Mittuniversitetet
MID SWEDEN UNIVERSITY

DT144G Webbapplikationssäkerhet

Projekt:
En säker webbapplikation

Daniel Bosk*

project.tex 1374 2013-10-14 12:25:00Z danbos

Innehåll

1 Introduktion

Allteftersom att populariteten hos webben växer, och alltså fler applikationer implementeras som webbapplikationer, stiger vikten av säkerheten hos dessa applikationer. Tidigare kunde applikationer som kördes lokalt och som lagrade data lokalt enbart kommas åt på det enskilda systemet, flytten till webben har drastiskt ändrat detta då dessa applikationer nu finns tillgängliga för alla. Privata data är därmed väsentligen mycket mer utsatt än tidigare.

Webbapplikationssäkerhet är dock inte helt enkelt. Det tog många år innan Facebook började använda säkra anslutningar (HTTPS) för alla sidor efter inloggning [Sin11]. Innan detta kunde alltså alla som loggat in till Facebook få sin session kapad av någon som hade tillgång till samma nätverk, exempelvis en annan kund vid samma nätcafé.

Kamkar [Kam10] visar hur en lång kedja med brister i olika webbapplikationer, däribland dem i hemkonsumentroutrar, kan nyttjas av angripare. Därefter

finns åtskilliga andra exempel på stora webbplatser som haft brister, exempelvis: Sony PlayStation Network [Ley11; Hun11], Ubisofts Uplay [Tho13], Yahoo Voices [Bra12; Goo12; Clu12], RockYou [Cub09] och Gawker [Gus10; Obe10].

2 Mål

Målet med projektet är:

- Att redogöra för de vanligaste attackerna mot webbapplikationer.
- Att förklara hur de vanligaste attackerna mot webbapplikationer fungerar.
- Att tillämpa metoder för att förebygga de vanligaste attackerna mot webbapplikationer.
- Att granska programkod för att finna säkerhetsbrister.

3 Läsanvisningar

Inför utvecklingen av projektet bör du ha läst till och med kapitlet "Secure Coding Principles" i *A Guide to Building Secure Web Applications and Web Services* [Wei+05]. Därefter har du övriga kapitel som referens under utvecklingens gång.

Du ska även ha läst kapitel 1–3 i *OWASP Testing Guide* [MKC08] inför projektet. Därefter har du kapitel 4 som stöd för granskningen av ett projekt.

4 Genomförande

Genomförandet av projektet består av två delar. Den första är att utveckla en säker webbapplikation. Den andra är att granska någon annans webbapplikation för att finna eventuella brister som finns eller verifiera säkerheten.

4.1 Utveckling av en säker webbapplikation

Du ska skapa ett system för hantering av användarkonton och lagring av användaruppgifter. Det kan exempelvis vara en prototyp för ett e-handelssystem. Funktionalitet som ska finnas med i systemet är följande:

- Det ska finnas möjlighet att skapa ett konto.
- Det ska finnas möjlighet att besöka sidan som ej inloggad och därefter ska det gå att logga in.
- En användares konto ska lagra känsliga personuppgifter, exempelvis adress och bankkortsinformation.
- Användare ska kunna lämna kommentarer som är läsbara för alla, även ej inloggade besökare.

Det är viktigt att tänka på att du redan från början av utvecklingen behandlar de olika riskerna i OWASP:s topp 10-lista [OWASP13]. Säkerhet måste integreras från början och genomsyra hela designen av systemet, annars krävs med stor sannolikhet en omfattande omstrukturering av systemet i efterhand – vilket är en onödigt stor arbetsinsats.

En annan viktig aspekt är enkel och tydligt strukturerad kod. Detta underlättar granskning av koden och minskar risken för att säkerhetsbrister uppstår.

4.2 Granskning av en webbapplikation

Du ska granska någon annans utvecklade webbapplikation. Testa först att använda systemet, lär dig hur det nya systemet fungerar, då blir det enklare att senare läsa koden. Du ska finna alla möjlig säkerhetsbrister, utgå från OWASP:s topp 10-lista, och i annat fall verifiera att det inte finns några brister.

Du kommer utöver koden även att ha tillgång till utvecklarnas projektrapport. Det är dock viktigt att du inte vilseleds av deras rapport, de kan ha gjort felaktigheter och det är dessa du ska finna.

5 Examination

Uppgiften får genomföras i grupper om maximalt två personer. Detta innefattar både utvecklingen av en webbapplikation och granskningen av någon annans sådan.

För att examinera den eget utvecklade webbapplikation ska ni skriva en akademisk rapport där ni tydligt redogör för att ni har behandlat de tio riskerna i OWASP:s topp tio-lista. Rapporten ska lämnas in i PDF-format, vara skriven med akademisk svenska eller engelska och ha korrekta referenser. För att få deltaga vid opponeringstillfället krävs att rapporten publiceras innan givet slutdatum, se kursmiljön för datum som gäller.

Granskningen är vad som kommer att ligga till grund för presentationerna vid opponeringstillfället. Opponenten, den som granskat webbapplikationen, är den som presenterar projektet och sina slutsatser. Den som utvecklat webbapplikationen får därefter göra tillägg om så önskas. Därefter får opponenten ställa frågor till utvecklaren. Och slutligen ställer examinator frågor till båda parter. Opponentens presentation bör ta 12–15 minuter och därefter 5 minuter för utvecklarens bemötande av presentationen.

Om arbetet har genomförts i grupp kommer examinator vid opponeringstillfället att utse en av gruppmedlemmarna som svara för alla frågor. Tanken är att ni ska arbeta tillsammans, inte dela upp arbetet – notera skillnaden!

Referenser

[Bra12] Anna Brading. *Yahoo Voices hacked, nearly half a million emails and passwords stolen.* Juli 2012. URL: `http://nakedsecurity.sophos.com/2012/07/12/yahoo-voices-hacked/`.

[Clu12] Graham Cluley. *The worst passwords you could ever choose exposed by Yahoo Voices hack*. Juli 2012. URL: http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/.

[Cub09] Nik Cubrilovic. *RockYou Hack: From Bad to Worse*. Dec. 2009. URL: http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/.

[Goo12] Dan Goodin. "Hackers expose 453,000 credentials allegedly taken from Yahoo service". I: *Ars Technica* (juli 2012). URL: http://arstechnica.com/security/2012/07/yahoo-service-hacked/.

[Gus10] Sam Gustin. "Gawker Media Websites Hacked, Staff and User Passwords Leaked". I: *Wired* (dec. 2010). URL: http://www.wired.com/threatlevel/2010/12/gawker-hacked/.

[Hun11] Troy Hunt. *A brief Sony password analysis*. Juni 2011. URL: http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html.

[Kam10] Samy Kamkar. *How I Met Your Girlfriend*. Föreläsning, DefCon18. URL: del 1 – http://www.youtube.com/watch?v=fEmO7wQKCMw, del 2 – http://www.youtube.com/watch?v=2ctRfWnisSk, del 3 – http://www.youtube.com/watch?v=vJtmZZGcR54. 2010.

[Ley11] John Leyden. "Security watchers unpick PlayStation hack". I: *The Register* (maj 2011). URL: http://www.theregister.co.uk/2011/05/13/veracode_playstation_hack_analysis/.

[MKC08] Matteo Meucci, Eoin Keary och Daniel Cuthbert, utg. *OWASP Testing Guide*. 2008. URL: http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf.

[Obe10] Jon Oberheide. *Brief analysis of the Gawker password dump*. Dec. 2010. URL: https://blog.duosecurity.com/2010/12/brief-analysis-of-the-gawker-password-dump/.

[OWASP13] The Open Web Application Security Project. *OWASP Top 10 - 2013: The Ten Most Critical Web Application Security Risks*. Juni 2013. URL: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf.

[Sin11] Ryan Singel. "Facebook Enables HTTPS So You Can Share Without Being Hijacked". I: *Wired* (jan. 2011). URL: http://www.wired.com/threatlevel/2011/01/facebook-https/.

[Tho13] Iain Thomson. "Ubisoft admits major hacking breach, advises password change". I: *The Register* (juli 2013). URL: http://www.theregister.co.uk/2013/07/02/ubisoft_data_breach/.

[Wei+05] Adrian Weismann, Mark Curphey, Andrew van der Stock och Ray Stirbei, utg. *A Guide to Building Secure Web Applications and Web Services*. 2005. URL: http://prdownloads.sourceforge.net/owasp/OWASPGuide2.0.1.pdf?download.