The Password Reset MitM Attack

✧ Summary

本篇旨在利用密碼重設流程設計上的缺失，藉由註冊與密碼重設兩者流程間的相似性來進行中間人攻擊。在使用者於攻擊者的頁面進行註冊時，攻擊者則向另一網站發起密碼重設請求(如:email 服務)，並將所遇到的問題轉發給使用者，再將使用者所回覆的答案 forward 回去。此外，作者亦考量了透過簡訊、語音電話或手機 app 來重設密碼的情況，並設計實驗以驗證作者想法在當時的確是有很高機率可以將使用者在其他各大網站的密碼進行重設的。

本篇亦提供一些可行的防禦方式與 guidelines 如：語音電話或簡訊重置訊息須包含發送方、驗證碼的意義用途、警告訊息等其他重要資訊；重置簡訊改為傳送超連結；縮短驗證碼的有效期；密碼重設後須透過簡訊或 email 告知使用者。

PRMitM 攻擊雖看似簡單無複雜技術，但並不代表威脅程度低。倘若使用者擁有很強的密碼，但密碼重設流程卻意外簡單，那麼防護仍形同虛設，畢竟資安強度是由最弱的一環來決定。

✧ Strenths

PRMitM 利用許多人惰性或粗心的弱點搭配重設流程的缺陷，在針對資訊不夠充足的 SMS 或語音電話時成效相當顯著，因此便可用來對付雙因子認證(2-FA)。這使攻擊者可以很有效率的接管使用者的 email 帳號。

除此之外，PRMitM 不像一般 XSS 或 CSRF，需要對目標網站足夠熟悉找到潛在的漏洞或需要誘導使用者登入特定網站，才能發動攻擊。也因此 PRMitM 不會受限於 zero-day bug，一旦被瀏覽器 patch 以後就會難以施展。在另一方面，PRMitM 相較於釣魚頁面，不需要先誘導使用者點擊該釣魚頁面並登入，而僅是透過伺服器端流程設計的 bug。且釣魚頁面目前已有許多防護機制，使用者也對釣魚手法有足夠的警覺。

✧ Weaknesses

若使用者在註冊攻擊者網站時(如:英文)所使用的語言與重設密碼的網站不同(如:中文)，那使用者便很有可能會起疑。另外，有不少網站重設密碼流程是客製化的，即依據使用者所做的回應給予不同的下一步指示，那麼攻擊者可能就需要依照流程來 forward 資訊，然而網路中間人攻擊最大缺點就是轉送與回應時間較長，除了使用體驗差使註冊者放棄外，也較易令使用者起疑；不僅如此，註冊的邏輯與所要求的資訊，都很可能令使用者察覺異狀。

另外一種情況是使用者很可能認為攻擊者的網站並非知名網站，而給予假的資訊，或回答不同的安全問題給予另類的答案，致使攻擊失敗，且此可能性並未在作者實驗中進行驗證。

在實驗方面，因為所挑選的學生皆為作者機構的學生且被告知為進行其他實驗，因此可能會基於信任的緣故而放鬆了警戒，在一般使用情境中警戒心應會較高。

此外，有部分網站(如:Google)也會依據使用者習慣、地域、時間等使用資訊判斷是否為本人行為，阻擋可疑的登入或其他敏感動作。因此 PRMitM 可能便會需要天時地利人和才得以成功，也就增加了侷限性。

最後，PRMitM 主要仍是只得針對 email 服務，因大多網站在密碼重設時往往都會先發送密碼重設信至 email 當中，便會暴露的攻擊者的意圖。

✧ Reflection

在攻擊方面，除了多提供吸引人的檔案或服務令使用者渴望註冊外，也可以在加入一些社交工程如 FB/Google 的 logo，註記 Power by XXX，或許也可進一步提升成功率。

在防禦方面，若能依據 user 的使用習性再搭配 app 才能重設，或是重設密碼流程加入是該網站才特有的問題，令使用者不得不想到該網站，便可大幅降低 PRMitM 攻擊。

安全性與方便性就是翹翹板的兩端，雖作者提供了許多防禦方針，但多少都會使重設密碼的流程變為複雜(如:傳送安全驗證碼至朋友手機中)，而影響使用者體驗的後果很可能是會接到更多的客訴電話，當然若網站的密碼對使用者而言是重要的，那麼保護帳號安全應該比密碼重設方便性重要的多。