

## Table of Contents

|                                |           |
|--------------------------------|-----------|
| <b>Default Scan</b> .....      | <b>2</b>  |
| Kritik .....                   | 2         |
| Yüksek .....                   | 7         |
| <b>Scan Precision 3:</b> ..... | <b>8</b>  |
| Kritik .....                   | 8         |
| Yüksek .....                   | 9         |
| <b>Scan Precision 2</b> .....  | <b>10</b> |
| Kritik .....                   | 10        |
| Yüksek .....                   | 11        |
| <b>Scan Precision 1:</b> ..... | <b>12</b> |
| Kritik .....                   | 12        |
| Yüksek .....                   | 12        |
| <b>Quick Scan</b> .....        | <b>13</b> |
| Kritik .....                   | 13        |
| Yüksek .....                   | 14        |

# Default Scan

## Kritik

The screenshot displays a security scan interface with a dark background. At the top, there are five folder icons representing severity levels: Critical (99), High (90), Medium (20), Low (318), and All (527). To the right of these icons are buttons for 'AUDIT' and 'CLAIM'. Below the folder icons, a list of vulnerabilities is shown, each with a right-pointing chevron and a progress indicator in brackets. The vulnerabilities listed are:

- > Access Control: Database - [0 / 12]
- > Command Injection - [0 / 1]
- > Cookie Security: Cookie not Sent Over SSL - [0 / 3]
- > Cookie Security: HTTPOnly not Set - [0 / 5]
- > Credential Management: Hardcoded API Credentials - [0 / 8]
- > Cross-Site Request Forgery - [0 / 150]
- > Cross-Site Scripting: DOM - [0 / 16]
- > Cross-Site Scripting: Persistent - [0 / 2]
- > Cross-Site Scripting: Self - [0 / 2]
- > Denial of Service - [0 / 1]
- > Denial of Service: StringBuilder - [0 / 4]

> Dynamic Code Evaluation: Unsafe Deserialization - [0 / 1]

> Dynamic Code Evaluation: Unsafe XStream Deserialization - [0 / 1]

> File Disclosure: Spring - [0 / 1]

> Hidden Field - [0 / 22]

> HTML5: Form Validation Turned Off - [0 / 3]

> HTML5: Missing Content Security Policy - [0 / 2]

> HTML5: Overly Permissive Message Posting Policy - [0 / 1]

> Insecure Randomness - [0 / 17]

> Insecure Randomness: User-Controlled Seed - [0 / 1]

> Insecure Transport: External Link - [0 / 1]

> J2EE Bad Practices: JVM Termination - [0 / 1]

> J2EE Bad Practices: Threads - [0 / 2]

> Key Management: Hardcoded Encryption Key - [0 / 2]

> Log Forging - [0 / 9]

> Log Forging (debug) - [0 / 3]

> Mass Assignment: Insecure Binder Configuration - [0 / 11]

> Often Misused: File Upload - [0 / 10]

> Open Redirect - [0 / 9]

> Password Management: Empty Password - [0 / 1]

> Password Management: Hardcoded Password - [0 / 8]

> Password Management: Insecure Submission - [0 / 5]

> Password Management: Password in Comment - [0 / 7]

> Password Management: Password in HTML Form - [0 / 4]

> Password Management: Weak Cryptography - [0 / 2]

> Path Manipulation - [0 / 33]

> Path Manipulation: Zip Entry Overwrite - [0 / 1]

> Poor Logging Practice: Use of a System Output Stream - [0 / 1]

> Privacy Violation - [0 / 9]

> Privacy Violation: Autocomplete - [0 / 30]

> Privacy Violation: Heap Inspection - [0 / 1]

> Resource Injection - [0 / 6]

> Server-Side Request Forgery - [0 / 1]

> Spring Security Misconfiguration: Disabled Security Headers - [0 / 1]

> SQL Injection - [0 / 27]

> System Information Leak - [0 / 4]

> System Information Leak: External - [0 / 48]

> System Information Leak: Internal - [0 / 17]

> Trust Boundary Violation - [0 / 9]

> Unchecked Return Value - [0 / 4]

> Weak Cryptographic Hash - [0 / 1]

> XML Entity Expansion Injection - [0 / 3]

> XML External Entity Injection - [0 / 3]

## Yüksek

> Credential Management: Hardcoded API Credentials - [0 / 1]

> Insecure Randomness - [0 / 17]

> Insecure Randomness: User-Controlled Seed - [0 / 1]

> Mass Assignment: Insecure Binder Configuration - [0 / 11]

> Open Redirect - [0 / 2]

> Password Management: Empty Password - [0 / 1]

> Password Management: Hardcoded Password - [0 / 8]

> Path Manipulation - [0 / 16]

> Privacy Violation: Autocomplete - [0 / 30]

> Privacy Violation: Heap Inspection - [0 / 1]

> Server-Side Request Forgery - [0 / 1]

> SQL Injection - [0 / 1]

## Scan Precision 3:

### Kritik

- > Credential Management: Hardcoded API Credentials - [0 / 7]
- > Cross-Site Scripting: DOM - [0 / 16]
- > Cross-Site Scripting: Persistent - [0 / 2]
- > Dynamic Code Evaluation: Unsafe XStream Deserialization - [0 / 1]
- > HTML5: Missing Content Security Policy - [0 / 2]
- > Key Management: Hardcoded Encryption Key - [0 / 2]
- > Open Redirect - [0 / 7]
- > Password Management: Insecure Submission - [0 / 5]
- > Password Management: Password in HTML Form - [0 / 4]
- > Path Manipulation - [0 / 17]
- > Privacy Violation - [0 / 9]
- > SQL Injection - [0 / 24]
- > XML External Entity Injection - [0 / 3]



## Yüksek

> Credential Management: Hardcoded API Credentials - [0 / 1]

> Insecure Randomness - [0 / 17]

> Insecure Randomness: User-Controlled Seed - [0 / 1]

> Mass Assignment: Insecure Binder Configuration - [0 / 11]

> Open Redirect - [0 / 2]

> Password Management: Empty Password - [0 / 1]

> Password Management: Hardcoded Password - [0 / 8]

> Path Manipulation - [0 / 16]

> Privacy Violation: Autocomplete - [0 / 30]

> Privacy Violation: Heap Inspection - [0 / 1]

> Server-Side Request Forgery - [0 / 1]

> SQL Injection - [0 / 1]

# Scan Precision 2

## Kritik

> Credential Management: Hardcoded API Credentials - [0 / 7]

> Cross-Site Scripting: Persistent - [0 / 2]

> Dynamic Code Evaluation: Unsafe XStream Deserialization - [0 / 1]

> HTML5: Missing Content Security Policy - [0 / 2]

> Key Management: Hardcoded Encryption Key - [0 / 2]

> Open Redirect - [0 / 2]

> Password Management: Insecure Submission - [0 / 5]

> Password Management: Password in HTML Form - [0 / 4]

> Path Manipulation - [0 / 15]

> Privacy Violation - [0 / 9]

> SQL Injection - [0 / 24]

> XML External Entity Injection - [0 / 3]

## Yüksek

> Credential Management: Hardcoded API Credentials - [0 / 1]

> Insecure Randomness - [0 / 17]

> Insecure Randomness: User-Controlled Seed - [0 / 1]

> Mass Assignment: Insecure Binder Configuration - [0 / 11]

> Open Redirect - [0 / 2]

> Password Management: Empty Password - [0 / 1]

> Password Management: Hardcoded Password - [0 / 8]

> Path Manipulation - [0 / 16]

> Privacy Violation: Autocomplete - [0 / 30]

> Privacy Violation: Heap Inspection - [0 / 1]

> Server-Side Request Forgery - [0 / 1]

> SQL Injection - [0 / 1]

# Scan Precision 1:

## Kritik

The screenshot shows a security scan dashboard with a dark theme. At the top, there are five folder icons representing severity levels: Critical (20), High (68), Medium (12), Low (218), and All (318). To the right of these are three buttons: 'AUDIT', 'CLAIM', and 'SUPP'. Below this, a list of findings is displayed in blue bars with white text. The findings are:

- > Credential Management: Hardcoded API Credentials - [0 / 7]
- > HTML5: Missing Content Security Policy - [0 / 2]
- > Key Management: Hardcoded Encryption Key - [0 / 2]
- > Password Management: Insecure Submission - [0 / 5]
- > Password Management: Password in HTML Form - [0 / 4]

## Yüksek

The screenshot shows a security scan dashboard with a dark theme. At the top, there are five folder icons representing severity levels: Critical (20), High (68), Medium (12), Low (218), and All (318). To the right of these are three buttons: 'AUDIT', 'CLAIM', and 'SUPPRESS'. Below this, a list of findings is displayed in blue bars with white text. The findings are:

- > Credential Management: Hardcoded API Credentials - [0 / 1]
- > Insecure Randomness - [0 / 17]
- > Mass Assignment: Insecure Binder Configuration - [0 / 11]
- > Password Management: Empty Password - [0 / 1]
- > Password Management: Hardcoded Password - [0 / 8]
- > Privacy Violation: Autocomplete - [0 / 30]

# Quick Scan

## Kritik

- > Credential Management: Hardcoded API Credentials - [0 / 7]
- > Cross-Site Scripting: Persistent - [0 / 2]
- > Dynamic Code Evaluation: Unsafe XStream Deserialization - [0 / 1]
- > HTML5: Missing Content Security Policy - [0 / 2]
- > Key Management: Hardcoded Encryption Key - [0 / 2]
- > Open Redirect - [0 / 2]
- > Password Management: Insecure Submission - [0 / 5]
- > Password Management: Password in HTML Form - [0 / 4]
- > Path Manipulation - [0 / 15]
- > Privacy Violation - [0 / 9]
- > SQL Injection - [0 / 24]
- > XML External Entity Injection - [0 / 3]

## Yüksek

> Credential Management: Hardcoded API Credentials - [0 / 1]

> Insecure Randomness - [0 / 17]

> Insecure Randomness: User-Controlled Seed - [0 / 1]

> Mass Assignment: Insecure Binder Configuration - [0 / 11]

> Open Redirect - [0 / 2]

> Password Management: Empty Password - [0 / 1]

> Password Management: Hardcoded Password - [0 / 8]

> Path Manipulation - [0 / 16]

> Privacy Violation: Autocomplete - [0 / 30]

> Privacy Violation: Heap Inspection - [0 / 1]

> Server-Side Request Forgery - [0 / 1]

> SQL Injection - [0 / 1]