Browser Session Hijacking Procedure

- Description
  - **Browser Session Hijacking**, also known as simply **Session Hijacking** or **Cookie Hijacking**, is an attack technique in which an attacker gains access to a user's session cookie through **cross-site-scripting**, **man-in-the-middle attacks**, **session sniffing**, etc. The attacker can then access user session information such as login credentials and anything the user has entered or done on their web page session.
- Incident Trigger
  - A user suddenly clicks on a spearphishing link and is prompted with a `javascript` pop-up displaying their session cookie. The user has no idea what this is but understands that it is not good by the looks of it.
- Triage
  - Determine the suspicious link(s) that caused the pop-up.
  - Copy down the email it was sent from, it may be useful later.
  - Keep a copy of the email.
  - Was the user on an insecure internet connection?
- Detection
  - Attempt to safely look through the malicious links sent to determine the techniques used to grab the user's session cookie.
  - Locate the mail server that was used to send the phishing email.
- Location of evidence
  - The location of evidence is simply the email that was sent in this case. In cases where the attacker uses **IP spoofing** or **session-sniffing** there may be even less evidence to work with. It may also be possible to check the DNS firewalls for any malicious traffic.
  - If the user was connected to an insecure internet connection, it may be possible to see all users who were or are still connected.
- Tools & Commands
  - For this procedure, using network commands such as `nslookup` are useful. `nslookup` can query the DNS server the link uses for DNS records.
- Mitigation
  - Unfortunately, there aren't many things a user can do to prevent session hijacking, it is mainly a server side problem that web developers should keep in mind. There are however, a few mitigations to keep in mind.
  - A user should never click on links or download attachments from emails they do not know. Even if the emailer is someone from your network, it is never a good idea to click on the link sent by them as this can instantly give the attacker an entry point to your machine or browser sessions.
  - **Always use HTTPS**. This is important because HTTPS encrypts your data. A site that does not use HTTP will not encrypt your data, and may actually have your session cookie in plain sight

  for attackers to grab. Installing browser plugins like `HTTPSEverywhere` can help mitigate usage of HTTP and even block certain HTTP websites from being accessed.
  - `HTTPOnly` is a cookie flag that should always be enabled. It essentially protects the session cookie from `XSS`.
  - Avoid using public WiFi or any insecure network. Most modern machines will notify you if a network is insecure. Insecure networks do not encrypt data transmitted.
- Eradication
  - To get rid of session hijacking, this is purely up to web developers and companies. They must use HTTPOnly flags for their session cookies, and they must install mitigation tactics such as Phishing alerts, VPN's, web frameworks, and malware detection/prevention software. It also helps if companies notify their employees on the dangers of session hijacking.