

Säkerhet och skydd mot sårbarhet i AktiveraMeras utmaningar

Parallellt med att nätverksmiljöer blir allt mer avancerade och komplexa ökar också exponeringen för olika typer av sårbarheter. För att upptäcka och åtgärda dessa sårbarheter innan någon med fel avsikter hinner utnyttja dem, krävs regelbundna kontroller och tester.

För att skydda tjänsterna och nätverksmiljön använder vi tre metoder i AktiveraMeras utmaningar:

1. Sårbarhetsscanning och penetrationstester
2. Intrångstester
3. Krypterad kommunikation



Sårbarhetsscanning och penetrationstester

För att upptäcka och undvika säkerhetsproblem i tjänsten kör vi regelbundna tester med OWASP ZAP. Verktöget testar att främmande kod inte kan köra i användarens webbläsare, att främmande kod inte läggs in i tjänsten och andra säkerhetshot.

Intrångstester

För att spåra attacker och intrångsförsök använder vi verktöget Snort, ett verktyg för nätverksövervakning. Med hjälp av Snort undersöker vi de metoder en angripare eller hacker skulle använda för en attack och kan på så sätt hitta brister svagheter under kontrollerade former.

Krypterad kommunikation

Kommunikationen till hemsidan krypteras med SSL-certifikat. På så sätt omöjliggörs det föröbehöriga att avlyssna trafiken mellan tjänsten och besökaren och på så sätt skydda lösenord och annan känslig information. För att garantera högsta säkerhetsnivån används SSL Labs rankingsystem där Company Races utmaningar är rankade på högsta nivån, A.



