跨站请求伪造

W2.1. 解释为什么 SameSite Cookie 有助于防止 CSRF 攻击。

W2.2. 解释网站如何使用秘密令牌防止 CSRF 攻击，以及这种方法为什么有效。

W2.3. 现在，大多数网站都使用 HTTPS，而不是 HTTP。还需要担心 CSRF 攻击吗？

W2.4. 使用 LiveHTTPHeaders 观察到，向 `www.example.com` 发送以下 GET 请求可以删除用户拥有的页面（只有页面所有者可以删除）。

```
http://www.example.com/delete.php?pageid=5

GET /delete.php?pageid=5
Host: www.example.com
...
```

请构造一个简单的恶意网页，使受害者访问时自动向 `www.example.com` 发送伪造请求，删除该受害者拥有的页面。

W2.5. 使用 LiveHTTPHeaders 观察到，向 `www.example.com` 发送以下 POST 请求可以删除用户拥有的页面（只有页面所有者可以删除）。

```
http://www.example.com/delete.php

POST /delete.php HTTP/1.1
Host: www.example.com
...
Content-Length: 8
pageid=5
```

请构造一个简单的恶意网页，使受害者访问时自动向 `www.example.com` 发送伪造请求，删除该受害者拥有的页面。

W2.6. 本章中针对 Elgg 构造的伪造 HTTP 请求需要 Boby 的用户 ID （`guid`）才能工作。如果 Alice 专门以 Boby 为目标，就必须在攻击前取得他的用户 ID。Alice 不知道 Boby 的 Elgg 密码，无法登录他的账户查看信息。请说明她还能怎样找到 Boby 的用户 ID。

W2.7. 某个请求必须携带服务器随机生成的用户 ID。该 ID 可从服务器返回的用户页面中找到。如果攻击者不知道目标用户的 ID，还能对该服务实施 CSRF 攻击吗？

W2.8. Alice 想攻击任何访问其恶意网页的人，因此事先不知道访问者是谁。（1）她还能通过 CSRF 修改受害者的 `Elgg` 个人资料吗？请说明原因。（2）她能否通过 CSRF 把自己加入受害者的好友列表？请说明原因。

W2.9. 网页向服务器发送请求时，浏览器总会在 HTTP 头的 Cookie 字段中附加会话 ID。某 Web 应用还要求从本站页面发出的请求在数据部分再次携带会话 ID：GET 请求把它放在 URL 中，POST 请求把它放在请求体中。这看似重复，因为 Cookie 中已经有会话 ID；但服务器可通过检查数据部分是否也包含该 ID 来判断请求是否由站外页面伪造。请解释原因。

W2.10. 浏览器知道一个 HTTP 请求是否跨站吗？

W2.11. 服务器知道一个 HTTP 请求是否跨站吗？

W2.12. 为什么 Web 服务器不能只依赖 Referer 头来判断请求是否跨站？

W2.13. 服务器为什么需要知道请求是否跨站？

W2.14. 能否简单地要求浏览器对所有跨站请求都不附加 Cookie？

W2.15. ★ ★ ★

来自 `www.example.com` 的页面包含一个显示 Facebook 页面内容的 `iframe`。从该 `iframe` 内发出的请求是否算作跨站请求？如果不是，为什么仍然安全？