Säktest á la ET

Dennis Haglund

Konsultchef Test Omegapoint AB

Omegapoint AB – Säkerställer framtagande och införande av affärsdrivna, högkvalitativa och säkra IT-lösningar.

omega point.

Omegapoint AB

- Medarbetarägt
- Ca 180 anställda
- Kontor: Stockholm, Göteborg, Malmö, Helsingborg, Falun, Umeå och New York
- Utveckling, arkitektur, projektledning, test
- Säkert

omega point.

Omegapoint och Test

- Traditionell test
- Test i agila team
- Kontextdriven test
- **Utforskande/Exploratory test**
- **Test med säkerhet**
- Penetrationstest
- Social Engineering – Hur man hackar en människa

omega point.

Säktest

- Vad är säkerhet? Är det något som är värt att tänka på?
- Säktest går utmärkt att göra utifrån ET-cykeln
- Säktestning behöver inte vara ostrukturerat hackande, även om det till en början inte går att skripta och förutsäga

Bakgrund

- Testare Haglund, ivrig och angelägen
- Testledarens direktiv:
  - Följ samtliga testcase och E2E-scenarion.
  - Allt annat är out of scope
  - ET är lek och bortkastad tid

- Testare Haglund sätter igång och blir självklart klar i förtid, och trots testledarens direktiv drömmer han sig bort i den utforskande världen…

Exploratory Testing
Exploratory Testing
Exploratory Testing

omega point.

Exploratory Testing

- ET-cykeln
  - Align yourself with the mission
  - Concieve a question, wich answered will lead closer to the mission
  - Device an experiment
  - Observe the outcome
- Testare Haglund kommer plötsligt ihåg att han var på kurs i ”Säker Applikationsutveckling” på Omegapoint…Säkerhet, kan man kombinera det med ET?
- Han beslutar sig för att prova.

- What could possibly go wrong?

Company.com

- Vilka inputvägar finns det?
- Användarnamn, lösenord - denhag, verkar funka som förväntat
- Klicka på länkar till nyheter
- Observera att id-siffran på urlen ändrar sig
- Det betyder att adressfältet är ett inputfält… hmm!

Testa

- Prova 1,3 => olika artiklar
- Prova 4711 => null. Databasen säger något om sin syn på världen
- Prova skräp * => SQL Exception
- Lär oss att * tydligen tolkas som del i SQL-sträng

Testa mer…

- Prova med något som är valid syntax: '
- Lär oss att det som står innan ' tydligen är del av unquoted string
- Prova att "förlänga strängen" AND 1=1
- Lär oss att databasen tolkar vår input
- Prova att provocera falskt AND 1=0
- Lär oss att vi kan ställa binära frågor till databasen

Don’t stop now

- Prova om metadata finns tillgängligt - vet att MSSQL har sysobjects
- AND (select count(*) from sysobjects)>20
- Vi har fått ut ”en” bit information om databasen!
- AND (select count(*) from sysobjects)>25
- AND (select count(*) from sysobjects)=25

Nyfiken?

- Nu skulle vi kunna fortsätta och fråga om det finns tabell som börjar på 'a'
- (select count(*) from sysobjects where substring(name,1,1) = 'a') > 0
- börjar på 'b' -> nej
- börjar på 'c' -> ja…
- börjar på 'i' -> ja
- börjar på ’aa' -> nej
- börjar på ’ab' -> nej
- …(name,1,7 = ’iwauser’)…!!!!

Hoppla Kerstin…

- Kan vi månne göra samma sak för kolumnerna i iwauser som börjar på 'a' osv …?
- JA! Vi kan faktiskt ta reda på hela databasens struktur!
- Vi kan hitta hur många rader finns det i respektive tabell, vi kan hitta värden i respektive rad!
- Vi kan till slut hitta väldigt användbar information.
- Men det tar ju en enorm tid…
- Fast, nu när vi använt oss av lite tanke så kan vi köra ett verktyg som hjälper oss att skripta detta. T ex Absinthe (Absinthe does not aid in the discovery of SQL Injection holes. This tool will only speed up the process of data recovery).

omega point.

Kan/får det verkligen vara så här?

- Ja det kan det… nej det får det inte!
- Om det är så här illa i adressfältet, hur fungerar Loginfälten?
- Vi testar! Vi vet ju från tidigare test att vi kan använda SQL i adressfältet…
- Slutsats… SQL Injection är möjligt på flera ställen
- Går vi vidare nu så är det inte längre säkerhetstest utan exploit!

Now what?

- Testare Haglund meddelar självklart testledaren att vi har använt utforskande testning för att utreda brister i applikationens säkerhet. Brister som utgör kritiska verksamhetsrisker!
- Varvid testledaren svarar:
  Out of Scope, no action needed (do not stray from the scripted path)!
- Testare Haglund blir en smula upprörd över att inte bli hörsammad och gör något man inte får göra.
- Gissa vad?
- Hade vi kunnat använt något allvarligare kommando?

omega point.

Omegapoint AB

“Säkerställer framtagande och införande av affärsdrivna, högkvalitativa och säkra IT-lösningar.“