SECURE CODE

WARRIOR

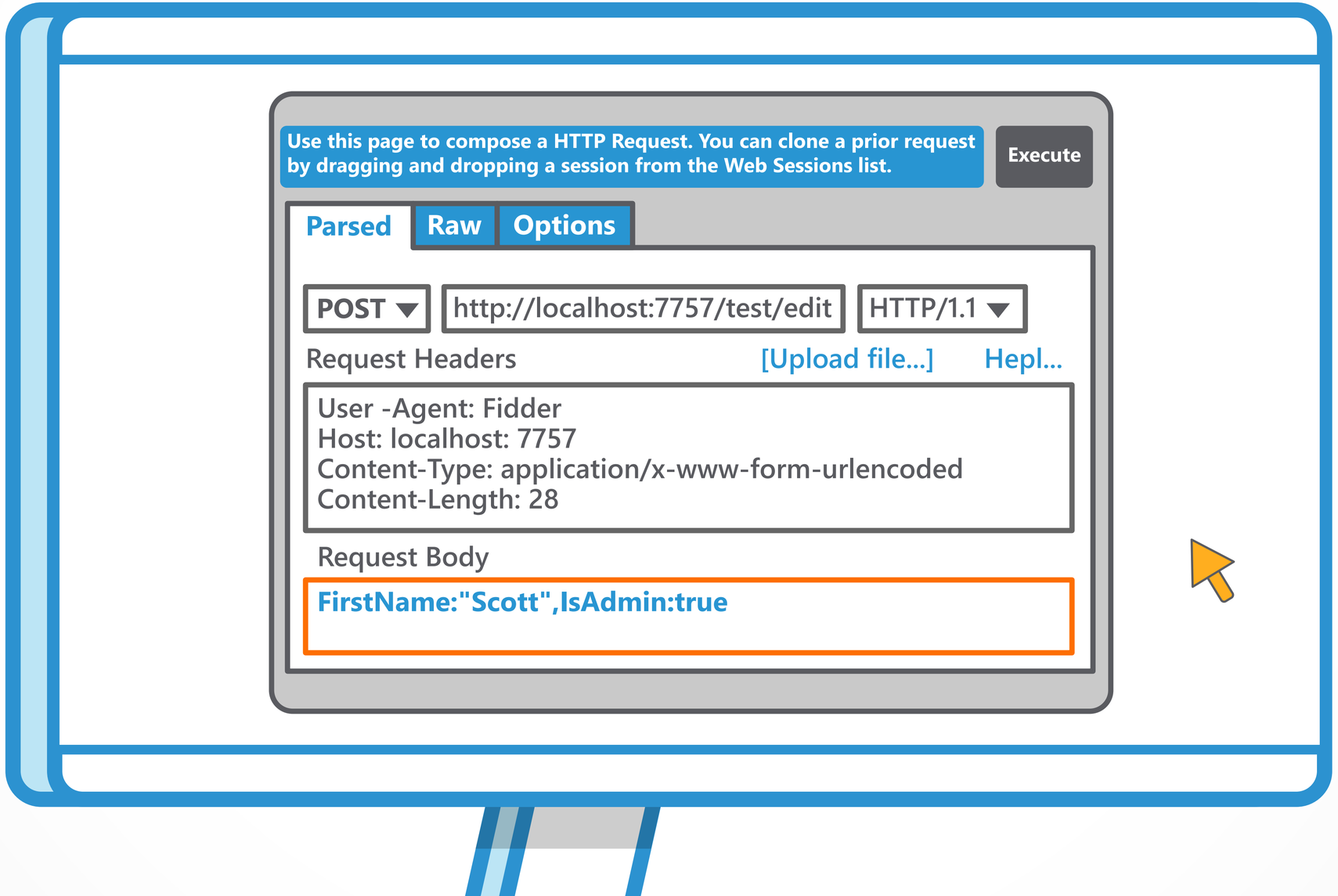
MASS ASSIGNMENT

We'll go through

some causes and preventions of vulnerabilities in this category.

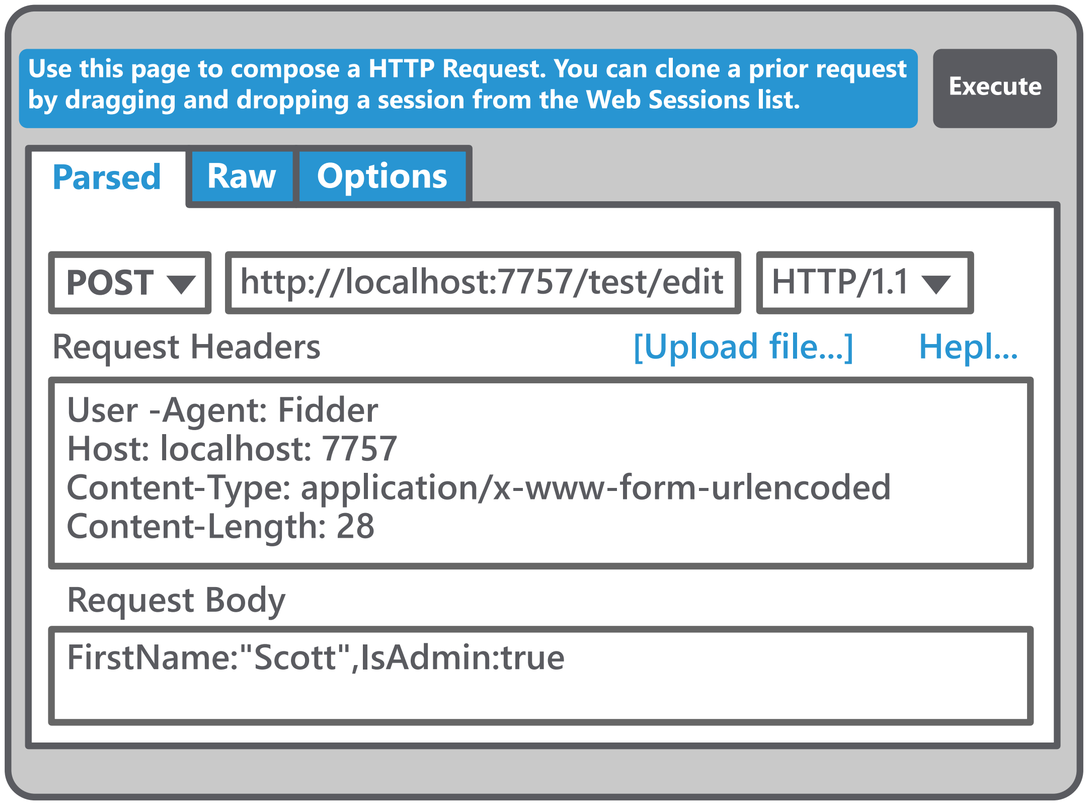
WHAT DO WE MEAN BY MASS ASSIGNMENT?

Mass Assignment is a vulnerability in which API endpoints do not restrict which properties of their associated object can be modified by the user.

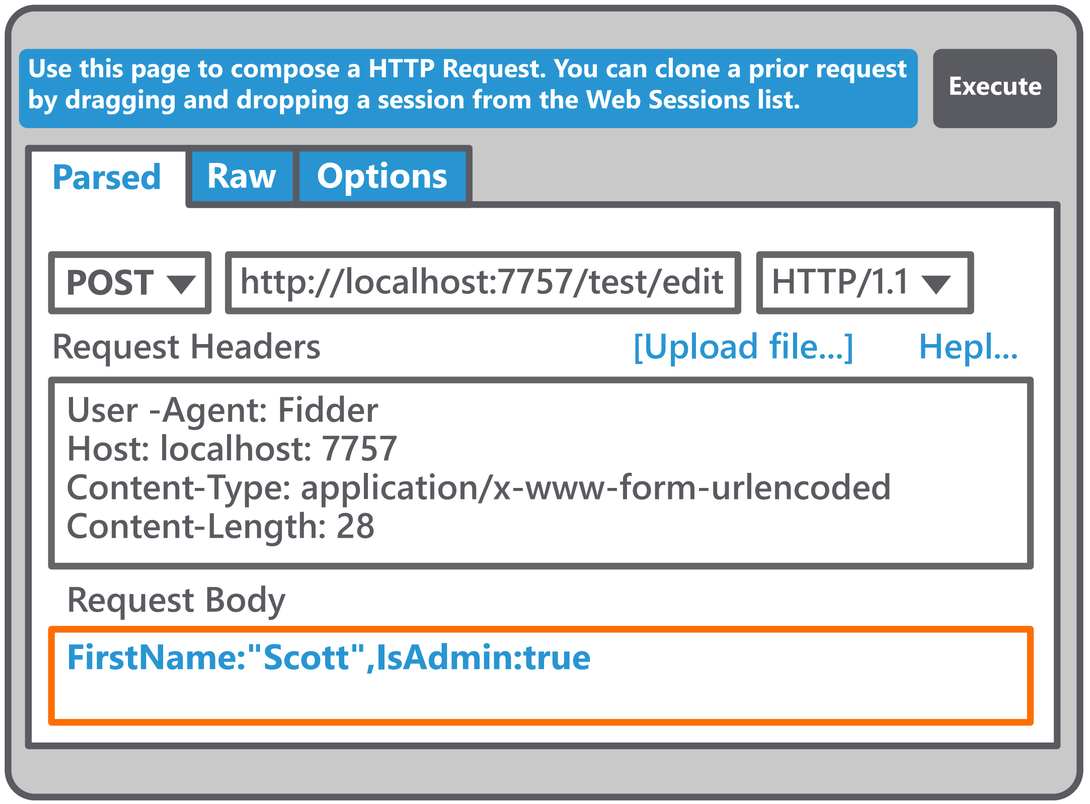


HOW CAN MASS ASSIGNMENT VULNERABILITIES OCCUR?

Mass Assignment vulnerabilities can occur when the object represented within the HTTP request is bound directly to the data model used for storage,



but fails to distinguish between fields that should be assignable and immutable.

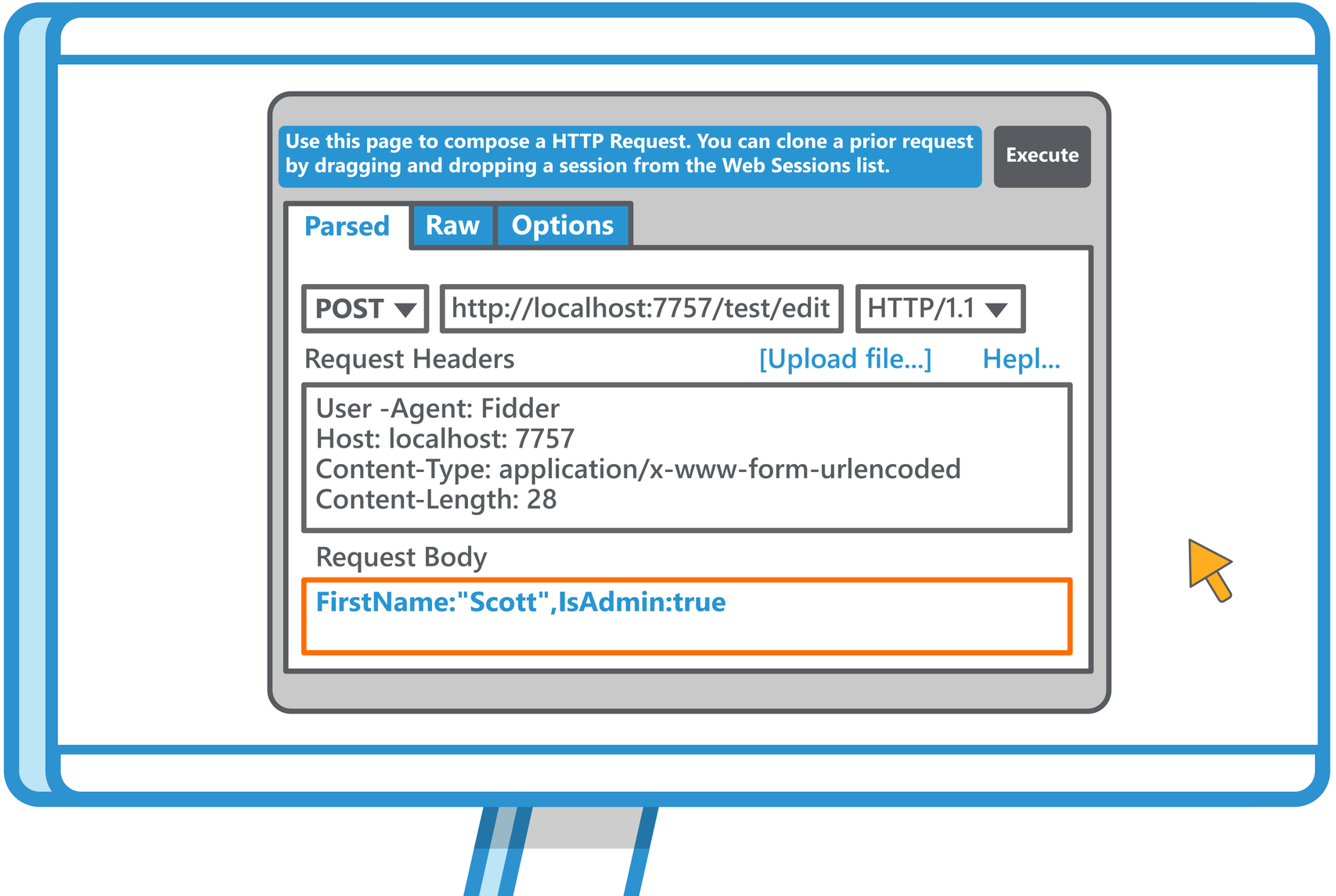


THIS CAN HAPPEN AUTOMATICALLY USING THE RECOMMENDED DEFAULTS IN SOME FRAMEWORKS OR AS A CONSCIOUS DECISION OF THE DEVELOPER THEMSELVES FOR A PARTICULAR SITUATION.

LET’S LOOK AT AN EXAMPLE

A hacker notices that the application is using the same endpoint to retrieve and update user details.

Seeing that their retrieved user also includes information about their role, they try adding that field to their update request.



The Server accepts all the fields, updating the hacker's role.

To prevent Mass Assignment function vulnerabilities, developers should:

- Parse the request values rather than binding directly to an object.
- Use a reduced Data Transfer Object rather than binding directly to an object.
- Ensure that sensitive properties are blacklisted or only safe properties are whitelisted for direct object binding.

Congratulations, you have now completed this module!

SECURE CODE
WARRIOR

www.securecodewarrior.com