OWASP Security Checker Application

07.03.2025

Dezvoltați un sistem de verificare a celor mai cunoscute vulnerabilități ale aplicațiilor WEB și de implementare a măsurilor de securitate aferente limitării expunerii resursei dezvoltate către entități malițioase. Sistemul ar trebui să aibă o interfață prietenoasă pentru utilizatori și să utilizeze o bază de date relațională (SQL) pentru stocarea informațiilor.

PREREQUISITES:

- Se vor folosi resurse disponibile pe Internet sau surse deschise pentru dezvoltarea și personalizarea soluției
- Se pot folosi reposite-uri din GitHub (exemplu, dar fără a se limita la acestea), cu scopul de a utiliza un sistem/aplicație pe post de țintă:
  - https://github.com/webpwnized/mutillidae
  - https://github.com/digininja/DVWA

OBIECTIVE:

- Înțelegerea tipurilor de atacuri specifice aplicațiilor web (ce vizează toate componentele din arhitectură – front-end și back-end)
- Executarea unor atacuri simulate (manual sau automatizat sub formă de script) pentru a vedea efectul atacului asupra infrastructurii – minim 3 tipuri distincte (exemplu, fără a se limita la acestea, input XSS, CSRF, SSRF, SQL injection, brute force, m-i-t-m, etc.)
- Implementarea de măsuri de securizare a aplicației țintă pentru a limita atacurile executate în pasul anterior (a se avea în vedere două stări: before – când aplicația era vulnerabilă și after – când aplicația a fost securizată de candidat prin implementare de funcționalități sau personalizări)

CONTRIBUȚIE PROPRIE:

- Implementarea unei aplicații web vulnerabile / Folosirea uneia deja existente din Internet (a se vedea pre-requisites)
- Implementarea unor tipuri de atacuri specifice (**OWASP Top 10**[1])
- Containerizarea acesteia (nu e obligatorie, dar reprezintă un plus)
- Implementarea măsurilor de securitate peste aplicația web vulnerabilă (bune practici de avut în vedere pentru limitarea atacurilor respective asupra infrastructurii) – prin optimizări/implementări de funcții la nivelul aplicației (coding), și, *opțional, instalare/configurare de tool-uri/add-on-uri pentru sporirea securității (această opțiune nu exclude partea de coding)*
- Documentarea contribuției (modul de deployment a soluției într-o infrastructură nouă, modul de realizare a atacurilor, contramăsurile de securitate implementate pentru a limita efectul atacurilor)

TERMEN: 21.03.2025

MODALITATE TRANSMITERE: se va realiza o arhivă a soluției, ce va include și o documentație de utilizare/exploatare și va fi transmisă la adresa de contact (vladuta.alexandru@spp.ro).

MODALITATE SUSȚINERE: se vor urma pașii de deployment din documentație și se va testa soluția pe un dispozitiv pus la dispoziție de beneficiar. Candidatul va prezenta funcționalitățile în fața comisiei direct pe dispozitivul pus la dispoziție, fără a solicita modificări personalizate ce nu sunt menționate în documentație.

[1] https://www.veracode.com/security/owasp-top-10/