

A

1

User logs in to vulnerable website.

User receives a link for attacker’s site.

User visits attacker’s site that contains an <img> element with source with s malicious URL. OR attacker site contains a link <a> whose target is malicious URL.

Clicking the link (or browser trying to download image) causes CSRF request to be sent to vulnerable site along with session cookie.

2

Client and server exchange hello messages sharing each other’s random number.

Both securely exchange or establish pre-master key S.

Master key is derived using a function that takes S and both randoms as input.

3

False alerts means wasted time in looking into the event details, ultimately users will start ignoring alarms.

Missing alerts means a false sense of security, attacks slipping through.

B

1

User logs in to vulnerable website.

Attacker sends user a malicious link, containing a <script>.

User clicks the link, request containing malicious <script> goes to vulnerable site.

Vulnerable site returns a response, which also reflects back the user’s script input.

Attacker’s script runs in user’s browser.

2

In order:

Fragmentation, compression, mac calculation, padding, encryption, adding header

3

The quicker the attack can be caught and blocked, the lesser the damage will be done. That’s why IDS aims to provide real time monitoring.