Agenda

- Cross Site Request Forgery
- Clickjacking
- Case Studies
Terms

- **Proof-of-Concept (PoC):** In computer security, proof of concept refers to a demonstration that in principle shows how a system may be protected or compromised, without the necessity of building a complete working vehicle for that purpose.
Cross Site Request Forgery

- a.k.a. one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts. -wikipedia
Preventing Cross Site Request Forgery

- CSRF token
- Example: when you want to transfer money to someone using online banking:
  - without a token: http://www.mybank.com/transfer?to=123456&amount=10000
  - with a token: http://www.mybank.com/transfer?to=123456&amount=10000&token=31415926535897932384626433832795028841971
Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.
Case Study: Cross Site Request Forgery

Paypal bug bounty: Updating the Paypal.me profile picture without consent (CSRF attack)
Case Study: Clickjacking on Mail.ru

https://hackerone.com/reports/8724
Hands-on: Clickjacking

Replacing the following url with a different url and save everything as one html file, then open the html file with your browser. See if the website can be loaded in the iframe. Try 5 different urls: 1 big IT company’s site (e.g., www.yahoo.com), 1 bsu main site (e.g., www.boisestate.edu), 1 bank site (e.g., www.bankofamerica.com), 1 celebrity website (e.g., www.arianagrande.com), 1 bug bounty program website (e.g., www.yelp.com).

<html>
<head>
<title>Clickjack test page</title>
</head>
<body>
<p>Website is vulnerable to clickjacking!</p>
<iframe src="http://promo.calendar.mail.ru/" width="500" height="500"></iframe>
</body>
</html>
Clickjacking Countermeasures

- Frame Busting
- X-Frame-Options
Clickjacking Countermeasure 1: Frame Busting or Framekiller

Framekillers are implemented using JavaScript that validates if the current window is the main window. The recommended approach is to block rendering of the window by default and only unblock it after confirming the current window is the main one:

```html
<style>
html{display:none;}
</style>
<script>
    if(self == top) {
        document.documentElement.style.display = 'block';
    } else {
        top.location = self.location;
    }
</script>
```
Clickjacking Countermeasure 2: Setting the HTTP Header
X-Frame-Options

- DENY: prevents any domain from framing the content.
- SAMEORIGIN: allows the current site to frame the content.
- ALLOW-FROM %uri%: permits the specified 'uri' to frame this page.

PHP example:

```php
<?php
header('X-FRAME-OPTIONS: DENY');
?>
```
A large portion of the material is adapted from:

- Fundamentals of Information Systems Security - David Kim, Michael G. Solomon