



الإدارة العامة لتقنية المعلومات



تقرير حل وسد الثغرات المكتشفة
عن طريق الأمن السيبراني

بتاريخ : 29/01/2023

الإدارة العامة لتقنية المعلومات



الثغرات المكتشفة

WAPT-HA230115## – SQLi - Critical 3
WAPT-HA230115## – SQLi - Critical 5
WAPT-HA230115## – XSS - High 7
WAPT-HA230115## – XSS - High 8
WAPT-HA230115## – XSS - High 8
WAPT-HA230115## – XSS - High 10
WAPT-HA230115## – XSS - High 12
WAPT-HA230115## – Security Misconfiguration - High 13
WAPT-HA230115## – Security Misconfiguration - Medium

تم سد جميع
الثغرات



WAPT-HA230115## – XSS - High

Vulnerability Walk-thru:

infected URL

(/new_portal/admin_news)

حل الثغرة

تم اغلاق الثغرة عن طريق انشاء فلتر خاص يمنع من ادخال أي بيانات تحتوي احرف
لو كلمات غير معروفة الي قاعدة البيانات
عن طريق استعمال الكود المرفق

`strip_tags` — Strip HTML and PHP tags from a string

Description ¶

`strip_tags(string $string, array|string|null $allowed_tags = null): string`

This function tries to return a string with all NULL bytes, HTML and PHP tags stripped from a given string. It uses the same tag stripping state machine as the `fgetss()` function.

```
strip_tags($input);
```



WAPT-HA230115## – Security Misconfiguration

Vulnerability Walk-thru:

infected URL

<http://89.237.139.28:61/ords/f?p=100:9999:9366473099860>

حل الثغرة

تم اغلاق الثغرة عن طريق انشاء اسم مستخدم وكلمة خاصة للخدمة



WAPT-HA230115## – Security Misconfiguration

Vulnerability Walk-thru:

infected URL

<https://adfapp.amanathail.gov.sa/ords/f?p=100:LOGIN:5385498898759::::::&tz=3:00>

حل الثغرة

تم اغلاق الثغرة عن طريق انشاء تغيير أسماء المستخدمة وكلمات المرور الي كلمات مرور قوية