# Squarespace

Riskit Squarespacen sivujen kävijöille sekä sivujen pitäjille.

# Clickjacking

- X-frame-optionsia ei ole konfiguroitu DENY tai SAMEORIGIN

  Tämä tarkoittaa sitä että tietty squarespace sivu voi olla upotettuna toiselle sivulle.

  Tämä taas mahdollistaa kun kyseisellä huijaus sivulla luulet painavasi jotain kuten kirjautumis nappia niin sivu viekin johonkin muualle.

# XSS

XSS(Cross site injection)
On lyhyesti sanottuna hyökkäys jossa hyökkääjä voi ajaa haitallista koodia selaimessasi ja varastaa selain dataasi.
XSS on mahdollista jos olet käynnyt haitallisella sivulla ja sitä kautta hyökkääjä on haavoittanut koneesi.

- CSP puutteellinen käyttö : CSP tarkoitus on rajoittaa mitä skriptejä sivu voi käyttää, mutta ilman CSP käyttöä on vaara että häkkerit voivat soveltaa

XSS(Cross site scripting) jolla he voivat laittaa sinut käyttämään heidän skriptejä sivulla, jonka takia he voivat varastaa sinun arvokasta dataa.

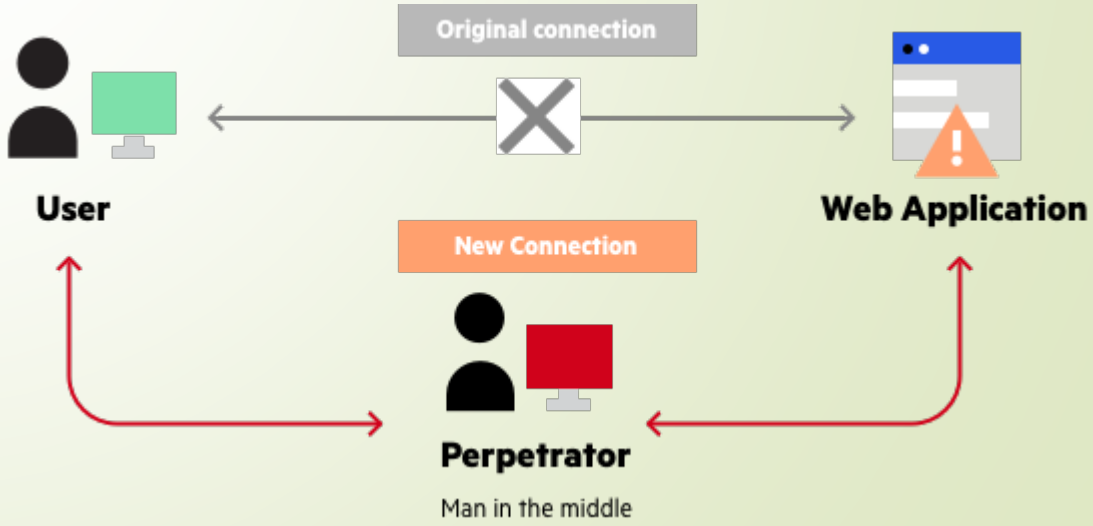
# MITM(Man in the middle)

- MITM on hyökkäys jossa hyökkääjä pääsee käyttäjän ja verkkosivuston yhteyden väliin ja pystyy näkemään datan minkä käyttäjä sekä verkkosivusto toisillensa lähettää.

- Sivustolla ei ole HSTS preloadia.

  Tämä tarkoittaa sitä että kun ensimmäisen kerran menet sivulle, voi sivu

  latautua ensiksi http eikä https yhteytenä joka mahdollistaa yhteyden kaappauksen MITM hyökkäykselle.



# Squarespace Hostina

- Squarespace yms ovat siltä kannalta turvallisia verkkosivujen luojille, että verrattuna paikallisesti hostattuihin verkkosivuihin on se että Squarespace pitää tietoturvalliset asiat ajantasalla, sekä luojan ei tarvitse itse pitää yllä verkkosivun omaa tietokantaa. Joka voi huonossa tapauksessa olla iso riski verkkosivujen tietoturvallisuudessa.

# Squarespace verrattuna muihin

- Jos vertaamme Squarespacea vaikka yleisimpään eli Wordpress niin on Squarespacella se iso etu että palvelu toimii samalla myös verkkosivuston serverinä, joka taas tarkoittaa sitä että on todennäköisempää että ohjelmat ovat päiväntasalla.
- Kun taas wordpressissä on mahdollista vain tehdä serveri jonka asiakas joutuu itse hostaamaan. Eli siis asiakas joutuu myös itse pitämään serverinsä päiväntasalla.

# Lähteet


- https://portswigger.net/web-security
- https://domsignal.com/
- https://hstspreload.org/
- https://www.upguard.com/security-report/squarespace