UBT-CERT Internship

Java e shtatë deri tek java e nëntë

Web Application Penetration Testing

Maj 2017

Përgatitur nga studentët e SHKI/UBT: Kujtim Morina student I vitit të I

Rrustem Shehu studentit i vitit të III

Edi Bushati student I vitit të II

Ardit Krasniqi student i vitit të II

Veton Bejtullahu student i vitit të II

Ndihmës: Atdhe Buja UBT-CERT manager

Blent Kurtalani UBT-CERT trajner

Përmbajtja

Hyrje

Ky dokument është përgatitur me qëllim që të vetëdijsoj të gjithë ata qe janë të angazhuar në fushën e TIK-ut dhe I dedikohet komunitetit te TIK-ut.

Përmirëson nivelin e sigurise së sistemeve kompjuterike te nje kompanie ose organizate, ndihmon perdoruesit e ketyre sistemeve per shfrytezim sa me te sigurt te tyre.

Gjatë këtij aktiviteti janë realizuar një seri e Web application Penetration Testing te ueb faqeve dhe sistemeve elektronike te universitetit UBT. Ky aktivitet eshte realizuar nga studentet e internshipit ne kuader te UBT-së.

Koncepti etik (defense cyber security)

Ky dokument pasqyron aspektin etik apo mbrojtës, duke identifikuar dobësit (ang. Vulnerabilities), verifikimin e funksionimit normal të mekanizmave të sigurisë dhe testimin e sistemeve kompjuterike dhe rrjetës, përmes përdorimit të veglave apo programeve të ndryshme.

Çka është "Web Application Penetration Testing"

Web Application Penetration Testing eshte metode e kontrollit, verifikimt, dhe testimit te web aplikacioneve, sistemeve apo paisjeve te TI-se.

Aplikimi i metodologjisë me disa hapa në testimin e ueb aplikacionit tuaj duke filluar nga mbledhja e informacioneve, identifikimi dhe zbulimi. Analiza e rezultatit në mënyrë automatike jep mundësi për të validuar të gjeturat, përcaktuar impaktin në biznes dhe në eliminimin e atyre gjetjeve që nuk janë reale.

Hapi i parë "I"

Marrja e aprovimit nga CEO I organizates apo institucionit per testim te ueb-it apo sistemit. Shihet si një vendim etik dhe profesional në rrugën e duhur për të mos bërë shkelje ligjore dhe penale.

NDA (non-disclosure agreement) Marrëveshja për ruajtjen e Fshehtësisë, aplikohet shumë tek këto projekte e që e kanë ndieshmërinë e madhë për shkak të të dhënave që përmbajn këto ueb apo sisteme.

Hapi i dyte"II"

Instruksionet apo skenari. Varësisht nga skenari që zgjedhim për të realizuar këtë testim ashtu edhe instruksionet jepen. Kjo mvaret shumë edhe nga klienti se çka dëshiron të shoh në raport nga të gjeturat e tij në infrastrukturë të TIK-ut. Normalisht tek instruksionet janë të caktuara veprimet që lejohen dhe aot që nuk lejohen psh shkatërrimi apo prishja e funksionimit të pajisjes apo sistemit nuk është në etikën e një profesionisti.

Targeti – mund të jetë i zbulueshëm dmth dihet direct se qka dhe ku është fokusi dhe mund të mos jetë i ditur, kjo mvaret shumë edhe nga skenari që ne zgjehdim ta realizojmë.

Rolet ne ekip – zakonisht këto testime relaizohen në ekip dhe për kohë të gjata, me javë të tëra.

Menyrat e testimit: manuale apo automatike. Kemi dy mundësi të realizimit të këtij web pen-test, mirëo në rastin tonë janë realizuar të dy mënyrat ajo automatike përmes disa veglave që ofrohen në treg dhe në mënyrë manual që sistemet e hapura psh Linux ofron shumë mundësi për realizimin e këtij procesi në një mënyrë shumë të mirë.

Hapi i tretë "III"

Raporti i gjetjeve te dobesive te web aplikacionit ose sistemit. Si produkt i gjithë këtij procesi të gjatë e të mundimshëm por shumë kreativ përgatitet edhe raporti i të gjeturave nga të gjitha veprimet teknike që janë ndërmarrë për të realizuar këtë testim të sigurisë. Në vijim po paraqesim një structure të raportit që ne në UBT-CERT kemi përdor gjatë këtij aktiviteti:

- Raporti i gjetjeve, strukura:
    - Titulli raportit "Penetration Testing Report"

- Emri i autorit “emri mbiemri”
- Data raportit
- Permbajtja liste
- Permbledhje e targeteve te testuara
- Gjetjet ang. Vulnerabilities (print screen)
    - Targeti 1, 2, 3, 4, 5
    - Dobesite e gjetura (pershkrimi, print screen, sugjerim)

Hapi i katert “IV”

Rekomandimet – në bazë të raportit të gjetjeve janë disa rekomandime për TI-në, këtë raport nuk mund ta bëjmë publik për shkak që mbrohet me NDA të nënshkruar në mes të klientit dhe kryesit të punës këtë rast studentët e Internshipit në UBT-CERT.