الجمهورية العربية السورية

الهيئة الوطنية لخدمات الشبكة

مركز أمن المعلومات

National Agency for Network Services
Information Security Center

الرقم: ١/٢٠١٣

التاريخ: ٢٠١٣/٧/١٠

التقرير نصف السنوي لعام ٢٠١٣

الخاص باختبارات المواقع الإلكترونية الحكومية

Half-Annual Report

Governmental Websites Security Test

2013

١) المقدمة:

يعمل مركز أمن المعلومات في الهيئة الوطنية لخدمات الشبكة، وفق قانون التوقيع الرقمي وخدمات الشبكة رقم /٤/ لعام ٢٠٠٩، على وضع المواصفات والمعايير الخاصة بأمن وحماية الشبكات ونظم المعلومات ومواقع الإنترنت، والإشراف على حسن الالتزام بها، ووضع المعايير الخاصة بمواجهة حالات الطوارئ على الانترنت أو غيرها من الشبكات المعلوماتية والحاسوبية، وتأليف فرق عمل للتصدي لهذه الحالات، إضافةً إلى إجراء الأبحاث الأمنية وتقييم المخاطر على النظم المعلوماتية، وبناء الخبرة في مجال المعلوماتية الشرعية، ونشر ثقافة أمن المعلومات بشكل عام.

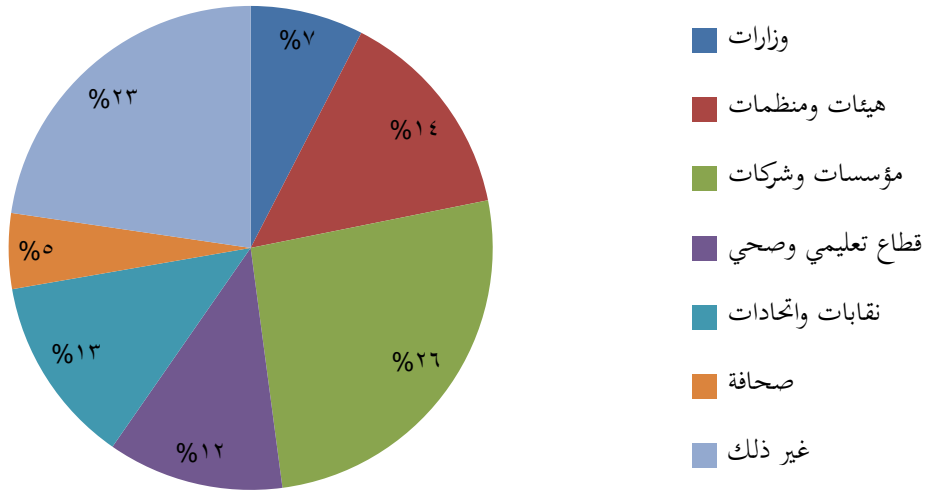
ولقد عمل المركز منذ تأسيسه في منتصف العام ٢٠١١ على تعزيز مستوى أمن وسلامة النظم المعلوماتية في الجهات العامة، وكان أحد أبرز نشاطاته في هذا المجال إجراء الاختبار الأمني الخارجي الدوري للمواقع الالكترونية الحكومية بشكل مجاني باستخدام برمجيات مفتوحة المصدر، وإعداد تقارير شاملة بالثغرات الأمنية المكتشفة وطرق حلها ومعالجتها تفادياً لأية تهديدات أمنية أو اختراقات قد تتعرض لها هذه المواقع مستقبلاً. وكنتيجة لهذا الإجراء تم إعداد هذا التقرير الموجز الذي يقدم معلومات إحصائية تقريبية عن مدى انتشار الثغرات الأمنية في المواقع الالكترونية الحكومية ومستوى تأثيرها، وأكثرها خطورةً.

٢) الدراسة الإحصائية:

(١). تم الاعتماد أثناء إعداد هذا التقرير على المعطيات التالية:

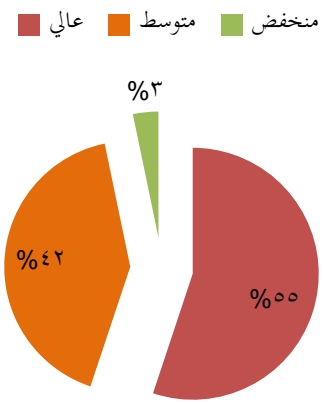
- نتائج الاختبار الأمني لـ (١٥٠) موقعاً الكترونياً خلال النصف الأول من العام ٢٠١٣، يشمل مختلف القطاعات الحكومية من وزارات وهيئات ومؤسسات شركات ونقابات ومختلف المجالات التعليمية والصحية والخدمية، والمبين نسب توزيعها في الشكل (١).
- إجمالي الثغرات الأمنية المكتشفة أثناء الاختبار الأمني والبالغ عددها (٥٠٠) ثغرة أمنية متعددة مستويات الخطورة.

الشكل (١): نسبة توزع الدراسة على القطاعات الحكومية

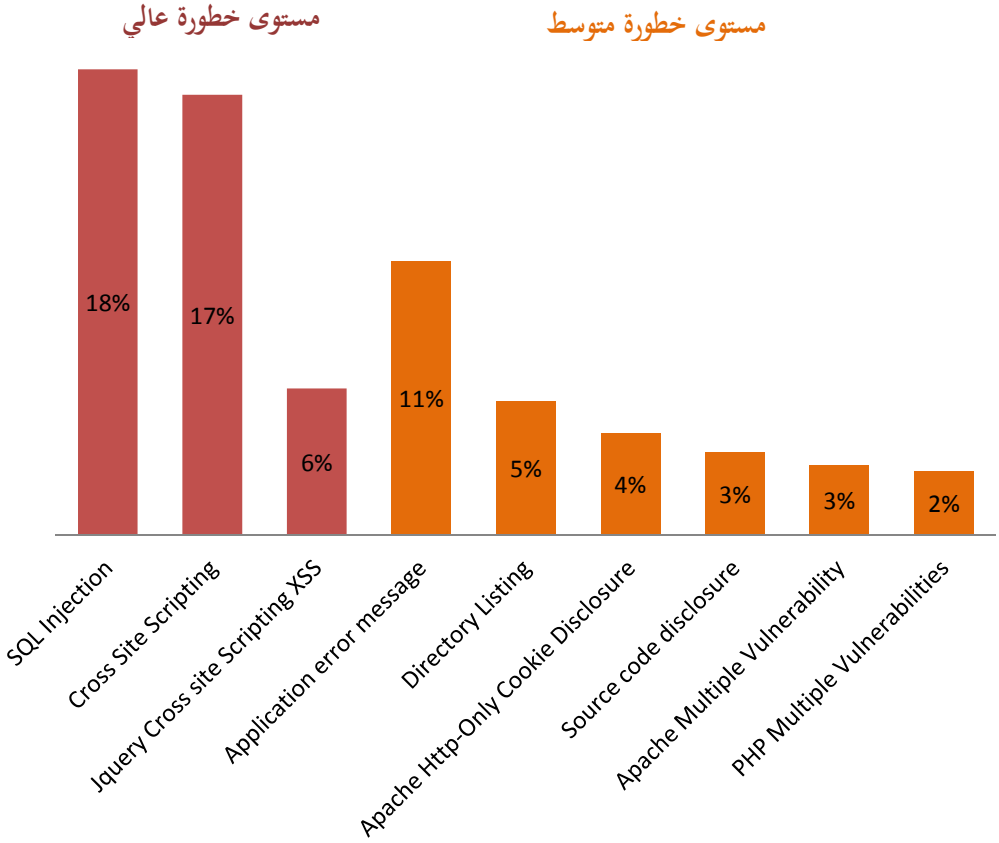


(٢). على الرغم من وجود العديد من الثغرات ذات مستوى الخطورة المنخفض (والتي قد لا تتجاوز في بعض الحالات مجرد ثغرات تكشف بيانات من الموقع قد تكون غير هامة) إلا أننا قد اخترنا في تقاريرنا المرسلة إلى الجهات العامة التركيز على الثغرات ذات المستوى العالي من الخطورة، مما جعل نسبة ورودها يقدر بـ ٥٥% ، ونسبة الثغرات ذات المستوى المتوسط من الخطورة تقدر بـ ٤٢%. كما هو مبين في الشكل (٢).

الشكل (٢): انتشار الثغرات الأمنية تبعاً لمستوى خطورتها



(٣). لقد تم تحديد الثغرات الأمنية الأكثر انتشاراً في المواقع الإلكترونية الحكومية والأكثر خطورة والتي تهدد أمن الموقع الالكتروني بشكل مباشر، ووجدنا أنه يكاد لا يخلو موقع الكتروني حكومي من ثغرة الحقن بلغة الاستعلام البنيوية SQL Injection والتي تكررت بنسبة ٢٦% من إجمالي الثغرات الأمنية المكتشفة، يليها ثغرة الحقن البرمجي عبر الموقع Cross-site Scripting (XSS) التي تكررت بمعدل ٢٥% . كما هو مبين في الشكل (٣).

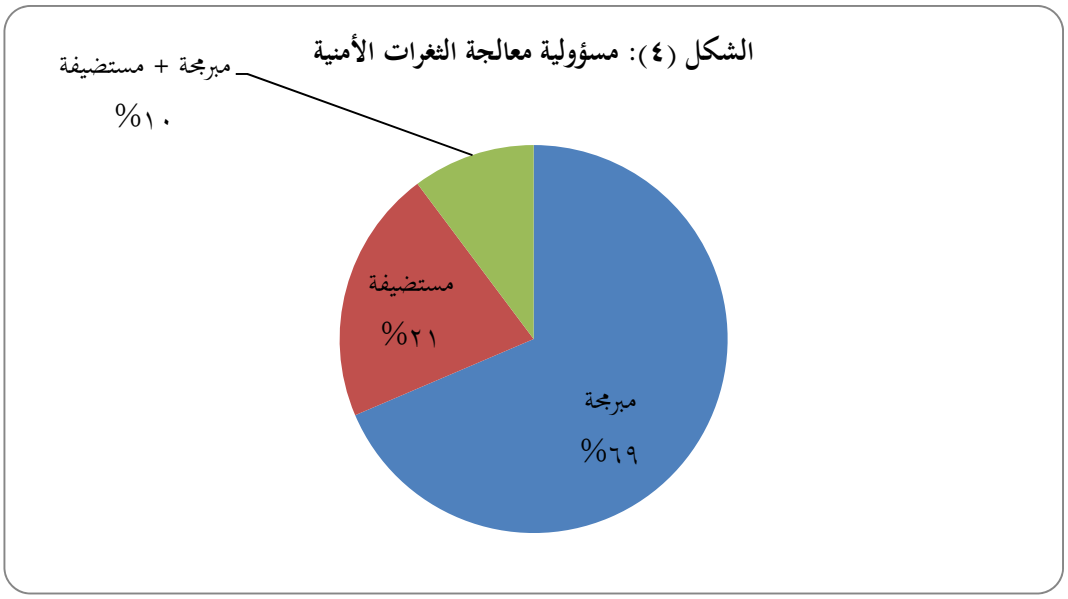


الشكل (٣): الثغرات الأمنية الأكثر تكراراً

(٤). نظراً لأهمية الثغرات المذكورة سابقاً وخطورتها على أمن المواقع الالكترونية وتكرارها في أغلب المواقع الإلكترونية التي تم اختبارها، فقد قمنا بإدراج شرح موجز عن هذه الثغرات كما يلي:

SQL Injection **الحقن بلغة الاستعلام البنيوية**	يتم الحقن بلغة الاستفسار البنيوية عن طريق استغلال الثغرات والأخطاء البرمجية الموجودة في قاعدة المعطيات الخاصة بالموقع أو في تطبيقات الويب التي تتعامل مع قاعدة المعطيات مباشرةً، وذلك بإضافة شفرة أوامر مكتوبة بلغة SQL للمتغيرات الممررة إلى الموقع عن طريق نماذج الإدخال سواءً المخصصة للبحث أو لتسجيل الدخول أو حتى في شريط العنوان الخاص بالموقع، بحيث يتم تنفيذ هذه الأوامر مع الشفرة الأساسية للموقع.
Cross-site Scripting (XSS) **الحقن البرمجي عبر الموقع**	يتم الحقن بطريقة XSS من خلال إضافة شفرة برمجية عادةً ما تكون مكتوبة بلغة Java Script ضمن إحدى صفحات الموقع الإلكتروني، كصفحة تسجيل الدخول إلى خدمة معينة. وعند حقن الشفرة البرمجية يتم تنفيذها تلقائياً والحصول على قيم مرتجعة من قاعدة معطيات الموقع.
Jquery Cross site Scripting	هذه الصفحة تستخدم إصدار قديم من مكتبة جافا سكريبت JQuery و هذا ما يجعل الموقع عرضة لهجوم بطريقة XSS .
Application Error message	عبارة عن رسالة خطأ برمجية تظهر أثناء تصفح إحدى صفحات الموقع، تمكن المهاجم من الحصول على بيانات ومعلومات حساسة يمكن استغلالها في تنفيذ هجمات أخرى.
Directory Listing	تتضمن هذه الثغرة إظهار قائمة بالملفات المتضمنة ضمن المجلد الحالي لموقع الويب على مخدّم الاستضافة.
Apache Http-only Cookie Disclosure	تتضمن بعض إصدارات مشغل تطبيقات الويب Apache 2.2.x ثغرة أمنية تسمح للمهاجم الحصول من بُعد على قيم ملفات الارتباط Cookies لبروتوكول HTTP عن طريق إرسال أمر برمجي يحتوي على ترويسة طويلة أو مشوهة مرتبطة مع سكريبت خاص معد لهذا الغرض.
Source code Disclosure	نقطة ضعف برمجية تؤدي إلى عرض النص البرمجي المصدري الكامل للتطبيق.

(٥). من أهم النقاط التي لا بد من الإشارة إليها هي أن غالبية الثغرات الأمنية المكتشفة وأكثرها خطورة تكون معالجتها من مسؤولية الشركة المبرمجة للموقع، في حين يقع على عاتق الشركة المستضيفة للموقع معالجة الثغرات المتعلقة بمشغل تطبيقات الويب والمخدّم المستضيف وإجراءات الترقية والتحديث بشكل دوري، بالإضافة لبعض الثغرات الأمنية التي قد يستطيع حلها أحد الطرفين. كما هو مبين في الشكل (٤).



٣) النتائج:

- إن غالبية المواقع الإلكترونية الحكومية لا توفر إجراءات التحقّق من مدخلات المستخدم وذلك باختبار نوع المدخل وشكله وطوله مما يجعلها عرضة للاختراق بطريقة الحقن SQL Injection و Cross-site Scripting (XSS).
- عدم التحديث الدوري لمخدّمات الاستضافة ومشغل تطبيقات الويب لتفادي الثغرات الأمنية المكتشفة حديثاً.
- الإعداد غير الصحيح للتطبيقات والبرمجيات ضمن مخدّمات الاستضافة، وعدم تحديد صلاحيات النفاذ إلى ملفات الموقع الحساسة، والتي قد تؤدي إلى تسريب معلومات مهمة يمكن استغلالها في تنفيذ هجمات أخرى.

دمشق في ٢٠١٣/٧/١٠ م