ملخص

على الرغم من ا لتطور الهائل فى شبكة المعلومات الدولية (الانترنت) و تزايد إستخدامها فى جميع مناحى الحياة ، كان التركيز على تأمين شبكة تبادل المعلومات و تأمين أنظمة التشغيل ، فـتأمين تطبيقات الويب عملية فى غاية الصعوبة ، فبمجرد عمل موقع على شبكة الانترنت يعد بمثابة فتح ثغرة على الشبكة الداخلية يسهل على القراصنة الدخول على أجهزتها (TOE) للحصول على ما تحويه من ممتلكات معلوماتية قيمة ، حيث أنه لم يأخذ تأمين تطبيقات الويب عناية خاصة الا بعد أحداث الحادى عشر من سبتمر عام 2001.

تحاول هذه الرسالة إيجاد الحل لبعض المعوقات الأمنية بإعتمادها على:

- استيعاب المعايير القياسية المختلفة للتأمين لإستخدام أحدها لوضع معايير إجراء اختبارات التأمين .
- استخدام المعايير القياسية لعمل طريقة للتأمين بالتقييم المساعد لتقييم اهداف تأمين تطبيق الويب.
- الفهم الجيد لأدوات التأمين المستخدمة فى إختراق الثغرات و إعادة ترتيبها فى مصفوفة الادوات لأستخدامها كطريقة لتقييم الخطورة المعرض لها النظام.
- إستخدام شجرة الثغرات لزيادة دقة إجراء التأمين.
- إستخدم الطريقة السابقة لفحص تنفيذ طريقة أدوات التأمين المختلفة.

تركز هذه الرسالة على إختبارات تطبيق الويب فى مرحلة التجريب فى دورة تطوير البرمجيات (SDLC) لتطبيقات الويب باسختدام طريقة التقييم المساعد (Security Assessment) أو وفقة التقييم (Posture Assessment). تعتمد هذه الطريقة على اختبارات الاختراق و هى الطريقة الأمثل لتحديد الثغرات الأمنية الموجودة فى الهدف المراد إختباره الغير معروفة باستخدام تقنيات القراصنة المختلفة. تعد طريقة اختبارات الاختراق المقترحة تعديلاً يدمج بين الاختبار بالقييم و طريقة اختبارات التأمين المفتوحة

الكود (OSSTMM) و هى الطريقة القياسية لاختبارات الإنترنت ، و تتكون من أربعة مراحل هى : الإكتشاف و التعداد و مطابقة الثغرات و الإختراق.

تضيف الطريقة المقترحة لاختبارات الاختراق عدة مراحل لطريقة اختبارات التأمين المفتوحة بتعديلها بإقتراح مرحلة الحيز المراد تأمينه (Scope) الذى يعد فى غاية الإهمية و التركيز على اهداف التأمين و قاعدة الاختبار ، حيث بأنه بوجوده يجعل التأمين فى غاية التحديد و يساعد على المشاركة فى استخدام المعلومات ، كما أنه يساعد المؤسسات على تطبيق افضل الطرق و تقييم طريقة التحديد و الاستجابة لمحاولات الاختراق لمنع حدوثها.

كما أنه باضافة مرحلة التحليل و التخطيط وترتيب جميع المعلومات عن الهدف المراد تأمينه يرسم الطريقة لتنفيذ التأمين. كما تضيف الطريقة المعدلة تكرارية العملية لتحديد الثغرات الامنية الموجودة فى الهدف المراد تأمينه لتقليل احتمالية الاختراق بالإضافة الى إضافة مزيد من الحماية.

إختبار النظام بطريقة التقييم المساعد بها العديد من المعوقات تشتمل على إعتمادها على خبرة فريق الإختبار لذا فيوجد العديد من طريق التقييم المختلفة و العديد من أدوات الإختراق مما يجعل عملية الإختراق فى غاية الصعوبة و تشمل جميع الثغرات الأمنية فى لحظة معينة بالهدف المراد تأمينه مما يقلل دقة إجراء الأختبار. كما يعانى من أن زمن إختيار يزيد و يحتاج إلى إختبارها فى منظومة وهمية قبل تجريبها على نظام فعلى ، كما أنه لا يوجد طريقة محددة لإجراء الإختبار غير محددة الآولويات ، كما أن معايير الأختبار تختلف من منظومة الى أخرى بإختلاف أهداف التأمين.

تم تعديل هذه السلبيات باستخدام مفصوفة الادوات المقترحة و التى قد تم اقتراحها على نتائج المسح لادوات الاختراق المختلفة و التى تجاوزت 2000 اداة اختراق و مفصوفة الادوات عبارة عن قاعدة بيانات تتكون من جدول به خمسة اعمدة هى: مرحلة اختبار الاختراق و عمود اسم الاداة و عمود خصائصها و

عمود وجودها على الانترنت (URL) لعمل التعلية المناسبة لها و عمود نظام التشغيل المراد لاختباره و تنفيذ الاداة من عليه.

تضيف مفصوفة الادوات العديد من المزايا لاختبارات التقييم المساعد منها تمثل قاعدة الادوات المرتبة طبقاً لمراحل الاختراق المختلفة ، تعد بمثابة المخزن لجميع ادوات الاختبار مما يسهل على القائم بعملية الاختبار و عدم اعتماد العملية على خبرة القائم بالاختبار وتقلل الزمن اللازم لاختيار الادوات كما تمكن من اجراء نفس الاختبار باستخدام عدة ادوات مما يقلل من إحتمالية الاختراقات المستقبلية.

و بالرغم من تغلب قاعدة بيانات الأدوات على بعض السلبيات إلا أنه توجد سلبيات لم يتم الغلب عليها مثل اولويات البدء فى إجراء الاختبارات و الالوية فى معالجتها ، فتم إستخدام شجرة الهجوم (Attack Tree) ، و الذى يعتبر طريقة تقليدية رياضية لإيجاد طرق إختراق الهدف المراد تأمينه فهى طريقة هرمية (شجرية) تسهل عملية التعرف على كيفية الإختراق و تسهل عملية ترابط المعلومات على مما يساعد متخذى القرار فى التقييم بالتأمين و يساعد على إجراء الاختبارات بطريقة دقيقة و مرتبة موافقة على النظام القياسى ISO/IEC 27005.

ينقسم هذا البحث الى سبعة ابواب هى كالتالى:

الباب الاول: مقدمة عامة عن الهدف من إجراء هذا البحث ، الباب الثانى يستعرض بصورة عامة أساسيات تطبيقات الويب و بعض المشاكل الأمنية ، الباب الثالث يستعرض نظرة عامة عن تقنيات إختبارات تقييم التأمين المختلفة ، و الباب الرابع يستعرض بالتفصيل طريقة اختبارات الإختراق المقترحة ، بينما الباب الخامس التطبيق العملى للطريقة المقترحة و بينما الباب السادس يظهر النتائج و التوصيات و خطة العمل المستقبلية.