A CSRF token in Django is a security feature that helps protect you while using a website. It acts like a special code that ensures the actions you perform on the website are legitimate and not coming from someone else trying to do harm. This way, Django makes sure your interactions on the website are safe and secure.

Suppose you have a Django view that handles a form submission. You want to make sure that the form is protected from CSRF (Cross-Site Request Forgery) attacks. To do this, you can use {% csrf_token %} template tag.

```html
<form  method="post">
    {% csrf_token %}
    {{form.as_p}}
    <input type="submit" value="submit">
</form>
```

The **{% csrf_token %}** template tag generates a hidden input field containing the CSRF token. When the form is submitted, the token is sent along with the data. Under the hood django checks if the token you sent matches the one it gave you at the beginning. To summarize - the CSRF token acts as an additional security layer to keep your interactions with the website safe.