SECURITY AUDIT REPORT

{company.name}

|  |  |  |
| --- | --- | --- |
| Classification | Public document  Internal document  Confidential document  Secret document | (C1)  (C2)  (C3)  (C4) |
| C3 |

|  |  |  |  |
| --- | --- | --- | --- |
| Object | {company.name} security report | | |
| Reference | *{company.name}\_report\_{date\_end}.docx* | Date | {date} |
| Editor | {creator.firstname} {creator.lastname}{#collaborators}  {firstname} {lastname}{/collaborators} | Place | [Place] |

{%company.logo\_small}

The information contained in this document remains the property of [COMPANY] and must not be disclosed by the recipient to third parties without the written consent of [COMPANY].

**SUMMARY**

[1. Your contacts 2](#_Toc133851429)

[2. Document tracking 2](#_Toc133851430)

[3. Introduction 4](#_Toc133851431)

[3.1 Context and Objectives 4](#_Toc133851432)

[3.2 [COMPANY] participants and customer referents 4](#_Toc133851433)

[3.3 Mailing list 4](#_Toc133851434)

[3.4 Period and Confidentiality 5](#_Toc133851435)

[3.5 Perimeter 5](#_Toc133851436)

[3.6 Notes concerning the audit 5](#_Toc133851437)

[4. Executive summary 8](#_Toc133851438)

[4.1 Work performed 8](#_Toc133851439)

[4.2 Overall level of security 9](#_Toc133851440)

[4.3 Presentation of vulnerabilities and findings 12](#_Toc133851441)

[4.4 Presentation of recommendations 15](#_Toc133851442)

[5. Detailed Works 18](#_Toc133851443)

[5.1 Vulnerabilities research 18](#_Toc133851444)

[5.2 Discovered VulnerabilitIes 19](#_Toc133851445)

[5.3 Hardening Measures 21](#_Toc133851446)

[6. Annexes 23](#_Toc133851447)

[6.1 Figures table 23](#_Toc133851448)

[6.2 Global security level scale 24](#_Toc133851449)

[6.3 Classification of recommendations 25](#_Toc133851450)

[6.4 Vulnerabilities classification – CVSS Scorring 26](#_Toc133851451)

[6.5 Top 10 OWASP 2021 27](#_Toc133851452)

# Your contacts

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Occupation** | **Phone** | **E-Mail** |
| Firstname LASTNAME | Cybersecurity Activity Director | XX.XX.XX.XX.XX | first.last@mail.com |
| Firstname LASTNAME | Auditor and Technical Team Referent | XX.XX.XX.XX.XX | first.last@mail.com |
| {creator.firstname} {creator.lastname} | Cybersecurity consultant | {creator.phone} | {@creator.email | mailto: creator.email | p: 'Contenudetableau'} |
| {#collaborators}{firstname} {lastname} | Cybersecurity consultant | {phone} | {@email | mailto: email | p: 'Contenudetableau'}{/collaborators} |

# Document tracking

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Editor’s name** | **Object** |
| 1.0 | {date\_end} | {creator.firstname} {creator.lastname} | Document creation |

CONTEXT, OBJECTIVES AND SCOPE

# Introduction

## Context and Objectives

The approach of {company.name} is part of a logic of continuous improvement of the quality of its services and the security of information, for its own security but also for that of its customers and partners.

The objectives of this audit are to:

* Have an expert opinion on the level of security,
* Ensure compliance with good practices and internal security rules,
* Assess and reduce the level of risk,
* Identify areas for improvement.

## [COMPANY] participants and customer referents

**[COMPANY]**

* {creator.firstname} {creator.lastname}, Cybersecurity consultant{#collaborators}
* {firstname} {lastname}, Cybersecurity consultant{/collaborators}

{company.name}

* {client.firstname} {client.lastname}, {client.title}

## Mailing list

|  |  |  |
| --- | --- | --- |
| **Company** | **Person** | **Occupation** |
| {company.name} | {client.firstname} {client.lastname} | {client.title} |
| [COMPANY] | {creator.firstname} {creator.lastname} | Cybersecurity consultant |
| {#collaborators}[COMPANY] | {firstname} {lastname} | Cybersecurity consultant{/collaborators} |

## Period and Confidentiality

The security audit took place over the following period(s):

|  |  |
| --- | --- |
| **Audit activity** | **Date** |
| Penetration Testing | From {date\_start } to {date\_end } |

All data collected during the audit will be transmitted to their owner ({company.name}) upon request and/or destroyed at the end of the mission.

## Perimeter

### Technical perimeter

{company.name} notified [COMPANY] of the Penetration Test authorization and provided the following resources:

* {-w:p scope}{name}{/scope}

The entire service is performed remotely from public IP addresses: [PUBLIC IPs].

## Notes concerning the audit

### Address ranges

Penetration tests from the Internet were conducted from a limited list of IPs, belonging to [COMPANY], unlike attackers who have several machines located on different attacking networks. Scans or attacks therefore have the addresses mentioned above as their source address. These attacks are then easily detected by your services.

### Methodical audit

Unlike attackers who orient themselves towards a path as soon as they find a lead, listeners favor an organized study. This makes it possible to scan the perimeter more widely and therefore to update many sensitive zones. Indeed, an attacker often uses the first vulnerability he discovers, but the objective of an audit is to identify a set of areas at risk.

The main disadvantage of this approach is that the auditors leave the time to the administrators to secure the possible flaws, because the “exploits” are carried out during the following stages of the audit. In the context of a real attack, attackers use the flaw only a few minutes after finding it: this gives them time to cover their tracks and therefore avoid being detected by administrators.

We would like to emphasize this difference. The goal of an attacker is generally not to identify all the vulnerabilities of a system but to exploit the one(s) that he could find. Completeness is therefore not sought, unlike in the case of the provision of expertise. An expert seeks, within a limited time and workload, to highlight a maximum of vulnerabilities, real or potential, and identifiable at a given moment. We therefore do not guarantee the exhaustiveness of the discoveries of vulnerabilities on the perimeter concerned in the time allowed.

### Limited period

We tested the vulnerabilities disclosed and published before and during the audit period, the dates of which are previously mentioned in the report.

If, during an audit, a major flaw is discovered, it is possible to exploit it during the few hours necessary for the administrator to install a patch.

The exploitation of a flaw during an audit is then subject to the vulnerabilities discovered during this period. An attacker, on the other hand, can wait several weeks before using a major flaw.

### Limits of the service

The purpose of the service is to provide an expert opinion on the security of the target information system, at a given time, together with recommendations and advice.

The measures put in place following the advice of our experts are intended to increase the confidence of {company.name} in its information system, if the recommended measures are correctly implemented.

We draw the attention of {company.name} to the limits of such a notice:

* As attack techniques evolve, a system that is secure at a given moment may no longer be so some time later. We advise {company.name} to maintain a technical watch on this subject and to apply the corrections recommended by certain specialized services as soon as possible;
* The purpose of the expert's opinion is to increase the level of confidence in safety at a given moment depending on the elements provided and the depth of the analysis he has been able to perform. This level of confidence cannot be considered absolute. Achieving this level of trust assumes that {company.name} correctly implements the recommended measures.

### Validation audit

A validation audit is strongly recommended to verify the implementation of security measures.

Executive summary

# Executive summary

## Work performed

A 3-phase methodology, illustrated by the diagram below, was implemented to meet the audit objectives.

Discovery and exploration of the perimeters

Discovery and exploration of the perimeters

Identification and exploitation of vulnerabilities

The work carried out revealed several vulnerabilities in the scope of the audit. The following parts present:

* The vulnerabilities identified with their level of severity,
* The breakdown in terms of severity of the identified vulnerabilities,
* Recommendations to remedy them.

## Overall level of security

Based on its experiences, [COMPANY] assesses the maturity of the audited perimeter in terms of security as being ... The company {company.name} has been able to implement security measures ....

**?**

**EXCELLENT A**

**GREAT B**

**AVERAGE C**

**LOW D**

**VERY LOW F**

In fact, …

The table below describes the major strengths and weaknesses of the Information System of the company {company.name}, using the [TOP 10 OWASP 2021](https://owasp.org/www-project-top-ten/) benchmark.

|  |  |
| --- | --- |
| **Caption** | |
| Very good level |  |
| Good level |  |
| Insufficient |  |
| Non-existent |  |

|  |  |  |
| --- | --- | --- |
| **Strengths and Weakness** | **Comments** | **Protection level** |
| Access control to restricted features | TODO |  |
| Cryptographic Failures (data protection) | TODO |  |
| Injections | TODO |  |
| Insecure Design | TODO |  |
| Security Misconfiguration | TODO |  |
| Vulnerable and Outdated components | TODO |  |
| Identification and Authentication Failures | TODO |  |
| Software and Data Integrity Failures | TODO |  |
| Security Logging and Monitoring Failures | N/A | N/A |
| Server Side Request Forgery (SSRF) | TODO |  |

## Presentation of vulnerabilities and findings

* List of vulnerabilities

The table below lists the vulnerabilities observed during the audit. Each vulnerability is associated with one or more recommendations, with one or more threats and with a severity level based on the CVSS scale, i.e. according to the impact and the ease of exploitation, in accordance state of the art.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **reference** | **Title** | **Scope** | **CVSS Score** | **RISK(s)** |
| {#findings | where: '(cvss.baseSeverity != "None" && cvss.baseSeverity != "")' | sortArrayByField: 'cvss.baseMetricScore':-1}{@'VULN-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | **{@cvss.cellColor}**  {@('CVSS ' + cvss.baseMetricScore) | linkTo: 'https://www.first.org/cvss/calculator/3.1#'+cvss.vectorString | p:'CVSS'} | {-w:p description}{@text | convertHTML: 'ContenudeTableauSmall'}{/description}{/} |

* LISTE DES MESURES DE DURCISSEMENT

The table below lists the tightening measures noted during the audit. A hardening measure is a weakness considered minor. Each control point is associated with one or more recommendations as well as one or more threats.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **reference** | **Title** | **Scope** | **CVSS Score** | **RISK(s)** |
| {#findings | where: '(cvss.baseSeverity == "None" || cvss.baseSeverity == "")'}{@'HARDENED-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | {@cvss.cellColor}  N/A | {-w:p description}{@text | convertHTML: 'ContenudeTableauSmall'}{/description}{/} |

* vulnerabilities per criticality

{c\_crit = (findings | count: 'Critical'); c\_high = (findings | count: 'High'); c\_med = (findings | count: 'Medium'); c\_low = (findings | count: 'Low'); c\_total = (c\_crit + c\_high + c\_med + c\_low); c\_hard = (findings | count: 'None'); cv\_i = ((c\_high && c\_med) || (c\_high && c\_low) || (c\_med && c\_low)); cv\_ii = (c\_med && c\_low); cv\_iii = (c\_med || c\_low); ''} The graph below provides an overall view of the level and number of vulnerabilities in the scope audited. The presence {#c\_crit}of {c\_crit} vulnerabilit{#c\_crit==1}y{/}{#c\_crit>1}ies{/} qualified as « critical »{#c\_crit!=c\_total}{#cv\_i},{/}{^cv\_i} and{/} {/}{/}{#c\_high}of {c\_high} vulnerabilit{#c\_high==1}y{/}{#c\_high>1}ies{/} qualified as « high »{#cv\_iii}{#cv\_ii},{/}{^cv\_ii} and{/} {/}{/}{#c\_med}of {c\_med} vulnerabilit{#c\_med==1}y{/}{#c\_med>1}ies{/} qualified as « medium » {#c\_low}and {/}{/}{#c\_low}of {c\_low} « low » vulnerabilit{#c\_low==1}y{/}{#c\_low>1}ies{/} involves {#c\_crit}immediate {/} actions from {company.name} or its providers. The hardening measure{#c\_hard>1}s are{/}{#c\_hard==1} is{/} also to be taken into account in order to improve the overall security of the exposed IS.{/}

## Presentation of recommendations

The table below lists the recommendations for dealing with vulnerabilities or audit findings.

Each finding or vulnerability is associated with one or more risks, one or more recommendations and a level of priority.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **reference** | **Title** | **Scpê** | **Recommendation(s)** | **Complexity** | **Priority level** |
| {#findings | where: '(cvss.baseSeverity != "None" && cvss.baseSeverity != "")' | sortArrayByField: 'cvss.baseMetricScore':-1}{@'VULN-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | {-w:p remediation}{@text | convertHTML: 'ContenudeTableauSmall'}{/remediation} | {@remediation.cellColorComplexity}  {#remediationComplexity == '1'}Faible{/}{#remediationComplexity == '2'}Moyenne{/}{#remediationComplexity == '3'}Elevée{/} | {@remediation.cellColorPriority}  {priority}{/} |
| {#findings | where: '(cvss.baseSeverity == "None" || cvss.baseSeverity == "")'}{@'HARDENED-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | {-w:p remediation}{@text | convertHTML: 'ContenudeTableauSmall'}{/remediation} | {@remediation.cellColorComplexity }  {#remediationComplexity == '1'}Faible{/}{#remediationComplexity == '2'}Moyenne{/}{#remediationComplexity == '3'}Elevée{/} | {@remediation.cellColorPriority}  {priority}{/} |

Detailed

Works

# Detailed Works

## Vulnerabilities research

[METHODOLOGY]

## Discovered VulnerabilitIes{#findings| where: '(cvss.baseSeverity != "None" && cvss.baseSeverity != "")' | sortArrayByField: 'cvss.baseMetricScore':-1}

### {title}

|  |  |  |
| --- | --- | --- |
| **{@cvss.cellColor}** | **{@cvss.cellColor}**  {@'VULN-'+($index+1) | bookmarkCreate | p : 'VulnDef'} | **{@cvss.cellColor}** |
| **Title** | **{title}** | **{@cvss.cellColor}**  {@('CVSS ' + cvss.baseMetricScore) | linkTo: 'https://www.first.org/cvss/calculator/3.1#'+cvss.vectorString | p:'CVSS'} |
| **Scope** | {@affected | convertHTML: 'Normal10'} |
| **Description** | {-w:p description}{@text | convertHTML: 'Normal10'}{/description} | |
| **Recommendation** | {-w:p remediation}{@text | convertHTML: 'Normal10'}{/remediation} | |
| **References** | {#references | loopObject}  {@value | linkTo: value | p: 'reflink'}  {/} | |

#### Findings

{-w:p observation}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/observation}

#### Proofs

{-w:p poc}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/poc}

#### Recommendations

{-w:p remediation}{@text | convertHTML}{/remediation}

{/}

## Hardening Measures {#findings | where: '(cvss.baseSeverity == "None" || cvss.baseSeverity == "")' }

### {title}

|  |  |  |
| --- | --- | --- |
| **{@cvss.cellColor}** | **{@cvss.cellColor}**  {@'HARDENED-'+($index+1) | bookmarkCreate | p : 'VulnDef'} | **{@cvss.cellColor}** |
| **Title** | **{title}** | **{@cvss.cellColor}**  **N/A** |
| **Scope** | {@affected | convertHTML: 'Normal10'} |
| **Description** | {-w:p description}{@text | convertHTML: 'Normal10'}{/description} | |
| **Recommendation** | {-w:p remediation}{@text | convertHTML: 'Normal10'}{/remediation} | |
| **References** | {#references | loopObject}  {@value | linkTo: value | p: 'reflink'}  {/} | |

#### Findings

{-w:p observation}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/observation}

#### Proofs

{-w:p poc}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/poc}

#### Recommendations

{-w:p remediation}{@text | convertHTML}{/remediation}

{/}

# Annexes

## Figures table

[Figure 1 **-** name 0](#_Toc99378187)

## Global security level scale

Insofar as :

* The security level of a component is not only linked to the security efforts undertaken but can also be dependent on the component itself;
* The approach to auditing and studying vulnerabilities takes into account the level of security at time “T” independently of the business impacts of vulnerabilities;
* A critical vulnerability presents an immediate and significant risk for the IS or the impacted component;
* The audit service is carried out in a partially constrained time and aims to ensure that vulnerabilities and configuration weaknesses are exhaustive.

[COMPANY] establishes the overall security level of the audited perimeter according to the following criteria.

|  |  |
| --- | --- |
| **Level** | **Description** |
| **Excellent** | No vulnerability with a "Critical" or "Major" risk has been identified. Adequate and optimal security measures are present, which makes it possible to have established confidence in the security of the audited IS and to limit the potential impacts of a vulnerability. The audited IS is far superior to the average for companies on equivalent scopes. |
| **Great** | No vulnerability with a "Critical" or "Major" risk has been identified. Some minor, medium vulnerabilities or hardening measures are present. The audited IS nevertheless presents security measures and is generally superior to the average of the IS audited on equivalent perimeters, in terms of security. |
| **Medium** | Several vulnerabilities with an “Important” or “Major” risk have been discovered. Some security measures are in place but are still insufficient to ensure the security of the IS. The audited IS is in the average of companies audited on equivalent perimeters in terms of security. |
| **Low** | At least one "Major" or "Critical" vulnerability has been identified within the scope of the audit and makes it possible to take control of a component or to recover sensitive data. Despite the possible presence of some measures, the maturity of the IS audited is considered unsatisfactory. The security of the audited IS is lower than the average for companies on equivalent perimeters. |
| **Very low** | Several “Critical” vulnerabilities have been discovered. The compromise of a component or the IS is possible from several axes and the security of the data is not guaranteed. The overall level of security is lower than the average of IS audited on equivalent perimeters and the maturity of the IS in terms of security is very unsatisfactory. |

## Classification of recommendations

### Correction complexity

Each recommendation issued by [COMPANY] is assigned an estimated level of complexity of implementation, provided as an indication and based on the necessary investments, particularly in terms of time. The following scale illustrates the different existing levels.

|  |  |
| --- | --- |
| **Complexity level** | **Description** |
| **Low** | Corresponds to a task that is not very complex, can be carried out in a few hours, does not entail any additional financial cost and has little or no operational impact (e.g. modification of a configuration parameter). |
| **Medium** | Corresponds to a moderately complex task, which may require work of a few days or a financial investment and requiring consideration of potential operational impacts (e.g. work around privileged accounts, service accounts, updating "client" machines) . |
| **High** | Corresponds to a complex task requiring preparation in order to take into account the potential impacts at the IS level. The complexity of the implementation can come from the duration necessary for the application, which can be several days or weeks (ex: important site of updates of machines) or from the evolution of the current processes of operation (ex: modification of a large number of passwords, development of technological solution). |

### Correction priority

In accordance with the level of risk and the severity of each vulnerability, [COMPANY] proposes an indicative priority for the application of each recommendation, in line with all of them. This priority also takes into account the complexity of implementation. The following scale illustrates the different levels of priority.

|  |  |
| --- | --- |
| **Priority level** | **Description** |
| **1** | The recommendation is not a priority given the risk involved and may be postponed in order to improve the security of the IS. |
| **2** | The recommendation requires further study before it can be implemented, or perhaps embarked on later modifications, without significant urgency. |
| **3** | The recommendation has a high priority and should be implemented in a relatively short time in order to limit the identified risks. However, it must be checked before application. |
| **4** | The recommendation is absolutely a priority and should be considered first in the action plan because it makes it possible to evacuate a direct risk (point of entry, elevation of privilege, compromise). |

## Vulnerabilities classification – CVSS Scorring



|  |
| --- |
| Common Vulnerability Scoring System (CVSS) is a standardized evaluation system of the criticality of vulnerabilities according to objective and measurable criteria. This evaluation is made up of 3 measures called metrics: the basic metric, the temporal metric and the environmental metric. |

Metrics :

The CVSS is built from the base metric which gives us an assessment of the base CVSS which will then be weighted with the time metric and then with the environmental metric. These three metrics are defined as follows:

* The basic metric is unique and immutable, it is based on the intrinsic qualities of the vulnerability;
* The temporal metric is unique but can change over time;
* The environmental metric is multiple and evolves according to the IT environment. It depends on the computer system in which it is present.

For more details: <https://www.first.org/cvss>

## Top 10 OWASP 2021

The "OWASP" foundation (Open Web Application Security Project) publishes a global project called "TOP 10 Web Application Security Risks" aimed at bringing together in the form of a detailed list the various most common applicable vulnerabilities.

Une image contenant texte, clipart

Description générée automatiquement

Project very widely adopted by the community and used as a reference in order to address the main risks in the development and production of applications, an update of the repository was published in September 2021. The latter makes it possible to provide a new version to the previous repository dating from 2017.

A01:2021-Broken Access Control moves up from the fifth position to the category with the most serious web application security risk; the contributed data indicates that on average, 3.81% of applications tested had one or more Common Weakness Enumerations (CWEs) with more than 318k occurrences of CWEs in this risk category. The 34 CWEs mapped to Broken Access Control had more occurrences in applications than any other category.

A02:2021-Cryptographic Failures shifts up one position to #2, previously known as A3:2017-Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed name focuses on failures related to cryptography as it has been implicitly before. This category often leads to sensitive data exposure or system compromise.

A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average incidence rate of 3.37%, and the 33 CWEs mapped into this category have the second most occurrences in applications with 274k occurrences. Cross-site Scripting is now part of this category in this edition.

A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, we need more threat modeling, secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.

A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.5%, and over 208k occurrences of CWEs mapped to this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for A4:2017-XML External Entities (XXE) is now part of this risk category.

A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.

A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. A8:2017-Insecure Deserialization is now a part of this larger category.

A09:2021-Security Logging and Monitoring Failures was previously A10:2017-Insufficient Logging & Monitoring and is added from the Top 10 community survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

**The following resources allow you to learn more about the project:**

* OWASP Top 10 Web Application Security Risks ([link](https://owasp.org/www-project-top-ten/))
* Introduction to OWASP Top 10 2021 ([link](https://owasp.org/Top10/fr/))