


## QUIZ

Complete the statement by selecting the correct answer.

 **Access controls** enforce web application security policies that prevent users from acting outside of their intended permissions.



You got it!

Determine the key aspect that is overlooked in this broken access control scenario:

A web application allows non-admin users to access an administrator account management page simply by appending `/adminPortal` to the end of the site URL.

Example: <https://www.yourbankaccount.org/adminPortal>

Permission Check



Correct! A simple permission check for the admin portal site will prevent access to other pages of the site from users without the appropriate permission..

Data Loss Prevention tools

Multi-Factor Authentication

Determine what needs to be implemented to prevent the below scenario:

The company SuperCoolWebsite Inc. has recently launched its company website. Unbeknownst to the company, the website has an exposed vulnerability at <http://www.supercoolwebsiteinc.com/supercoolimage.jsp?file=content>.

By appending `../../../../etc/passwd` to the end of the filename in the URL, an attacker may access a different file in a different directory on the host system.

Access Controls



Congratulations! This is correct. Strong access controls would prevent any unauthorized user from accessing areas of a web application or hosting system.

Multi-Factor Authentication (MFA)

Intrusion Prevention System

Splunk

Fill in the correct answer.

Access controls in web applications rely on three key aspects: ☒ authentication, authorization, and permissions checks.



You got it!

Complete the sentence below:



☒ Access Controls enforce web application security policies that prevent users from acting outside of their intended permissions.



You got it!

True or False:

When access controls are broken in a web application, attackers may identify the gap in access controls to exploit the web application or underlying system.

False, when access controls are NOT broken in a web application, attackers may identify the gap in access controls to exploit the web application or underlying system.

True, when access controls are broken in a web application, attackers may identify the gap in access controls to exploit the web application or underlying system.



Good work!

True or False:

Broken Access Control can lead to other vulnerabilities being exploited.

True, Broken Access Control can lead to other vulnerabilities being exploited.



Good Job! Broken Access Control lends itself well to opening up new opportunities for attackers.

False, Broken Access Control can NOT lead to other vulnerabilities being exploited.

Fill in the correct answers.

Failures in access controls will lead to unauthorized access to information and may allow the unauthorized ☒ modification or ☒ destruction of data and critical systems.



You got it!

