Attaque XST (Cross Site Tracing)

XST (Cross Site Tracing) est une attaque exploitant la méthode HTTP TRACE pour récupérer des informations sensibles, notamment des cookies d'authentification, via des scripts malveillants côté client. Elle combine souvent d'autres vulnérabilités comme le Cross-Site Scripting (XSS).

Fonctionnement

1. La méthode TRACE est une fonctionnalité HTTP standard servant au débogage, permettant de voir ce que le serveur reçoit dans une requête.
2. Lorsqu'un navigateur envoie une requête TRACE, le serveur renvoie exactement ce qu'il a reçu.
3. Un attaquant peut injecter un script malveillant (via XSS par exemple), qui envoie une requête TRACE.
4. Si les cookies, les en-têtes d'authentification ou d'autres données sensibles sont présents dans cette requête, ils sont renvoyés dans la réponse.
5. Le script peut alors lire la réponse, en extraire les cookies, et les envoyer à l'attaquant.

Conséquences

- Vol de cookies de session ou d'authentification
- Bypass de sécurités HTTP comme HttpOnly (dans certains cas obsolètes)
- Exposition d'informations sensibles contenues dans les en-têtes
- Compromission de comptes utilisateurs