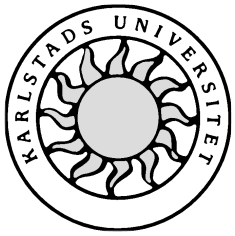


Datavetenskap

---

**Opponent(er):**

**Niclas Hanold**

**Samiar Saldjoghi**

**Respondent(er):**

**Carl-Henrik Svanemark**

**Joakim De Jong**

# Definition och Implementering av Säkerhetsevaluering

---

Oppositionsrapport, C/D-nivå

2009:xx

# 1 Sammanfattat omdöme av examensarbetet

Carl-Henrik och Joakim, har med detta examensarbete arbetat sig fram till en samling säkerhetsfrågor som man kan ta hänsyn till vid testning av webbapplikationer. Projektet verkar ha haft en lyckad utgång med goda resultat för uppdragsgivaren att använda sig av.

Uppsatsen de skrivit är mycket välskriven med få misstag och fel.

# 2 Synpunkter på uppsatsen knuten till examensarbetet

## Titel

”Definition och Implementering av Säkerhetsevaluering” är en bra titel som beskriver vad som innefattades av deras projekt och vilka mål och syften gruppen har haft. Däremot har inte implementeringen av säkerhetskriterierna fått särskilt stort utrymme i rapporten, och känns sekundärt i sammanhanget.

## Uppsatsens disposition

Uppsatsen är tydligt strukturerad med utförlig bakgrundsinformation för de som inte är insatta i datasäkerhet. Vi tycker dock att kapitlet ”Slutsats” hade kunnat fyllas med ett par sidor till, för att väga upp mot den tunga tekniska informationen i resten av uppsatsen.

## Begreppsapparat

Begrepp används konsekvent och är överlag väl förklarade där så behövs. En förteckning över alla förkortningar och begrepp skulle underlätta för läsaren, då många konstiga förkortningar används.

## Argumentering och slutsatsdragning

Argumentationen är i stora drag konsekvent, väl underbyggd och tydlig. Vi hade velat se mer argumentation i slutsatsen, då vi finner det svårt att se hur man har kommit fram till vissa säkerhetsfrågor.

## Sammanfattningen

Sammanfattningen är välskriven och ger en bra inblick i vad uppsatsen behandlar.

## Språkbehandling

Språket som används i uppsats är överlag mycket bra, och på en god vetenskaplig nivå. Vi har stött på ett litet antal stavfel, men inte tillräckligt för att det ska påverka förståelsen för rapporten.

Vi har upptäckt en mening som vi tror innehåller ett syftningsfel:

”Omkring år 2001 publicerades ett antal attacker som tillåtit attackerarna att ta för lite betalt[15].”

Vi tolkar stycket så att det inte är attackerarna som tar betalt, utan det är de som betalar. Därför bör meningen säga att attackerarna betalar för lite, inte att de tar för lite betalt.

## Referat och källförteckning

Uppsatsförfattarna har till synes varit mycket noggranna med att hänvisa till källor när man använt sig av sådana. Vi har inte hittat någon källhänvisning som varit felaktig eller irrelevant.

# 3 Genomgång av uppsatsen kapitelvis

## Kapitel 1

Inledningen ger en tydlig bild av projektet och uppsatsen. Författarna förklarar utförligt vilka avgränsningar man gjort i projektet och varför.

## Kapitel 2

Författarna ger en tydlig beskrivning av deras uppdragsgivare, Compare Testlab, och några av deras samarbetspartners.

Syftet, att definiera ett säkerhetstest, är väl beskrivet och man beskriver på ett bra sätt varför mjukvarutestning är icketrivialt och en behövlig process.

## Kapitel 3

Man ger i kapitel 3 en definition av vad som innefattas av datasäkerhet. Här kunde författarna inkludera en konkurrerande definition av datasäkerhet, för att ge en bredare bild av säkerhet.

Avgränsningen av systemet beskrivs här lite tydligare än i inledningen, och man ger understöd med hjälp av relevanta argument.

## Kapitel 4

Författarna återger tydligt vilka problem man hade under förstudien. Man argumenterar väl för varför man valde att lösa problemen på det sätt man gjorde, nämligen att ta hjälp av uppdragsgivaren.

## Kapitel 5

Kapitlet ger en god redogörelse för vilka aspekter av ett system man kan testa. Man ger en lång och tydlig beskrivning på varje punkt. Punkterna inleds oftast med en formell definition, vilket är oftast är att föredra framför en definition som författaren själv ger.

Vid beskrivning av tekniken SSL används termen SSL RP, utan någon förklaring av vad RP betyder. Här skulle begreppsförteckningen vi nämnde förut komma väl till nytta. Förslagsvis kunde också termen förklaras i den löpande texten.

### Kapitel 6

Kapitlet tar upp Fysisk säkerhet och Policy som punkter som inte ingår i författarnas tester. På sida 4 står ”Dessutom kommer vi inte inkludera mjukvarans omgivning, till exempel operativsystem, eventuell brandvägg, databas och nätverksuppbyggnad.”. Kanske skulle denna avgränsning även tas upp i kapitel 6.

### Kapitel 7

Författarna beskriver testapplikationer som är relevanta för deras projekt på ett översiktligt sätt. I kapitlet beskrivs också ett flertal virtualiseringsmiljöer på ett begripligt sätt.

### Kapitel 8

Slutsatserna och lärdomarna av projektet presenteras här på ett bra och överskådligt sätt. Som vi nämnt tidigare hade vi här velat se lite mer argumentation vad gäller de säkerhetsfrågor man kommit fram till.

De säkerhetsfrågor man kommit fram till beskrivs på ett bra sätt, och har man läst kapitel 5 så förstår man alla dessa frågor och varför de är viktiga.

## 4 Slutliga kommentarer

Denna uppsats vi opponerat på är mycket läsvärd och vi kan rekommendera den till alla som är intresserade av datavetenskap i allmänhet och säkerhetsfrågor i synnerhet. Vi anser att uppsatsen håller mycket hög klass vad gäller språkbruk och struktur.

Uppsatsens innehåll är mycket intressant och ger en god inblick i vilka frågor man kan arbeta med inom det breda begreppet säkerhet. Vi anser att resultatet, de säkerhetsaspekter man bör

titta närmare på, är en användbar samling frågor som vi tror kan komma väl till pass på Compare Testlab.