Developing Security with Siren Hofvander

Under ett par underbara dagar i slutet av maj besökte vi återigen sköna Örenäs slott, för att här medverka på en av Websteps kompetenshelger.

Ämnet denna gång var säkerhet, något som jag personligen brinner för och vi hade här bjudit in Siren Hofvander, säkerhetsansvarig (eller som hon säger själv ”Professional glitter wizard”) hos Verisure, som föreläsare för att leverera en intressant blandning av kunskap och paranoia.

Innan själva kursen tog fart hade vi fredag kvällen på oss att njuta av det vackra Örenäs slott, här bjöds på fantastisk mat och en bar som såg till att det var hög stämning hela vägen fram in på småtimmarna. Efter en gedigen frukost var det så äntligen dags att inleda lördagens program.

Siren inledde med en genomgång om hotmodellering med fokus på verktygen STRIDE och DREAD.

STRIDE används för att hitta olika kategorier av hot som kan finnas på ett givet system..

- Spoofing
- Tampering
- Repudation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

STRIDE är ett verktyg som låter användaren fokusera sig på relevanta delarna inom varje risk område, som t.ex. processor, data lagring, data flöden eller externa entitor. Men för att någon ska ge oss tid att ta hand om dessa hot så behöver vi något sätt att väga dom mot varandra så vi kan prioritera dom på ett vettigt sätt. Det är här DREAD kommer in.

DREAD är ett verktyg som mäter påverkningen av hot, genom..

- Damage
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Siren delade sen in oss i flera olika grupper där vi gavs ett diagram över en fiktiv webbshop, där vi skulle lösa ett antal uppgifter. För att göra sceneriet mer realistiskt så blev vi dock snabbt avbrutna av en marknadsansvarig som hade en väldigt viktig kampanj som skulle tas hand om, eller en utvecklingschef som plötsligt fick problem med sina servrar. Vårt mål blev att identifiera potentiella problem via STRIDE och sedan använda DREAD för att ha den nödvändiga informationen för att kunna övertala ledningen av e-handelslösningen om att man har valt rätt lösning.

Poängen med denna övning var helt enkelt att visa oss att det inte räcker att man hittar säkerhetsluckorna i ett system, det krävs ofta en del övertygande för att få tid och resurser att fixa dom också.

Under eftermiddagen bytte vi fokus från hotmodellering till mer specifika tips riktat mot back-end utveckling.

Närhelst man designar en applikation så gäller det göra det på en så liten yta så att man kan reagera snabbare om/när man blir attackerad. Stäng här av funktioner på en server som inte används, blockera alla portar som inte används, minimera in-/ut trafiken etc.

Validera alltid all input som om dom kommer från din värsta fiende.

Se till att säkerheten ligger på alla nivåer, det räcker inte att man bara säkrar sin front-end klient, säkerheten måste också finnas på API och även på databas nivå.

Något som kanske verkar dumt, men ändå är väldigt viktigt: - När man hittar säkerhetsfel så måste man också se till att fixa dom.

"*Siren Hofvander spoke about security in the code and mentioned how SQL Injections are still considered as one of the top 10 web application vulnerabilities. Personally I think that this topic is brought up in all of the security discussions and meetups that I attend. Still, to me, it's so strange that developers are not paying enough attention to this simple, yet important topic as it deserves.*" – säger **Maryam Sarrafkia, konsult hos Webstep**

Efter en genomgång av dessa, och många fler tips, var det dags att ta en titt på OWASP topp 10 lista över vanligaste förekommande säkerhetsproblem. Listan speglar vårt digitala landskap och utgår från rapporter från företag över hela världen

- INJECTIONS
  (både SQL och andra former av skriptinjektions)
- BROKEN AUTHENTICATION ANS SESSION MANAGEMENT
  (vilket ofta betyder att folk kan missbruka login systemet till att antingen skapa många sessioner som överbelastar en server eller ger dom rättigheter dom inte borde ha)
- CROSS-SITE SCRIPTING (XSS)
  (vilket kan ha otroligt många användningsområden, i stil med keyloggers, länkar, DOM, javascript mm. som ofta lurar användaren till att "*logga in igen*" och ge bort sin kontoinformation)

Avslutningsvis blev vi lämnade med ett råd, om vi inte tog något annat med oss från hela kursen så var det att "**alltid validera allting**". Alldeles för många säkerhetsproblem kan lösas eller undvikas genom stark och genomgående validering av både input och output.

Louis Hansen, avid Speaker and Consultant @ Webstep

Louis Hansen is a driven developer always striving to learn new things and share this knowledge with those around him. A co-organizer for multiple user groups at Foo Café in Malmö he enjoys discussions about craftsmanship and the many ways that a dedication to our craft can make our daily lives simpler and deliver more value to our users.

För mer information samt pressbilder, vänligen besök:
http://www.webstep.se/
http://www.mynewsdesk.com/se/webstep

För ytterligare frågor, vänligen kontakta:
Tina Kervall, Regionschef på Webstep, Malmö, +46 (73) 351 43 06
Johan Sandström, Marknadsföringsansvarig på Webstep, +46 (73) 514 21 04