

Pentesti raporti näidis

Süntheetiline näidis, mis näitab raporti struktuuri ja tõendite taset: ulatus, metoodika, leiud, parandusplaan ja kordustest. Kõik nimed, domeenid ja leiud on väljamõeldud.

Kokkuvõte

Tellija: Näidis OÜ (väljamõeldud). **Sihtmärk:** kliendiportaal ja partner-API, testkeskkond. **Aeg:** viis tööpäeva. **Tulemus:** kolm kinnitatud leidu, millest üks kriitiline. Kõik leiud on tõendatud testkontodega; päris kasutajaandmeid ei kasutatud.

Kokkuvõte on mõeldud juhtkonnale: mida leiti, miks see oluline on ja mis järjekorras parandada. Tehniline detail on leidude peatükis.

Ulatus ja metoodika

Test hõlmas kliendiportaaali sisselogimist, rollide eraldatust ja dokumentide nähtavust ning partner-API objektipõhist juurdepääsu. Ulatuses olid ainult testkeskkond ja sünteetilised kliendid A ja B. Tootmiskeskkond, kolmandate osapoolte teenused ja mobiilirakendus jäid välja.

- Metoodika:** PTES-i töövoog ja OWASP WSTG kontrollid; API osas OWASP API Security Top 10.
- Lähteinfo:** halli kasti test – kaks testkontot, API dokumentatsioon ja arhitektuuri ülevaade.
- Piirangud:** koormustestid, masspäringud ja päris andmete muutmine olid keelatud.
- Tõendid:** maskeeritud päringud ja vastused, ajatemplid ja keskkonna kirjeldus.

Testimise faasid

- Ettevalmistus:** ulatuse kinnitus, testkontod, keskkond, keelatud tegevused ja kontaktid.
- Autentimine ja sessioonid:** sisselogimine, parooli taastamine, sessiooni lõpetamine ja MFA.
- Juurdepääsukontroll:** rollid, objektipõhine õiguskontroll ja horisontaalne/vertikaalne eskalatsioon.

- 4. **API ja äriloogika:** objektiviited, massomistamine, kiirusepiirangud ja olekumasinad.
- 5. **Raporteerimine:** tõendite kontroll, mõju hinnang, parandussoovitus ja kordustesti plaan.

Faasid ei ole lineaarsed: leid ühes faasis suunab järgmise testi. Näiteks ebaturvaline objektiviide viib kontrollini, kas sama muster esineb teistel otspunktidel.

Leiud

Iga leiu juures on mõju, tõend ja parandus. Järjekord ei tulene ainult tõsidusest, vaid ka sellest, kui lihtne on leidu ära kasutada.

F-01

Leid

BOLA: teise kliendi arve avamine ID-d muutes

Tõsidus

Kriitiline

Mõju

Teise kliendi andmete lugemine

F-02

Leid

Admin-kontol puudub MFA

Tõsidus

Kõrge

Mõju

Parooli lekkimisel haldusõigused

F-03

Leid

Veateated näitavad tehnilisi detaile

Tõsidus

Madal

Mõju

Info lekkimine ja ründepinna kaardistamine

F-01 BOLA: objektipõhine õiguskontroll puudub

Kirjeldus: testkonto A tokeniga päring `GET /api/v1/invoices/B-1001` tagastas kliendi B arve. Server kontrollis autentimist, kuid mitte objekti omandiõigust.

Tõend: kaks päringut sama tokeniga – oma arve (200) ja teise kliendi arve (200). Vastused maskeeritud; päris andmeid ei kasutatud.

Mõju: kliendiandmete konfidentsiaalsus; sama muster võib kehtida dokumentide ja tellimuste otspunktidel.

Parandus: kontrolli objekti omandiõigust serveris igal päringul, mitte kliendi vaates; lisa regressioonitest kahe tenantiga. **Prioriteet:** kohe.

F-02 Admin-kontol puudub MFA

Kirjeldus: halduskeskkonda sai sisse ainult parooliga. Testkontol õnnestus sisselogimine ilma teise faktorita.

Mõju: üks lekkind parool annab haldusõigused; mõju sõltub parooli taaskasutusest ja phishing-riskist.

Parandus: kehtesta MFA kõigile haldus- ja privileegikontodele, lisa tingimuslik juurdepääs ja logi MFA muudatused. **Prioriteet:** 7 päeva.

F-03 Veateated näitavad tehnilisi detaile

Kirjeldus: vigase päringu vastus sisaldas raamistiku versiooni ja stack trace'i fragmenti.

Mõju: hõlbustab tehnoloogia ja versioonide tuvastamist; üksi ei anna ligipääsu.

Parandus: tagasta kasutajale üldine veateade, logi detail serveris ja jälgi logide ligipääsu.

Prioriteet: plaan.

Tõendite standard

Hea leid on korratav ilma testija mälestusteta. Näidises on iga leiu juures keskkond, testkonto roll, päringu sammud, maskeeritud vastus ja ajatempel. Kui tõendit ei saa teine inimene korrata, on tegu hoiatusega, mitte kinnitatud leiuga.

- Maskeeri isikuandmed ja sessioonitokenid; säilita piisav detail kontrollimiseks.
- Erista kinnitatud leid, skanneri hoiatus ja hüpotees.
- Kirjelda mõju andmete ja toimingute kaudu, mitte ainult tehnilise nimega.
- Lisa paranduse kontrollitingimus, et kordustest oleks üheselt mõistetav.

Parandusplaan

1. **Kohe:** F-01 omandiõiguse kontroll ja regressioonitest; kontrolli samu mustreid teistel otspunktidel.
2. **7 päeva:** F-02 MFA ja tingimuslik juurdepääs; vaata üle kõik privileegikontod.
3. **Plaan:** F-03 veateadete üldistamine ja logimise korrastamine.

Iga punkti juures on vastutaja ja tähtaeg; ilma nendeta jääb plaan soovitude loeteluks.

Kordustest

Kokkulepitud kordustest kontrollib F-01 ja F-02 parandust samade testkontode ja objektidega. F-03 jäi järgmisse iteratsiooni. Kordustest ei hõlma kogu algset testi ega uusi funktsioone.

- F-01: teise kliendi arve päring tagastab nüüd 403/404.
- F-02: admin-sisselogimine nõuab teist faktorit.
- F-03: veateade on üldine, detail on serverilogis.

Kuidas seda näidist kasutada

Kasuta näidist pakkumuste võrdlemiseks. Küsi igalt pakkujalt, kas tema raport sisaldab sama taseme tõendeid ja kas kordustest on eraldi kokku lepitud.

- **Ulatus:** kas on kirjas, mida testiti, mida mitte ja millised piirangud kehtisid?
- **Tõendid:** kas leiud on korratavad ja andmed maskeeritud?
- **Prioriteetid:** kas parandusplaan seob leiu mõju ja tähtaja?
- **Kordustest:** kas on selge, mida ja millal uuesti kontrollitakse?

Näidis ei asenda hinnapakkumist ega tõesta, et sinu süsteemis samad leiud esinevad. See näitab ainult raporti struktuuri ja tõendite taset.

Küsimused näidise kohta

Kas see on päris kliendi raport?

Ei. Kõik nimed, domeenid ja leiud on sünteetilised ning mõeldud raporti struktuuri ja tõendite taseme näitamiseks.

Mida peaks hea pentesti raport sisaldama?

Testitud ulatust ja piiranguid, metoodikat, iga leiu tõendeid ja mõju, konkreetset parandussoovitust ning kordustesti tingimusi.

Kas leiu tõsidus on sama mis CVSS skoor?

Ei. CVSS annab üldise hinnangu, kuid tõsidus sinu jaoks sõltub mõjust, ärakasutatavusest ja andmetest, mida leid puudutab.

Mida teha pärast raporti kättesaamist?

Järjesta leiud mõju järgi, paranda kriitilised kohe, pane ülejäänud tähtajad paika ning lepi kokku kordustest.