wib

OWASP API6:

Mass Assignment

OWASP top 10

The process of simultaneously assigning values to several variables or object characteristics is known as "mass assignment." Data objects in API requests may have many different properties. Client-side features should be able to alter some properties directly (such as name or address), but not others (such as an "is_admin" flag) should not. Changing this flag might give an attacker admin rights and compromise all systems. Mass assignment typically happens when an API automatically converts client-provided parameters into internal object properties without filtering.

How Hackers Exploit It

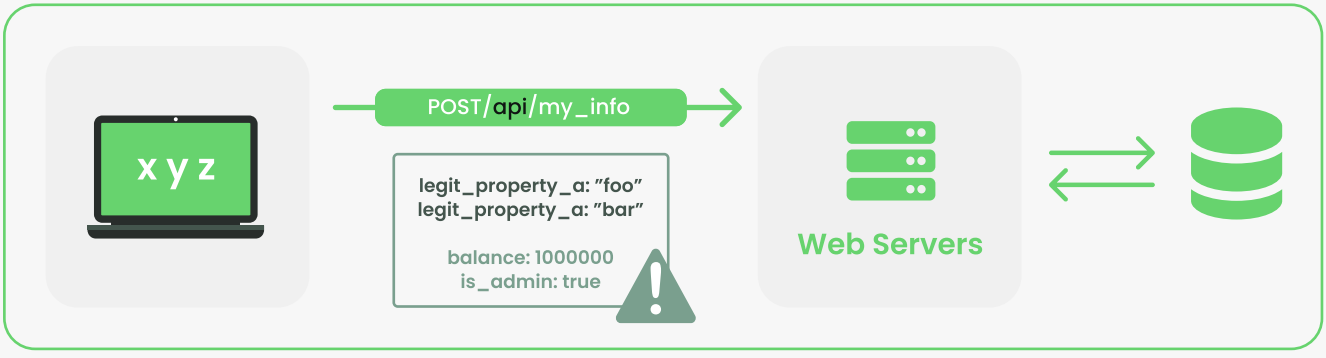
Suppose a user can edit their basic profile information using an application. This process calls an API.

PUT /api/users/my_profile
with the following JSON object:
{"Name":"jack","Gender":"male"}
GET /api/v1/users/my_profile

However, the request includes an additional balance property:
{"Name":" jack"," Gender":" male", "Amount": 1000}

This vulnerability allows an attacker to repeat the request, but this time modifying the additional attribute, resulting in the payload:
PUT /api/users/my_profile
{"Name":" jack"," Gender":" male", "Amount": 999999}

As a result, the attacker assigns new values to the user record and steals money by exploiting the mass assignment vulnerability.



Why You Should Care

An attacker who takes advantage of mass assignment vulnerabilities can illegitimately change object properties. Data manipulation is the most basic vulnerability; for example, a user (not an attacker) could modify his age. In our case, an attacker may get illegal funds and do direct financial harm to a company. However, an experienced attacker might also gain admin access and compromise the entire system's data.

Traditional Tools Will Not Protect You

Traditional security controls, like WAFs and API Gateways, have difficulty identifying whether the user utilized the PUT method to submit additional requests. This API request seems regular to these traditional controls. As threats become more complicated and sophisticated, these tools miss attacks that target the logic of APIs. They do not have enough context to realize that this person is not an administrator and should not have access to these extra options.

How to Combat Mass Assignment Threats

You must do four things to protect your APIs from mass assignment threats:

1. Avoid routines that automatically connect a client's input to code variables or internal objects if possible
2. Only add attributes to the allowlist that the client should be able to modify
3. Use built-in features to create a blocklist of properties that clients cannot access
4. Explicitly define and enforce schemas for the input data payloads, if relevant

In the example above, an API security solution in production will set a baseline for this API and recognize that this API typically does not change the money field. It could then flag the activity as an attack.

How Wib Can Help You

Wib is a full-lifecycle API security platform, defending against API security threats. The platform ensures comprehensive protection across the entire API software lifecycle from development to testing to production.

Wib utilizes state-of-the-art proprietary AI and ML to analyze millions of requests in real-time. It provides complete visibility of existing APIs, with actionable insights and comprehensive protection across the entire lifecycle. It learns your APIs inside and out and can provide complete visibility of your existing APIs, analyze their integrity, identify vulnerabilities, and detect attacks in real-time.

If you are building or using APIs in your applications (and you probably are), **sign up for a demo to see Wib in action and learn more.**