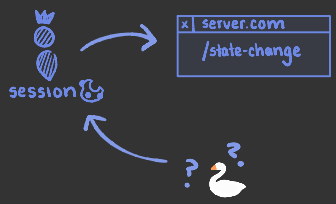
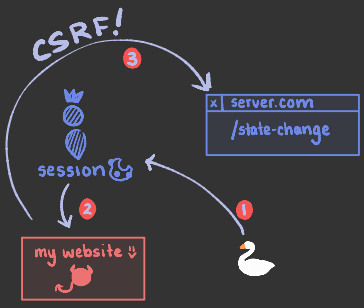
CRSF Cross-Site Request Forgery



You want to make admin change their password, but you obviously can't do it yourself

Basically, how do you make admin change their pw without them knowing?



1. Make admin visit attacker website
2. When admin visits attacker website, scripts hosted on there instigate a request back to the vuln-server, to change pw of the user who made the request
3. When a request is made, admin's sessional cookies are packaged with it, so vuln server will change the pw of admin-w/out admin explicitly making the request knowingly

HOW DOES THIS WORK

A CSRF requires 3 things:

- State-changing request on server
  - ↳ like changing a password or email, transferring money, etc. Requests which display data to the user won't work since CORS prevents us from looking at the response of a cross-site request
- The server only using cookies for sessional checks.
  - ↳ Most browsers will package in a user's cookies in an HTTP request. If the vulnerable server only authenticates on sessional cookie alone, a victim will never know a request was made on their behalf.
- The request containing deterministic parameters ONLY
  - ↳ Requests with unexpected or non-determenistic params will be hard for an attacker to predict the values for

NOTES

- CSRF attacks can theoretically arise when an application packages in a user's credentials in a request automatically
- Similar to XSS in that CSRF requires a victim user to visit some site an attacker controls.