Titel: Utvärdering av webgoat.
Deltagare: Kamil Hakim
Person nr: 880324-0293
Handledare: Mads Dam

Sammanfattning:
Jag tänker evaluera om det är möjligt att använda Webgoat som en plattform för en laboration i en framtida kurs i mjukvarusäkerhet för årskurs fyra på KTH.

Bakgrund:
Idag finns det ca 234 miljoner webbapplikationer på internet[1] och bara under 2009 kom 47 miljoner nya. Enligt en rapport som Gartner Resarch[2] släppte förra året sjunker säkerheten på webbapplikationer varje år. Sammantaget innebär detta att många av de nya webbapplikationerna som kommer upp är osäkra och relativt enkla att hacka.

OWASP har ett open source projekt vid namn Webgoat. Webgoat är en webserver som OWASP har gjort osäker så att går att attackera den. Webgoat har många mycket viktiga lektioner i hur man utför t.ex. en SQL injection eller en cross site scripting(XSS) attack.

Problemformulering:
Målet med detta projekt är att konstruera en fiktiv data-laboration för en framtida kurs i mjukvarusäkerhet. Utformningen av uppgifterna bör ske på sådant sätt att liknande laborationer med enkelhet kan återskapas i framtiden.

Webgoat har redan väl formulerade och konstruerade uppgifter, min uppgift blir därför att utifriån dessa välja de mest relevanta och lärorika.

Den fiktiva laboration som jag skall konstruera får anses lyckad om man med enkelhet kan ändra innehållet utan att modifiera angreppsmetoden.

Projektplan
Jag skall inleda min research med att noggrant gå igenom varje lektion på Webgoat för att sedan kunna selektera de lektioner jag anser vara mest lärorika. Jag kommer även att inhandla en bok som behandlar området webbapplikations-säkerhet. Boken ger verktygen för att kunna lösa lektionerna på Webgoat, med andra ord ska jag matcha bokens innehåll med lektionerna på Webgoat. När jag väl har matchat boken med Webgoat så kan jag avgöra vilka lektioner man kan klara med hjälp av boken.

Jag väljer sedan 2-3 st av de lektioner som går att slutföra med hjälp av boken till min laboration. Egna inledningar till varje del av laboration skall författas, med syfte att berätta om hur en sådan laboration går till väga.

Boken jag avser att köpa heter Stuttard, Pinto: The Web Application Hacker's handbook: Discovering and Exploiting Security Flaws, Wiley 2007.

[1] http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/
[2] Security and risk management, Gartner Research

Tidsplan

- Jan 29: Lämna in spec
- I mitten av februari bör jag vara klar med matchningen av bokens innehåll och Webgoats innehåll. Jag tänker då spendera resten av februari månad med att försöka välja ut 2-3st av Webgoats lektioner.

- I början av mars bör jag ha skelettet för uppsatsen klar för mig, jag bör även ha börjat med att författa inledningarna till varje moment i laborationen.

- Mar 10: Mittvägs möte, innan mötet mötet bör jag ha skrivit klart så mycket jag hinner med på rapporten för att sedan kunna fila på den under resten av mars och april.

- I början av april så bör alla texter vara författade så att jag kan börja bearbeta dem.

- Maj 3: Lämna in uppsatsen

Referenser

http://www.lumension.com/Solutions/Vulnerability-Management.aspx

http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/

Security and risk management, Gartner Research(12 augusti -09)

Stuttard, Pinto: The Web Application Hacker's handbook: Discovering and Explointing Security Flaws, Wiley 2007(skall köpa)