دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

العنوان:	بناء أداة برمجية للبحث والوقاية من ثغرة البرمجة عبر المواقع في تطبيقات الويب
المؤلف الرئيسي:	عبدالله، محمد حسن أحمد
مؤلفين آخرين:	يوسف، عوض الكريم محمد(مشرف)
التاريخ الميلادي:	2016
موقع:	الخرطوم
الصفحات:	1 - 294
رقم MD:	854144
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة دكتوراه
الجامعة:	جامعة النيلين
الكلية:	كلية الدراسات العليا
الدولة:	السودان
قواعد المعلومات:	Dissertations
مواضيع:	تطبيقات الويب، لغات البرمجة، أمن المعلومات، الاختراق والمخترقين، الهاتف الذكي، التطبيقات الالكترونية، الشيفرة البرمجية
رابط:	http://search.mandumah.com/Record/854144

© 2021 دار المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو دار المنظومة.

بسم الله الرحمن الرحيم

جامعة النيلين

كلية الدراسات العليا

بحث لنيل درجة الدكتوراه في نظم المعلومات بعنوان:

بناء أداة برمجية للبحث والوقاية من ثغرة البرمجة عبر المواقع في تطبيقات الويب

Build a Software Tool for Search and Prevention against Cross Site Scripting Vulnerability in Web Applications

إعداد الطالب: محمد حسن أحمد عبدالله

إشراف: أ.د.عوض الكريم محمد يوسف

أغسطس 2016م

الإهـداء

إلى من أرضعتني الحب والحنان،،،،

إلى رمز الحب وبلسم الشفاء،،،،،

إلى القلب الناصع بالبياض (والدتي الحبيبة)،،

إلى من جرع الكأس فارغاً ليسقيني قطرة حب،،،

إلى من كلّت أنامله ليقدم لي لحظة سعادة

إلى من حصد الأشواك عن دربي ليسهد لي طريق العلم

إلى القلب الكبير(والدي العزيز)،،،

إلى القلوب الطاهرة الرقيقة والنفوس البريئة إلى رياحين حياتي(أختي)

الى رفيقت دربي في الحياة زوجتي الغالية

الآن تفتح الأشرعة وترفع المرساة لتنطلق السفينة في عرض بحر واسع مظلم هو بحر الحياة وفي هذه الظلمة لا يضيء إلا قنديل الذكريات ذكريات الأخوة البعيدة إلى الذين أحببتهم وأحبوني(أصدقائي).

الشكر والتقدير

قال تعالى : ﴿ وَمَا تَوْفِيقِي إِلاَّ بِاللّهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ﴾ صدق الله العظيم.

الكلمة الطيبة ، والنصيحة الصادقة ، المستمدتان من الكتاب والسنة ، ومن نبل أخلاق الدين الفاضلة ، ومن سلوك أسرة كلية علوم الحاسوب و تقانة المعلومات ، إن هذه الكلمة وتلك النصيحة لتشدان الهمم وخاصة لطلاب العلم والمعرفة في الأمة بوصفهم مصابيح ظلامها ومعارج رفعتها ، فبهم تزدهر وتتقدم ، ومن هنا كانت حاجتنا إلى الرعاية الخاصة والنصح والإرشاد ، لأن في ذلك تحفيزاً للنفوس ، وتقوية للعزيمة ، ليشمر المرء عن ساعد الجد والإجتهاد في طريق رضوان الله وبناء مستقبل زاهر وجاءت هذه الدراسة لتضم من العلم والتطبيق ما ترتاح له النفس، كما أنه دعوة صادقة لكل موهوب أن هيا إلى المجد وأقبل على المعالي ، فلا مكان لمتخلف بين متقدمين ولا مكان لخامل بين مجدين ، ونسأل المولى عز وجل أن تعم به الفائدة ، وأن ينفع به جميع المسلمين.

والسلام ، ، ،

الحمد لله رب العالمين والصلاة والسلام على إمام المرسلين وعلى آله وصحبه والتابعين. وبعد ؛؛؛

فهذا البحث وضعناه لكل صاحب همة وراقب عزيمة، ورفيق طموح ، يريد النجاح في الدنيا والآخرة ، فيكون مقبولاً عند الله وعند خلقه ، راضياً عن ربه وربه راضياً عنه ، محبوباً عند أهله وذويه وأصحابه ، لحياته معنى وله قضية ، ولديه مبدأ، وهذه كلمات نقولها لكل موهوب وطموح ، تقول له : هيا إلى المجد ، وأقبل إلى المعالي وفارق الكسل وأصعد سلم الإبداع ، وترق في درج الكمال وأهتف بقلبك ﴿**انْفِرُوا خِفَافاً وَثِقَالاً**﴾ وأسأل الله تعالى بأسمائه الحسنى وصفاته العلى أن يبلغنا جميعاً منازل الناجحين الفالحين مع الذين أنعم الله عليهم من النبيين والصديقين والشهداء والصالحين وبعد شكر الله سبحانه وتعالى ومن منطلق من لا يشكر الناس لا يشكر الله لا يسعنا في هذا المقام إلا أن أرفع أسمي آيات الشكر والعرفان لكل من ساعدني وأيدني في هذا الدرب وحثّني علي المسير فيه وأخص بشكرنا : الأستاذ الفاضل بروفيسور **عوض الكريم محمد يوسف** المشرف على هذا البحث والذي حرص أن يكون بحثي هذا أنموذجاً لكل البحوث ، وكان بحق أباً وأخاً وصديقاً وأستاذاً ، تجاوز بوقته وجهده واجبات الإشراف ليثري هذا البحث بعلمه وملاحظاته ، فكان على ماهو عليه الآن كما اتوجه بالشكر لجميع الأساتذة الأفاضل الذين منحونا الوقت والجهد في الإستشارات الأكاديمية وقدموا لنا الكثير من المعلومات التي أثرت هذه الدراسة ومنهم على سبيل الذكر وليس الحصر: البروفيسر الفاضل **السماني عبدالمطلب أحمد** والدكتور والاخ والصديق **عثمان النور سليمان فضل الله** ورفيق دربي وصديقي الصدوق الاستاذ **محمد الطيب أحمد حمادي** الذين لهم كل الإحترام والتقدير، والشكر أيضاً موصول لكل الأساتذة والعاملين والمشرفين **بكلية علوم الحاسوب و تقانة المعلومات** الذين لم يترددوا في تقديم العون والنصيحة والمشورة لي خلال فترة دراستي بهذه الكلية الشامخة.

الباحث ،،

المستخلص

تعاني تطبيقات الويب حالياً من إنعدام الأمن في طبقة التطبيقات، وذلك نتيجة لإتخاذ المطورين طرق مختصرة لتطويرها واعتمادهم علي عدد من البرمجيات الجاهزة والمفتوحة المصدر لتطوير العديد من مواقع الويب دون النظر بعمق في هيكلية هذه اللغات ودراسة مدى السرية والأمان الذي يمكن أن تقدمه هذه اللغات لبرامجهم والتي تمكن المخترقين من مهاجمة البنية التحتية الضعيفة للتطبيق. إن الكثير من هذه الهجمات يعتمد بشكل أساسي على ثغرات وأخطاء برمجية يرتكبها مطوري هذه المواقع والتطبيقات. ولعل من أشهر هذه الثغرات وأكثرها خطورة، ثغرة Cross Site Scripting وذلك بحسب مؤسسة Trustwave Global Security.

إن مدخلات المستخدم غير المعقمة تعتبر هي البوابة التي يستغلها الكثير من المخترقين لحقن شيفرات برمجية خبيثة تؤدي إلى منحهم كافة الصلاحيات على تطبيقات ومخدمات الويب. وعلى الرغم من خطورة ما ذكر، إلا أنه لا توجد خطوات بحجم المشكلة لتطوير أدوات تقوم بمحاولة اكتشاف ومنع هذه الثغرات الخطيرة.

تهدف هذه الدراسة لبناء أداة برمجية مؤتمتة لحل مشكلة ثغرة Cross Site Scripting. وقد تمت الاستفادة من مزايا مفاهيم تصميم المترجمات وتقنيات التعابير القياسية Regular Expression في بناء هذه الأداة.

تتكون هذه الأداة من أداتين فرعيتين كل منها يمكن أن يعمل بمفرده. وعند التعامل معهم كوحدة واحدة نجد أنهم مترابطين منطقياً. حيث نجد أن الأداة الأولى تستخدم التحليل الاستاتيكي لتحليل أي تطبيق ويب تمت كتابة شيفرته البرمجية عن طريق لغة PHP مع نظام إدارة قواعد البيانات MySQL واكتشاف ثغرة Cross Site Scripting به مع تحديد موضع الثغرة بكل دقة. أما الأداة الثانية فتم بناؤها على أساس أن كل أدوات التحليل المعروفة الأخرى تقوم باكتشاف الثغرة دون تقديم حلول واضحة لهذه المشكلة، أما هذه الأداة فتستهدف تعقيم جميع مستقبلات مدخلات المستخدم قبل التعامل معها(أي ترميزها وتصفيتها).

تم اختبار الأداة على عدد من مواقع الويب الحقيقية. حيث أظهرت نتائج الاختبار التي تمت على العديد من مواقع الويب نتائج مرضية جداً وفعالة. إلا أن الأداة أظهرت بعض الضعف في التطبيقات التي تمت برمجتها عن طريق البرمجة الكائنية التوجه Object Oriented Programming وإطارات العمل Frameworks.

لذا يوصي الباحث بتطوير هذه الأداة من خلال زيادة عدد الثغرات المستهدفة، ربط الأداة بأداة أخرى تعمل بمبدأ التحليل الديناميكي، ومعالجة الضعف المصاحب للأداة.

Abstract

Web applications currently Suffer from insecurity in the application layer, as a result of using shortcuts and open sources to develop them without looking deeply into the structure of these languages and study the extent of secrecy and security that languages can offer for their programs, which enables hackers to attack the poor infrastructure of the application. Many of these attacks mainly depends on the gaps and errors committed by the software developers of these sites and applications. The most famous and dangerous vulnerability is the Cross Site Scripting, according to Trustwave Global Foundation Security.

The non-sterile user inputs considered as gate that hackers can exploit to inject malicious software codes that lead them to obtain full privileges on the applications and Web servers. In spite of the seriousness of that, but there are no real steps towards the solution, and developing tools to detect and prevent these serious vulnerabilities.

The aim of this study is to build an automated software tool to solve the problem of Cross Site Scripting. The researcher take the advantage and the benefits of Compiler Design and techniques of Regular Expressions to build this tool.

This tool compose of two sub-tools, each of which can act alone. When dealing with them as a single unit, we find that they are logically interrelated. The first tool uses static analysis to analyze any Web application software that written using PHP and MySQL database management system, and it can discover the Cross Site Scripting vulnerability and locating the vulnerability position exactly. The second tool solve the problem of the other tools, that they detect the vulnerability without offering a clear solution to this problem, but this tool are targeted to sterilize all user inputs before dealing with them (sanitize and filter them).

The tool has been tested on a number of real Web sites. Where test results are satisfactory and effective. However, the tool showed some weaknesses of the applications that have been programmed using Object Oriented Programming and Frameworks.

So the researcher recommends to develop this tool by increasing the number of target vulnerabilities, combine the tool with a dynamic one, and address the tool weakness.

فهرس الموضوعات

الآية ..... أ
الإهـــداء ..... ب
الشكر والتقدير ..... ج
المستخلص ..... د
Abstract ..... ه

الفصل الأول: الإطار العام للدراسة

1-1 مـقدمة: 2
2-1 مشكلة الدراسة: 4
3-1 أهداف الدراسة: 5
4-1 أهمية الدراسة النظرية والتطبيقية: 5
5-1 منهجية الدراسة: 6
6-1 الدراسات السابقة: 7
7-1 هيكلية الدراسة: 11

الفصل الثاني: مفاهيم تطبيقات الويب

1-2 مقدمة: 14
2-2 المفهوم الأول: شبكة الزبون/المخدم Client/Server Network 15
1-2-2 أولاً: التقنيات والمفاهيم المرتبطة بالزبون: 17
3-2 المفهوم الثاني: معمارية الويب Web Architecture 46
1-3-2 معمارية تطبيق الويب البسيطة 48

الفصل الثالث: مفاهيم أمن المعلومات

1-3 مقدمة 52
2-3 ماهية الأمن 53
3-3 الحقب الزمنية المتعددة لأمن المعلومات 55
4-3 الخصائص الأمنية للمعلومات 58
5-3 مصطلحات أمن المعلومات الأساسية: 67
6-3 أمنية شبكة الإنترنت 76
7-3 الاحتياطيات الأمنية العامة 77

الفصل الرابع: الإختراقات والتهديدات الأمنية لتطبيقات الويب والهواتف الذكية

1-4 مقدمة 83
2-4 الإختراق والمخترقين 84
1-2-4 التصنيفات المختلفة للمخترقين 88
3-4 تاريخ الاختراق Hacking History 93

4-4 أخطر الاختراقات التي تمت عن طريق Cross Site Scripting 93
4-5-1 الآليات الأمنية لنظام الأندرويد Android Security Mechanisms 115
4-5-2 التقييم الأمني لإطار عمل الأندرويد: 123
4-5-3 هجمات الـ XSS على Android Web View 127
4-5-3 دراسات أمنية عن ثغرات نظام الاندرويد: 129
4-5-4 الحلول الأمنية لتحسين أمن وحماية نظام الأندرويد 134
4-6 الاختراقات وأثرها على الاقتصاد 144
4-6-1 الأضرار التي يمكن أن يتعرض لها الفرد: 144
4-6-2 الأضرار التي يمكن أن تتعرض لها الشركات والمؤسسات الكبرى: 145
4-6-3 الأضرار التي يمكن أن تتعرض لها الأجهزة الحكومية للدول: 145

الفصل الخامس: ثغرة البرمجة عبر المواقع Cross Site Scripting

5-1 مقدمة: 154
5-2 تاريخ ثغرة الـ XSS 155
5-3 مفهوم ثغرة الـ (Cross-Site Scripting) 158
5-4 طريقة عمل ثغرة الـ (Cross-Site Scripting): 159
5-4-1 لماذا الـ XSS 164
5-5 أنواع ثغرة الـ Cross Site Scripting 167
5-6 نماذج لبعض المواقع المصابة بثغرة الـ XSS: 187
5-7 طرق الحماية من ثغرة الـ Cross Site Scripting 194
5-7-1 الترميز Encoding: 198
5-7-2 التحقق validation: 200
5-7-3 أي تقنية تستخدم للحماية من الـ XSS : Which prevention technique to use 203
5-7-4 سياسة أمن المحتوى Content Security Policy (CSP) 204

الفصل السادس: التقنيات المستخدمة في الدراسة

6-1 مقدمة 211
6-2 الترجمة Compiling 212
6-2-1 اللغات المفسرة واللغات المترجمة 213
6-2-2 مراحل الترجمة 216
6-3 التعبير القياسي Regular Expression 222
6-3-2 استخدام محدد الكميات 232
6-3-3 استخدام فئات الأحرف 234
6-3-4 دوال لغة PHP لإيجاد التطابق PHP Functions to find Matching: 235
6-4 فحص الشيفرة البرمجية 237
6-4-1 التحليل الاستاتيكي Static Code Analysis 242

2-4-6 التحليل الديناميكي Dynamic Analysis: 253

الفصل السابع: التحليل - التصميم - التنفيذ

1-7 مقدمة 257
2-7 تحليل الأداة الأولى Scanner: 258
1-2-7 تحليل المدخلات للأداة Scanner: 264
2-2-7 تحليل المخرجات للأداة Scanner: 265
3-7 تحليل الأداة الثانية Sanitizer: 266
1-3-7 تحليل المدخلات للأداة Sanitizer: 268
2-3-7 تحليل المخرجات للأداة Sanitizer: 268
4-7 وصف عملية التصميم 269
1-4-7 تصميم الخوارزميات: 271
1-1-4-7 تصميم المخطط الانسيابي لخوارزمية الأداة Scanner 271
2-1-4-7 تصميم المخطط الانسيابي لخوارزمية الأداة Sanitizer 272
2-4-7 تصميم شاشات النظام 273
1-2-4-7 تصميم الشاشة الرئيسية Home: 273
2-2-4-7 تصميم شاشة الأداة Scanner: 274
3-2-4-7 تصميم شاشة الأداة Sanitizer: 275
3-4-7 تصميم التقارير 276
1-3-4-7 تقرير الأداة Scanner: 276
5-7 وصف تنفيذ النظام: 278
1-5-7 تنفيذ الشاشات: 279
1-1-5-7 تنفيذ الشاشة الرئيسية: 279
2-1-5-7 تنفيذ شاشة الأداة Scanner: 280
3-1-5-7 تنفيذ شاشة الأداة Sanitizer: 283
6-7 التنفيذ والتقييم Implementation and Evaluation: 286

الفصل الثامن: النتائج والتوصيات والخاتمة

1-8 النتائج: 288
2-8 التوصيات: 289
3-8 الخاتمة: 290
4-8 قائمة المصادر والمراجع: 291

فهرس الأشكال

الشكل (2-1) يوضح هيكلية الزبون/المخدم..... 15
الشكل (2-2) يوضح كيفية استقبال الطلبات ومعالجتها 16
الشكل (2-3) يوضح شريط عنوان المتصفح 19
الشكل (2-4) يوضح موضع بروتوكول HTTP..... 30
الشكل (2-5) يوضح الاختلاف بين URI و URL و URN 38
الشكل (2-6) يوضح مفهوم مخدم الويب 41
الشكل (2-7) يوضح مفهوم مخدم التطبيقات 43
الشكل (2-8) يوضح معمارية تطبيقات الويب..... 48
الشكل (4-1) يوضح الصفحة المزيفة لموقع ebay 95
الشكل (4-2) يوضح الصفحة المصابة بثغرة XSS لموقع ebay..... 96
الشكل (4-3) يوضح الصفحة المصابة بثغرة XSS لموقع PayPal 98
الشكل (4-4) يوضح الصفحة المصابة بثغرة XSS لموقع المملكة المتحدة..... 100
الشكل (4-5) يوضح صفحة البحث المصابة بثغرة XSS لموقع المملكة المتحدة..... 101
الشكل (4-6) يوضح نموذج للروابط الخبيثة في بريد Yahoo 103
الشكل (4-7) يوضح صورة لمنتديات اوبنتو المخترقة بواسطة XSS 105
الشكل (4-8) يوضح صورة للثغرة الامنية في windows live من نوع XSS..... 108
الشكل (4-9) يوضح صورة لموقع مجلة Forbes المصاب بثغرة XSS. 110
الشكل (4-10) يوضح صورة لموقع PHP المشوه بثغرة XSS. 111
الشكل (4-11) يوضح رسالة التنبيه لموقع phpbuilder التي تمت عن طريق XSS..... 112
الشكل (4-12) يوضح الهيكلية الاساسية لنظام أندرويد..... 116
الشكل (4-13) يوضح طريقة سرقة ملفات الـ Cookies في الاندرويد عن طريق الـ XSS 128
الشكل (4-14) يوضح طريقة سرقة بعض المعلومات الحساسة في الاندرويد عن طريق الـ XSS..... 129
الشكل (5-1) يوضح مفهوم ثغرة الـ XSS 159
الشكل (5-2) يوضح مثال لشرح طريقة عمل ثغرة الـ XSS 160
الشكل (5-3) يوضح عملية إدخال إسم المستخدم 160
الشكل (5-4) يوضح شاشة عرض إسم المستخدم 161
الشكل (5-5) يوضح الشفرة البرمجية لشاشة عرض إسم المستخدم..... 161
الشكل (5-6) يوضح ناتج إدخال وسم HTML مع إسم المستخدم 162
الشكل (5-7) يوضح الشفرة البرمجية بعد إدخال وسم HTML مع إسم المستخدم..... 162
الشكل (5-8) يوضح ناتج تنفيذ شفرة جافا اسكريبت في التطبيق. 163
الشكل (5-9) يوضح التقرير الامني للWhiteHat Security للعام 2014 حول ثغرة XSS 165
الشكل (5-10) يوضح تصنيف نقاط الضعف حسب لغات البرمجة. 166
الشكل (5-11) يوضح تقرير Trustwave Global Security حول ثغرة XSS للعام 2016م. 166
الشكل (5-12) يوضح مفهوم الـ DOM Based XSS..... 168
الشكل (5-13) يوضح طريقة عمل دوال المصدر..... 170
الشكل (5-14) يوضح طريقة عمل دالة location.pathname 170
الشكل (5-15) يوضح عملية قراءة المدخلات المرسلة للصفحة..... 171
الشكل (5-16) يوضح عملية طباعة العبارات داخل شفرة HTML. 172
الشكل (5-17) يوضح طريقة تغيير محتوى الصفحة عن طريق جافا اسكريبت..... 173
الشكل (5-18) يوضح طريقة عمل دالة الـ location.hash. 174
الشكل (5-18) يوضح طريقة ارسال XSS Payload للصفحة. 175
الشكل (5-19) يوضح ثغرة من نوع Dom-Based XSS في موقع Redhat.com. 176
الشكل (5-20) يوضح مفهوم الـ Storing XSS..... 177
الشكل (5-21) يوضح مثال لصفحة مصابة بثغرة Storing XSS. 178

الشكل (5-22) يوضح عملية حقن شفرة خبيثة في مكان تعليق المستخدم 179
الشكل (5-23) يوضح ناتج تنفيذ الشفرة الخبيثة..... 180
الشكل (5-24) يوضح مفهوم الـ Reflected XSS. 182
الشكل (5-25) يوضح طريقة عمل الـ Reflected XSS. 184
الشكل (5-26) يوضح الصفحة الرئيسية لموقع etsexpress.com..... 185
الشكل (5-27) يوضح إصابة موقع etsexpress.com بثغرة الـ Reflected XSS..... 186
الشكل (5-28) يوضح صفحة البحث لموقع caribbeanbusiness.pr..... 187
الشكل (5-29) يوضح اصابة موقع caribbeanbusiness.pr بثغرة XSS..... 188
الشكل (5-30) يوضح الصفحة الرئيسية لموقع deephousepage.com..... 188
الشكل (5-31) يوضح إصابة موقع deephousepage.com بثغرة XSS..... 189
الشكل (5-32) يوضح الصفحة الرئيسية لموقع etsexpress.com..... 189
الشكل (5-33) يوضح مصابة بثغرة XSS لموقع etsexpress.com. 190
الشكل (5-34) يوضح عملية استغلال ثغرة الـ XSS لسرقة ملفات الـ Cookies. 190
الشكل (5-35) يوضح الصفحة الرئيسية لموقع Registry.adoption.com..... 191
الشكل (5-36) يوضح صفحة البحث لموقع Registry.adoption.com المصابة بثغرة XSS..... 192
الشكل (5-37) يوضح صفحة البحث المصابة بثغرة XSS لموقع voices.iit.edu..... 193
الشكل(6-1) يوضح كيفية البحث عن كلمة mo في سلسلة حرفية. 224
الشكل (6-2) يوضح استخدام مفهوم الإيعازات 226
الشكل (6-3) يوضح استخدام علامة الانبوب 228
الشكل (6-4) يوضح استخدام مفهوم التفرع 229
الشكل (6-5) يوضح استخدام مفهوم الاقواس 230
الشكل (6-6) يوضح استخدام مفهوم تعقيد الأقواس 231
الشكل (6-7) يوضح مخطط التحكم في تدفق البرنامج..... 246
الشكل (7-1) يوضح مفهوم ثغرات التلوث 259
الشكل (7-3) يوضح مخطط تدفق الأداة Sanitizer 272
الشكل (7-4) يوضح تصميم الشاشة الرئيسية للأداة..... 273
الشكل (7-5) يوضح تصميم شاشة الأداةScanner..... 275
الشكل (7-5) يوضح تصميم شاشة الأداةSanitizer 276
الشكل (7-6) يوضح تصميم التقرير الخاصة بالأداة Scanner 277
الشكل (7-7) يوضح تصميم الشاشة الرئيسية للأداة..... 279
الشكل (7-8) يوضح شاشة الأداة Scanner 280
الشكل (7-9) يوضح شاشة التقرير الخاصة بالأداة Scanner لملف مصاب..... 281
الشكل (7-10) يوضح شاشة التقرير الخاصة بالأداة Scanner لملف سليم 282
الشكل (7-11) يوضح شاشة الأداة Sanitizer..... 283
الشكل (7-12) يوضح الشاشة التي تطلب فتح أو حفظ الملف المعقم 284
الشكل (7-13) يوضح جزء من الشيفرة البرمجية المراد تعقيمها 285
الشكل (7-14) يوضح الشيفرة البرمجية بعد إضافة دالة التعقيم Sanitizer 285

الفصل الأول

الإطار العام للدراسة

1-1 مقدمة:

عادة ما نتوقع من الحاسبات أن تتصرف حسب الطرق التي أمرناها بالتصرف وفقها. ففي واقع الأمر نحن نعتمد على البرمجيات كي تكون وسيطاً بيننا وبين الحواسيب. ولكن الحواسيب الحديثة وبرمجياتها أصبحت معقدة جداً بحيث باتت هناك عدة طبقات برمجية ما بين النقرة على الفارة وبين النتيجة التي نتوقع رؤيتها. ولكي نستفيد من قوة حواسيبنا، نحن نعتمد على صحة كل تلك الطبقات التي بيننا. من الممكن أن يكون في أي من هذه الطبقات ثغرة ما، حيث من الممكن أن لا تعمل البرمجيات كما أراد مبرمجوها. وهذه الثغرات تبدأ من أشياء بسيطة قد تؤدي الى إزعاج مستخدمي أنظمة الحاسوب كهجمات تعطيل الخدمة DOS Attacks، إلى تأثيرات قد تؤدي إلى انهيار نظام برمجي بالكامل كفيض الذاكرة Buffer Overrun، الذي يترك المتطفلين العابثين ينفذون الشيفرة التي يريدونها بدلاً من شيفرة التطبيق الاصلية أو هجمات Cross Site Scripting التي تتيح للمخترقين حقن شفرات برمجية خبيثة في التطبيق مما يؤدي الى سرقة بيانات المستخدمين في الموقع أو تشويه شكل الموقع ككل.

إن بعض المؤسسات تركز إلى حد كبير على توفير الأمن على مستوى الشبكةNetwork layer من خلال الجدران النارية firewalls واستخدام طرق التشفيرEncryption المختلفة ولكنها لا تركز على طبقة التطبيقات Application layer، مما يتيح وسيلة للمخترقين لمهاجمة التطبيقات.

تعاني تطبيقات الويب حاليا من إنعدام الأمن في طبقة التطبيقات، وذلك نتيجة لاتخاذ المطورين طرق مختصرة لتطويرها واعتمادهم علي عدد من البرمجيات الجاهزة والمفتوحة المصدر لتطوير العديد من مواقع الويب دون النظر بعمق في هيكلية هذه اللغات ودراسة مدى السرية والأمان الذي يمكن أن تقدمه هذه اللغات لبرامجهم والتي تمكن المخترقين من مهاجمة البنية التحتية الضعيفة للتطبيق في غضون ساعات، وذلك باستخدام متصفح الويب. فتصميم مواقع ويب وأنظمة غير آمنة برمجياً عادة ما يؤدي لمشاكل ذات آثار خطيرة جداً علي المعلومات التي تتعامل معها هذه المواقع والأنظمة.

نجد أن كثير من المبرمجين يقومون بتصميم تطبيقات ويب ثم يقومون برفعها مباشرة على شبكة الويب دون فحص الثغرات البرمجية الموجودة بها، والتي تؤدي الى أخذ بيانات غير موثوقة وإرسالها لقاعدة البيانات عبر المتصفح من غير ضوابط ولا تقييد وهذا ما يتسبب في ثغرة الـ (Cross Site Scripting). تتمثل هذه العملية في إدخال (حقن Injection) شفرات Java script او أي لغة script أخري ليتم تنفيذها مباشرة من قبل أي متصفح ضمن صفحة ما بحيث يتم حفظ هذه الشفرات بشكل دائم في قاعدة بيانات الموقع، لذلك نجد أن عملية إدخال البيانات الشخصية للأفراد وتقديم الخدمات ذات البيانات عالية الخصوصية عبر ملء نماذج الويب أمر في غاية الخطورة في عصرنا هذا. حيث يستغل القراصنة هذه العمليات لتنفيذ هجمات الـ XSS (Cross Site Scripting).

إن ثغرة الـ Cross Site Scripting هي عبارة عن نوع من أنواع الحقن Injection، حيث تحدث عندما يستخدم أحد المهاجمين تطبيق ويب لإرسال شفرات برمجية خبيثة. تكمن خطورتها في تعديل محتوى صفحات الموقع التي تظهر للمستخدم وذلك عن طريق حقن شفرات HTML أو JavaScript كأنك تقوم بالضبط بالتعديل على ملفات الـ html و JavaScript الخاصة بالموقع من خلال أحد برامج محررات صفحات الويب. فثغرة XSS تساعد المخترق على تعديل صفحات الموقع وعمل صفحات مزورة مع الاحتفاظ بنفس رابط الصفحة والـ(Domain) ، كما يستغلها البعض لسرقة الـ Sessions او الـ Cookies الخاصة بالمستخدمين و هو يعد أخطر استغلال لثغرات XSS .

يشير التقرير الأمني لـ (Trustwave Global Security) في العام 2016 الى ان ثغرة الـ XSS من الثغرات البرمجية الاعلى خطورة التي تم تحديدها عن طريق Penetration Testing.

حيث أصبحت من الثغرات الأمنية التي تشكل تهديدا لا يقتصر على مستخدمي الويب من الأفراد وإنما أصبح يؤثر على اقتصاد وأمن الدول التي تعتمد علي الانترنت. وتعتبر الاختراقات من أهم التحديات التي تواجه أمن المعلومات في العصر الحالي، وتتطلب تضافر الجهود من اجل مكافحتها والتقليل من خسائرها.

2-1 مشكلة الدراسة:

نقاط الضعف المعتمده في تطبيقات الويب تشكل تحدياً خاصاً في الكشف عنها، عندما يقوم المطورين بانشاء التطبيق فانه غالباً ما يكون لديهم صورة واضحة عن الكيفية التي يجب أن يكون فيه التطبيق مثالي في عقولهم ولكن للأسف، من خلال الممارسة العملية، عند تنفيذ التطبيق في كثير من الأحيان لا يكون كما كانوا يتصورون و بعبارة أخرى، مدخلات المستخدم غير المتوقعة والتدفقات المنطقيه يمكن أن تسمح للمهاجمين بتنفيذ هجومهم على التطبيق.

هذا الأمر مثل لي دافعاً أساسياً للقيام بهذه الدراسة، ويمكن تلخيص مشكلة هذه الدراسة في التالي:

1. عدم توفر الأمن لكثير من مواقع الويب وتعرضها للاختراق بسبب ضعف في كتابة الشيفرات البرمجية. هذا الضعف أدى إلى إحداث ثغرات كثيرة جداً أخطرها على الإطلاق ثغرة Cross Site Scripting، وذلك بحسب التقرير الأمني Trustwave Global Security للعام 2016م .
2. صعوبة فحص ملفات تحتوي على الآلاف من الأسطر البرمجية بصورة يدوية، وإن تم ذلك فإنه سيحتاج للكثير من الزمن والجهد والتكلفة.
3. عدم وجود أداة مؤتمتة لحماية الشيفرات البرمجية من ثغرة Cross Site Scripting، وتحديداً حماية مستقبلات مدخلات المستخدم والتي تعرف باسم Super Global، بل تعتمد معظم الأدوات الموجودة على تحديد أماكن الضعف البرمجية دون تقديم حل كامل لها.

1-3 أهداف الدراسة:

1. تطوير أداة برمجية لتحليل الشيفرات المصدرية لتطبيقات الويب المكتوبة بلغة PHP، بصورة مؤتمتة من أجل كشف ثغرة الـ Cross Site Scripting بها.
2. تطوير أداة لتعقيم وتنقية مستقبلات مدخلات المستخدم Super Globals، والتي يتم استغلالها من قبل المخترقين لحقن شيفرات برمجية خبيثة تقود لتنفيذ هجمات الـ Cross Site Scripting.
3. الاستفادة من مزايا كل من تصميم المترجمات والتعابير القياسية لتطوير أداة فاعلة في مواجهة ثغرة الـ Cross Site Scripting.
4. زيادة التوعية بالثغرات الأمنية ونقاط الضعف البرمجية التي ينتشر وجودها في معظم الأنظمة ومواقع الويب من خلال عرض نماذج لبعض مواقع الويب المصابة بثغرة الـ Cross Site Scripting.
5. التأكد من جودة الأداة من خلال استخدامها على مواقع حقيقية وتوضيح مدى فاعليتها.

1-4 أهمية الدراسة النظرية والتطبيقية:

السياسات الأمنية مطلب ضروري لمعظم مواقع المنشآت الإلكترونية ، فهي تلعب دوراً هاماً في تقليل المخاطر التي قد تتعرض لها المنشأة وتؤثر عليها تقنياً عن طريق تدمير أنظمة المنشأة وخادماتها، أو معنوياً وذلك بتشويه سمعتها في حال تسربت إحدى المعلومات السرية التي تحتفظ بها المنشأة ممّا يؤدي إلى إنعدام ثقة عملائها بها. لذلك نجد أن عملية إغلاق الثغرات البرمجية لمواقع الويب مسألة في غاية الاهمية.

تكمن أهمية الدراسة النظرية في جمع ودراسة الشيفرة المصدرية للعديد من المواقع، ومن ثم تحليل شيفرتها المصدرية من أجل اكتشاف ثغرة Cross Site Scripting بها، وجعلها قاعدة يتم الاعتماد عليها لتلافي الكثير من المشاكل المستقبلية. وتعمل الدراسة علي توسيع مدارك المعرفة بمخاطر الاختراقات الأمنية ومدي أهمية الانتباه لها، والتعريف بأهمية التحليل الاستاتيكي Static Analysis لفحص ومراجعة الشيفرات البرمجية لتطبيقات الويب، وتسليط الضوء

على تقنيات التعابير القياسية Regular Expression وتصميم المترجمات Compiler Design للحماية من الثغرات البرمجية عموماً وثغرة Cross Site Scripting تحديداً. كما يتم التعريف بنماذج تهديدات ثغرة Cross Site Scripting من أجل تثقيف مطوري الويب لبناء تطبيقات برمجية آمنة وتلافي خطر الوقوع بالثغرة. كل هذه الأشياء تجعل الدراسة تمثل مرجعية علمية لمطوري البرمجيات يمكن استخدامها لتطوير برمجيات آمنة المصدر خالية من المشاكل وعيوب التصميم الأمنية ضد ثغرة Cross Site Scripting.

تكمن أهمية الدراسة العملية في تطبيق العديد من المفاهيم والنماذج البرمجية الآمنة علي الشفرات المصدرية التي تم جمعها في الإطار النظري، والعمل علي تحسين البنية الأمنية لها. كما تقوم الدراسة بتطوير أداة برمجية لها القدرة علي اكتشاف نقاط الضعف البرمجية التي يمكن استغلالها لتنفيذ هجوم Cross Site Scripting Attack. كما توفر الأداة البرمجية إمكانية تعقيم القيم الممررة بواسطة مستقبلات مدخلات المستخدم للحماية من خطر هذه الثغرة وتجنب العديد من التهديدات الأمنية.

1-5 منهجية الدراسة:

تعتبر المواقع الإلكترونية من الأنظمة المهمة في المؤسسات التعليمية المختلفة لأنها تمثل البناء الرئيسي الذي يقوم عليه العمل بالمؤسسة وبدونه تصبح كثير من الأشياء غير ذات معني أصلاً. ولأهمية هذه المواقع ومدي فائدة الحصول علي المعلومات الدقيقة وبالسرعة المطلوبة والامان التام كان لابد من إتخاذ جميع التدابير الامنية لإغلاق جميع الثغرات الامنية ما أمكن ذلك.

سوف يتم استخدام المنهج التحليلي لملائمته لهذه الدراسة حيث يتم تحليل الثغرات الموجوده في التطبيق المراد فحصه بناءا على مجموعه من البيانات الثابته.

1-6 الدراسات السابقة:

قمت بمراجعة عدد كبير جداً من الأوراق العلمية وعشرات من رسائل الدكتوراه والماجستير، ويمكن تلخيص بعضها في التالي:

الدراسة الأولى: عنوان الدراسة:

Developing a tool for Intrusion Detection and Prevention against SQL Injection,Neelain University.

كاتب الدراسة: عثمان النور سليمان فضل الله.

تاريخ نشر الدراسة: 21 يونيو 2016م.

ملخص الدراسة:

تهدف هذه الدراسة لتطوير أداة برمجية مؤتمتة لحل مشكلة ثغرة SQL Injection المنتشرة بالشيفرات البرمجية لتطبيقات الويب السودانية. وقد تم بناء هذه الأداة اعتماداً على المزايا التي تقدمها كل من مفاهيم تصميم المترجمات وتقنيات التعابير القياسية Regular Expression.

وتتكون هذه الأداة من ثلاث أدوات فرعية كل منها يمكن أن يعمل بمفرده. وعند التعامل معهم كوحدة واحدة نجد أنهم مترابطين منطقياً. حيث نجد أن الأداة الأولى تقوم بمنع تطبيقات الويب من إرسال رسائل خطأ يمكن الاستفادة منها في تنفيذ أي هجوم عن طريق ثغرة SQL Injection. أما الأداة الثانية فتقوم بالاستفادة من مزايا التحليل الاستاتيكي لتحليل أي تطبيق ويب تمت كتابة شيفرته البرمجية عن طريق لغة PHP مع نظام إدارة قواعد البيانات MySQL واكتشاف ثغرة SQL Injection به مع تحديد موضع الثغرة بكل دقة. أما الأداة الثالثة فتم بناؤها على أساس أن كل أدوات التحليل المعروفة الأخرى تقوم باكتشاف الثغرة دون تقديم حلول واضحة لهذه المشكلة، أما هذه الأداة فتستهدف تعقيم جميع مستقبلات مدخلات المستخدم قبل التعامل معها لتنفيذ أي استعلام على قاعدة البيانات.

الدراسة الثانية: عنوان الدراسة:

Mitigating Cross-Site Scripting Attacks with a Content Security Policy

كاتب الدراسة: Imran Yusof و Al-Sakib Khan Pathan.

تاريخ نشر الدراسة: 14 مارس 2016م.

ملخص الدراسة:

سياسة أمن المحتوى content security policy (CSP) يمكن أن تساعد مطوري التطبيقات على شبكة الإنترنت ومسؤولي الخوادم Server administrators في الوصول الى مستوى رقابة عالي على الانترنت وتجنب التعرض لهجمات الـ Cross Site Scripting. تمت تجربة الـ CSP من قبل الباحثين على نموذج أولي لموقع، على اربعة من المتصفحات الشائعة حيث اثبتت نتائج التنفيذ نجاحه في الوقاية من جميع أنواع هجمات الـ XSS.

الدراسة الثالثة: عنوان الدراسة:

Client-side Automated Sanitizer for Cross-Site Scripting Vulnerabilities.

كاتب الدراسة: D. K. Patil, K. R. Patil

تاريخ نشر الدراسة: يوليو 2015م

ملخص الدراسة:

في هذه الدراسة تم تنفيذ معقم sanitizer لإكتشاف ثغرة الـ Cross Site Scripting في جانب العميل Client وحماية تطبيقات الويب من استغلال المخترقين لهذه الثغرة.

الدراسة الرابعة: عنوان الدراسة:

Precise client-side protection against DOM-based Cross-Site Scripting.

كاتب الدراسة: Ben Stock, Sebastian Lekies, Tobias Mueller, Patrick Spiegel, Martin Johns.

تاريخ نشر الدراسة: 22 أغسطس 2014م.

ملخص الدراسة: تقوم هذه الدراسة على تصميم filter للوقاية من هجمات ثغرة الـ DOM-based XSS التي يقوم بها المخترقين على تطبيقات الويب. ولقد اثبت النموذج فعاليته، إذ يحتوي على نسبة ضئيلة من الخطأ.

الدراسة الخامسة: عنوان الدراسة:

Specific Vulnerabilities, Program Analyses of Web Applications for Detecting Application
University of California.

كاتب الدراسة: Fangqi Sun.

تاريخ نشر الدراسة: مارس 2014م

ملخص الدراسة:

على وجه الخصوص هناك نقاط ضعف معتمده على نوع التطبيق سهلة الاستغلال وغالباً ما يكون لها عواقب وخيمة في حين أن الكشف عن نقاط الضعف المستقله في التطبيق مثل ثغرات، (XSS) وSQL injection يتوجب فحص صفحات الويب بشكل فردي عنها، اما الكشف عن الثغرات المعتمده على نوع التطبيق فانها تتطلب فحص كل صفحات الويب ومدخلات المستخدم لكل صفحة.

الكشف عن نقاط الضعف الخاصة بالتطبيق هو أكثر تحديا ولأن مثل هذه الثغرات تختلف عبر تطبيقات مختلفه لذا فان تصميم قواعد الكشف العام عن هذه الثغرات أمر صعب. إن طريقة الـ Manual code review هي عرضة للخطأ وتستغرق وقتا طويلاً، فمن المهم أن يتم تطوير تقنيات تقوم بعملية الكشف بصورة ألية. تقدم هذه

الأطروحة برنامج عملي تحليلي للكشف عن ثغرات تطبيقات الويب، وبشكل خاص تلك المعتمده على نوع التطبيق وهي تبدأ من خلال الكشف عن XSS worm من جانب العميل .

الدراسة السادسة: عنوان الدراسة:

Systematic Techniques for Finding and Preventing Script Injection vulnerabilities, University of California

كاتب الدراسة: Prateek saxena.

تاريخ نشر الدراسة: مايو 2013م.

ملخص الدراسة:

تقوم هذه الدراسة بحل مشكلة حقن الشفرات Script Injection بطريقة تلقائية عن طريق البحث عن نقاط الضعف في التطبيق والحماية من نقاط ضعف الـ Script Injection. اولاً تم اقتراح اثنين من التقنيات التي تقوم بالكشف عن نقاط اضعف script injection في جانب العميل ضمن مكونات Java Script لتطبيقات الويب. ثانياً، تم عمل دراسة تجريبية لاستخدام الية التعقيم sanitization، وهو أسلوب الدفاع السائد لمنع هذه الهجمات. ثالثاً تم اقتراح منهجية type-based لتصحيح الية التعقيم sanitization للتطبيقات بصورة تلقائية. وأخيراً تم عرض إطار عمل مفاهيمي conceptual framework لعملية التعقيم Sanitization والحماية من نقاط ضعف حقن الشفرات Script Injection.

الدراسة السابعة: عنوان الدراسة:

TOWARD AUTOMATED DISCOVERY OF WEB APPLICATION SECURITY VULNERABILITIES, California State University, Fullerton

كاتب الدراسة: Moohanad Hassan.

تاريخ نشر الدراسة: 22 أبريل 2013م

ملخص الدراسة:

تقوم هذه الدراسة على تطوير تقنية واداة Tool للبحث بصورة تلقائية عن الثغرات الأمنية في تطبيقات الويب.

الدراسة الثامنة: عنوان الدراسة:

Towards Evidence-Based Assessment of Factors Contributing to the Introduction and Detection of Software Vulnerabilities, University of California, Berkeley

كاتب الدراسة: Matthew Smith Finifter.

تاريخ نشر الدراسة: Spring 2013.

ملخص الدراسة:

تقوم هذه الدراسة على الدراسة التحليلية حيث تم استخدام مجموعة من البيانات من 9 تطبيقات من نفس مواصفات البرمجيات من أجل استكشاف العلاقة بين أدوات تطوير التطبيقات على شبكة الإنترنت وأمن التطبيقات التي طورت باستخدام هذه الأدوات. كما تم عمل تحليل لمجموعة بيانات Data Set لإثنين من نماذج نقاط الضعف Vulnerability.

1-7 هيكلية الدراسة:

تحتوي الدراسة على ثمانية فصول منقسمة ما بين الجانب النظري والجانب العملي على النحو التالي:

الفصل الأول: يتناول الإطار العام للبحث. والذي يشمل مشكلة الدارسة، وأهميتها النظرية والتطبيقية، وأهدافها ومنهجيتها والدراسات السابقة.

الفصل الثاني: يتناول المفاهيم الخاصة بالويب، تطبيقاته، بروتوكولاته، معماريته وكافة التفاصيل الخاصة به.

الفصل الثالث: يدور حول مفاهيم أمن المعلومات تفصيلاً، تأريخه، خصائصه، التعريف بالمفاهيم والمصطلحات العلمية المتداولة في مجال أمن المعلومات وكافة التفاصيل الخاصة به.

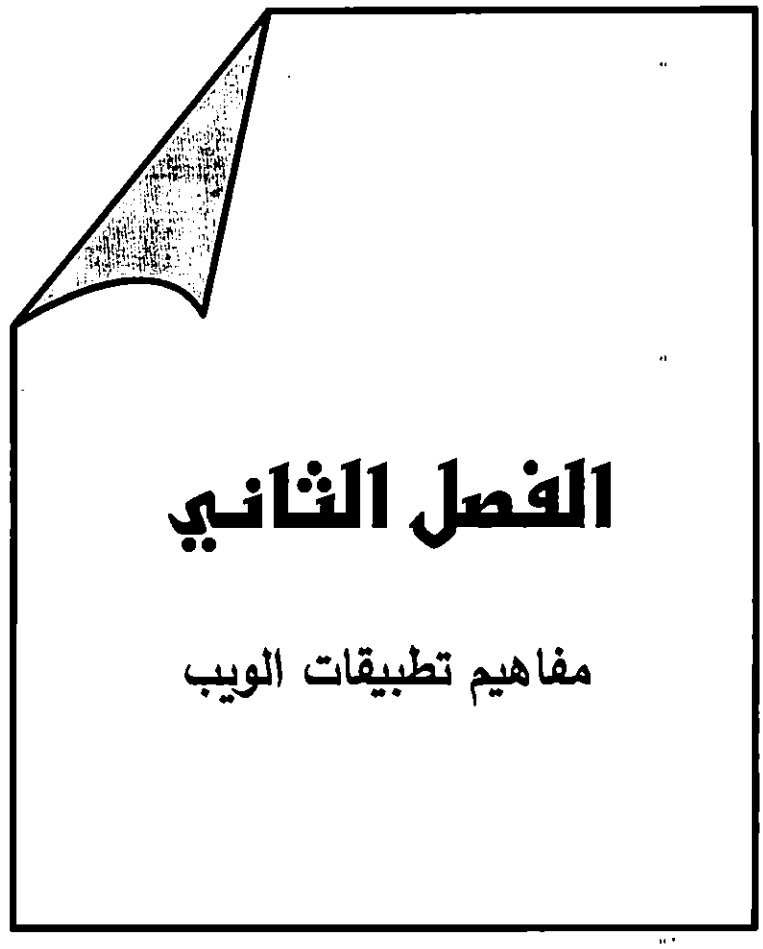
الفصل الرابع: يتناول بالتفصيل مفاهيم الاختراق، تأريخه، الاختراقات التي حدثت عن طريق ثغرة Cross Site Scripting تحديداً، وتهديدات أنظمة تشغيل الهواتف الذكية Android وطرق الحماية منها، والدراسات الأمنية الحديثة في مجال الهواتف الذكية، الأثر الاقتصادي لعمليات الاختراق المختلفة.

الفصل الخامس: يبحر في المصطلحات المرتبطة بثغرة البرمجة عبر الموقع Cross Site Scripting . ومن ثم تناول الثغرة نفسها تفصيلاً، تعريفها، أسباب اختيارها، كيفية حدوثها، كيفية اكتشافها، نماذج مصورة لمواقع مصابة بها، أنواعها، تقنيات الحماية من الثغرة.

الفصل السادس: يتناول التقنيات المستخدمة في البحث وتشمل: مفاهيم أساسية في تصميم المترجمات، التعابير القياسية Regular expression بتفاصيلها وأهميتها في مطابقة الأنماط، فحص الشيفرة البرمجية Code Review ومفاهيم التحليل الاستاتيكي والديناميكي.

الفصل السابع: التحليل والتصميم والتنفيذ.

الفصل الثامن: النتائج، التوصيات، الخاتمة، والمصادر والمراجع.



الفصل الثاني

مفاهيم تطبيقات الويب

2-1 مقدمة:

على مدي عقد من الزمان تم تبني تطبيقات الويب عن طريق ملايين الشركات كقناة قليلة التكلفة للتواصل وتبادل المعلومات بين الأفراد والمؤسسات، والقيام بالعمليات التعليمية المختلفة إلى أن وصلت حالياً لمرحلة الجامعات الافتراضية Virtual Universities، وإجراء المعاملات التجارية البسيطة والضخمة مع العملاء. من وجهة نظر تقنية، تعرف الويب على أنها بيئة برمجة عالية المستوى تسمح بالتخصيص الشامل Mass Customization لمجموعة كبيرة ومتنوعة من التطبيقات، لملايين المستخدمين على مستوى العالم . وتوفر الويب وسيلة فعالة للمسوقين Marketers للتعرف على الزبائن الذين يزورون مواقعهم والبدء في التواصل معهم. وواحدة من أهم هذه الطرق للقيام بذلك، سؤال زوار الموقع للاشتراك في النشرات الإخبارية Newsletters، ملء استمارة Application Form عند طلب الزبائن معلومات عن منتجات محددة أو تقديم تفاصيل معينة أثناء تصفحهم من أجل تسهيل تعاملهم مع الموقع عند زيارتهم التالية له.

تعتبر بيئات الويب اليوم من أميز قنوات البيع العالمية وأكثرها فاعلية لعدد لا يحصى من المؤسسات التجارية صغيرة كانت أم كبيرة: فمع أكثر من ثلاثة مليار مستخدم للإنترنت عن طريق الهواتف المحمولة فقط (المصدر: Internet Society، مايو 2015) ومعدل إنفاق للحكومة الأمريكية فقط على التجارة الإلكترونية بلغ 56.1 مليار دولار في الربع الأول من العام 2014 (المصدر: Com Score Networks، أكتوبر 2015) لا يستطيع أحد أن يتخيل كمية الأموال الضخمة المتداولة عبر الإنترنت.

كل هذه المعلومات يجب التعامل معها بطريقة أو بأخرى، وتخزينها ومعالجتها ونقلها ومن ثم استخدامها آنياً أو في أي وقت لاحق. تطبيقات الويب، تكون في شكل حقول إرسال Submit Fields، نماذج تسجيل الدخول والاستفسارات Enquires and Login Forms، عربات التسوق Shopping carts وأنظمة إدارة المحتوى Content Management Systems كل ذلك وغيره. ولذا أصبح من الضروري للشركات من أن ترفع مستوى