

Server Security Misconfiguration: - Default Credentials

ماهي ثغرة Server Security Misconfiguration؟

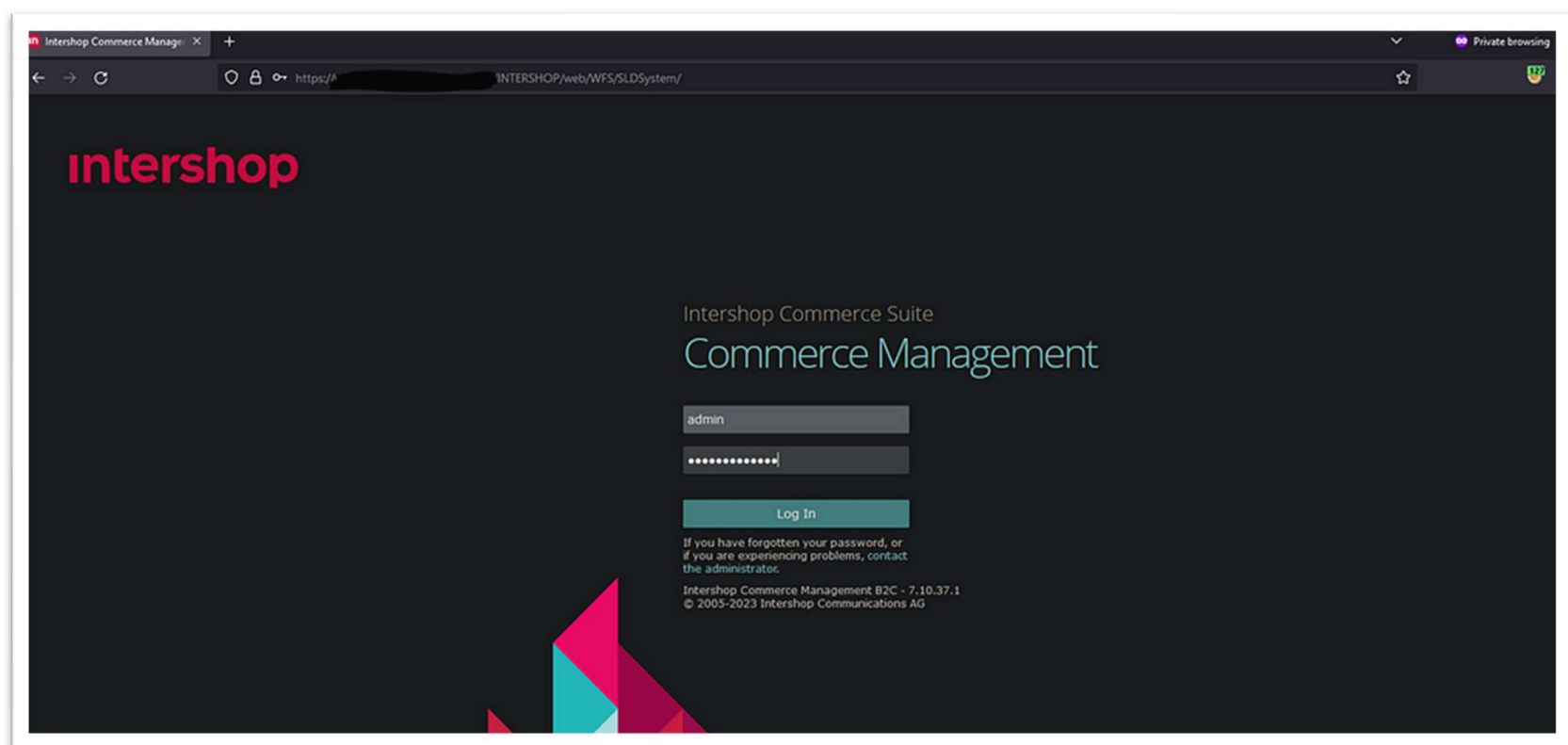
هي ثغرة ناتجة عن سوء إعداد الانظمة أو البرامج مفتوحة المصدر من مدراء الانظمة. أي يعني أنها ليست أخطاء ناتجة عن البرمجة.

إذاً الآن ما هو المقصود ب Default Credentials؟

هناك أنواع شائعة من ثغرات Server Security Misconfiguration، ولكن سوف نكتفي بهذا النوع الآن.. وفيما بعد بإذن الله تعالى سوف أشرح الأنواع الأخرى.

المقصود ب بيانات الاعتماد الافتراضية أي بيانات تسجيل الدخول أو التحقق Username و Password أنها موجودة على الوضع الافتراضي.

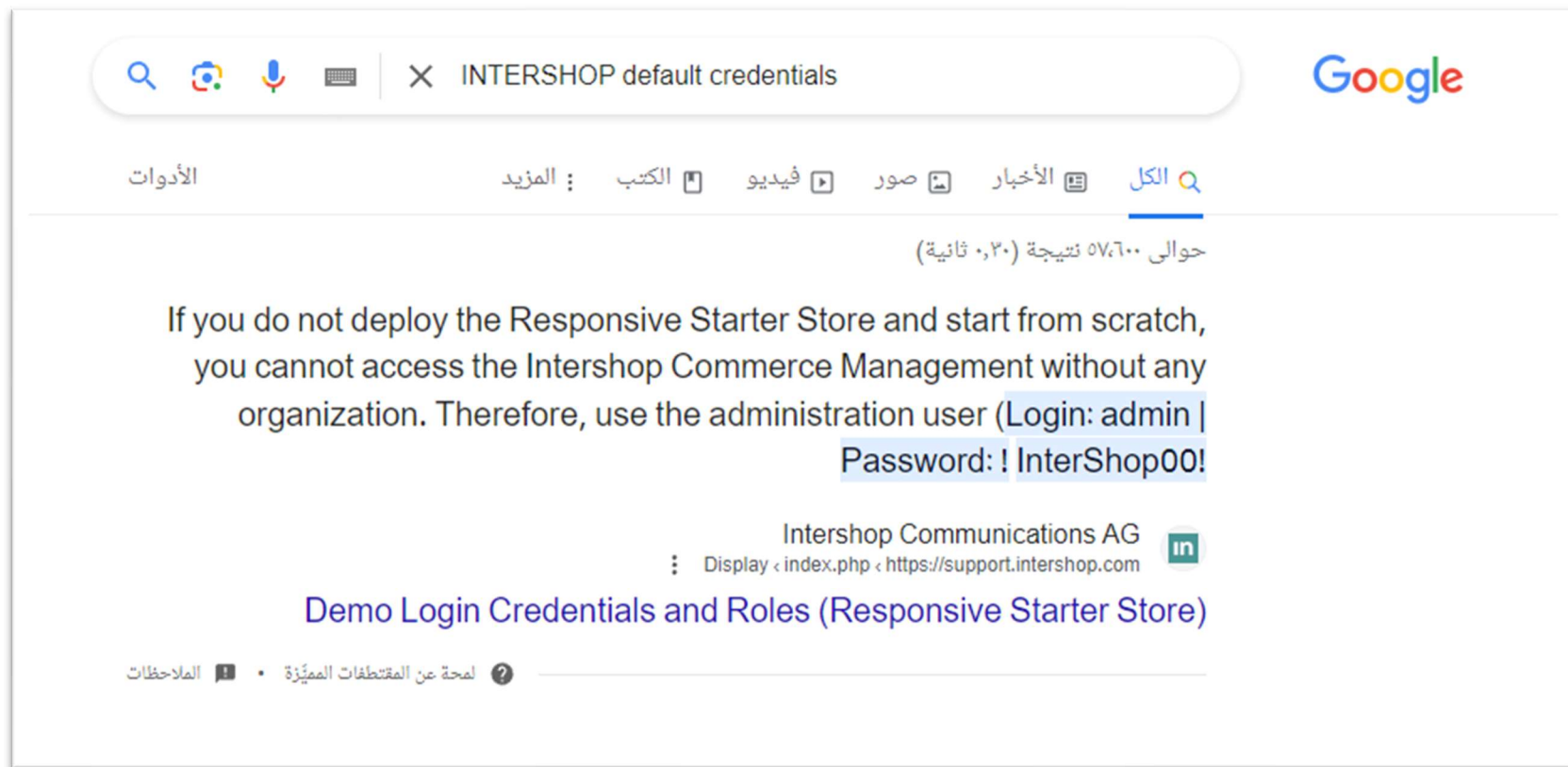
على سبيل المثال هنا شخص وجد صفحة تسجيل دخول على موقعاً ما وعند البحث عن بيانات الاعتماد الافتراضية وجد أن البيانات على الوضع الافتراضي، ولم يقوم مدير الانظمة بتغييرها!!!!



أسم المستخدم: admin

الرقم السري: !InterShop00!

عند البحث عن بيانات الاعتماد الافتراضية لنظام Intershop على قوقل، سوف تجد النتائج من الموقع الرسمي.



رابط المقالة كاملة للاطلاع: <https://infosecwriteups.com/default-credentials-p1-with-reward-in-a-bug-bounty-program-1aad9c008619>

وهنا شخص آخر وجد بيانات اعتماد افتراضية لكاميرا ستاربكس.

[Learn more about HackerOne](#)[Log in](#)

21


#398797


DVR default username and password

Share: [f](#) [t](#) [in](#) [y](#) [v](#)

radosec submitted a report to Starbucks.

Summary:
default username and password i found in one of your DVR camera system

Description:
hi
after scanning on starbucks register ip from this site <http://bge.he.net>
i start to scan the ip subnet : [REDACTED]
then i found this ip : [REDACTED] then i try to browse it then i found login page for DVR cam system
as can see in this picture :

F337222

then i start to test the default username and password
like user -- user
then i successfully login to your dvr system and browse you cams as i show in this photo :

F337223

Steps To Reproduce:
1. scanning in this ip subnet [REDACTED] and found [REDACTED]
2. browse [REDACTED] and i found web client for DVR system
3. login by default username and password username : user --- password : user

Impact
an attacker can control your DVR system and changing setting ... etc

ristretto updated the severity from Critical to Medium (6.1).

ristretto changed the status to ● Triaged.
Hi @radooz, Thank you for your report. We will work with our internal team on the resolution of this issue and get back once we receive an update.
Once again, Thanks for your report!

Reported August 24, 2018, 2:54am UTC

August 24, 2018, 9:09pm UTC

August 24, 2018, 9:11pm UTC

»

Reported August 24, 2018, 2:54am UTC

radosec

Participants

Report Id #398797 Resolved

Reported to Starbucks Managed

Disclosed

Severity

Weakness

Bounty

Time spent

CVE ID

Account de...

October 15, 2018, 10:31pm UTC

Medium (6.1)

None

None

None

None

None

الرابط للاطلاع: <https://hackerone.com/reports/398797>

الثغرة لا تقتصر على صفحات تسجيل الدخول المخصصة فقط لبعض المواقع، كذلك لصفحات تسجيل الدخول الخاصة بـراوترات وقواعد البيانات والكاميرات وكذلك بعض بروتوكولات الشبكة مثل FTP وغيرها من البروتوكولات الأخرى.

خطورة الثغرة: تصنف غالباً على أنها **Critical (١٠/٩)** أو **P1**. ولكن التصنيف يكون على حسب البيانات الحساسة التي وصلت لها عن طريق الثغرة.

وهنا رابط كامل بأغلب كلمات المرور الافتراضية لأغلب الأنظمة:

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv>

<https://github.com/danielmiessler/SecLists/tree/master/Passwords/Default-Credentials>

وهذا الموقع تعطيه أسم الراوتر ويعطيك بيانات الاعتماد الافتراضية لتسجيل الدخول:

<https://www.routerpasswords.com>

أي سؤال أي استفسار حياكم الله

Twitter: [iProgrammer16](#)

Telegram: iProgrammer16