A3 - Broken Authentication and Session Management

Ründajad

Ühtede kontode omanikud tahavad röövida teisi kontosid või keegi üritab seestpoolt (nt kasutaja) peita jälgi oma tegudest.

Haavatavus

Ründaja kasutab autentimise või sessiooni (paroolid, kasutaja ID-d) vigu, et esitada end kellegi teisena.

Levimus ja avastatavus

Arendajate jaoks on pidevalt erinevate tuvastusmeetodite loomine ja sessiooni erinevalt kasutamine puhtalt, ilma vigadeta väga raske. Muudetud parameetrite kasutamisel tekivad vead välja logimisel, paroolide halduses, salaküsimustes, kontode uuendamistes jne. Selliste vigade leidmine on keeruline.

Mõju

Need vead võimaldavad mitmete või kõigi kontode ründamist. Kui see õnnestub, siis saab ründaja teha kõike, mida rünnatavgi.

Mõju ärile

Vigade korral firmade väärtus langeb, eriti veel, kui nende haavatavusest teavitatakse avalikkust.

Kas ma olen haavatav?

Eelkõige on vaja kaitsta sessiooni ID-sid ja erinevaid volitusi.

Kuidas vältida katkisi autentimisi ja sessioone?

Parim soovitus organisatsioonidele on seada arendajatele tugev autentimine ning sessioonihoolduse seaded. Need seaded peavad vastama kõigile autentimise ja sessioonihoolduse nõuetele, mis on defineeritud OWASPis: V2 (Authentication) ja V3 (Session Management). Samuti peab seadetel olema lihtne liides arendajatele. Internetist võib leida häid näiteid:

http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Authenticator.html

Organisatsioonide arendajad peavad tegema suuri jõupingutusi vältimaks XSS vigu, millega saab varastada sessiooni ID-sid.

Näide 1

Järgnevas lingis esineb sessiooni ID, millega oleks näiteks võimalik ühel kasutajal anda teisele voli kasutada tema sessiooni ja ehk ka krediitkaarti. Tegu on lennupiletite ostul kujundatud sessiooni ID-d sisaldava lingiga.

- http://example.com/sale/saleitems;
  jsessionid=2P0OC2JDPXM0OQSNDLPSKHCJUN2JV
  ?dest=Hawaii

Näide 2

Aegviide (timeout) pole korralikult seatud. Sisse loginud kasutaja sulgeb veebiakna, logimata end välja. Järgmine arvutikasutaja pääseb tema kontosse siis, kui sessiooniküpsis pole aegunud.

OWASP V2: http://code.google.com/p/owasp-asvs/wiki/Verification_V2

OWASP V3: http://code.google.com/p/owasp-asvs/wiki/Verification_V3

A10 - Unvalidated Redirects and Forwards

Ründajad

Võimalik üle kavaldada inimesi suunamiste abil sisestama kellegi kodulehele mittevajalikku infot. Iga veebileht või HTML *feed*, mida kasutajad kasutavad, võimaldab seda.

Haavatavus

Ründaja lingib valideerimata suunamisi ning kavaldab ohvreid sellele klikkima. Ohvrid suure tõenäosusega teevad seda, kuna link on näiliselt valideeruv. Ründaja suunab ebaturvalisel moel turvakontrollidest mööda.

Levimus ja avastatavus

Rakendused suunavad kasutajaid tihti teistele lehtedele või kasutavad sisemisi suunamisi samal moel. Mõnikord on sihtleht määratud valideerimata parameetritega, lubades ründajatel sihtlehte ise valida.

Mõju

Sellised suunamised võivad üritada installeerida pahavara või üritavad sundida kasutajat avaldama oma paroole või muud vajalikku infot. Ebaturvalised suunamised võivad lubada ligipääsukontrollist möödumist.

Mõju ärile

Kasutajad võivad kaotada usu firma vastu, kuna sealt võib tulla pahavara või häkitakse kontodesse sisse.

Kas ma olen haavatav suunamiste suhtes?

Parim viis leidmaks, kas rakenduses kasutatakse mitte valideeruvaid suunamisi või mitte:

- Tuleks vaadata koodis olevaid suunamise jälgi, kas suunatakse kuhugi või mitte. Igal suunamisel tuvastada, kas sihtaadressis on mõni parameetri väärtus. Kui nii, siis tuleb kontrollida nende valideerumist, et see sisaldaks ainult lubatud sihtkohta või selle osa.
- Tuleks uurida, kas leht loob suunamisi (HTTP vastuskoodid 300-307, tavaliselt 302). Kontrollida parameetreid, mis edastatakse suunamisele, kas need ilmuvad sihtaadressis või aadressi osas. Kui nii, siis tuleks muuta aadressi sihti ning vaadata, kas suunatakse teise kohta.
- Kui kood pole kättesaadav, tuleks kontrollida kõiki parameetreid, et näha, kas need tunduvad edasisuunamise aadressi moodi ning testida neid.

Kuidas vältida mitte valideeruvaid suunamisi?

Turvaliselt saab suunamisi kasutada näiteks nii:

- Vältides suunamisi
- Kui kasutada, siis kasutaja parameetreid ei tohiks sihtkoha arvutamisel kasutada.
- Kui sihtkoha parameetreid ei saa vältida, siis tuleks veenduda lisatud väärtuste valideeruvuses ja et kasutajal on nendele õigus.

Näide 1

Rakendusel on leht nimega „redirect.jsp“, mis kasutab ühte parameetrit „url“. Ründaja kasutab teist aadressi ja suunab ohtlikule lehele, mis varastab andmeid ja installeerib pahavara:

http://www.example.com/redirect.jsp?url=kuri_leht.ee

Näide 2

Rakendus kasutab suunamist erinevate leheosade vahel. Selle lihtsustamiseks kasutatakse parameetreid, et määrata, kuhu kasutaja tuleb saata, kui toiming õnnestub. Sellisel juhul kasutab ründaja aadressi, mis möödub rakenduse ligipääsukontrollist ja suunab ründaja administreerivate funktsioonide juurde, mida ei tohiks tal olla tegelikult võimalik kasutada.

http://www.example.com/suvaline.jsp?fwd=admin.jsp