الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# مركز أمن المعلومات

## التقرير السنوي

## 2021

إعداد

مركز أمن المعلومات

# Table of Contents

## 1- تعريف بمركز أمن المعلومات

"هو الوحدة التنظيمية المسؤولة عن وضع المواصفات والمعايير وكافة الوثائق الخاصة بأمن وحماية المعلومات والشبكات بما فيها المواقع الالكترونية على الشبكة والإشراف على حُسن الالتزام بها، وإنجاز الأبحاث والاختبارات اللازمة والممكنة في إطار تأمين بيئة عمل آمنة ومناسبة، ووضع المعايير الخاصة بمواجهة حالات الطوارئ على الشبكة أو غيرها من الشبكات المعلوماتية واتخاذ ما يمكن من إجراءات وقائية وعلاجية وإدارة فرق عمل للتصدي لها".

لقد دأب مركز أمن المعلومات منذ تأسيسه على تطوير واقع أمن المعلومات على المستوى الوطني ضمن سوريا، من خلال وضع السياسات والمعايير والمواصفات الوطنية الخاصة بأمن المعلومات، وإجراء الاختبارات الأمنية للمنظومات المعلوماتية الحكومية، والعمل على نشر ثقافة أمن المعلومات والتوعية الأمنية، والاستجابة لحالات الطوارئ المعلوماتية التي تتعرض لها الشبكات والمنظومات المعلوماتية، وأدى ذلك إلى رفع سوية الأمان المعلوماتي ضد الهجمات الإلكترونية في الفضاء السيبراني وفيما يتعلق بمحاولات الاختراق بشكل ملحوظ، كما بينت الدراسات الإحصائية التي يعدها المركز سنوياً، وفيما يلي سنعرض التقرير السنوي لمجمل أعمال ونشاطات المركز خلال العام 2021.

## 2- نظام خدمات مركز أمن المعلومات

تم تجهيز المخبر الوطني لأمن المعلومات بأحدث التجهيزات والتطبيقات البرمجية المطوّرة من قبل شركات عالمية متخصصة بأمن المعلومات والتي تمكّن المركز من تطوير الخدمات التي يقدمها كماً ونوعاً، ولاستثمار المخبر بالشكل الأمثل كان لا بد من تنظيم عملية تقديم هذه الخدمات من خلال إصدار نظام خاص بالخدمات التي يقدمها المركز، حيث يقدم هذا النظام توصيفاً دقيقاً للخدمات والجهات المستهدَفة بالإضافة إلى الأجور المترتبة للحصول على هذه الخدمات من قبل الجهات العامة والخاصة وتم تعديل النظام إلى النسخة 2.1 لعام 2021.

فيما يلي وصفاً موجزاً للخدمات التي يقدمها المركز حسب هذا النظام

### 2.1- خدمات المسح الأمني واختبار الاختراق الاحترافية

1. خدمة المسح الأمني العادية: يقدم المركز هذه الخدمة عند الطّلب لجميع المواقع الإلكترونية العامة والخاصة، وهي مجاناً للجهات العامة ولمرة واحدة خلال العام.

2. خدمة المسح الأمني الاحترافية: يقدم المركز هذه الخدمة عند الطّلب للجهات العامة والخاصة، وتقسم إلى ثلاثة أنواع:
   أ. خدمة المسح الأمني الاحترافية للمواقع الإلكترونية ومخدمات الويب.
   ب. خدمة المسح الأمني الاحترافية للبرمجيات.
   ت. خدمة المسح الأمني الاحترافية للشّبكات.
3. خدمة اختبار الاختراق الاحترافية: تتضمن خدمة المسح الأمني الاحترافية السّابقة، ويضاف إليها اختبار اختراق منظومة العميل بطرق تحاكي هجوم حقيقي بالتنسيق مع الجهة صاحبة المنظومة.

## 2.2- خدمات الاستجابة للطوارئ المعلوماتية

1. استعادة بيانات أو معلومات مفقودة.
2. التعامل الفوري مع الطوارئ المعلوماتية.
3. استخراج الدليل الرقمي لجريمة معلوماتية أو تقليدية.

## 3.2- خدمة اختبار الإغراق:

**تم إضافة هذه الخدمة الجديدة لخدمات المركز خلال عام 2021**

ويقصد بهذه الخدمة إجراء عمليات محاكاة لهجمات حجب الوصول بنوعيها الموزعة وغير الموزعة ويكون الهدف عادةً خدمة الكترونية معيّنة كتطبيقات الويب، المواقع الالكترونية، المخدمات التشغيلية والشبكات وغيرها، بواسطة إغراق البيئة المضيفة للخدمة بشكل تدريجي حيث يتم زيادة عدد الطلبات بشكل متواتر ومدروس، مع الاستمرار بقياس مؤشرات الاستجابة بهدف تحديد نقاط الضعف كالبطء وتوقف الخدمة جزئياً أو كلياً، يتم إعداد تقارير تفصيلية للجهات تتضمن كافة البيانات المتعلقة بإغراق البيئة المضيفة بالإضافة إلى عددٍ من المؤشرات التي تهدف لمساعدة هذه الجهات لتلافي الأخطاء ونقاط الضعف والمشكلات التقنية من أجل رفع مستوى كفاءة وتوافرية خدماتهم.

كما يمكن تحميل نظام خدمات المركز من خلال الرابط:

https://www.nans.gov.sy/ar/page/information_security_center_documents

# 3- أعمال المركز خلال عام 2021

## 3.1- المسح الأمني العادي

قام المركز خلال عام 2021 باختبار 146 موقعاً حكومياً ضمن إطار خطة المسح السنوية لعام 2021، وقد تم إعداد تقارير المسح الأمني لـ 116 موقعاً وإرسالها الى الجهات الحكومية صاحبة المواقع لتتم معالجة الثغرات ونقاط الضعف المكتشفة، أما الاختبارات التي لم يتم إعداد تقاريرها فيرجع السبب في ذلك إلى خلوها من الثغرات الهامة ونقاط الضعف، وقد تم مخاطبة جميع الجهات التي أُرسلت لها تقارير المسح لعرض الخدمات الاحترافية الأخرى التي يقدمها المركز.

## 3.2- المسح الأمني الاحترافي

قام المركز خلال عام 2021 بإجراء عمليات المسح الاحترافي لـ 7 مواقع الكترونية وتطبيقات ويب مع إعداد التقارير ذات الصلة، حيث يتم تقديم هذه الخدمة بناءً على طلب مسبق من الجهات وحسب نظام خدمات المركز بالإضافة إلى توقيع عقود عمل تتضمن شروطاً وتفاصيل إضافية للإنجاز.

## 3.3-اختبار الاختراق

تُعتبر خدمة اختبار الاختراق إحدى الخدمات الاحترافية التي يقدمها المركز بناءً على طلب مسبق من الجهات ضمن شروط معينة، وقد قام فريق المركز بإجراء 44 عملية اختبار اختراق لمواقع وتطبيقات ويب بالإضافة إلى تطبيقات مخصصة للهواتف المحمولة ضمن منهجيات عمل قياسية ومعيارية تتضمن إعداد التقارير الفنية التفصيلية ذات الصلة.

## 3.4- الاستجابة للطوارئ المعلوماتية

يُشترط لتقديم هذه الخدمة شرطين أولا وقوع حادث معلوماتي ما بالإضافة إلى إبلاغ فريق المركز عن هذا الحادث، ضمن هذا الإطار قام فريق المركز بالاستجابة إلى 56 حالة طارئة مختلفة في العام 2021 تتعلّق بحالات اختراق وإصابة ببرمجيات خبيثة وتجسس على الشبكات، حيث تم الاستجابة لهذه الحالات وفق الإجراءات المعيارية وإعداد التقارير ذات الصلة وإرسالها الى الجهات المعنية.

نظراً لاضطلاع المركز بالتصدي لحالات الطوارئ المعلوماتية على الشبكات المختلفة، برزت الحاجة لاستخدام برمجيات وتجهيزات احترافية يعتمد عليها فريق الاستجابة للطوارئ المعلوماتية، لذلك أعد المركز دفتر شروط خاص باستكمال تجهيز المخبر الوطني لأمن المعلومات بمشروع الاستجابة للطوارئ المعلوماتية وبالفعل تم نشر الإعلان، حيث يعتمد فريق الاستجابة حالياً في عمله على برمجيات مجانية أو مفتوحة المصدر، وهي غير كافية وذات أداء محدود.

## 3.5- التوعية الأمنية

في إطار التحذير المبكر من الأخطار المعلوماتية على الشبكة ونشر ثقافة أمن المعلومات قام المركز بتنفيذ مجموعة من النشاطات:

- تقديم استشارات أمنية للجهات العامة حول معالجة الثغرات الأمنية وكافة القضايا التي تتعلق بأمن المعلومات بشكل عام.
- نشر عدد من التحذيرات بخصوص برمجيات خبيثة وهجمات إلكترونية وثغرات خطيرة هددت الشبكة السورية.
- قام المركز بأعمال مختلفة في مجال التوعية الأمنية والتحذير المبكر بلغ عددها 9.
- ورشات عمل في مجالات أمن المعلومات المختلفة بلغ عددها ورشتي عمل.
- إعداد لائحة تضم معلومات الاتصال الخاصة بمدراء المعلوماتية ومسؤولي أمن المعلومات في جهات القطاع العام مع تحديثها باستمرار.
- تخصيص مجال مناسب ضمن مشروع التخزين السحابي في الهيئة من أجل إتاحة الأبحاث والوثائق والملفات ذات الصلة لكافة الجهات العامة بالإضافة إلى توفير الاستشارات اللازمة ودراسة ومعاينة أية وثائق تتعلق بأمن المعلومات قد ترفعها الجهات.

## 3.6- اعتماد الأنواع

في إطار دور مركز أمن المعلومات الوطني، قام الفريق التقني في المركز بدراسة وتدقيق عدد من أنواع التجهيزات ذات الصلة بموضوع أمن المعلومات المختلفة والموافقة على إدخال اعتماد سبعة أنواع منها.

## 3.7- زيارة المركز الوطني للسلامة المعلوماتية في سلطنة عمان

قام فريق من الهيئة بزيارة عمل إلى مركز السلامة المعلوماتية والمركز الإقليمي للأمن السبراني في سلطنة عمان والاطلاع على التجربة العمانية الغنية في مجال الأمن السبراني ومركز الاستجابة للطوارئ المعلوماتية العماني للاستفادة منها في تأسيس مركز الاستجابة للطوارئ المعلوماتية في سوريا وفق أفضل الممارسات والمعايير وأبدى الجانب العماني استعداده لدعمنا في عدد من الجوانب الاستشارية.

## 3.8- نشاطات متفرقة

قام الفريق التقني في مركز أمن المعلومات بعدد من النشاطات المتفرّقة ضمن عام 2021 غير الأعمال المخططة لعام 2021:

- المشاركة الفعالة في رسم الاستراتيجية الوطنية للأمن السبراني من خلال عضوية اللجنة المعنية المشكلة من قبل السيد وزير الاتصالات والتقانة.
- تنظيم مسابقة أمن المعلومات السوريّة CTF Syria.
- المشاركة في التدريب الأول للأمن السيبراني، والذي نظمه مركز الأمن السيبراني الإفريقي AfricaCERT.
- المشاركة في التدريب الإقليمي التاسع للأمن السيبراني، والذي نظمه مركز الأمن السيبراني لمنظمة التعاون الإسلامي OIC-CERT
- عدد من النشاطات المختلفة ضمن إطار عضوية الهيئة الوطنية لخدمات الشبكة-مركز أمن المعلومات في "المركز الإقليمي للأمن السيبراني لدول منظمة التعاون الإسلامي OIC-CERT" وتضمنت حضور ورشات عمل وتدريبات تركزت حول مواجهة المخاطر المعلوماتية في ظروف انتشار جائحة كورونا.
- إعداد عدد من وثائق الشروط الفنية لمشاريع وطنية مختلفة في مجال أمن المعلومات والمجالات التقنية الأخرى من خلال عضوية تقنيي المركز في عدد من اللجان الفنية المحلية والمركزية.
- متابعة تأهيل وتدريب الكادر التقني في المركز من خلال دورات تدريبية تخصصية في مجالات أمن المعلومات المختلفة في مركز التميز السوري الهندي.
- متابعة الأعمال المعتادة في المخبر الوطني لأمن المعلومات كالتحديث الدوري لأنظمة وتطبيقات المخبر وإجراء العمليات المعتادة على تجهيزات المخبر حرصاً على استمرارية العمل.

# 4- إحصائيات

## 4.1 الاختبارات الأمنية

| # | عمليات المسح | التقارير المرسَلة |
|---|---|---|
| مسح عادي | 146 | 116 |
| مسح احترافي | 07 | 07 |
| اختبار اختراق | 44 | 44 |
| الاستجابة للحالات الطارئة | - | 56 |

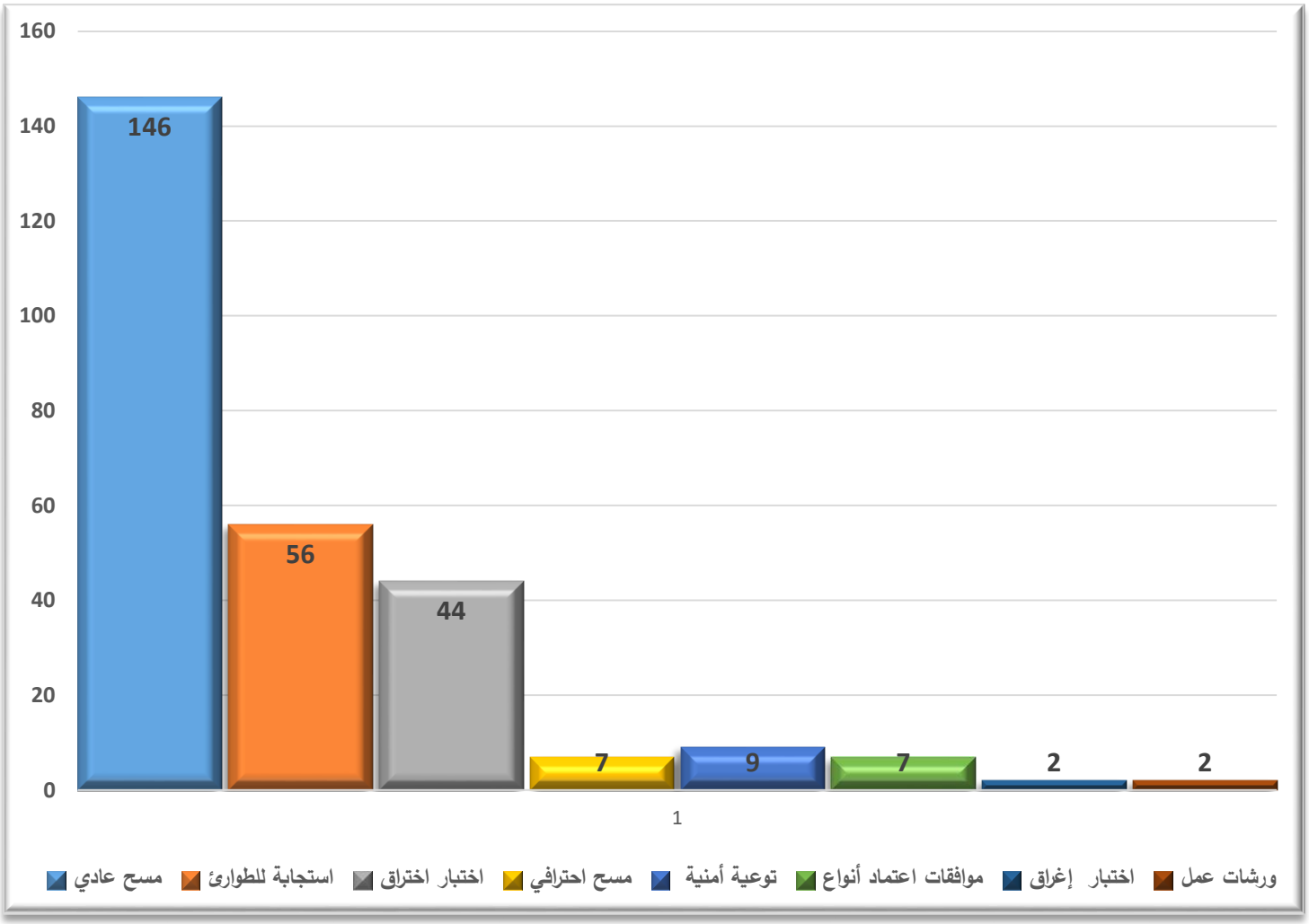
**توضيح:**

بالنسبة للمسوحات العادية التي لم يتم إعداد تقارير لها فيرجع ذلك إلى أن نتائج المسح لم تحوي ثغرات أو أنها تضمنت ثغرات غير هامة ولا تشكل خطراً على أمن التطبيقات المختبَرة، وبلغت نسبة هذه المواقع التي تعتبر آمنة حوالي **21%** من المواقع الحكومية المختبرة.

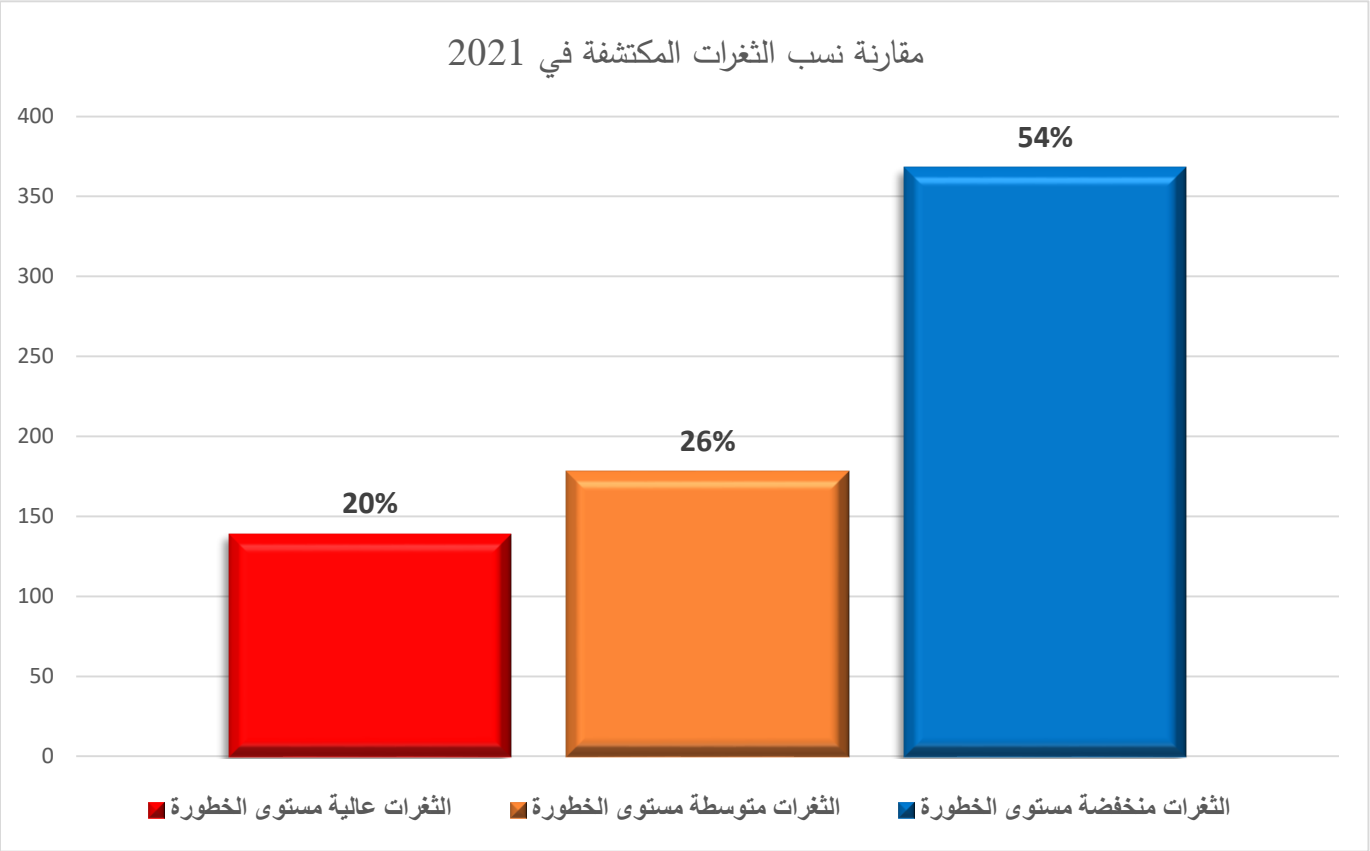
تُصنَف الثغرات حسب المراجع العالمية المعنيّة بدراسة وتقييم الثغرات إلى ثغرات عالية مستوى الخطورة وثغرات متوسطة مستوى الخطورة وثغرات منخفضة مستوى الخطورة، حيث تم تمييز المستويات المختلفة للثغرات بواسطة مبدأ النقاط التجميعية، فيما يلي التوصيف العام القياسي لمستويات الثغرات:

| مستوى خطورة الثغرة | | النقاط |
|---|---|---|
| عالٍ | High | 7.0--10.0 |
| متوسط | Medium | 4.0--6.9 |
| منخفض | Low | 0.0--3.9 |

**4.1.1**- يبيّن المخطط البياني التالي لمحة موجزة عن مجمل أعمال مركز أمن المعلومات في العام 2021 موزّعة حسب عدد الحالات لكل من الخدمات المعتمَدة في المركز

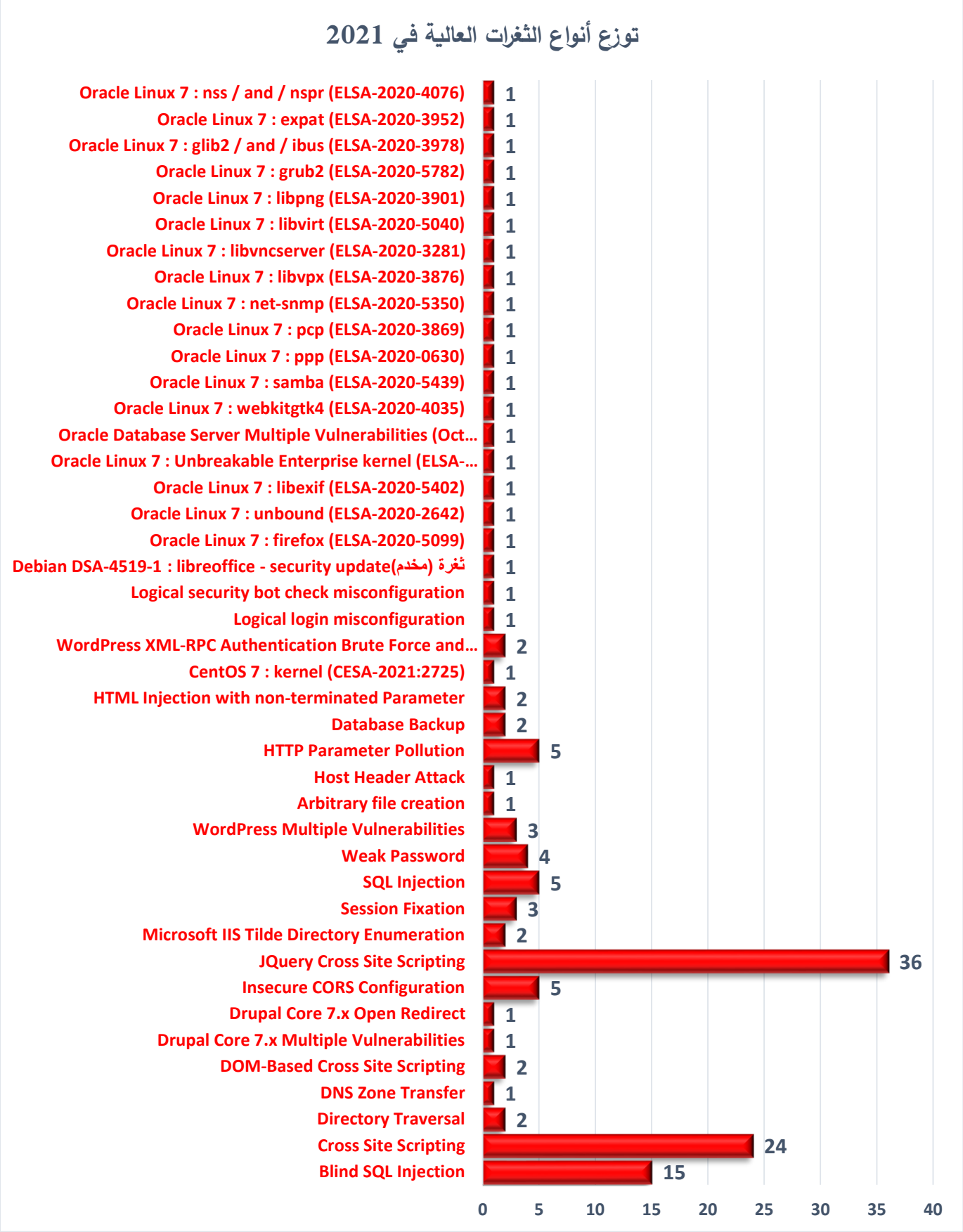


**4.1.2**- يبين المخطط التالي نسب توزع الثغرات المكتَشفة في الاختبارات بكافة أنواعها التي أجراها فريق مركز أمن المعلومات في عام 2021 موزّعة حسب مستويات الخطورة الثلاثة:

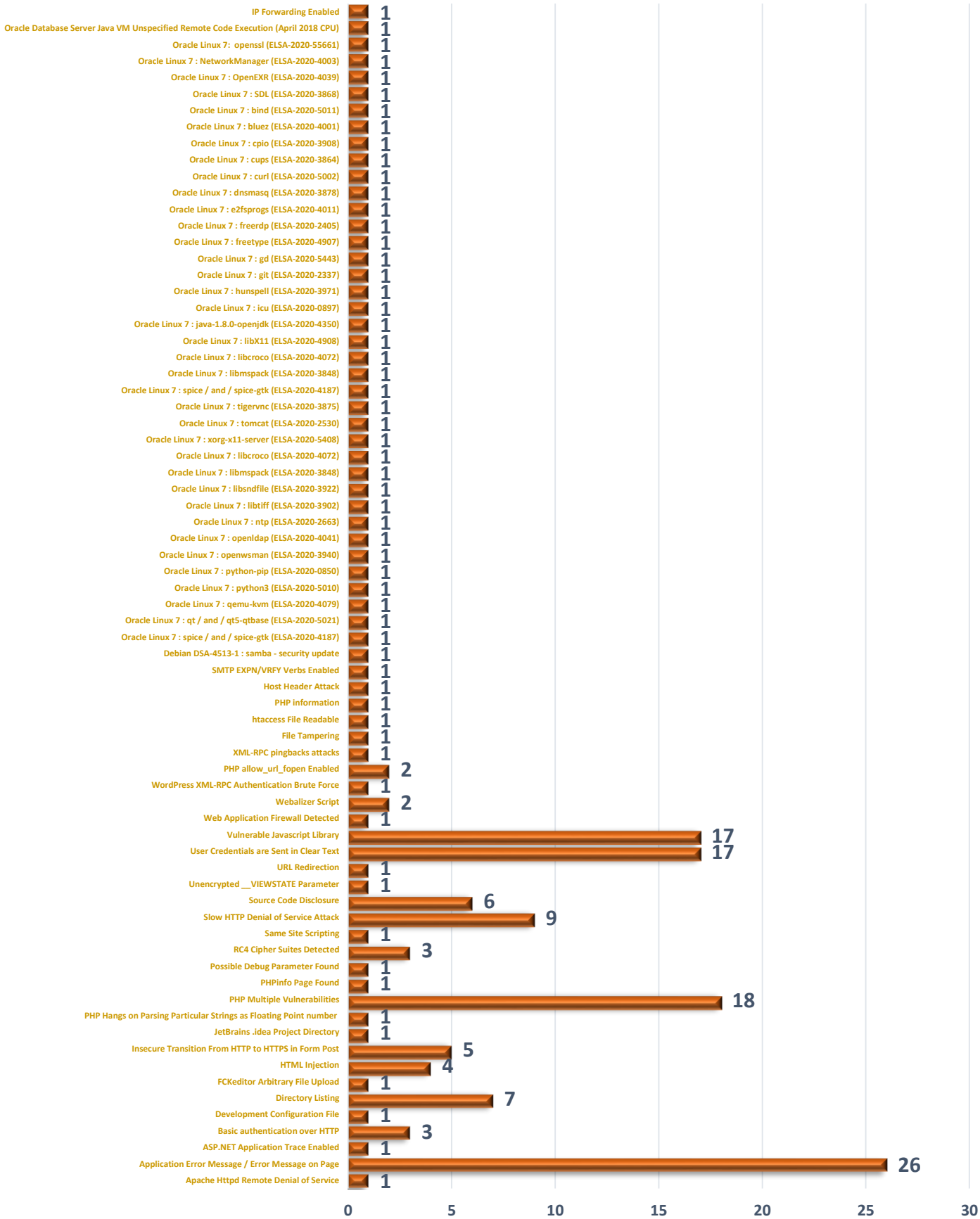



يتبيّن من خلال المخطط السابق أنه قد بلغت نسبة الثغرات عالية الخطورة 20% فقط من إجمالي الثغرات التي تم اكتشافها في الاختبارات التي أجراها المركز، وهو مؤشر جيد لكون هذه الثغرات خطيرة ومعظمها قد يؤدي إلى اختراق المواقع والتطبيقات.

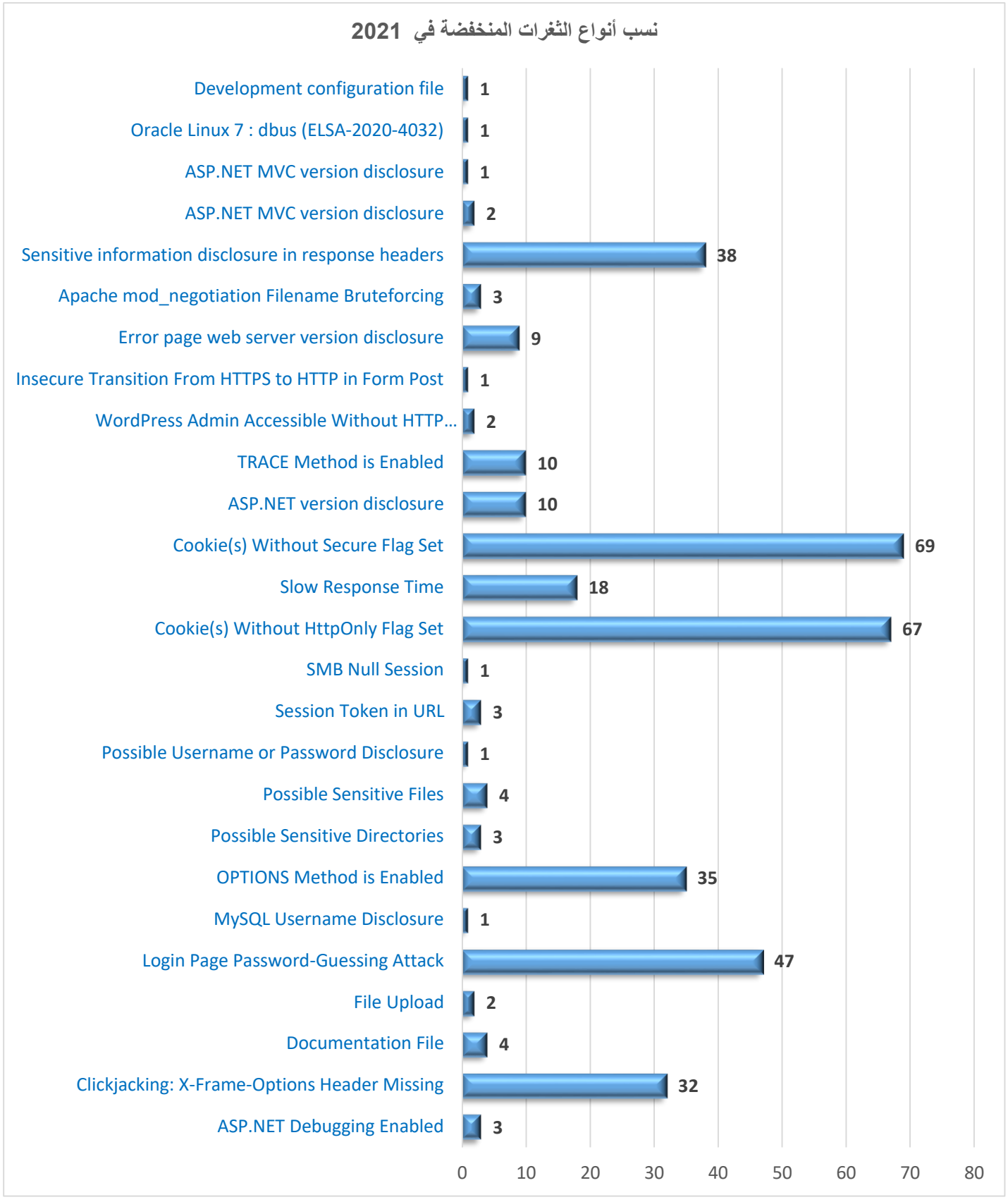
**4.1.3**- يبيّن المخطط التالي توزع أنواع الثغرات عالية مستوى الخطورة المكتَشفة في نتائج اختبارات المركز



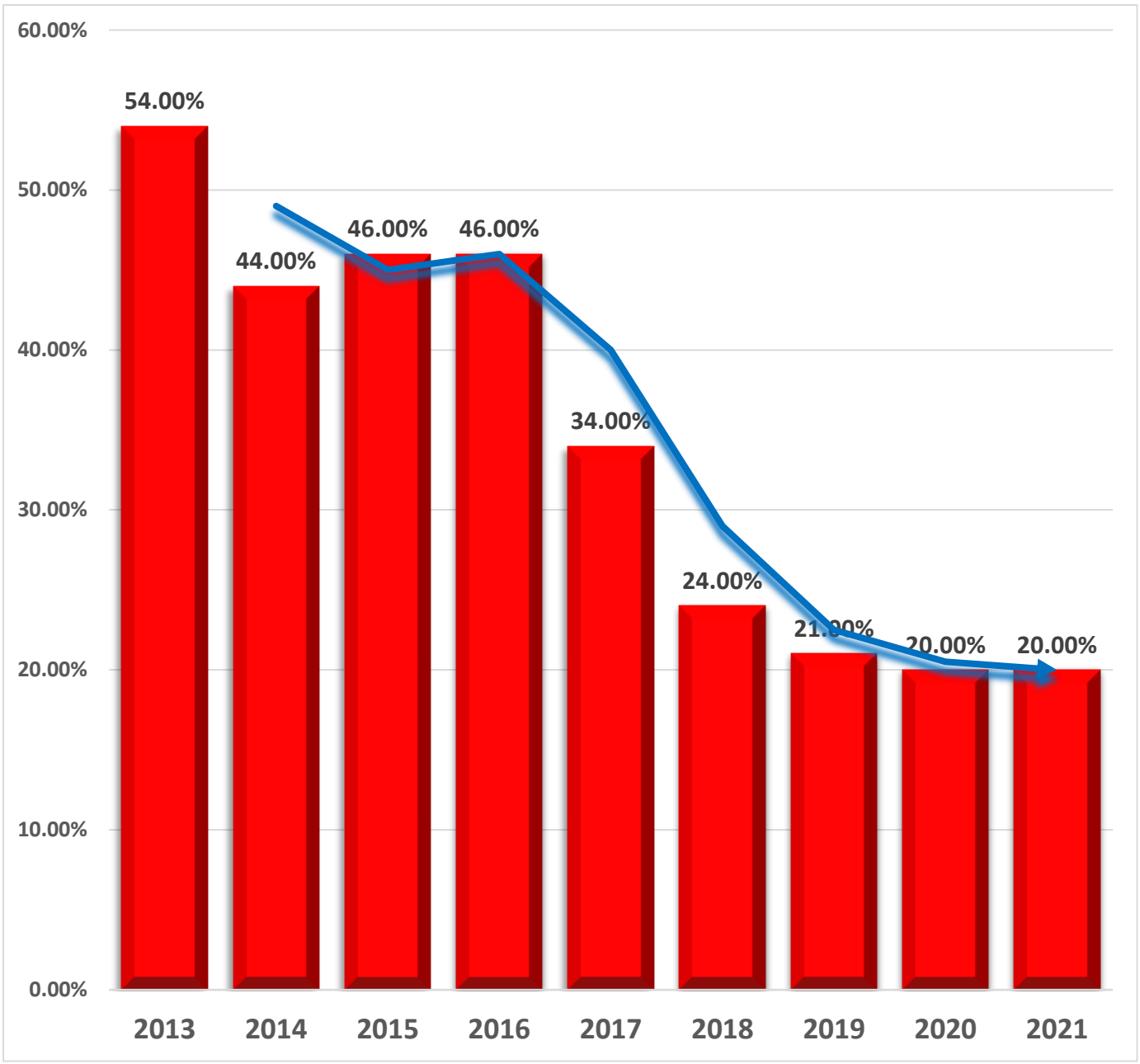
## 4.1.4- نسب الثغرات متوسطة مستوى الخطورة المكتَشفة في نتائج اختبارات المركز 2021



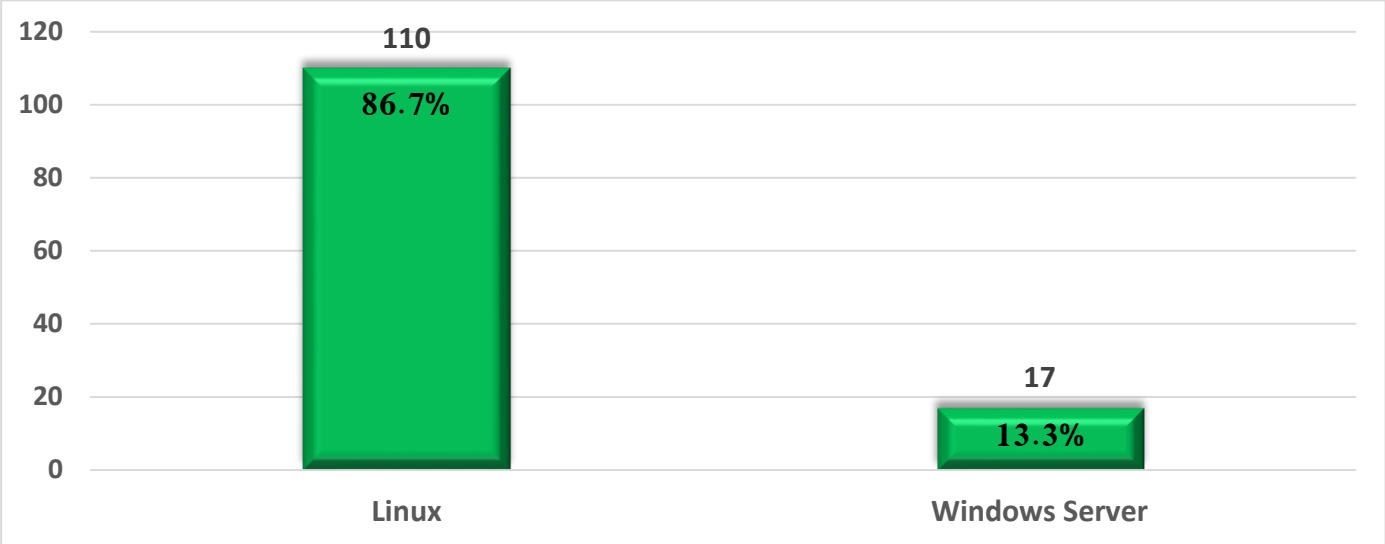
### 4.1.5- نسب أنواع الثغرات المنخفضة الخطورة



### 4.1.6- مقارنة نسب الثغرات عالية مستوى الخطورة المكتَشفة في عام 2021 مع الأعوام السابقة

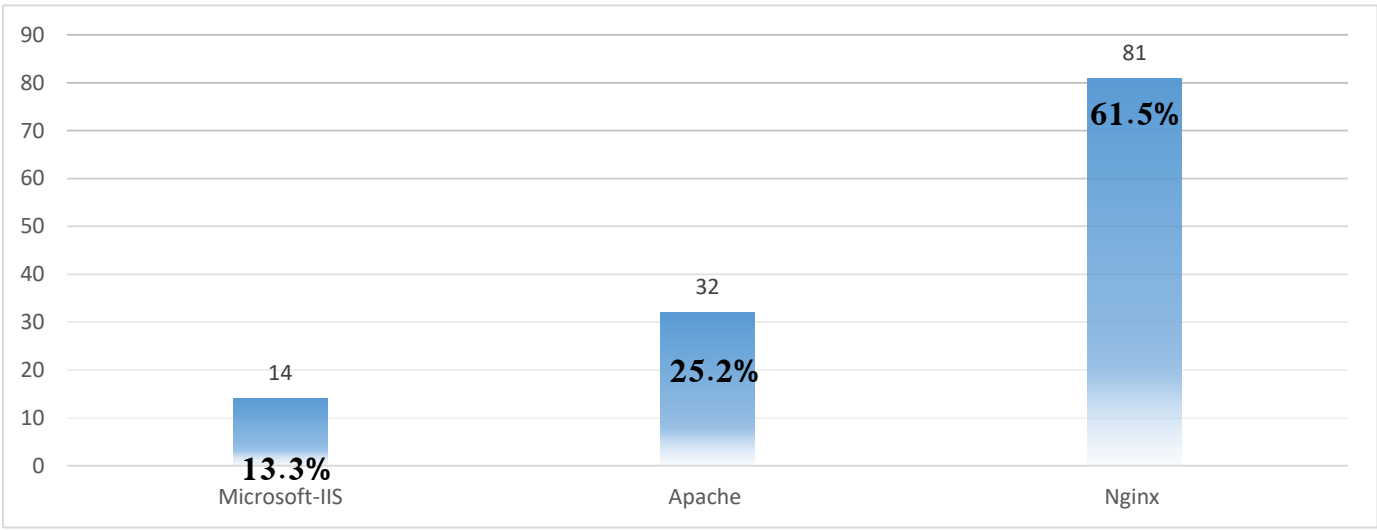


## 4.2- إحصائية نسب أنواع أنظمة تشغيل المخدمات المضيفة



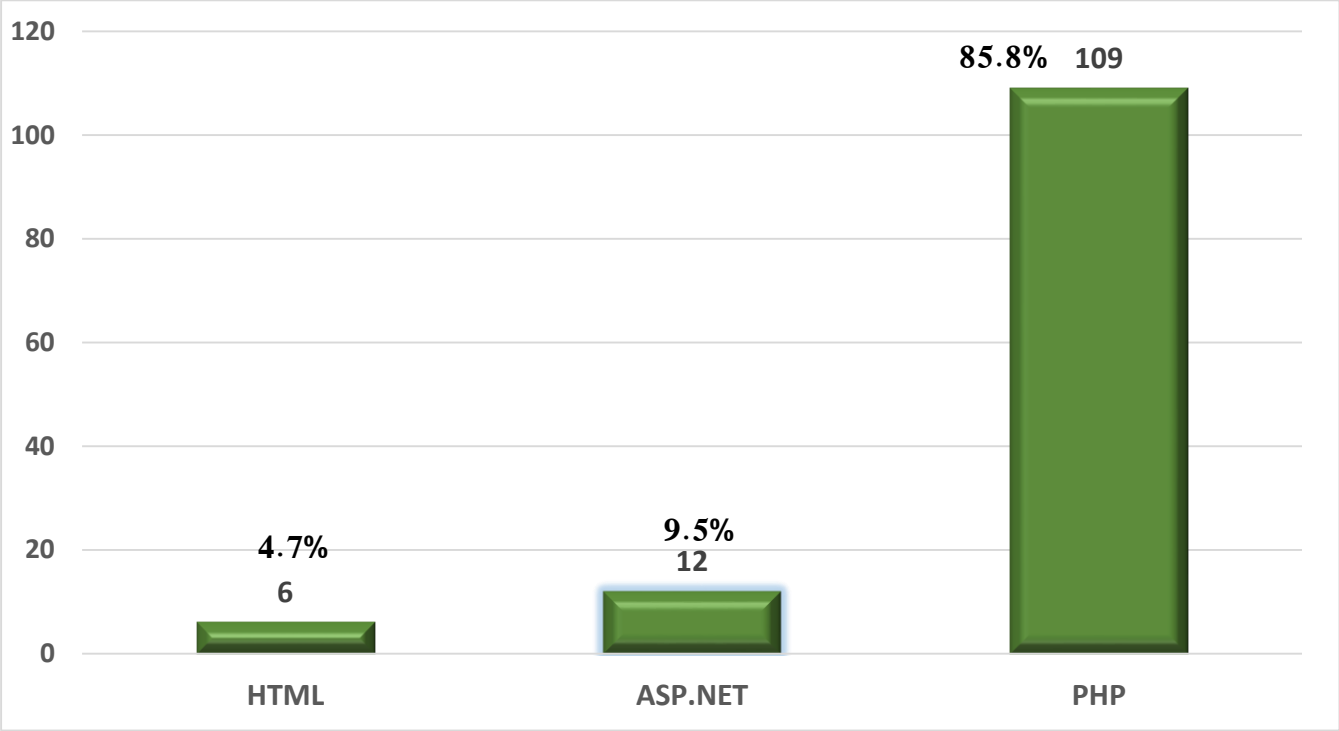

تظهر الإحصائية السابقة بوضوح بأن التوجه العام في أنظمة تشغيل المخدمات المضيفة هو اختيار أنظمة تشغيل مفتوحة المصدر لما لها من مزايا تشغيلية وأمنية متعددة.

## 4.3- إحصائية نسب أنواع مخدمات الويب




من الواضح الاعتماد بشكل كبير على مخدمات الويب ذات الإصدار مفتوح المصدر.

### 4.4- إحصائية لغات البرمجة التي تعتمدها بيئات التطوير



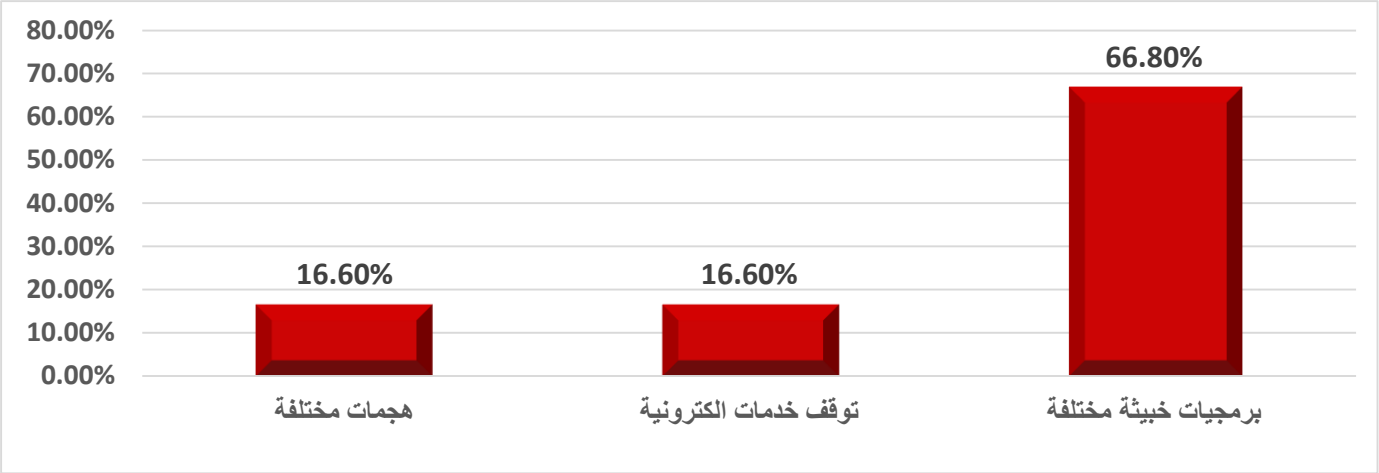

توضح الإحصائية السابقة اعتماد معظم المواقع الالكترونية على لغة البرمجة PHP التي تعدّ من أكثر لغات تطوير تطبيقات الويب انتشاراً.

### 4.5- الاستجابة للطوارئ المعلوماتية

تم خلال العام 2021 الاستجابة لـ 56 حالة طارئة تنوعت بين حالات اختراق برمجيات خبيثة منها فيروسات الفدية وهجمات أخرى، حيث قام المركز بالتعامل مع هذه الحالات تباعاً واتخاذ الإجراءات اللازمة وإعداد التقارير الفنية ذات الصلة، علماً بأن مركز أمن المعلومات يتعامل مع الحالات الطارئة التي يتم تبليغه بها بإحدى القنوات الرسمية، ومنها ما يتم اكتشافه من قبل المركز وتحذير الجهة المعنية، تنوعت حالات الاستجابة ضمن الفئات الرئيسية التالية:

- إصابة ببرمجيات خبيثة.
- توقف خدمات إلكترونية.
- اختراق منظومات معلوماتية باستغلال نقاط الضعف.

توضح الإحصائية التالية توزع أهم أنواع الاستجابة التي أنجزها المركز:




بالإضافة إلى قيام المركز ضمن دوره بالتحذير المبكر من الأخطار المعلوماتية بنشر عدد من التنبيهات والتحذيرات ضمن الوسائط المختلفة عن تهديدات محتملة تنوعت بين برمجيات خبيثة، روابط احتيالية، ثغرات برمجية وغيرها من الأخطار التي تهدد الوسائط المعلوماتية الشخصية والمنظومات المؤسساتية.

## 5- التوصيات والتوجهات المستقبلية

- السعي لتأمين الموارد البشرية اللازمة التي يحتاجها المركز لتقديم خدماته بالشكل الأمثل بالإضافة إلى العمل على تأهيل وتدريب الكادر التقني في المركز بشكل مستمر بهدف تزويده بالمعارف والمهارات اللازمة لرفع جودة الخدمات التي يقدمها المركز وتقديم خدمات جديدة.
- دعم مركز الاستجابة للطوارئ المعلوماتية بهدف ترقيته لمستوى مركز وطني للقيام بمهامه بالشكل الأمثل وتزويده بما يلزم من برمجيات وتجهيزات وخبرات بشرية مناسبة.
- الاستمرار بنشر الوعي وثقافة أمن المعلومات، سواء من خلال الدورات التدريبية أو المحاضرات أو المشاركة بورشات العمل التي تقوم بها الهيئة لشريحة واسعة من المسؤولين عن تقديم وادارة الخدمات الإلكترونية في الجهات العامة، أو من خلال التوعية الأمنية عن طريق النشرات الدورية التي يصدرها المركز.
- إضافة خدمات جديدة لنظام خدمات المركز مثل خدمة تقييم المخاطر، خدمة تدقيق أمن نظم المعلومات، خدمة تطوير سياسات أمن المعلومات وخدمة وضع خطط الاستجابة للحوادث الطارئة بالتوازي مع تأمين الكوادر المناسبة.
- تنفيذ المهام التي يُكلّف بها المركز في إطار دوره الوطني في مجالات أمن المعلومات المختلفة.
- تنفيذ المشاريع والأعمال المشار إليها في خطة عمل المركز لعام 2022.
- تقديم الخدمات الاستشارية والخبرات الفنية في مجال أمن المعلومات للجهات التي ترغب بذلك.
- إعداد قائمة بالمواقع الإلكترونية والتي تعتبر الأكثر أماناً بين المواقع المختبرة لعام 2021، كذلك الأمر مراسلة الجهات العامة التي لم تتواصل مع المركز لبيان ما قامت به من إجراءات بناء على تقارير المسح المرسلة لها خلال العام 2021، والوقوف على الأسباب والصعوبات ومعالجتها.

**مركز أمن المعلومات**

**2022**