BlackOps-tietoturva-testauksen kuvaus

Tai: Kuinka paljastamme totuuden softastanne

BlackOps-tietoturvatestaus perustuu Open Web Application Security Projektin (OWASP) top 10 listaukseen web-sovelluksiin kohdistuvista tietoturvauhkista. OWASP on maailmanlaajuinen voittoa tavoittelematon organisaatio, jonka tavoitteena on parantaa web-sovellusten tietoturvaa. Listauksen uusin versio on syyskuulta 2021.

A01 Puutteellinen pääsynhallinta

Käyttäjällä tulee olla pääsy ainoastaan objekteihin ja toimintoihin, jotka ovat sallittuja kyseiselle käyttäjälle. Puutteet pääsynhallinnassa voi liittyä tietojen vuotamiseen, datan muokkaamiseen tai poistamiseen tai suoritettuihin toimintoihin, jotka eivät kuulu käyttäjälle.

A02 Puutteet kryptografiassa

Datan luonteesta riippuen tulee se suojata riittävällä tasolla sekä siirrettäessä että tallennettaessa. Esimerkiksi salasanat, luottokorttitiedot, terveys- ja henkilökohtaiset tiedot vaativat erityistä suojausta varsinkin, kun niihin kohdistuu lakisääteisiä määritteitä ja velvoitteita (esim. GDRP).

A03 Injektio

Ilkeämielinen data tuntemattomasta lähteestä voi päätyä ohjelmiston osaan, joka suorittaa hyökkääjän asettaman komennon. Komento voi olla esimerkiksi tietokantakutsu (esim. SQL injektio), komentorivikäsky (esim. OS command injection) tai ilkeämielinen koodi, joka suoritetaan käyttäjän selaimessa (Cross-site scripting).

A04 Turvaton suunnittelu

Tarkasti suunnitelman mukaisesti rakennetut tekniset toteutukset voivat sisältää turvallisuusongelmia, joita ei ole suunnitteluvaiheessa huomioitu. Tällaisia voivat olla esimerkiksi virheet liiketoimintalogiikassa, selaintason suojan ohittaminen sekä hyökkääjän mahdollisuus asettaa itse tiedostonimiä- ja polkuja. Puutteet suunnittelussa voi tulla ilmi erityyppisinä haavoittuvuuksina.

A05 Heikot tietoturva-asetukset

Heikot tietoturva-asetukset voivat ilmetä hyvin monella eri tavalla: esimerkiksi turhia tai vanhentuneita ominaisuuksia on käytössä, virheenkäsittely paljastaa liikaa tietoa järjestelmän sisäisestä toiminnasta tai palvelimen, kirjastojen, tietokantojen jne. tietoturva-asetukset eivät ole käytössä. Vaikka asetuksia ei pysty katselmoimaan suoraan Black-box testauksessa, heikot tietoturva-asetukset tulevat ilmi haavoittuvuuksina.

BlackOps-tietoturva-testauksen kuvaus

Tai: Kuinka paljastamme totuuden softastanne

A06 Vanhentuneet ja haavoittuvaiset komponentit

Kun komponentin nimi ja versionumero ovat tiedossa, sen tunnettuja haavoittuvuuksia voidaan etsiä useilta eri sivustoilta, kuten http://cve.mitre.org/ ja http://nvd.nist.gov/. Nämä haavoittuvuudet ovat yleisesti tunnettuja ja usein korjattu komponentin uusimpaan versioon.

A07 Heikkoudet autentikoinnissa ja todentamisessa

Puutteelliseen todentamiseen liittyvät hyökkäykset kohdistuvat yleensä käyttäjän todentamiseen, autentikointiin ja session hallintaan. Pääsy järjestelmään tulee olla ainoastaan käyttäjillä, joilla on validit tunnukset järjestelmään. Esimerkiksi sisäänkirjautumisen ohittaminen antaa hyökkääjälle mahdollisuuden päästä kiinni tietoon, johon hänellä ei ole oikeutta.

A08 Heikkoudet ohjelmiston ja datan eheydessä

Aplikaatioiden, jatkuvan integroimisen/toimittamisen ja automaattisten päivitysten tulisi aina tulla luotettavista lähteistä ja niiden eheys tulisi varmistaa. Hyökkääjän lähettämä data on aina epäluotettavaa ja erityisesti serialisoitu data vaatii sen tarkastamista tai digitaalisen allekirjoituksen, jotta turvaton deserialisaatio voidaan ehkäistä.

A09 Heikkoudet lokituksessa ja monitoroinnissa

Järjestelmän pitäisi tallentaa kattavasti lokia, lokin perusteella pitäisi nostaa hälytyksiä, hälytyksiä tulisi seurata ja epäilyttävää toimintaa havaitessa hälytyksiin tulisi reagoida. Hyökkääjät voivat luottaa joissain tapauksissa siihen, ettei web-sovelluksessa ole riittävää monitorointia ja hakkeroinnin yhteydessä heidän toimintojansa ei havaita.

A10 Server-Side Request Forgery

Kun web-applikaatiossa on mahdollisuus noutaa ulkoisia resursseja, kuten kuvia muista palveluista ilman URL-osoitteen validointia, Server-side Request Forgery -haavoittuvuus (SSRF) voi ilmetä. Tällä tavalla hyökkääjä voi lähettää palvelimelta ilkeämielisiä pyyntöjä ei-toivottuihin osoitteisiin.

Yhteystiedot

Pasi Keski-Korsu
Security TestGuru
p. +358 45 676 1826
pasi.keski-korsu@prove.fi

www.prove.fi

BEYOND PROVE TESTING