..

Clickjacking

Clickjacking je útok na uživatelské rozhraní, který zneužívá důvěry uživatele v legální webovou stránku. Cílem je přimět uživatele k provedení akce, kterou by dobrovolně neudělal – například ke smazání účtu, odeslání peněz, změně hesla nebo k udělení přístupu k webové kameře.

Název vznikl spojením slov „click“ (kliknutí) a „hijacking“ (únos).

Jak Clickjacking funguje?

Útočník vytvoří neviditelnou past pomocí HTML a CSS:

```
1. **Návnada:** Útočník vytvoří lákavou stránku (např. "Vyhráli jste iPhone, klikněte zde").
2. **Neviditelný rám:** Do této stránky vloží legitimní web (např. nastavení Facebooku nebo internetové bankovnictví) pomocí prvku ''<iframe>''.
3. **Průhlednost:** Pomocí CSS (vlastnost ''opacity: 0'') učiní legitimní web zcela neviditelným a umístí jej přesně nad tlačítko "návnady".
4. **Interakce:** Uživatel se snaží kliknout na "Výhru", ale ve skutečnosti jeho kliknutí směřuje do neviditelného rámu na tlačítko "Potvrdit transakci".
```

Typy Clickjacking útoků

- **Likejacking:** Útočník donutí uživatele nechtěně kliknout na tlačítko „To se mi líbí“ u konkrétní stránky na sociální síti, čímž zvyšuje její dosah.
- **Filejacking:** Pokus o přístup k souborovému systému uživatele tím, že je oklamán, aby klikl na neviditelný formulář pro nahrání/stažení souborů.
- **Cookiejacking:** Útočník se snaží získat data z cookies prohlížeče, aby mohl převzít identitu uživatele.

Obrana proti Clickjackingu

Existují dva hlavní způsoby, jak se jako majitel webu bránit:

1. HTTP hlavička X-Frame-Options

Tato starší, ale stále účinná metoda říká prohlížeči, zda smí být stránka zobrazena v rámu:

- **DENY:** Stránka nesmí být vložena do rámu nikým (nejbezpečnější).
- **SAMEORIGIN:** Stránku lze vložit do rámu pouze na stejné doméně.

2. Content Security Policy (CSP)

Moderní a flexibilnější metoda využívající direktivu **frame-ancestors**, která nahrazuje X-Frame-Options:

```
Content-Security-Policy: frame-ancestors 'self';
```

Tento příkaz povolí vkládání stránek do rámů pouze vlastnímu webu.

Historický kontext: Frame Busting

Před zavedením standardů jako CSP se vývojáři bránili pomocí JavaScriptu (tzv. „Frame Busting“ skripty). Tyto skripty kontrolovaly, zda je okno prohlížeče „hlavní“, a pokud ne, pokusily se rám rozbít. Tato metoda je však dnes považována za nespolehlivou, protože útočníci se naučili tyto skripty vypínat nebo obcházet.

Související pojmy: Content Security Policy (CSP), OWASP, XSS, HTTP, Iframe, Sociální inženýrství.