第四讲 CSRF攻击

陈伟
Email: chenwei@njupt.edu.cn
Tel: 18951896489

CSRF攻击

- 跨站请求伪造（Cross-Site Request Forgery，CSRF）是指HTTP用户端发出的请求被伪造。
- 用户端和服务器端使用HTTP协议进行交互
- 利用请求-响应的方式
- 完全不同于XSS攻击
  - XSS攻击侧重于获取用户的权限和信息（如何将恶意代码嵌入用户的html页面，让目标浏览器执行恶意代码）
  - CSRF攻击侧重于伪造特定用户的请求，欺骗服务器（是恶意代码的一种形式）

举例：GET请求类型的CSRF

<a href="">的含义就是刷新跳转原网页

- 这是最简单的CSRF攻击。例如，您收到一封包含以下内容的电子邮件：

```
<a href="http://bank.com/transfer?account_number_from=123456789
&account_number_to=987654321&amount=100000">View my
Pictures!</a>
```

- 如果用户仍然登录在bank. com网站，此简单的GET请求将从一个帐户向另一个帐户转账。
  - 当然，在大多数情况下，这不会成功。网站可能有多个控件来审核该请求。

CSRF攻击的三个条件

- 用户处于登录状态
- 伪造的链接与正常应用请求链接一致
- 后台未对用户业务开展的合法性做效验

CSRF漏洞利用场景

短链接是对原来冗长的网址的一种“包装”和“美化”，在保证目的网页不被改动的状况下，使得冗长的网址显现的更为简短和美观，或者使得品牌的信息更为突出。

- 利用条件比较苛刻，但危害巨大
- 管理员：在管理员不知情的情况下，使用管理员身份发起重要的业务请求
  - 添加帐号
  - 删帖子
- 个人用户：结合存储型XSS，在当前用户页面上嵌入攻击伪造链接，增加用户点击的可能性
- 管理系统：部分管理系统为了方便用户，可以实现参数调整，如果CSRF伪造管理员的高危功能管理，会造成非常大的危害

针对CSRF的防护方案1

- 原因：对当前用户身份的验证不足而造成的
- 思路：为关键业务添加合理的验证方式
- 1 添加中间环节：攻击者只能仿冒用户发起请求，但是不能接收到服务器的响应内容
  - 添加验证过程：弹窗要求用户确认
  - 添加验证码：在关键流程点使用，注意用户体验

针对CSRF的防护方案2

- 2 验证用户请求合法性
- 保证当前请求为用户本人
  - 验证referer
    - 验证请求来源的方式
  - 利用token
    - 利用token识别当前用户身份的真实性
    - 攻击者无法获取当前用户的token

token 和 cookie 区别
cookie 是 http 规范，token 是自定义传递的。
cookie 自动被浏览器存储，下一次请求时便会带上，而 token 需要自己存储在浏览器，下一次请求时再请求头中带上。为了防止csrf，Token必须为一次性，且有较强的随机性

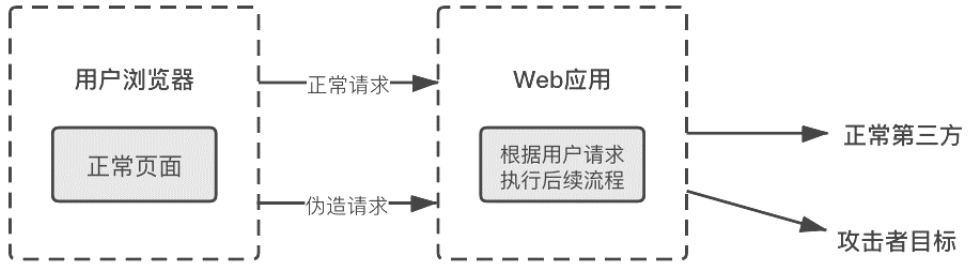
```
function token_start() {
$_SESSION['token']=md5(rand
(1,10000));
}

If(isset($_POST['test'])){
  if(!valid_token()){
       echo "token fail";
   {else{
       echo 'success';
} }
```

SSRF攻击

- 服务器端请求伪造（Server Side Request Forgery, SSRF）是另一种服务器端请求伪造的形式
  - 攻击者可构造有服务器端发起请求的安全漏洞
- Web应用中，存在着大量需要由服务器端向第三方发起请求的业务
  - 例如：天气显示功能
  - 用户请求包含恶意的参数信息
  - 服务器并没有对参数的合法性验证

SSRF攻击

- 相比XSS，SSRF可以执行一些在用户侧无法实现的效果
  - 内网探测
  - 加载特定图片
  - 加载特定文件
  - ……



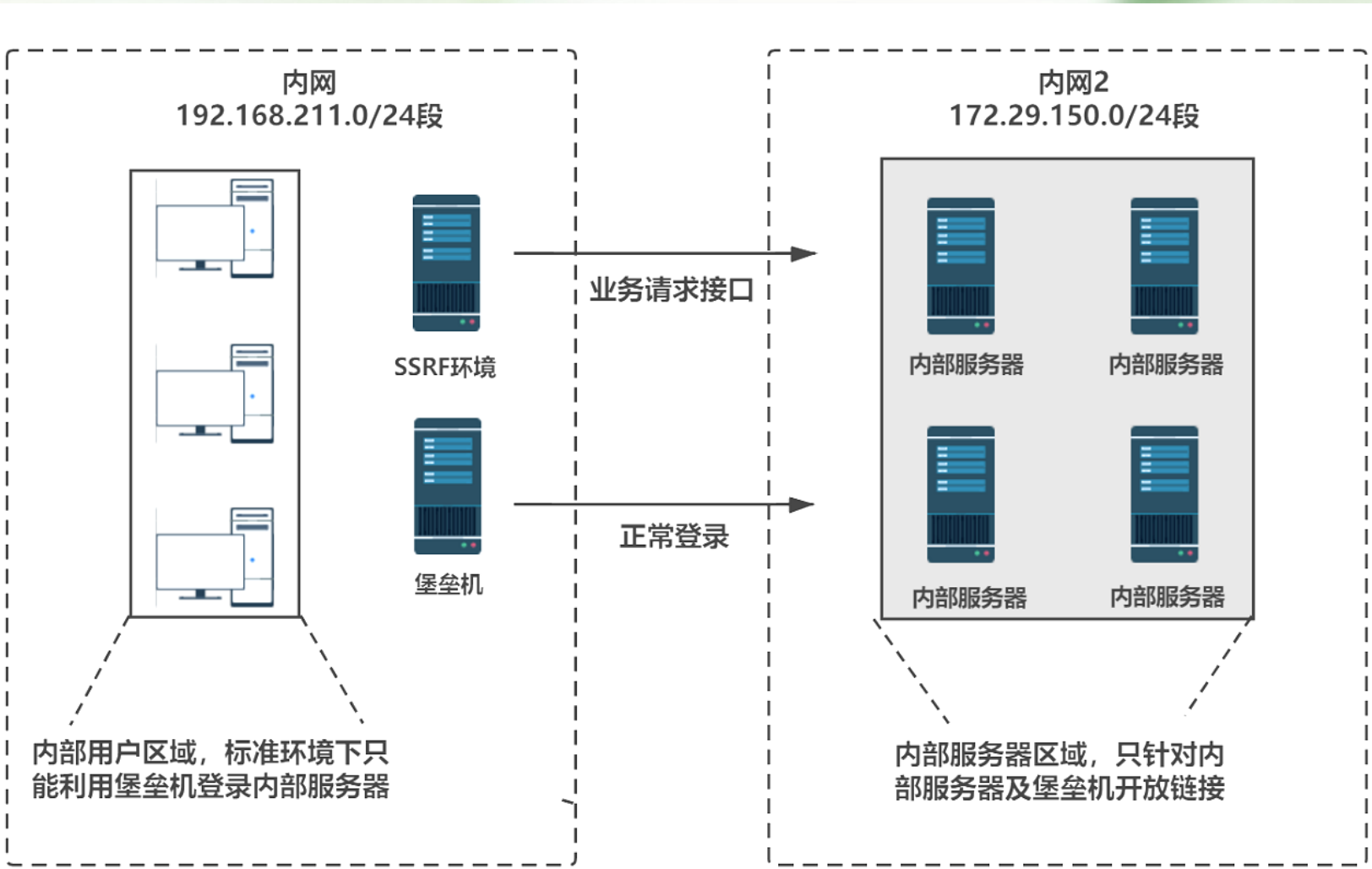
SSRF漏洞原理

- 相对CSRF攻击来说，在于伪造的身份不同
- SSRF漏洞本质上是利用服务器的高权限实现对当前系统敏感信息的访问

SSRF漏洞缺陷的目标

- **图片加载与下载功能**
  - 通过URL地址远程加载或下载图片，降低当前服务器的资源消耗
- **本地处理功能**
  - 如获取提交的URL中的header信息等
- **各类辅助功能**
  - 针对用户输入的参数，提升参数的可视化效果
- **图片、文章收藏功能**
  - 将远程地址进行本地保存

SSRF漏洞利用场景


内网
192.168.211.0/24段
SSRF环境
堡垒机
业务请求接口
正常登录
内网2
172.29.150.0/24段
内部服务器
内部服务器
内部服务器
内部服务器
内部用户区域，标准环境下只能利用堡垒机登录内部服务器
内部服务器区域，只针对内部服务器及堡垒机开放链接

SSRF漏洞利用场景

- 可实现的攻击效果
- 对内网Web应用特征进行发现
- 对服务器所在内网进行各类信息探测
- 利用File协议读取本地文件
- 针对特定目标进行攻击时隐藏攻击发起地址

SSRF漏洞在防护方面需要重点解决两个问题

- 用户请求的合法性
- 服务器行为的合规性

- **有效方法**
  - 黑白名单/正则表达式
    - 禁止访问内网地址
  - 双向过滤用户端参数
    - 限定输入参数、返回结果的数据类型和内容
  - 限制请求行为端口
  - 尽可能实现业务集中化调用