

Høgskolen i Sør-Trøndelag

E.C. Dahlsgate 2
N-N-7004 TRONDHEIM

Att.: Gunnar Bendheim

it's learning as

P.O. Box 2686, Møhlenpris
5836 BERGEN
NORWAY

Visiting address:

O.J. Brochs gate 16B
5006 Bergen
Norway

T: +47 55 23 60 70
F: +47 55 23 60 71
E: post@itslearning.com
Web: www.itsolutions.no
Org. nr.: MVA 980 682 765

Deres ref:

Vår ref: 6/13593

1. februar 2007

Tilbakemelding på test av it's learning

Vi viser til hyggelig og konstruktiv møte i Trondheim 23. januar om sikkerhetsproblemstillinger som er reist i forbindelse med testing av it's learning der ansatte og studenter fra HiST har deltatt. Vi ønsker med dette brevet å gi tilbakemelding på de problemstillingene som ble reist og hva som er våre aktiviteter og forslag til løsninger.

Innledningsvis ønsker vi også å si at den prosessen vi har hatt med Høgskolen siden i høst har gjort at vi nå har gjort en ekstra innsats på sikkerhetspørsmål i programvaren. Fremover styrker vi også fokuset på dette både i vår infrastruktur og i vår applikasjonsutvikling. Vi har for øyeblikket 5 av våre ansatte som jobber med de konkrete sikkerhetsproblemstillingene som Høgskolen har identifisert.

Sikkerhetsproblemstillingene**Høsten 2006**

I høst ble vi av HiST gjort oppmerksom på sikkerhetsproblemstillinger i it's learning. Som Høgskolen kjenner til, ble de konkrete problemstillingene hurtig tatt tak i, sikkerhetsoppdateringer ble gjort på systemet og deretter testet av høgskolens ansatte/studenter.

Noen av de generelle teknikker for innbrudd i datasystemet (f.eks det som kalles Cross Side Scripting - XSS) vil først bli løst når vi gjennomfører alle tiltak som er listet opp nedenfor.

Sluttrapport fra HiST 2006/2007

Vi ble i sluttrapporten fra HiST gjort oppmerksom på noen nye problemstillinger som vi nå har aktiviteter på og som vi nedenfor har beskrevet løsninger på.

HiSTs overordnede problemstilling i dag

Etter møtet i Trondheim 23. januar er vår overordnede forståelse at HiST i dag føler usikkerhet når det gjelder anvendelse av it's learning – om dette er trygt nok. Vårt mål med de tiltak vi har satt i verk er at:

- HiST og våre øvrige kunder skal oppleve at vi tar sikkerhetsforhold svært alvorlig både i utvikling og leveranse av it's learning
 - Både når situasjoner oppstår

- I vårt løpende arbeide
- HiST og våre øvrige kunder skal føle seg trygg på programvaren, slik at feks.
 - Øvingsoppgaver i it's learning trygt kan anvendes
 - Andre brukere ikke kan få tilgang til lærere eller medstudenters kontoer og manipulere data

Med dette som bakgrunn har vi under kommentert de forhold som fremkommer i sluttrapporten fra Høgskolen:

Vi deler aktivitetene inn i fire faser:

1. Brute Force – gjentatte forsøk på innlogging med kombinasjoner av brukernavn/passord:
 - **problemstillingen kan løses allerede idag** med administratorinnstillinger på Høgskolens it's learning installasjon (begrensning av antall påloggingsforsøk).
2. Konferanseverktøyet – innbrudd med deltagelse og avlytting i synkron kommunikasjon
 - Problemstilling som er beskrevet **har blitt utbedret** i en sikkerhetsoppdatering i programvaren **02.02.07**.
3. XSS – med mulighet for manipulering av andres data
 - Problemstilling der HTML filteret vårt ikke stopper all ulovlig kode - **vil bli utbedret i første oppdatering etter uke 5**. (Normalt 1-3 uker senere). Vi har her tidligere hatt et såkalt "blacklist filter" som inneholder en oversikt over *ulovlige tagger*. Det har vist seg at dette ikke er tilstrekkelig da "kreative" hackere kan finne varianter av kode som kan passere filteret. Vi har derfor endret filteret til å være et "whitelist filter" som snur problemstillingen og som i stedet inneholder oversikt over *lovlige tagger*. Dermed vil det ikke med denne metoden være mulig å benytte XSS teknikk etter denne endringen. Det er nødvendig med brukertesting av dette – med bakgrunn i den reduserte funksjonaliteten som dette kan gi for våre brukere. Vi vil ifbm. denne sikkerhetsoppdateringen, vurdere beste måte å gjøre brukertesting av konsekvensen dette vil gi for alminnelige brukere i deres daglige arbeide i it's learning.
4. Eget filområde under it's learning dome (XSS) - med mulighet for manipulering av andres data
 - Problemstillingene rundt filhåndtering er mer omfattende og krever ytterligere spesifikasjonsarbeid før vi kan si noe om når dette kan bli løst. I prinsippet vil filene flyttes til eget domene, slik at XSS teknikk ikke kan benyttes ved filene som lastes opp i its learning. Vi **jobber med spesifikasjoner nå på løsningen**, og hvilke konsekvenser en slik flytting av filer vil få for våre brukere. Når spesifikasjonen er klar vil vi ha oversikt over omfanget av arbeid som må gjøres.

Konklusjon

Sikring av it's learning og it's learnings funksjoner er en kontinuerlig prosess. Men selv om vi ikke kan utelukke at det i fremtiden dukker opp nye sikkerhetsutfordringer knyttet til it's learning eller omliggende infrastruktur mener vi, at med de tiltak som allerede er gjort eller planlagt i løpet av kort tid, kan it's learning trygt benyttes av Høgskolen.

Når det gjelder HiSTs videre forhold til test av sikkerhet i programvaren, har vi denne prosessen konkludert med at det vil være korrekt både for oss og høgskolen at it's learning knytter til seg et eksternt profesjonelt miljø som deltar i testing og kvalitetssikring av disse aktivitetene. Vi har derfor allerede startet en prosess der et eksternt sikkerhetsselskap som vil gjøre videre analyser med utgangspunkt i rapporten som har kommet i fra HiST. Vi ønsker samtidig å takke for samarbeidet med studentene.

Dersom det er forhold som ytterligere kan være med til å bidra rundt tryggheten i sikkerhetsspørsmål knyttet til it's learning ved HiST så står vi til rådighet. Forhold som vi mener er aktuelle å se på i en slik sammenheng kan være:

- Etablering av eksternt autentisering til it's learning mot egen LDAP tjeneste eller FEIDE. Dette vil ytterligere sikre bruk av it's learning ved å eliminere nødvendigheten av å ha flere brukernavn og passord og skape et enhetlig sikkerhetsregime.
- Workshop og informasjonsarbeid rundt lov om personvern for å sikre at leverandørs og kunders rutiner er i tråd med krav i lovverk og forskrifter.

Med vennlig hilsen
it's learning as

Erik Aadland
Markedsdirektør