TURKISH TECHNOLOGY

Mass Assignment

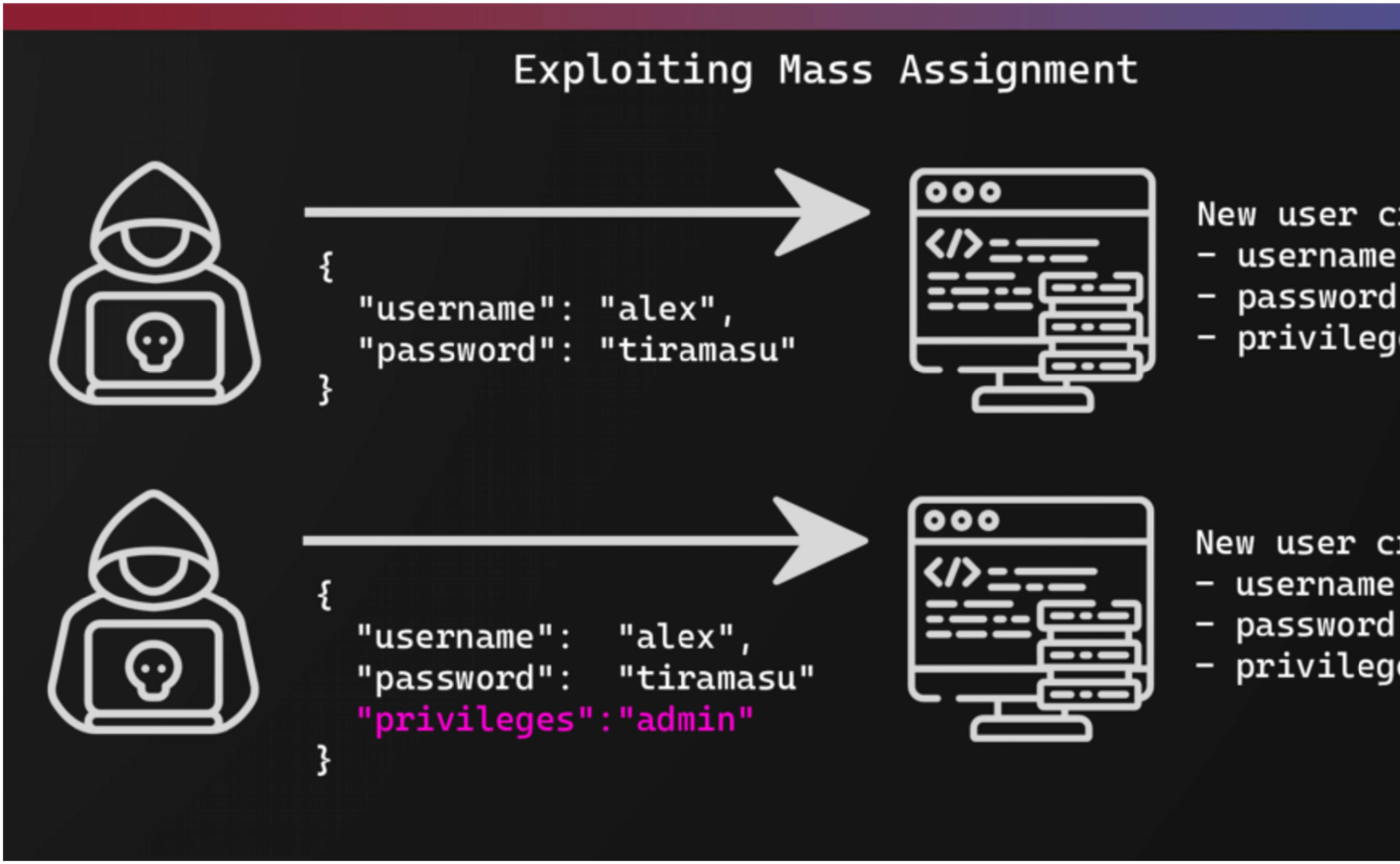
Mass Assignment Zafiyeti

Mass assignment zafiyeti **auto-binding** olarak da bilinir.

Yazılım framework'leri request parametrelerini internal bir nesnedeki alanlara
olarak bağladığında ortaya çıkar.

Mass assignment zafiyeti developer'ın bind etmeyi istemediği parametreler
nesnedeki alanlarla eşleşmesine sebep olur.

Mass Assignment Zafiyeti



Mass Assignment Vulnerability

https://portswigger.net/web-security/api-testing/lab-exploi
assignment-vulnerability

Server-side Template Injection Önleme

DTO (Data Transfer Object) kullanılarak. İşlem ve rol bazında ayrıştırmalar ile katmanlı şekilde güvenli nesneler ile request bind işlemi yapılabilir.

```
public class UserRegistrationFormDTO{

private String name;
private String password;
private String email;


//Not: is Admin alanı mevcut değil

//Getters & Setters

}
```

Server-side Template Injection Önleme

Tek nesne kullanıldığında binder üzerinden beyaz liste ya da kara liste belirleni
bind işlemi için kısıtlamalar getirilebilir.

```
@Controller

public class UserController
{
@InitBinder
public void initBinder(WebDataBinder binder, WebRequest request)
{
    binder.setAllowedFields(["userid","password","email"]);
}

...

}
```

```
@Controller
public class UserController
{

@InitBinder
public void initBinder(WebDataBinder binder,
{
    binder.setDisallowedFields(["isAdmin"])
}
```