**Cross Site Scripting Inclusion**

**Description 1**

Browsers prevent pages of one domain from reading pages in other domains. But they do not prevent pages of a domain from referencing resources in other domains. In particular, they allow images to be rendered from other domains and scripts to be executed from other domains. An included script doesn't have its own security context. It runs in the security context of the page that included it. For example, if www.evil.example.com includes a script hosted on www.google.com then that script runs in the evil context not in the google context. So any user data in that script will "leak." [1]

**Example**

Lets say www.amazon.com has a script that reads your private account information from its servers. That script can be added to www.hackersite.com. When you access www.hackersite.com, it will pull information included in your private account from Amazon's server and can store it HackerSite's server. [2]

More examples in OWASP lecture [3]

Refrences

[1] https://google-gruyere.appspot.com/part3

[2] <http://jggge.blogspot.com/2014/04/cross-site-script-inclusion-xssi.html>

[3]https://www.owasp.org/images/f/f3/Your\_Script\_in\_My\_Page\_What\_Could\_Possibly\_Go\_Wrong\_-\_Sebastian\_Lekies%2BBen\_Stock.pdf