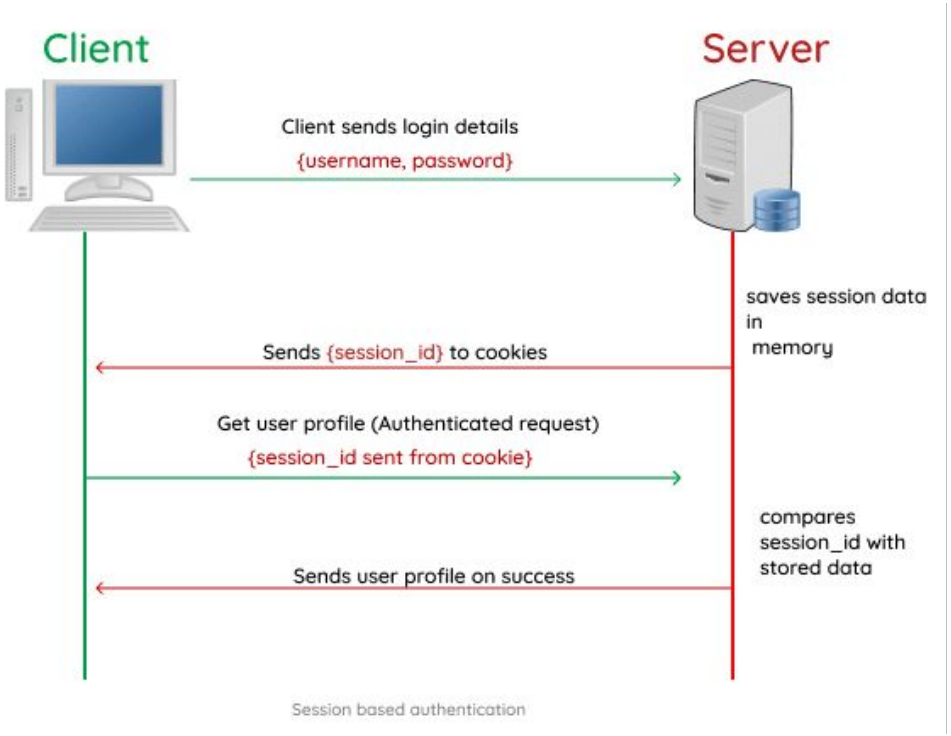
Cross Site Request Forgery

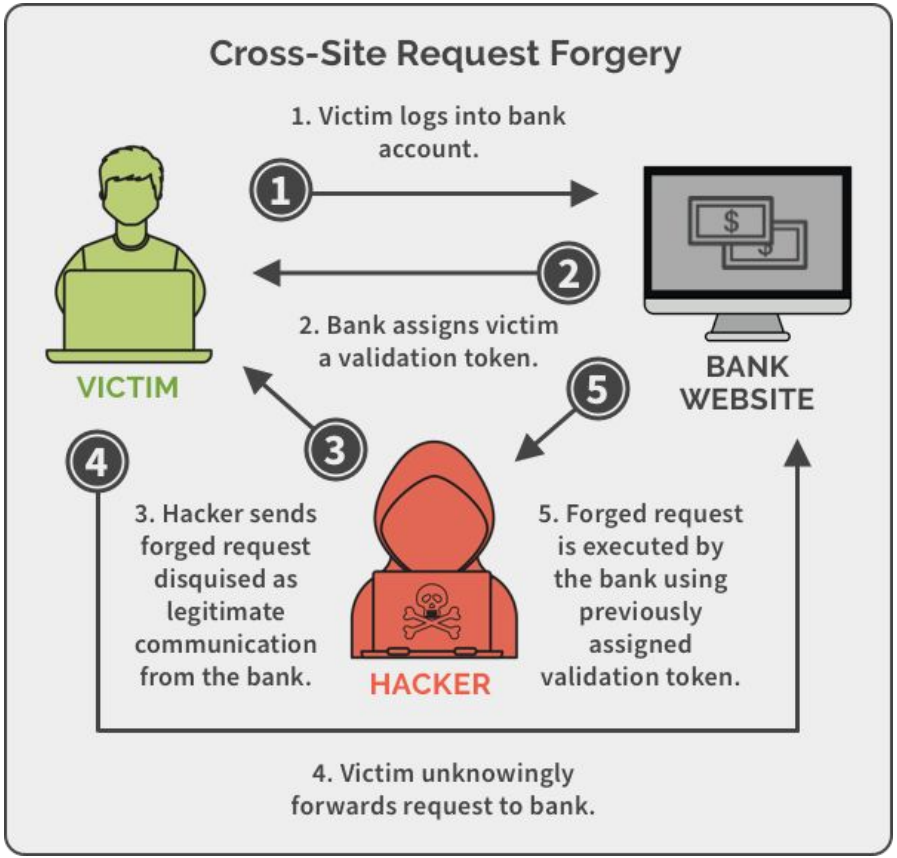
CSRF

A vulnerabilidade



Como funciona

Explora a validação de requisições do sistema.



Como funciona

Para realizar o ataque, o hacker poderia simplesmente enviar uma mensagem ou e-mail para a vítima com um link de uma imagem ou de algum site que, quando fosse aberto, disparasse requisições para a aplicação.

Essa é a ideia por trás do ataque CSRF, que acaba sendo realizado por um usuário legítimo de uma aplicação Web que nela está autenticado e tem permissão de acesso às suas funcionalidades.

Como proteger uma aplicação?

O único jeito de proteger a aplicação é criando algum mecanismo que consiga diferenciar as requisições verdadeiras, ou seja, aquelas que são disparadas pelas páginas da própria aplicação, das requisições forjadas, ou seja, aquelas que forem feitas a partir de páginas falsas que não pertencem à aplicação.

Tokens de segurança!

Exemplo

```
<form action="processos/cancelar" method="post">
    <input type="hidden" name="processo.id" value="57">

    <label for="data">Data do Cancelamento:</label>
    <input id="data" name="processo.cancelamento.data">

    <label for="justificativa">Justificativa:</label>
    <textarea id="justificativa"
        name="processo.cancelamento.justificativa"></textarea>

    <input type="submit" value="Gravar">
    <a href="processos">Voltar</a>
</form>
```

```html
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>Document</title>
</head>
<body>
    <form
        action="http://www.tribunalcdc.com.br/processos/cancelar"

        method="post">
        <input type="hidden" name="processo.id" value="57">
        <input name="processo.cancelamento.data">
        <input name="processo.cancelamento.justificativa">

        <input type="submit" value="Gravar">
    </form>
</body>
</html>
```