

Cross-Site Request Forgery



A blue rounded square icon with the letters 'API' in white. The icon has a slight 3D effect with a shadow underneath.

**API**

http://B.com

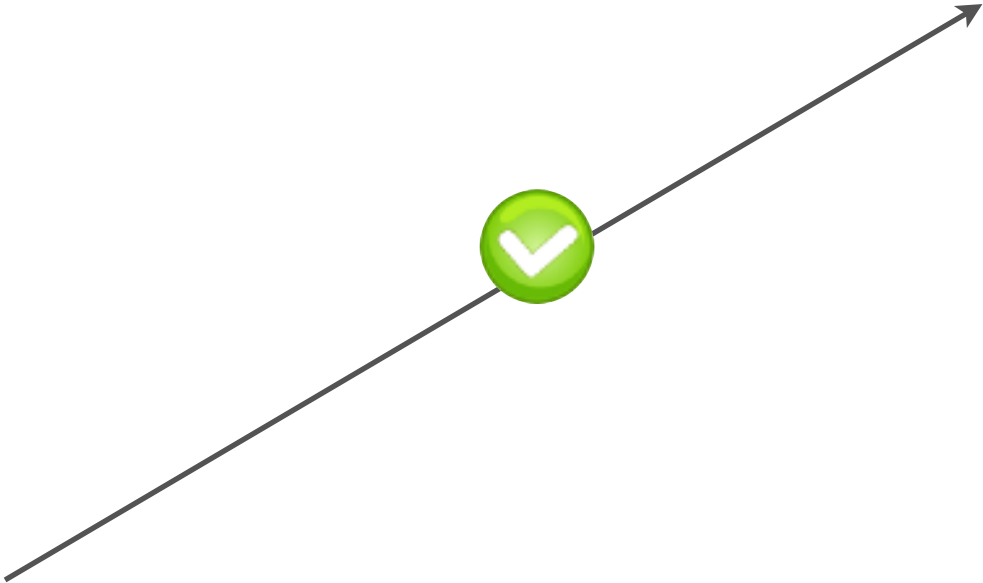


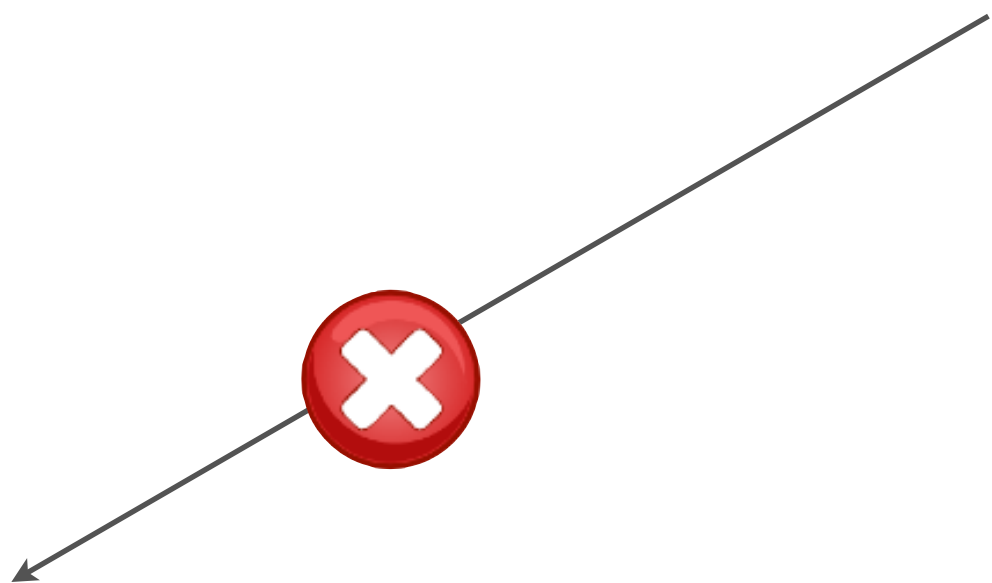
A blue rounded square icon with the letters 'API' in white. The icon has a slight 3D effect with a shadow underneath.

**API**



<http://A.com>









A red callout box with a pointed top and rounded bottom corners, containing white text. The text describes a security vulnerability where an attacker can execute unwanted authenticated actions by setting up a malicious website.

An attacker can executes unwanted but yet authenticated actions by setting up a malicious website with **authenticated cross-origin requests**

## Examples

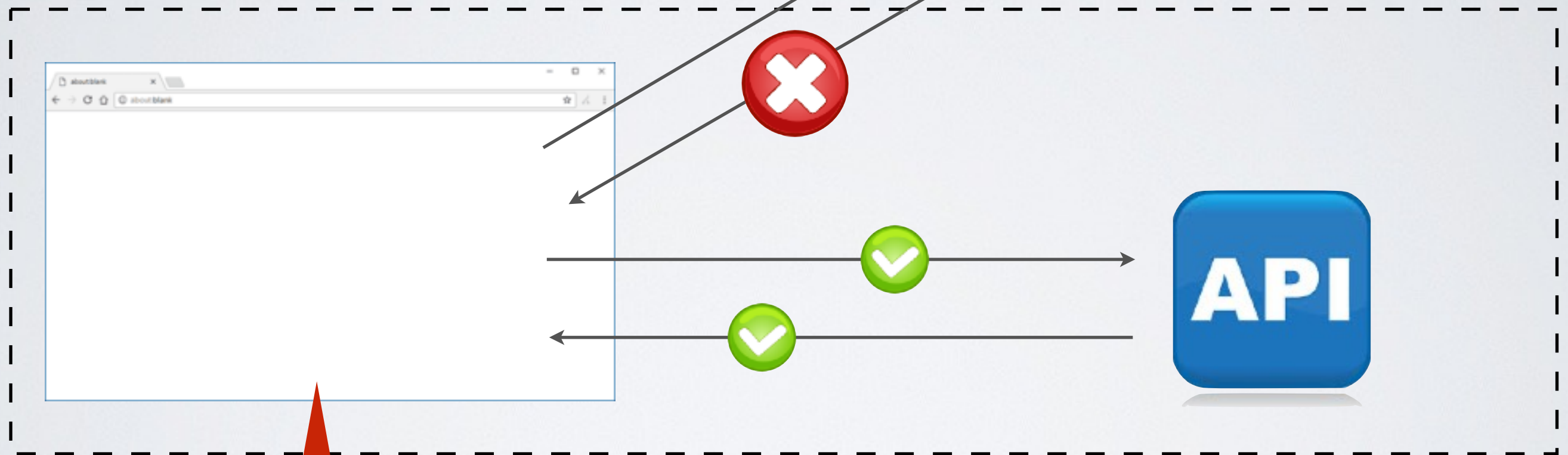
```
POST /transfer/ {to: Mallory, amount: $1000}
```

```
DELETE /account/ {owner: Mallory}
```

# Cross-Site Request Forgery

## Examples

```
POST /transfer/ {to: Mallory, amount: $1000}  
DELETE /account/ {owner: Mallory}
```



An attacker can execute unwanted but yet authenticated actions by setting up a malicious website with **authenticated cross-origin requests**



# SameSite cookie flag

- ✓ The cookie will not be sent over cross-origin requests
- ➡ Prevents forwarding the authentication cookie over cross-origin requests