Missing Functional Level Access Control

OWASP Web App Top 10

What is it?

"Missing Functional Level Access Control" occurs when users can perform functions they have not been authorized for or when resources can be accessed by unauthorized users.

What could happen?

An attacker could forge requests in order to access functionality without proper authorization. An attacker could gain access to the administrative panel of your application. An employee from the sales department could view information from the financial department.

What causes it?

Functional level access control is missing when access checks have not been implemented or when a protection mechanism exists but is not properly configured.

How to prevent it?

Protect all business functions using a role based authorization mechanism, server side. Authorization should be implemented using centralized authorization routines. Deny access by default.

Missing Functional Level Access Control

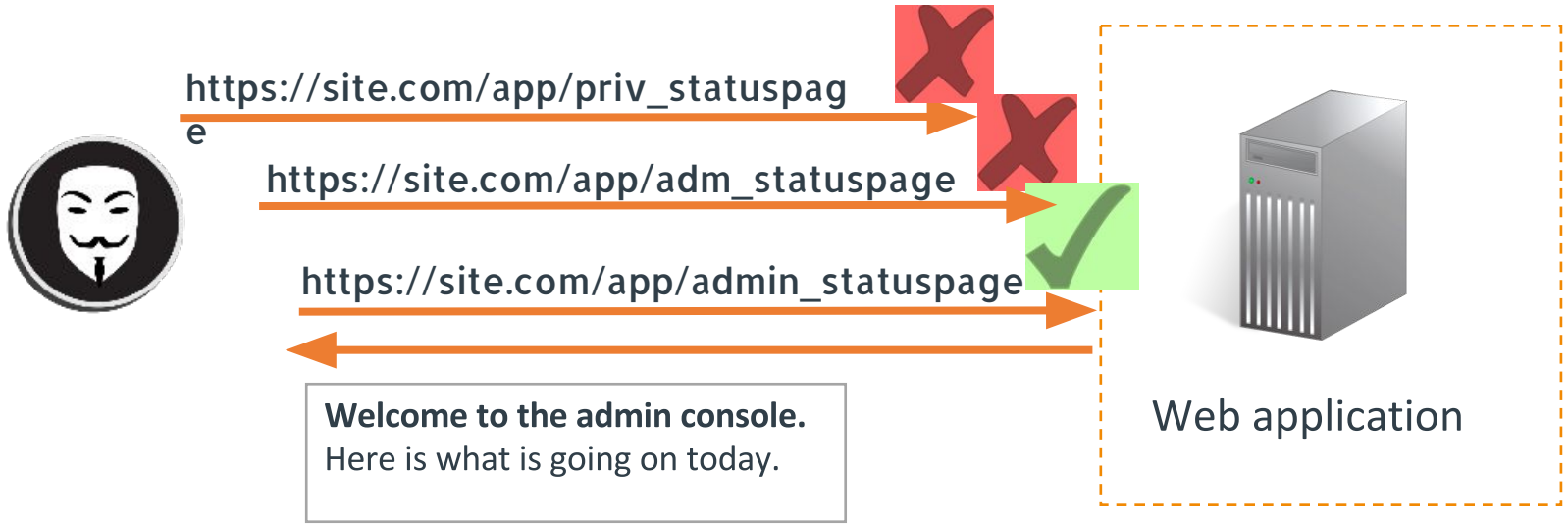
Understanding the security vulnerability

Force browsing URLs

An attacker is an authenticated user of a site. He's trying to gain elevated access to the application.

By either guessing or brute forcing URL's he is eventually able to find an unprotected administrative page.

He browses to this page and can access a status page that is only intended for administrators to view.



Missing Functional Level Access Control

Understanding the security vulnerability

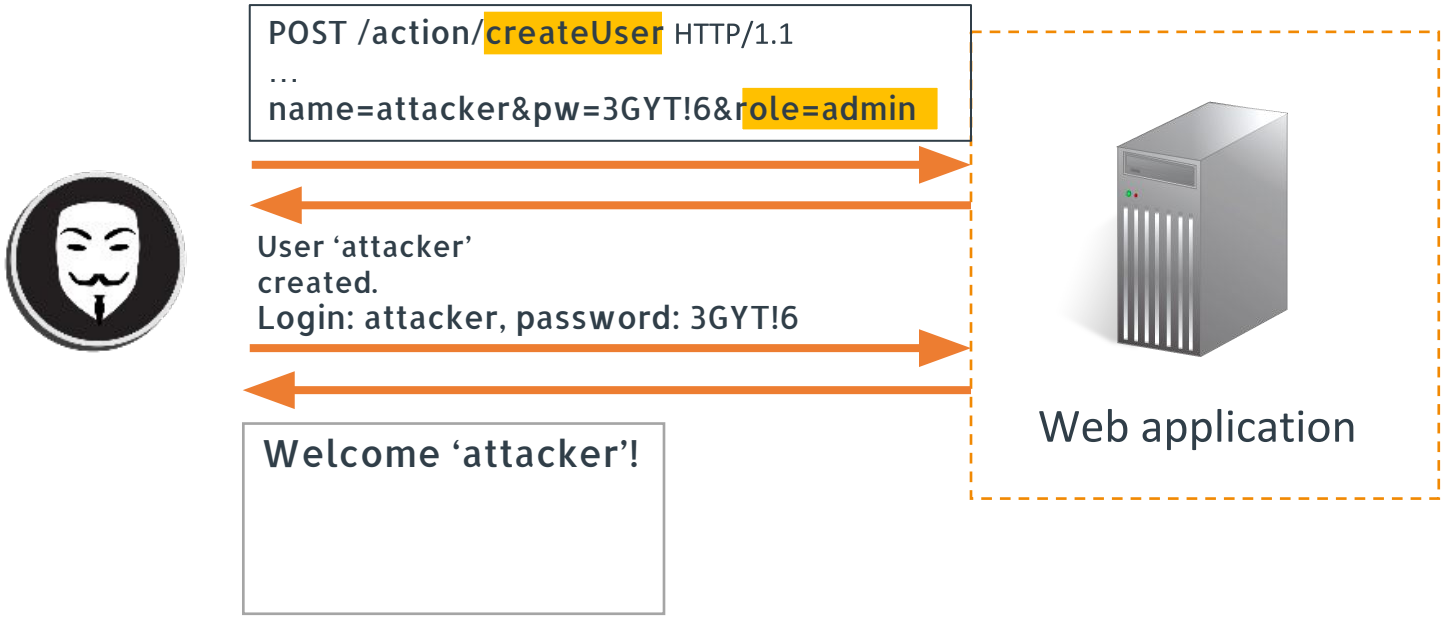
Unauthorized functions

An attacker is an authenticated user of a site. The site uses a popular framework.

Knowing the framework, the attacker crafts a request to create a new user with elevated permissions.

Since the 'createUser' function is not properly protected by control checks, the request succeeds and a new user is created.

The attacker logs in using the credentials of the newly created admin user. He steals all the customer data.



Missing Functional Level Access Control

Realizing the impact

Accounts could be taken over, including privileged ones. With a stolen account, an attacker could do anything the victim could do.

Sensitive end-user (customer) data could be stolen, leading to reputational damage and revenue loss.

A stolen administrator account could lead to disruption of the website, causing loss of customers and revenue.

Missing Functional Level Access Control

Preventing the mistake

All business functions should be authorized.

Implement authorization using a role based mechanism.

Use centralized authorization routines.
Easy to use external modules.

Deny access by default.
see also “Least Privilege”

Perform access control, server side.