



ENEDIS

L'ELECTRICITE EN RESEAU

Mai-juin 2024

- Enedis Limoges (Zone Ester)
- Projet 1 : Audit d'applications web
- Projet 2 : Eventuelles corrections des failles



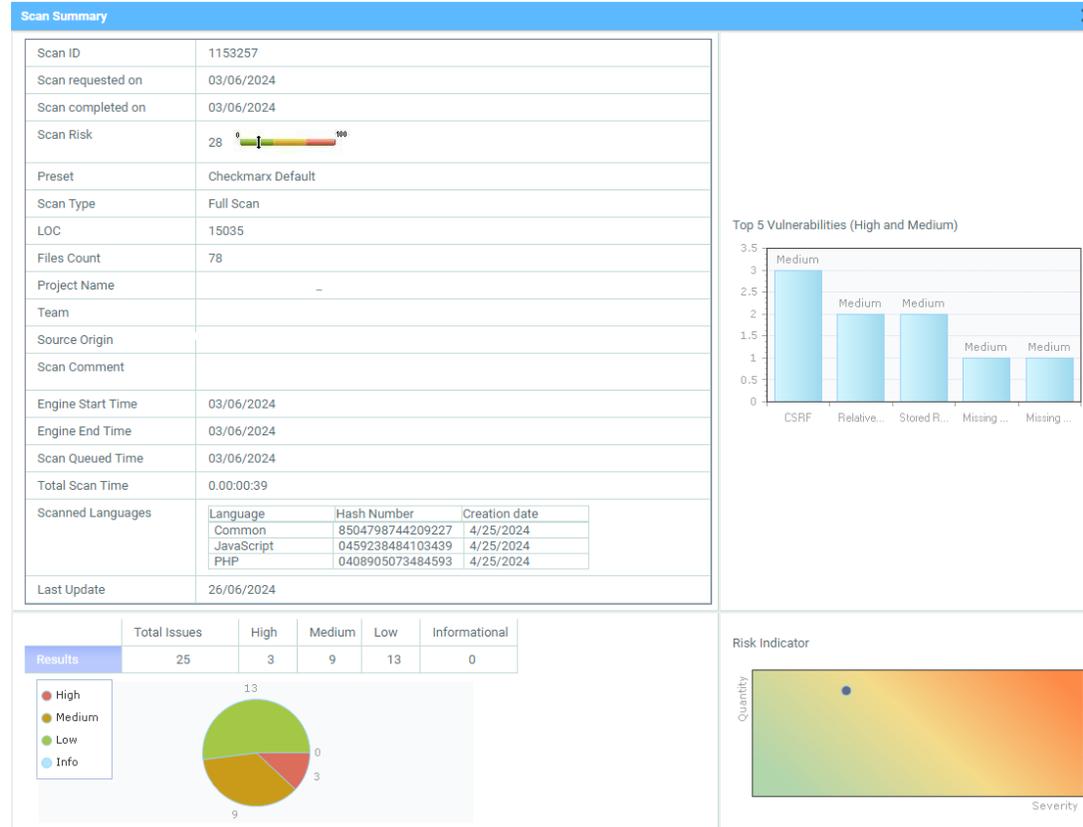
Partie 1:

A l'aide de l'outil Checkmarx. Des scans sont réalisés sur les applications web données. Par la suite celui-ci indiquera toutes les failles qui sont présentes sur ces applications.

	LAST SCAN DATE	TEAM	LOC	RISK LEVEL SCORE	HIGH VULNERABILITIES	MEDIUM VULNERABILITIES
	10/06/2024 18:55:28	CxServer\DR\LIM	12,009	(100)	188	176
	03/06/2024 10:23:15		730,773	(80)	47	178
	03/06/2024 11:07:17		27,499	(10)	0	0
	03/06/2024 11:35:27		91,219	(56)	31	292
	03/06/2024 13:48:30		42,826	(100)	20	23
	03/06/2024 13:54:13		74,363	(55)	5	77
	26/06/2024 10:33:17		15,042	(28)	3	9
	03/06/2024 16:20:14		22,710	(16)	3	3
	03/06/2024 16:28:15		18,971	(11)	0	4
	03/06/2024 16:30:15		12,714	(8)	0	4
	03/06/2024 16:39:01		516,597	(17)	0	5
	27/05/2024 10:20:42		17,808	(8)	0	2
	05/06/2024 13:10:30		110,231	(100)	197	54
	04/06/2024 08:14:15		243,490	(100)	198	59

Page size: 20

Pour chaque application Checkmarx détaillera chaque faille, Il nous donnera les statistiques et nous préciser si une faille est faible moyenne ou haute, Par la suite nous pouvons analyser les failles au niveau du code sources et proposer d'éventuelle corrections



Partie 2:

- A la fin de chaque scan, Checkmarx nous détaille toutes les failles de chaque application au niveau du code sources ce qui nous permet par la suite de nous même étudier chaque failles de chacunes des applications et de les corriger.

The screenshot displays the Checkmarx interface. On the left, a code editor shows PHP code for file extraction and scanning. Line 64, `$lstFiles = scandir($tempFolder);`, is highlighted. On the right, a data flow graph shows the variable `tempFolder` being passed through `scandir`, `lstFiles`, and `file` to `pathFile`. At the bottom, the 'Scan Results' panel shows a 'Low (7)' severity finding. The description states: 'Method `indexAction` at line 64 of `80v-main\src\Controller\ImportPieceJointeController.php` gets dynamic data from the `tempFolder` element. This element's value then flows through the code and is eventually used in a file path for local disk access in `indexAction` at line 75 of `80v-main\src\Controller\ImportPieceJointeController.php`. This may cause a Path Traversal vulnerability. Similarity ID: -458186165'. The interface also includes tabs for 'Results', 'Graph', 'Vulnerability Description', and 'Codebashing'.

```
51
52 // Extraction des fichiers
53 $zip = new ZipArchive;
54 $res = $zip->open($uploadFilePath, ZipArchive::CREATE);
55 if ($res === TRUE) {
56     $zip->extractTo($tempFolder);
57     $zip->close();
58 } else {
59     $error = "Erreur lors de l'ouverture du fichier compressé, avez-vous bien importé un fichier .zip ? Code " . $res;
60     goto end;
61 }
62
63 // Lecture des fichiers
64 $lstFiles = scandir($tempFolder);
65
66 // Parsing et vérif
67 $lstFilesParse = array();
68 foreach ($lstFiles as $file) {
69     $pathFile = $tempFolder . "/" . $file;
70
71     if (in_array($file, array(".", ".."))) {
72         continue;
73     }
74
75     if (!is_file($pathFile)) {
76         $error = "Le zip contient le dossier '" . $file . "', mais il ne doit contenir que des fichiers";
```

tempFolder
▼
scandir
▼
lstFiles
▼
lstFiles
▼
file
▼
file
▼
pathFile
▼
pathFile

Scan Results Severity
JavaScript
Low (7)

Method `indexAction` at line 64 of `80v-main\src\Controller\ImportPieceJointeController.php` gets dynamic data from the `tempFolder` element. This element's value then flows through the code and is eventually used in a file path for local disk access in `indexAction` at line 75 of `80v-main\src\Controller\ImportPieceJointeController.php`. This may cause a Path Traversal vulnerability. Similarity ID: -458186165

Results Graph Vulnerability Description Codebashing

