TIEA222 Tietoturva, laboratoriotyö 3
SQL-injektio

Joel Lehtonen

15.10.2010, v1.1

1 Johdanto

Virheelliseen syöttötietoon perustuvat hyökkäykset ovat jo pidemmän aikaa vaivanneet Web-pohjaisia sovelluksia. Dynaamisten Web-sovellusten myötä hyökkäykset ovat entisestään yleistyneet, sillä monimutkaisten sovellusten takana käytetään entistä enemmän erilaisia tietokantapohjaisia ratkaisuja kuten MySQL. Nämä hyökkäykset hyödyntävät sitä seikkaa, että suurin osa sovelluksista ei tee selkeää eroa käyttäjän antaman syötteen ja ohjelmalle annettavien käskyjen välillä. Tämä mahdollistaa sen, että hyökkääjä pystyy piilottamaan esimerkiksi Web-sivun lomakkeeseen kenttiin ohjelmatason käskyjä, jotka muokkaavat sovelluksen toimintaa hyökkääjän haluamaan suuntaan.

Structured Query Language (lyh. SQL), joka on alan vakiintunut standardi tietokantojen käsittelyyn, on käytössä lähes jokaisessa Web-sovelluksessa, joka käyttää jonkinlaista tietokantaratkaisua. Sen syntaksi on sekoitus ohjelmakäskyjä ja käyttäjän antamia syötteitä, ja huonosti määritettynä käyttäjän antama syöte voidaan tulkita virheellisesti ohjelmatason käskyksi. Tämän syötteen hyökkääjä joutuu usein etsimään sokeasti, mutta syötteet kuten

- `' OR 1=1 --`
- `') OR 1=1 --`

toimivat hyvin usein. Virheellisestä hausta aiheutuvat virheilmoitukset antavat myös erittäin paljon hyödyllistä tietoa hyökkääjälle. Koska suurin osa SQL-tietokannoista mahdollistaa useamman perättäisen syötteen antamisen, kunhan syntaksi pysyy oikeana, voidaan näiden avulla katkaista ohjelman normaali toiminta.

Tehtävänäsi on kokeilla tällaisen hyökkäyksen tekemistä turvallisessa laboratorioympäristössä virtualisoidulla laitteistolla.

2 Valmistelu

Valitse *Käynnistä*-valikosta *Oracle VM Virtualbox...Virtualbox*. Valitse *Tiedosto*-valikosta *Tuo laitteistokuva*. *Valitse*-painikkeen takaa avautuu tiedostoluettelo. Hae sieltä hakemistossa `C:\MyTemp\tiea222` löytyvä virtuaalikone *Desktop*. Toista käsittely myös virtuaalikoneille *server1* ja *server2*.

Virtuaalikoneiden tuonti kestää useita minuutteja. Välillä tulee varoitus profiilin täyttymisestä. Siitä ei tarvitse murehtia. Tila vapautetaan lopuksi.

Käynnistä virtuaalikoneet. Käynnistä ensin *server1*, joka on verkon reititinkone. Odota, että ruudulle tulee kirjautumiskehote. Sen jälkeen käynnistä koneet *desktop* ja *server2*. Palvelinikkunat voi pienentää, koska niihin kirjautuminen ei ole tarpeen. Lopuksi työpöytäkoneen voi halutessaan suurentaa koko ruutuun painamalla Host+F (Host = oikea ctrl). Pois pääset samalla näppäimellä.

3 SQL-injektio

Kirjaudu työpöytäkoneelle. Salasana on *passwd*.

Käynnistä virtuaalikoneen sisällä Web-selain ja navigoi osoitteeseen http://kapital.example.com . Selaimeen avautuu kuvitteellisen yrityksen etusivu, jonne voit jättää yhteystietosi.

Mikäli Web-lomakkeen käsittely kestää monta sekuntia, voit yrittää nopeuttaa sitä sallimalla ulkoiset yhteydet *server1*-koneelle. Kyseisestä ikkunasta valitse *Laitteet...Network adapters..Sovitin 2...Kaapeli liitetty*. Muutos astuu voimaan ilman uudelleenkäynnistystä.

Lomakkeen syöte käsitellään seuraavasti:

```
$sth = $dbh->prepare("insert contact (email) values ('".$email."');".
                     "select count(*) from contact;");
```

Selvitä, miten ja miksi ylläoleva koodinpätkä on haavoittuvainen SQL-injektiolle. Löydettyäsi haavoittuvuuden käytä tietokantakurssilla oppimiasi SQL-kielen taitoja omien SQL-komentojen injektointiin. Muistin virkistämiseksi ohjeet muutamaan yleisimpien komentojen käyttöön MySQL-tietokannassa:

SELECT	http://dev.mysql.com/doc/refman/5.0/en/select.html
INSERT	http://dev.mysql.com/doc/refman/5.0/en/insert.html
DELETE	http://dev.mysql.com/doc/refman/5.0/en/delete.html

Lisäksi tiedät etukäteen, että tietokannan taulujen rakenne on seuraavanlainen:

taulu	sarakkeet
contact	id, email
employee	id, name, salary

Käyttämällä näitä tietoja hyväksi toteuta tietomurto, jossa selvität yhteystiedot, jotka on palveluun jätetty ennen vierailuasi. Löydätkö kolme sähköpostiosoitetta? Selvitä myös yrityksen pääkapitalisti K. Marxin palkka. Lopuksi voit yrittää tuhota kaikki tietokantaan tallennetut sähköpostiosoitteet.

Q1: Miksi palvelin on altis SQL-injektiolle?

Q2: Miten käyttäjän syötteet tulisi käsitellä PDO:ssa (PHP:n kirjasto) oikeaoppisesti?

Q3: Mitkä kolme sähköpostiosoittetta palvelusta löytyivät?

Q4: Kuinka paljon K. Marx ansaitsee?

Liitä vastauksiin myös se merkkijono, jolla sait ylläolevat tiedot urkittua.

4 SQL-liikenteen tutkiminen

Nyt ollaan samassa lähiverkossa MySQL-tietokannan ja Web-palvelimen kanssa. Tutkitaan hiukan MySQL:n viestintää.

Käynnistä pääte (*Applications...Accessories...Terminal*) ja käynnistä siellä *wireshark* pääkäyttäjänä seuraavasti:

```
$ sudo wireshark
```

Kaappaa verkossa liikkuvaa dataa ja tutki SQL-protokollalla välitettyä liikennettä. Vastaa seuraaviin kysymyksiin:

Q5: Käytetäänkö MySQL:n protokollassa salausta?

Q6: Pystyisitkö selvittämään tietokantapalvelimen salasanan?

Q7: Mitä uusia mahdollisuuksin tietokannan informaation vääristämiseen on, kun päästään samaan lähiverkkoon, jossa palvelimet sijaitsevat?

5 Bonus

Tämä on bonustehtävä niille, joilla jäi aikaa vielä jäljelle.

Palvelimissa on ainakin yksi tunnettu ja korjaamaton tietoturva-aukko. Etsi se ja hanki pääkäyttäjän oikeudet. Raportoi lyhyesti, mitä tietoturva-aukkoa käytit ja mitkä olivat työn vaiheet.

Jos haluat kokeilla local-to-root -hyökkäystä, voit ensin kirjautua Web-palvelimelle osoitteessa `10.0.0.1`. Käyttäjätunnus on `user` ja salasana on `passwd`. Tietoturva-aukko ei tosin tässä tapauksessa ole tämä heikko salasana tai se, että pääkäyttäjän oikeudet saa sudolla. ;-) Hyökkäyksessä mahdollisesti käyttämäsi tiedostot voit siirtää koneelle esimerkiksi oman muistitikun avulla *desktop*-koneelta käsin.

6 Siivoa jälkesi

Jotta pääset uloskirjautumaan Windowsista, tulee tilaa vapauttaa poistamalla profiilihakemistossa olevat Virtualboxin tiedostot.

Aluksi sulje Virtualbox ja kaikki käynnissä olevat virtuaalikoneet. Sitten poista hakemisto `C:\Documents and Settings\TUNNUS\.VirtualBox`, jossa `TUNNUS` on oma käyttäjätunnuksesi.

7 Työseloste

Vastaa työssä esitettyjen kysymysten lisäksi alla oleviin kysymyksiin ja palauta vastauksesi viikon kuluessa sähköpostitse osoitteeseen tietoturva@zouppen.iki.fi .

Q8: Mikä oli käyttämäsi työohjeen versionumero?

Q9: Mitä opit tästä laboratoriotyöstä? Oliko työstä muuta hyötyä kuin kurssimerkintä?

Q10: Mitä ongelmia sinulla oli tämän laboratoriotyön tekemisessä?

Kiitos.