UNIVERSITY OF TARTU
Institute of Computer Science
Conversion Master in IT Curriculum

Doris Sarapuu

Penetration Testing of Glia's Web Application

Master's Thesis (15 ECTS)

Supervisor(s): Kristjan Krips, MSc
Carlos Paniagua, MSc

Tartu 2019

Penetration Testing of Glia's Web Application

Abstract: Penetration testing is a simulation of real attacks to assess the risks associated with potential security vulnerabilities. Penetration testing requires various levels of expertise to manually verify security requirements, to review web application source code and configure automated tests. Nonprofit organization OWASP provides several documents for software security assessment. Glia's Operator Application was tested against all OWASP Top 10 2017 threats. For threat verification, OWASP ASVS 4.0 level 2 requirements along with additional customized test cases were checked. In addition to manual security requirement verification, automated Burp Suite tools were used. For each detected vulnerability, risk severity was assessed by taking into account the threat prevalence likelihood and impact. Risk mitigation suggestions were provided to all OWASP Top 10 threats.

Keywords: web application, penetration testing, risk assessment

CERCS code and name: P175 Informatics, systems theory

Glia veebirakenduse läbistustestimine

Lühikokkuvõte: Läbistustestimine on reaalsete veebirünnakute simulatsioon, et hinnata turvaaukudest tulenevaid potensiaalseid riske. Läbistustestimine nõuab testijalt mitmekülgseid professionaalseid oskusi, et manuaalselt kontrollida turvalisuse nõudeid, teostada veebirakenduse lähtekoodi ülevaatamist ning seadistada automatiseeritud teste. Mittetulundusühing OWASP pakub tarkvara turvalisuse hindamiseks mitmeid dokumente. Glia arendatud operaatori veebirakendust testiti kõigi OWASP Top 10 2017 ohtude suhtes. Ohutegurite kontrollimiseks kasutati OWASP ASVS 4.0 teise taseme nõudeid, mõnel puhul ka kohandatud nõudeid. Lisaks manuaalselt tuvastatavatele turvanõuete kontrollile kasutati ka Burp Suite rakenduse erinevaid automatiseeritud tööriistu. Iga tuvastatud turvaaugu puhul hinnati selle riski taset, võttes arvesse ohu leviku tõenäosust ja mõju veebirakendusele. Kõikidele OWASP Top 10 ohtude kohta anti riskide maandamise soovitusi.

Võtmesõnad: veebirakendus, läbistustestimine, riskihindamine

CERCS kood ja nimetus: P175, Informaatika, süsteemiteooria

Appendix 14. Licence

Non-exclusive licence to reproduce thesis

I, Doris Sarapuu,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

reproduce, for the purpose of preservation, including for the purpose of preservation in the DSpace digital archives until the expiry of the term of copyright,

Penetration Testing of Glia's Web Application,

supervised by Kristjan Krips and Carlos Paniagua.

Publication of the thesis is not allowed.

2. I am aware of the fact that the author retains the right specified in p. 1.

3. This is to certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Doris Sarapuu
16.05.2019