Introduction to the OWASP Top 10 – 2021

# Risk A5: Security Misconfiguration

## Key Concepts

### Key Concept 1: Security Control

- An information system safeguard or countermeasure
- Designed to protect confidentiality, integrity, or availability

### Key Concept 2: Misconfiguration

- Introduces common security vulnerabilities
- Occurs because the configuration has not been hardened
- Result of keeping default settings

Security Misconfiguration is a broad category and often referred to as the “catchall” of the OWASP Top 10 because there are many different types of misconfigurations which can lead to many different types of vulnerabilities

Additional Information

A security control is a safeguard (or countermeasure) of an information system, that is designed and deployed to protect the confidentiality, integrity, or availability of information.

In application security, misconfiguration introduces vulnerabilities. This can occur because the configuration has not been hardened and sometimes, is a result of keeping default settings. An example of this is having the default username and password within your application. Think of a default user account for an administrator with username *admin* and password *Password1*. Default username password combinations are classic cases of security misconfiguration.

Recall A4 was also a broad category because there could be many designs which are insecure.

## Definition

Failing to implement the necessary controls to secure the configurations of your application.

- Application is missing the necessary security hardening
- Default accounts are still active
- Unnecessary features are installed and enabled

- Also includes poorly documented configuration

Additional Information

The definition of A5 of 2021 – Security Misconfiguration – is failing to implement the necessary controls to secure the configurations of your application. Common reasons that cause this risk involve your application missing the necessary security hardening, default accounts being still active, or because unnecessary features are installed and enabled.

Overall, configuration that puts your systems and data at risk falls in the category of A5. This risk also includes poorly documented configuration. If you are making configuration changes without understanding what you are doing, you are probably about to fall victim to A5, namely security misconfiguration.

# Example

Example using Apache Struts, an open-source framework very popular when building Java web applications.

## Bad Example

```
<global-exceptions>
 <exception key="global.error.invalidLogin" path=""
scope="request" type="InvalidLoginException" />
</global-exceptions>

<global-forwards>
 <forward name="sign-in" path="Sign-in.jsp" />
</global-forwards>
```

## Good Example

```
userAccess   <global-forwards>
 <forward name="sign-in" path="/Sign-in.jsp" />
</global-forwards>
```

Additional Information

As a bad example, of what not to do, by having an empty path, or a path that does not begin with a “/”, we have not specified which page is the correct resource to serve in the case of an error or a forward.

As a good example, we are specific in the Struts configuration of the exact path necessary to handle the request. simple example where a forward “/” can make all the difference.

As a rule of thumb, we want to be checking that our configuration does not have any such bad syntax. Ideally, we want these checks before we deploy into our production environment. Our target is to have a

repeatable process to check configuration for errors. This process will be effectively checking for application security misconfigurations before they happen.

## Challenges

- A small configuration change can introduce very serious vulnerabilities
- People do not read the manual – **RTM!**
- Know enough to understand the deployment environment and frameworks you use
  - Try to deploy configurations which are not secure to understand what good and bad looks like
  - This will allow you to build checks in your production environments, so that configurations are checked before any vulnerabilities occur

Additional Information

We now understand how security misconfigurations happen, let us look at why they a common issue.

Sometimes a small configuration change can introduce very serious vulnerabilities. Security misconfiguration can span anything from password length to file permissions to access control and a lot more.

Another reason as to why security misconfigurations are common is people do not read the manual. You do not need to be an expert in every framework you use.  Make sure you know enough to be able to understand the deployment environment and frameworks you use.

## Best Protection Strategies

### VARKAS

**Verify** configurations
**Assume** insecure if you cannot verify
**Read** existing hardening and security guides
**Know** your frameworks and libraries
**Apply** security settings available to you
**Study** to know enough about your platforms

Additional Information

Above you have some of the best protection strategies against A5 of the Top 10 – Security Misconfiguration