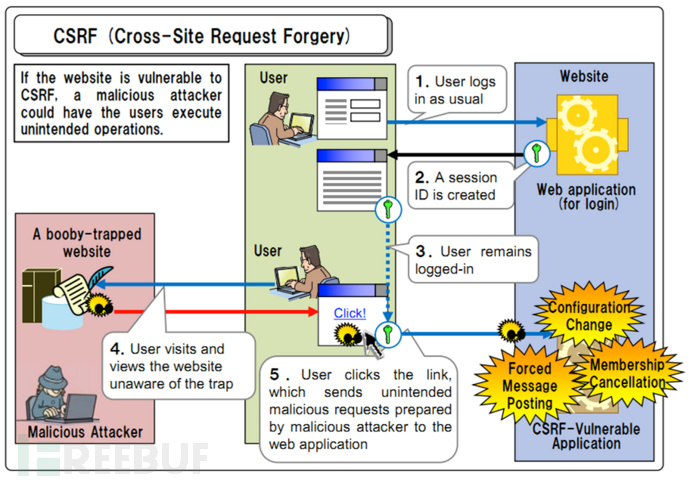
# 简介

## 什么是 CSRF？

CSRF，全称跨站伪造请求(Cross-site request forgery)，也称为 one click attack/session riding，还可以缩写为 XSRF。

通俗的说就是利用被害者的身份去发送请求！

## CSRF 原理



示例

http://www.a.com/del?id=3333 删除id为3333的文章（登录后可操作）

http://www.b.com/csrf.html

<img src='http://www.a.com/del?id=3333'>

浏览器的 Cookie 保存机制

Session Cookie，浏览器不关闭则不失效

本地 Cookie，过期时间内不管浏览器关闭与否均不失效

## CSRF 与 XSS 的区别

XSS：利用对用户输入的不严谨然后执行JS语句

CSRF：通过伪造受信任用户发送请求

CSRF 可以通过 XSS 来实现

# 攻击方式

## HTML CSRF

通过 HTML 元素发起 CSRF 请求

HTML CSRF 可以发起 GET 请求的标签

<link href=''>

<img src=''>

<frame src=''>

<script src=''>

<video src='’>

Backgroud:url('')

## JSON HiJacking

构造自定义的回调函数

http://www.b.com/csrf.html

<script>

function hijack(data){console.log(data)};

</script>

<script src='http://www.a.com/json?callback=hijack'>

## Flash CSRF

通过 Flash 来实现跨域请求

import flash.net.URLRequest;

function get(){

var url = new URLRequest('http://a.com/json?callback=hijack');

url.method='GET';

sendToURL(url);

};

# 防御

## 通过验证码进行防御

## 检查请求来源

## 增加请求参数 token