

[← Previous](#)

Q49 - Servlet Security

[Next →](#)

49 / 67

## Q49 - Servlet Security

Considering Servlets 3.0 Security, which statements are true:

- a. Security constraints can be managed through Deployment Descriptor
- b. Security constraints can be managed programmatically, using `ServletRegistration.Dynamic#setServletSecurity(-)` method
- c. Security constraints can be managed using `@WebServletSecurity` annotation
- d. The `@WebServletSecurity` annotation have three attributes: `value`, `httpMethodConstraints` and `rolesAllowed`.

[Hide answer](#)

a, b

**Reference:** page 122, 13.4 "Programmatic Access Control Annotations"

**Explanation:** All three ways (DD, programmatically, annotations) of managing security constraints are **valid**, but the annotation name is `@ServletSecurity` - **not** `@WebServletSecurity`. Hence, the a and b are correct and c is incorrect.

The `@ServletSecurity` annotation has two attributes - `value` and `httpMethodConstraint`.

The `rolesAllowed` attribute is a part of `@HttpConstraint` or `@HttpMethodConstraint`, not the `@ServletSecurity`.