VAJA: XSS (ang. Cross-Site Scripting)

Namen

Namen te vaje je razumevanje mehanizmov in potencialnih posledic napadov XSS (Cross-Site Scripting). Vaja spozna kako napadalci izkoriščajo ranljivosti v spletnih aplikacijah, da izvedejo zlonamerne skripte. Poleg spoznavanja napadov je cilj usmerjen v pridobivanje praktičnih znanj, potrebnih za zaščito spletnih aplikacij pred takšnimi napadi.

Uvod

Cross-site scripting (XSS) je vrsta varnostne ranljivosti spletnih aplikacij, ki omogoča napadalcem, da v spletnih brskalnikih žrtev izvajajo zlonamerno skripto. Ta ranljivost se pojavi, ko spletna aplikacija pošilja uporabnikom podatke, ki niso ustrezno preverjeni ali očiščeni od zlonamernih skript. Napadalci lahko izkoristijo XSS za izvajanje različnih zlonamernih dejanj, vključno s krajo piškotkov, prevzemanjem sej, preusmeritvijo na zlonamerne spletne strani in celo prevzemom nadzora nad računom žrtve.

HTML (HyperText Markup Language) je standardni označevalni jezik za ustvarjanje spletnih strani in spletnih aplikacij. Z uporabo HTML lahko razvijalci definirajo strukturo spletnih strani, vključno z besedilom, hiperpovezavami, slikami in drugimi elementi. XSS napadi izkoriščajo ranljivosti v načinu, kako spletni brskalniki razlagajo HTML in izvajajo JavaScript, ki je pogosto vključen v HTML za dodajanje interaktivnosti spletnim stranem. Zlonamerna skripta se običajno vstavi v spletno stran z zlorabo vhodnih polj ali drugih mehanizmov, ki omogočajo uporabniku, da spletni aplikaciji pošlje neobdelano vsebino.

Zaradi te dvojne narave ranljivosti - kombinacije neustrezne obdelave vhodov s strani spletnih aplikacij in moči, ki jo JavaScript omogoča v brskalniškem okolju - je zaščita pred XSS kompleksna. Zahteva skrbno sanitacijo vseh uporabniških vhodov, uporabo varnostnih politik, kot je Content Security Policy (CSP), in stalno izobraževanje razvijalcev o varnih praksah kodiranja.

Naloge:

1. Raziskovanje ranljivosti XSS:
   1.1. Odprimo spletno stran v brskalniku Firefox: http://cybersec.ltfe.org/xss in se prijavimo z vnosom imena. Komentirajmo dogajanje! Kaj opazimo v URL?

   1.2. Namesto imena v vnosno polje vnesemo različne testne vhode (npr. html značke), ki jih najdemo na spletni strani. Komentirajmo, kaj se zgodi! Kako spletna stran obravnava te vhode?

2. Manipulacija s povezavami:
   2.1. Razmislite, kako bi povezavo spremenili (skrili) in jo poslali morebitni žrtvi. Uporabite poljuben URL spletni enkoder/dekoder za to nalogo.

   2.2. Razpravljajmo o metodah, ki jih lahko uporabimo za skrivanje zlonamernih povezav.

3. Prepoznavanje in zaščita pred napadi XSS:
   3.1. Za končne uporabnike: Na kaj moramo biti kot končni uporabnik pozorni, da prepoznamo in se zaščitimo pred napadi XSS?

   3.2. Za razvijalce: Na kaj moramo biti kot razvijalci pozorni pri pisanju spletnih aplikacij, da preprečimo napade XSS? Razmislimo o prečiščevanju vhodov, uporabi varnih funkcij za obravnavanje uporabniških vhodov in drugih varnostnih praksah.

4. Praktična zaščita pred napadi XSS:
   4.1. Izvedimo primer zaščite pred XSS napadi na primeru preproste spletne aplikacije. Uporabimo orodja in tehnike, ki so bile omenjene v razpravi.

   4.2. Testirajmo aplikacijo z različnimi zlonamernimi in neškodljivimi vhodi ter analizirajmo rezultate.