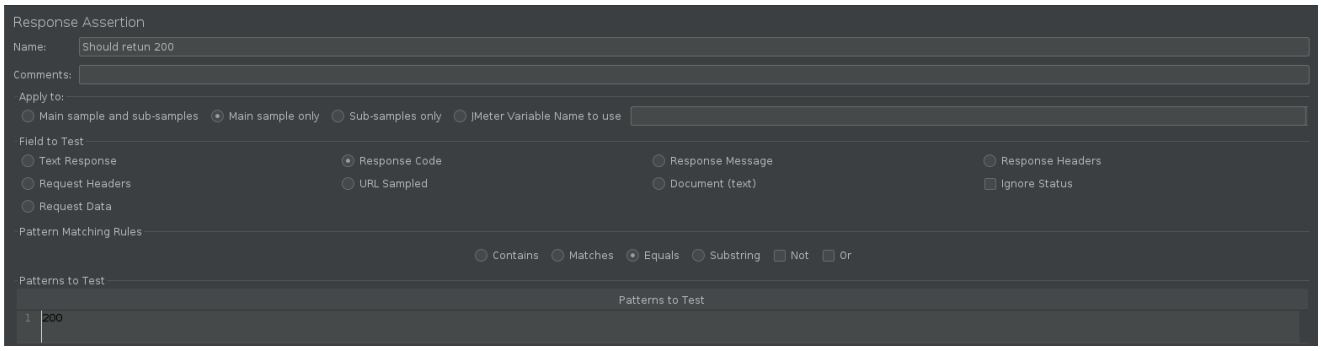


***Figure 27 Apache JMeter assertion response***

| SN | Test Label | API Endpoint URL |
|---|---|---|
| **1** | Authenticate to KBR API using correct credentials | http://localhost:4444/auth/login |
| **2** | Authenticate to KBR API using invalid credentials | http://localhost:4444/auth/login |
| **3** | Retrieve articles | http://localhost:4444/api/articles |
| **4** | Retrieve articles using pagination | http://localhost:4444/api/articles?limit=900&startIndex=80 |
| **5** | Create first article | http://localhost:4444/api/newArticle |
| **6** | Create second article | http://localhost:4444/api/newArticle |
| **7** | Create third article | http://localhost:4444/api/newArticle |
| **8** | Authenticate to KBR API as a validator | http://localhost:4444/auth/login |
| **9** | Approve first article | http://localhost:4444/api/article/approve |
| **10** | Retrieve first article | http://localhost:4444/api/getArticleJson |
| **11** | Reject and delete second article | http://localhost:4444/api/article/reject |
| **12** | Delete first article | http://localhost:4444/api/article/5f839f650a6b567b0871e2a9 |
| **13** | Delete third article | http://localhost:4444/api/article/5f839f650a6b567b0871e2ab |

***Table 3 Tested API endpoints for the SPHINX KBR API***

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

## 5.1 Evaluation Results

The JMeter tool does not only enable us to validate the functional behaviour of each API endpoint individually, but also it allows us to perform stress tests on our system; for example our test scenarios aim to prove the system's reliability in case of repeated "Retrieve articles" requests, "Authenticate to KBR" requests,, etc. In addition, the overall performance of this system can be evaluated through this tool by measuring the response time to any HTTP request made. Table 3 presents the results for each tested endpoint. The received HTTP response codes verified the availability of the tested API endpoints whereas the HTTP Assertion success column indicates the tested API endpoints conformance to their specifications. Finally, the Latency column demonstrates the capability of the system to handle fast the submitted requests (the majority of the responses were below 15msec). Note: the response codes mean: 200 indicates successful requests and 400 indicates that a request with the wrong format was performed. A complete list of the HTTP codes can be found in IANA's Hypertext Transfer Protocol (HTTP) Status Code Registry [9].

***Table 4 Assertion results for the tested SPHINX KBR API endpoints***

| SN | Test Label | Response Code | HTTP Assertion success | Latency (ms) |
|---|---|---|---|---|
| **1** | Authenticate to KBR API using correct credentials | 200 | TRUE | 80 |
| **2** | Authenticate to KBR API using invalid credentials | 401 | TRUE | 61 |
| **3** | Retrieve articles | 200 | TRUE | 5 |
| **4** | Retrieve articles using pagination | 200 | TRUE | 4 |
| **5** | Create first article | 200 | TRUE | 5 |
| **6** | Create second article | 200 | TRUE | 5 |
| **7** | Create third article | 200 | TRUE | 3 |
| **8** | Authenticate to KBR API as a validator | 200 | TRUE | 62 |
| **9** | Approve first article | 200 | TRUE | 7 |
| **10** | Retrieve first article | 200 | TRUE | 3 |
| **11** | Reject and delete second article | 200 | TRUE | 4 |
| **12** | Delete first article | 200 | TRUE | 9 |
| **13** | Delete third article | 200 | TRUE | 4 |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# 6 Conclusions

In the first iteration of this task, we have implemented the first version on the SPHINX Knowledge Base Repository and the SPHINX Common Cyber Security Toolbox. SPHINX Knowledge Base is an important tool in SPHINX's toolkit. The KBR itself is not a solution for ensuring security but a useful tool that augments other security solutions in order to have more information about an attack and help them work faster and more efficiently. More specifically, the KBR collects information from reputable repositories and other SPHINX Components and organizes them in order for this information to be used by another SPHINX Component and help them address the detected attack. Currently, the SPHINX KBR consist of four components, the KBR Dashboard, the KBR API, the KBR DB and the KBR Knowledge Extractor. All the information that is gathered by the KBR Knowledge is categorized and processed by the KBR in order to be saved by the KBR Database. The information can then be show and edited from the user-friendly KBR Dashboard. The KBR also supports HTTP (synchronous) communication via the REST API named KBR API. From the KBR API a user can retrieve the articles on the KBR DB. For the next iteration phase (D5.10) we plan on creating an additional API for the KBR that will allow other SPHINX Components to share threat intelligence information to and from the KBR in machine-readable form using the STIX Format. [4]

The SPHINX Common Cyber Security Toolbox is an easy to use and interactive web portal that can be used to deploy digital security solutions on their SPHINX Platform. From the CCST Portal, digital solutions can be preconfigured as per the need of the user and those solutions lifecycle can be managed with the CCST Dashboard by the user. Finally, users can use the SPHINX CCST in order to find the best digital security solution of their needs. For the next iteration phase (D5.10) we plan on the integration and the evaluation of all the relevant SPHINX APIs (SPHINX CIP, SPHINX SM…)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Annex I: **References**

[1] H. Scout, "Knowledge Base 101: Definition, Benefits, Examples, and Tips," [Online]. Available: https://www.helpscout.com/playlists/knowledge-base/.

[2] ATLASSIAN, "What is a knowledge base?," [Online]. Available: https://www.atlassian.com/itsm/knowledge-management/what-is-a-knowledge-base.

[3] ITeXchange, "CyberSecurity Knowledge Bases: The Brain of Security Systems," [Online]. Available: https://www.itexchangeweb.com/blog/cybersecurity-knowledge-bases-the-brain-of-security-systems/.

[4] ANOMALI, "What are STIX/TAXII," [Online]. Available: https://www.anomali.com/resources/what-are-stix-taxii).

[5] SEKOIA.io, "Introduction to STIX and TAXII," [Online]. Available: https://medium.com/sekoia-io-blog/stix-and-taxii-c1f596866384.

[6] MITRE, "CVE," [Online]. Available: https://cve.mitre.org/.

[7] CAPEC, "Common Attack Enumeration Protocol," [Online]. Available: https://capec.mitre.org/. [Accessed 20 10 2020].

[8] Apache, "Apache JMeterTM," [Online]. Available: https://jmeter.apache.org/.

[9] IANA, "IANA's Hypertext Transfer Protocol (HTTP) Status Code Registry," [Online]. Available: https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Annex II: KBR API swagger file

```
openapi: "3.0.0"
info:
  version: 1.0.0
  title: SPHINX KBR API
  license:
    name: MIT
servers:
  - url: http:/s/localhost:4444
    description: Localhost API server
paths:
  /auth/login:
    post:
      tags:
        - Authorization
      summary: Login to SPHINX KBR
      operationId: 'loginKB'

      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/Login'
      responses:
        '200':
          description: Correct credentials
          content:
            application/json:
              schema:
                type: object
                properties:
                  jwt:
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
            type: string
      '400':
        description: User with requested email does not exist
      '401':
        description: Invalid credentials
  /auth/register:
    post:
      security:
        - bearerAuth: []
      tags:
        - Authorization
      summary: Create a new user
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/User'
      responses:
        '200':
          description: User created
        '401':
          description: Unauthorized
  /api/keywords:
    get:
      security:
        - bearerAuth: []
      tags:
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Annex III: KBR Interconnection API with other SPHINX Components swagger file


```
{
 "type": "bundle",
 "id": "",
 "spec_version": "2.0",
 "objects": [
  {
   "type": "attack-pattern",
   "id": "",
   "created": "2014-06-23T00:00:00.000Z",
   "modified": "2020-07-30T00:00:00.000Z",
   "name": "",
   "description": "",
   "external_references": [
    {
     "source_name": "",
     "url": "",
     "external_id": "",
     "description": ""
    }
   ],
   "object_marking_refs": [
   ],
   "x_capec_abstraction": "",

   "x_capec_consequences": {
    "Access_Control": [
    ],
    "Accountability": [
    ],
    "Authentication": [
```

```
        ],
        "Authorization": [
        ],
        "Confidentiality": [
        ],
        "Integrity": [
        ],
        "Non-Repudiation": [
        ]
      },
      "x_capec_example_instances": [],
      "x_capec_execution_flow": "",
      "x_capec_likelihood_of_attack": "",
      "x_capec_prerequisites": [],
      "x_capec_resources_required": [],
      "x_capec_skills_required": {
        "High": "",
        "Medium": "",
        "Low": ""
      },

      "x_capec_status": "",
      "x_capec_typical_severity": "",
      "x_capec_version": "3.3"
    }
  ]
}
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

# Annex IV: **JMeter Configuration File**

```
<?xml version="1.0" encoding="UTF-8"?>
<jmeterTestPlan version="1.2" properties="5.0" jmeter="5.3">
 <hashTree>
  <TestPlan guiclass="TestPlanGui" testclass="TestPlan" testname="SPHINX KBR" enabled="true">
   <stringProp name="TestPlan.comments">Evaluation of KBR API</stringProp>
   <boolProp name="TestPlan.functional_mode">false</boolProp>
   <boolProp name="TestPlan.tearDown_on_shutdown">true</boolProp>
   <boolProp name="TestPlan.serialize_threadgroups">false</boolProp>
   <elementProp name="TestPlan.user_defined_variables" elementType="Arguments" guiclass="ArgumentsPanel" testclass="Arguments" testname="User Defined Variables" enabled="true">
    <collectionProp name="Arguments.arguments">
     <elementProp name="API" elementType="Argument">
      <stringProp name="Argument.name">API</stringProp>
      <stringProp name="Argument.value">localhost</stringProp>
      <stringProp name="Argument.metadata">=</stringProp>
     </elementProp>
     <elementProp name="APIPORT" elementType="Argument">
      <stringProp name="Argument.name">APIPORT</stringProp>
      <stringProp name="Argument.value">4444</stringProp>
      <stringProp name="Argument.metadata">=</stringProp>
     </elementProp>
    </collectionProp>
   </elementProp>
   <stringProp name="TestPlan.user_define_classpath"></stringProp>
  </TestPlan>
  <hashTree>
   <SetupThreadGroup guiclass="SetupThreadGroupGui" testclass="SetupThreadGroup" testname="Main group" enabled="true">
    <stringProp name="ThreadGroup.on_sample_error">continue</stringProp>
    <elementProp name="ThreadGroup.main_controller" elementType="LoopController" guiclass="LoopControlPanel" testclass="LoopController" testname="Loop Controller" enabled="true">
     <boolProp name="LoopController.continue_forever">false</boolProp>
     <stringProp name="LoopController.loops">1</stringProp>
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


```
      </elementProp>
      <stringProp name="ThreadGroup.num_threads">1</stringProp>
      <stringProp name="ThreadGroup.ramp_time">1</stringProp>
      <boolProp name="ThreadGroup.scheduler">false</boolProp>
      <stringProp name="ThreadGroup.duration"></stringProp>
      <stringProp name="ThreadGroup.delay"></stringProp>
      <boolProp name="ThreadGroup.same_user_on_next_iteration">true</boolProp>
    </SetupThreadGroup>
    <hashTree>
     <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Authenticate to KBR API using correct credentials" enabled="true">
       <boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
       <elementProp name="HTTPsampler.Arguments" elementType="Arguments">
        <collectionProp name="Arguments.arguments">
         <elementProp name="" elementType="HTTPArgument">
          <boolProp name="HTTPArgument.always_encode">false</boolProp>
          <stringProp name="Argument.value">{&#xd;
         &quot;email&quot;:&quot;sphinx@guest.com&quot;,&#xd;
         &quot;password&quot;:&quot;sphinx@guest.com&quot;&#xd;
}</stringProp>
          <stringProp name="Argument.metadata">=</stringProp>
         </elementProp>
        </collectionProp>
       </elementProp>
       <stringProp name="HTTPSampler.domain">${API}</stringProp>
       <stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
       <stringProp name="HTTPSampler.protocol">http</stringProp>
       <stringProp name="HTTPSampler.contentEncoding"></stringProp>
       <stringProp name="HTTPSampler.path">/auth/login</stringProp>
       <stringProp name="HTTPSampler.method">POST</stringProp>
       <boolProp name="HTTPSampler.follow_redirects">true</boolProp>
       <boolProp name="HTTPSampler.auto_redirects">false</boolProp>
       <boolProp name="HTTPSampler.use_keepalive">true</boolProp>
       <boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Response Assertion" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
</collectionProp>
</HeaderManager>
<hashTree/>
<JSONPostProcessor guiclass="JSONPostProcessorGui" testclass="JSONPostProcessor" testname="JSON Extractor" enabled="true">
<stringProp name="JSONPostProcessor.referenceNames">JWT</stringProp>
<stringProp name="JSONPostProcessor.jsonPathExprs">$.token</stringProp>
<stringProp name="JSONPostProcessor.match_numbers"></stringProp>
</JSONPostProcessor>
<hashTree/>
</hashTree>
```

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.*


```
<HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Authenticate to KBR API using invalid credentials" enabled="true">
<boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
<elementProp name="HTTPsampler.Arguments" elementType="Arguments">
<collectionProp name="Arguments.arguments">
<elementProp name="" elementType="HTTPArgument">
<boolProp name="HTTPArgument.always_encode">false</boolProp>
<stringProp name="Argument.value">{&#xd;
&quot;email&quot;:&quot;sphinx@guest.com&quot;,&#xd;
&quot;password&quot;:&quot;wrongemail@guest.com&quot;&#xd;
}</stringProp>
<stringProp name="Argument.metadata">=</stringProp>
</elementProp>
</collectionProp>
</elementProp>
<stringProp name="HTTPSampler.domain">${API}</stringProp>
<stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
<stringProp name="HTTPSampler.protocol">http</stringProp>
<stringProp name="HTTPSampler.contentEncoding"></stringProp>
<stringProp name="HTTPSampler.path">/auth/login</stringProp>
<stringProp name="HTTPSampler.method">POST</stringProp>
<boolProp name="HTTPSampler.follow_redirects">true</boolProp>
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Login should fail" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="51509">401</stringProp>
</collectionProp>
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

<stringProp name="Assertion.custom_message"></stringProp>

<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>

<boolProp name="Assertion.assume_success">false</boolProp>

<intProp name="Assertion.test_type">8</intProp>

</ResponseAssertion>

<hashTree/>

<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">

<collectionProp name="HeaderManager.headers">

<elementProp name="" elementType="Header">

<stringProp name="Header.name">Content-Type</stringProp>

<stringProp name="Header.value">application/json</stringProp>

</elementProp>

</collectionProp>

</HeaderManager>

<hashTree/>

</hashTree>

<HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Retrieve articles " enabled="true">

<elementProp name="HTTPsampler.Arguments" elementType="Arguments" guiclass="HTTPArgumentsPanel" testclass="Arguments" testname="User Defined Variables" enabled="true">

<collectionProp name="Arguments.arguments"/>

</elementProp>

<stringProp name="HTTPSampler.domain">${API}</stringProp>

<stringProp name="HTTPSampler.port">${APIPORT}</stringProp>

<stringProp name="HTTPSampler.protocol">http</stringProp>

<stringProp name="HTTPSampler.contentEncoding"></stringProp>

<stringProp name="HTTPSampler.path">/api/articles</stringProp>

<stringProp name="HTTPSampler.method">GET</stringProp>

<boolProp name="HTTPSampler.follow_redirects">true</boolProp>

<boolProp name="HTTPSampler.auto_redirects">false</boolProp>

<boolProp name="HTTPSampler.use_keepalive">true</boolProp>

<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>

<stringProp name="HTTPSampler.embedded_url_re"></stringProp>

<stringProp name="HTTPSampler.connect_timeout"></stringProp>

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
<stringProp name="Header.value">Bearer ${JWT}</stringProp>
</elementProp>
</collectionProp>
</HeaderManager>
<hashTree/>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should retun 200" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
</hashTree>
<HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Retrieve articles using pagination" enabled="true">
<elementProp name="HTTPsampler.Arguments" elementType="Arguments" guiclass="HTTPArgumentsPanel" testclass="Arguments" testname="User Defined Variables" enabled="true">
<collectionProp name="Arguments.arguments"/>
</elementProp>
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


```
<stringProp name="HTTPSampler.domain">${API}</stringProp>
<stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
<stringProp name="HTTPSampler.protocol">http</stringProp>
<stringProp name="HTTPSampler.contentEncoding"></stringProp>
<stringProp name="HTTPSampler.path">/api/articles?limit=900&amp;startIndex=80</stringProp>
<stringProp name="HTTPSampler.method">GET</stringProp>
<boolProp name="HTTPSampler.follow_redirects">true</boolProp>
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
<stringProp name="Header.value">Bearer ${JWT}</stringProp>
</elementProp>
</collectionProp>
</HeaderManager>
<hashTree/>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should retun 200" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


```
          <stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
          <boolProp name="Assertion.assume_success">false</boolProp>
          <intProp name="Assertion.test_type">8</intProp>
        </ResponseAssertion>
        <hashTree/>
      </hashTree>
      <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Create first article" enabled="true">
        <boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
        <elementProp name="HTTPsampler.Arguments" elementType="Arguments">
          <collectionProp name="Arguments.arguments">
            <elementProp name="" elementType="HTTPArgument">
              <boolProp name="HTTPArgument.always_encode">false</boolProp>
              <stringProp name="Argument.value">{&#xd;
 &quot;kb_title&quot;: &quot;Some awesome article&quot;,&#xd;
 &quot;kb_permalink&quot;: &quot;&quot;,&#xd;
 &quot;kb_published&quot;: true,&#xd;
 &quot;kb_password&quot;: &quot;&quot;,&#xd;
 &quot;kb_author_email&quot;: &quot;sphinx@guest.com&quot;,&#xd;
 &quot;kb_project&quot;: &quot;&quot;,&#xd;
 &quot;kb_body&quot;: &quot;Some body&quot;,&#xd;
 &quot;kb_keywords&quot;: &quot;keyword1&quot;,&#xd;
 &quot;kb_featured&quot;: false,&#xd;
 &quot;kb_seo_title&quot;: &quot;&quot;,&#xd;
 &quot;kb_seo_description&quot;: &quot;&quot;&#xd;
}</stringProp>
              <stringProp name="Argument.metadata">=</stringProp>
            </elementProp>
          </collectionProp>
        </elementProp>
        <stringProp name="HTTPSampler.domain">${API}</stringProp>
        <stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
        <stringProp name="HTTPSampler.protocol">http</stringProp>
        <stringProp name="HTTPSampler.contentEncoding"></stringProp>
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
<stringProp name="HTTPSampler.path">/api/newArticle</stringProp>
<stringProp name="HTTPSampler.method">POST</stringProp>
<boolProp name="HTTPSampler.follow_redirects">true</boolProp>
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return 200" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
<stringProp name="Header.value">Bearer ${JWT}</stringProp>
</elementProp>
</collectionProp>
</HeaderManager>
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


```
        <hashTree/>
        <JSONPostProcessor guiclass="JSONPostProcessorGui" testclass="JSONPostProcessor" testname="JSON Extractor" enabled="true">
          <stringProp name="JSONPostProcessor.referenceNames">FIRST_ARTICLE_ID</stringProp>
          <stringProp name="JSONPostProcessor.jsonPathExprs">$.message</stringProp>
          <stringProp name="JSONPostProcessor.match_numbers"></stringProp>
        </JSONPostProcessor>
        <hashTree/>
      </hashTree>
      <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Create second article" enabled="true">
        <boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
        <elementProp name="HTTPsampler.Arguments" elementType="Arguments">
          <collectionProp name="Arguments.arguments">
            <elementProp name="" elementType="HTTPArgument">
              <boolProp name="HTTPArgument.always_encode">false</boolProp>
              <stringProp name="Argument.value">{&#xd;
 &quot;kb_title&quot;: &quot;Some awesome article 2&quot;,&#xd;
 &quot;kb_permalink&quot;: &quot;&quot;,&#xd;
 &quot;kb_published&quot;: true,&#xd;
 &quot;kb_password&quot;: &quot;&quot;,&#xd;
 &quot;kb_author_email&quot;: &quot;sphinx@guest.com&quot;,&#xd;
 &quot;kb_project&quot;: &quot;&quot;,&#xd;
 &quot;kb_body&quot;: &quot;Some body&quot;,&#xd;
 &quot;kb_keywords&quot;: &quot;keyword1&quot;,&#xd;
 &quot;kb_featured&quot;: false,&#xd;
 &quot;kb_seo_title&quot;: &quot;&quot;,&#xd;
 &quot;kb_seo_description&quot;: &quot;&quot;&#xd;
}</stringProp>
              <stringProp name="Argument.metadata">=</stringProp>
            </elementProp>
          </collectionProp>
        </elementProp>
        <stringProp name="HTTPSampler.domain">${API}</stringProp>
        <stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
```


```
<stringProp name="HTTPSampler.protocol">http</stringProp>
<stringProp name="HTTPSampler.contentEncoding"></stringProp>
<stringProp name="HTTPSampler.path">/api/newArticle</stringProp>
<stringProp name="HTTPSampler.method">POST</stringProp>
<boolProp name="HTTPSampler.follow_redirects">true</boolProp>
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return 200" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
<stringProp name="Header.value">Bearer ${JWT}</stringProp>
</elementProp>
```


```
        </collectionProp>
       </HeaderManager>
       <hashTree/>
       <JSONPostProcessor guiclass="JSONPostProcessorGui" testclass="JSONPostProcessor" testname="JSON Extractor" enabled="true">
        <stringProp name="JSONPostProcessor.referenceNames">SECOND_ARTICLE_ID</stringProp>
        <stringProp name="JSONPostProcessor.jsonPathExprs">$.message</stringProp>
        <stringProp name="JSONPostProcessor.match_numbers"></stringProp>
       </JSONPostProcessor>
       <hashTree/>
      </hashTree>
      <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Create third article" enabled="true">
       <boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
       <elementProp name="HTTPsampler.Arguments" elementType="Arguments">
        <collectionProp name="Arguments.arguments">
         <elementProp name="" elementType="HTTPArgument">
          <boolProp name="HTTPArgument.always_encode">false</boolProp>
          <stringProp name="Argument.value">{&#xd;
 &quot;kb_title&quot;: &quot;Some awesome article 2&quot;,&#xd;
 &quot;kb_permalink&quot;: &quot;&quot;,&#xd;
 &quot;kb_published&quot;: true,&#xd;
 &quot;kb_password&quot;: &quot;&quot;,&#xd;
 &quot;kb_author_email&quot;: &quot;sphinx@guest.com&quot;,&#xd;
 &quot;kb_project&quot;: &quot;&quot;,&#xd;
 &quot;kb_body&quot;: &quot;Some body&quot;,&#xd;
 &quot;kb_keywords&quot;: &quot;keyword1&quot;,&#xd;
 &quot;kb_featured&quot;: false,&#xd;
 &quot;kb_seo_title&quot;: &quot;&quot;,&#xd;
 &quot;kb_seo_description&quot;: &quot;&quot;&#xd;
}</stringProp>
          <stringProp name="Argument.metadata">=</stringProp>
         </elementProp>
        </collectionProp>
       </elementProp>
```


```
<stringProp name="HTTPSampler.domain">${API}</stringProp>
<stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
<stringProp name="HTTPSampler.protocol">http</stringProp>
<stringProp name="HTTPSampler.contentEncoding"></stringProp>
<stringProp name="HTTPSampler.path">/api/newArticle</stringProp>
<stringProp name="HTTPSampler.method">POST</stringProp>
<boolProp name="HTTPSampler.follow_redirects">true</boolProp>
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return 200" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

<stringProp name="Header.value">Bearer ${JWT}</stringProp>

</elementProp>

</collectionProp>

</HeaderManager>

<hashTree/>

<JSONPostProcessor guiclass="JSONPostProcessorGui" testclass="JSONPostProcessor" testname="JSON Extractor" enabled="true">

<stringProp name="JSONPostProcessor.referenceNames">THIRD_ARTICLE_ID</stringProp>

<stringProp name="JSONPostProcessor.jsonPathExprs">$.message</stringProp>

<stringProp name="JSONPostProcessor.match_numbers"></stringProp>

</JSONPostProcessor>

<hashTree/>

</hashTree>

<HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Authenticate to KBR API as a validator" enabled="true">

<boolProp name="HTTPSampler.postBodyRaw">true</boolProp>

<elementProp name="HTTPsampler.Arguments" elementType="Arguments">

<collectionProp name="Arguments.arguments">

<elementProp name="" elementType="HTTPArgument">

<boolProp name="HTTPArgument.always_encode">false</boolProp>

<stringProp name="Argument.value">{

"email":"sphinxadmin@f-in.eu",

"password":"sphinxadmin@f-in.eu"

}</stringProp>

<stringProp name="Argument.metadata">=</stringProp>

</elementProp>

</collectionProp>

</elementProp>

<stringProp name="HTTPSampler.domain">${API}</stringProp>

<stringProp name="HTTPSampler.port">${APIPORT}</stringProp>

<stringProp name="HTTPSampler.protocol">http</stringProp>

<stringProp name="HTTPSampler.contentEncoding"></stringProp>

<stringProp name="HTTPSampler.path">/auth/login</stringProp>

<stringProp name="HTTPSampler.method">POST</stringProp>

<boolProp name="HTTPSampler.follow_redirects">true</boolProp>

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


```
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Response Assertion" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
</collectionProp>
</HeaderManager>
<hashTree/>
<JSONPostProcessor guiclass="JSONPostProcessorGui" testclass="JSONPostProcessor" testname="JSON Extractor" enabled="true">
<stringProp name="JSONPostProcessor.referenceNames">VALIDATOR_JWT</stringProp>
<stringProp name="JSONPostProcessor.jsonPathExprs">$.token</stringProp>
<stringProp name="JSONPostProcessor.match_numbers"></stringProp>
</JSONPostProcessor>
```


*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.*


```
        <hashTree/>
      </hashTree>
      <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Approve first article" enabled="true">
        <boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
        <elementProp name="HTTPsampler.Arguments" elementType="Arguments">
          <collectionProp name="Arguments.arguments">
            <elementProp name="" elementType="HTTPArgument">
              <boolProp name="HTTPArgument.always_encode">false</boolProp>
              <stringProp name="Argument.value">{&#xd;
 &amp;quot;id&amp;quot;:&amp;quot;${FIRST_ARTICLE_ID}&amp;quot;&#xd;
}</stringProp>
              <stringProp name="Argument.metadata">=</stringProp>
            </elementProp>
          </collectionProp>
        </elementProp>
        <stringProp name="HTTPSampler.domain">${API}</stringProp>
        <stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
        <stringProp name="HTTPSampler.protocol">http</stringProp>
        <stringProp name="HTTPSampler.contentEncoding"></stringProp>
        <stringProp name="HTTPSampler.path">/api/article/approve</stringProp>
        <stringProp name="HTTPSampler.method">POST</stringProp>
        <boolProp name="HTTPSampler.follow_redirects">true</boolProp>
        <boolProp name="HTTPSampler.auto_redirects">false</boolProp>
        <boolProp name="HTTPSampler.use_keepalive">true</boolProp>
        <boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
        <stringProp name="HTTPSampler.embedded_url_re"></stringProp>
        <stringProp name="HTTPSampler.connect_timeout"></stringProp>
        <stringProp name="HTTPSampler.response_timeout"></stringProp>
      </HTTPSamplerProxy>
      <hashTree>
        <HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
          <collectionProp name="HeaderManager.headers">
            <elementProp name="" elementType="Header">
```

<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
<stringProp name="Header.value">Bearer ${VALIDATOR_JWT}</stringProp>
</elementProp>
</collectionProp>
</HeaderManager>
<hashTree/>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return 200" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
</hashTree>
<HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Retrieve first article" enabled="true">
<boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
<elementProp name="HTTPsampler.Arguments" elementType="Arguments">
<collectionProp name="Arguments.arguments">
<elementProp name="" elementType="HTTPArgument">
<boolProp name="HTTPArgument.always_encode">false</boolProp>
<stringProp name="Argument.value">{
"kb_id":"${FIRST_ARTICLE_ID}"
}</stringProp>
<stringProp name="Argument.metadata">=</stringProp>
</elementProp>
</collectionProp>

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
        </elementProp>
        <stringProp name="HTTPSampler.domain">${API}</stringProp>
        <stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
        <stringProp name="HTTPSampler.protocol">http</stringProp>
        <stringProp name="HTTPSampler.contentEncoding"></stringProp>
        <stringProp name="HTTPSampler.path">/api/getArticleJson</stringProp>
        <stringProp name="HTTPSampler.method">POST</stringProp>
        <boolProp name="HTTPSampler.follow_redirects">true</boolProp>
        <boolProp name="HTTPSampler.auto_redirects">false</boolProp>
        <boolProp name="HTTPSampler.use_keepalive">true</boolProp>
        <boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
        <stringProp name="HTTPSampler.embedded_url_re"></stringProp>
        <stringProp name="HTTPSampler.connect_timeout"></stringProp>
        <stringProp name="HTTPSampler.response_timeout"></stringProp>
      </HTTPSamplerProxy>
      <hashTree>
        <HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header
Manager" enabled="true">
          <collectionProp name="HeaderManager.headers">
            <elementProp name="" elementType="Header">
              <stringProp name="Header.name">Content-Type</stringProp>
              <stringProp name="Header.value">application/json</stringProp>
            </elementProp>
            <elementProp name="" elementType="Header">
              <stringProp name="Header.name">Authorization</stringProp>
              <stringProp name="Header.value">Bearer ${VALIDATOR_JWT}</stringProp>
            </elementProp>
          </collectionProp>
        </HeaderManager>
        <hashTree/>
        <ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return
200" enabled="true">
          <collectionProp name="Asserion.test_strings">
            <stringProp name="49586">200</stringProp>
          </collectionProp>
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
</hashTree>
<HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Reject and delete second article" enabled="true">
<boolProp name="HTTPSampler.postBodyRaw">true</boolProp>
<elementProp name="HTTPsampler.Arguments" elementType="Arguments">
<collectionProp name="Arguments.arguments">
<elementProp name="" elementType="HTTPArgument">
<boolProp name="HTTPArgument.always_encode">false</boolProp>
<stringProp name="Argument.value">{
"id":"${SECOND_ARTICLE_ID}"
}</stringProp>
<stringProp name="Argument.metadata">=</stringProp>
</elementProp>
</collectionProp>
</elementProp>
<stringProp name="HTTPSampler.domain">${API}</stringProp>
<stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
<stringProp name="HTTPSampler.protocol">http</stringProp>
<stringProp name="HTTPSampler.contentEncoding"></stringProp>
<stringProp name="HTTPSampler.path">/api/article/reject</stringProp>
<stringProp name="HTTPSampler.method">POST</stringProp>
<boolProp name="HTTPSampler.follow_redirects">true</boolProp>
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
</HTTPSamplerProxy>
<hashTree>
 <HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
  <collectionProp name="HeaderManager.headers">
   <elementProp name="" elementType="Header">
    <stringProp name="Header.name">Content-Type</stringProp>
    <stringProp name="Header.value">application/json</stringProp>
   </elementProp>
   <elementProp name="" elementType="Header">
    <stringProp name="Header.name">Authorization</stringProp>
    <stringProp name="Header.value">Bearer ${VALIDATOR_JWT}</stringProp>
   </elementProp>
  </collectionProp>
 </HeaderManager>
 <hashTree/>
 <ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return 200" enabled="true">
  <collectionProp name="Asserion.test_strings">
   <stringProp name="49586">200</stringProp>
  </collectionProp>
  <stringProp name="Assertion.custom_message"></stringProp>
  <stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
  <boolProp name="Assertion.assume_success">false</boolProp>
  <intProp name="Assertion.test_type">8</intProp>
 </ResponseAssertion>
 <hashTree/>
</hashTree>
<HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Delete first article" enabled="true">
 <elementProp name="HTTPsampler.Arguments" elementType="Arguments" guiclass="HTTPArgumentsPanel" testclass="Arguments" testname="User Defined Variables" enabled="true">
  <collectionProp name="Arguments.arguments"/>
 </elementProp>
 <stringProp name="HTTPSampler.domain">${API}</stringProp>
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


```
<stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
<stringProp name="HTTPSampler.protocol">http</stringProp>
<stringProp name="HTTPSampler.contentEncoding"></stringProp>
<stringProp name="HTTPSampler.path">/api/article/${FIRST_ARTICLE_ID}</stringProp>
<stringProp name="HTTPSampler.method">DELETE</stringProp>
<boolProp name="HTTPSampler.follow_redirects">true</boolProp>
<boolProp name="HTTPSampler.auto_redirects">false</boolProp>
<boolProp name="HTTPSampler.use_keepalive">true</boolProp>
<boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
<stringProp name="HTTPSampler.embedded_url_re"></stringProp>
<stringProp name="HTTPSampler.connect_timeout"></stringProp>
<stringProp name="HTTPSampler.response_timeout"></stringProp>
</HTTPSamplerProxy>
<hashTree>
<ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return 200" enabled="true">
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
<stringProp name="Header.value">Bearer ${JWT}</stringProp>
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

```
        </elementProp>
       </collectionProp>
      </HeaderManager>
      <hashTree/>
      <JSONPostProcessor guiclass="JSONPostProcessorGui" testclass="JSONPostProcessor" testname="JSON Extractor" enabled="true">
       <stringProp name="JSONPostProcessor.referenceNames">ARTICLE_ID</stringProp>
       <stringProp name="JSONPostProcessor.jsonPathExprs">$.message</stringProp>
       <stringProp name="JSONPostProcessor.match_numbers"></stringProp>
      </JSONPostProcessor>
      <hashTree/>
     </hashTree>
     <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="Delete third article" enabled="true">
      <elementProp name="HTTPsampler.Arguments" elementType="Arguments" guiclass="HTTPArgumentsPanel" testclass="Arguments" testname="User Defined Variables" enabled="true">
       <collectionProp name="Arguments.arguments"/>
      </elementProp>
      <stringProp name="HTTPSampler.domain">${API}</stringProp>
      <stringProp name="HTTPSampler.port">${APIPORT}</stringProp>
      <stringProp name="HTTPSampler.protocol">http</stringProp>
      <stringProp name="HTTPSampler.contentEncoding"></stringProp>
      <stringProp name="HTTPSampler.path">/api/article/${THIRD_ARTICLE_ID}</stringProp>
      <stringProp name="HTTPSampler.method">DELETE</stringProp>
      <boolProp name="HTTPSampler.follow_redirects">true</boolProp>
      <boolProp name="HTTPSampler.auto_redirects">false</boolProp>
      <boolProp name="HTTPSampler.use_keepalive">true</boolProp>
      <boolProp name="HTTPSampler.DO_MULTIPART_POST">false</boolProp>
      <stringProp name="HTTPSampler.embedded_url_re"></stringProp>
      <stringProp name="HTTPSampler.connect_timeout"></stringProp>
      <stringProp name="HTTPSampler.response_timeout"></stringProp>
     </HTTPSamplerProxy>
     <hashTree>
      <ResponseAssertion guiclass="AssertionGui" testclass="ResponseAssertion" testname="Should return 200" enabled="true">
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.


```
<collectionProp name="Asserion.test_strings">
<stringProp name="49586">200</stringProp>
</collectionProp>
<stringProp name="Assertion.custom_message"></stringProp>
<stringProp name="Assertion.test_field">Assertion.response_code</stringProp>
<boolProp name="Assertion.assume_success">false</boolProp>
<intProp name="Assertion.test_type">8</intProp>
</ResponseAssertion>
<hashTree/>
<HeaderManager guiclass="HeaderPanel" testclass="HeaderManager" testname="HTTP Header Manager" enabled="true">
<collectionProp name="HeaderManager.headers">
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Content-Type</stringProp>
<stringProp name="Header.value">application/json</stringProp>
</elementProp>
<elementProp name="" elementType="Header">
<stringProp name="Header.name">Authorization</stringProp>
<stringProp name="Header.value">Bearer ${JWT}</stringProp>
</elementProp>
</collectionProp>
</HeaderManager>
<hashTree/>
<JSONPostProcessor guiclass="JSONPostProcessorGui" testclass="JSONPostProcessor" testname="JSON Extractor" enabled="true">
<stringProp name="JSONPostProcessor.referenceNames">SECOND_ARTICLE_ID</stringProp>
<stringProp name="JSONPostProcessor.jsonPathExprs">$.message</stringProp>
<stringProp name="JSONPostProcessor.match_numbers"></stringProp>
</JSONPostProcessor>
<hashTree/>
</hashTree>
<ResultCollector guiclass="ViewResultsFullVisualizer" testclass="ResultCollector" testname="View Results Tree" enabled="true">
<boolProp name="ResultCollector.error_logging">false</boolProp>
<objProp>
```


*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.*

```
        <name>saveConfig</name>
        <value class="SampleSaveConfiguration">
         <time>false</time>
         <latency>true</latency>
         <timestamp>false</timestamp>
         <success>true</success>
         <label>true</label>
         <code>true</code>
         <message>true</message>
         <threadName>false</threadName>
         <dataType>false</dataType>
         <encoding>false</encoding>
         <assertions>true</assertions>
         <subresults>false</subresults>
         <responseData>false</responseData>
         <samplerData>false</samplerData>
         <xml>false</xml>
         <fieldNames>true</fieldNames>
         <responseHeaders>false</responseHeaders>
         <requestHeaders>false</requestHeaders>
         <responseDataOnError>false</responseDataOnError>
         <saveAssertionResultsFailureMessage>true</saveAssertionResultsFailureMessage>
         <assertionsResultsToSave>0</assertionsResultsToSave>
         <url>true</url>
        </value>
       </objProp>
       <stringProp name="filename">/home/mkcodergr/Documents/fint documents/testplans/d5.5/results-
2.csv</stringProp>
      </ResultCollector>
      <hashTree/>
     </hashTree>
    </hashTree>
  </hashTree>
</jmeterTestPlan>
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.