"إطار أمان متعدد الطبقات الشامل لموقع الجامعة الإلكتروني"

الوصف:
تم تأمين موقع الجامعة الإلكتروني من خلال نهج متعدد الطبقات لضمان الحماية القصوى ضد التهديدات الإلكترونية، الوصول غير المصرح به، وتعطيل الأداء. تشمل إجراءات الأمان الرئيسية ما يلي:

الاستضافة والتشفير:

- يتم استضافة الموقع على **Hostinger Cloud Enterprise** مع وجود شهادة **SSL/TLS** (وضع **Full Strict**) لتشفير البيانات أثناء النقل.
- تم تفعيل **Always Use HTTPS** لإجبار جميع الاتصالات على استخدام اتصالات **HTTPS** الآمنة.

التكامل مع:Cloudflare

- يتم توجيه **DNS** والنطاق والحركة المرورية عبر **Cloudflare** لتوفير أمان متقدم وتحسين الأداء.

قواعد جدار الحماية المخصصة:(WAF)

تم تفعيل **خمس قواعد مخصصة** لحظر الجهات الخبيثة، بما في ذلك:

1. **القاعدة 1 :** تحظر الروبوتات غير المصرح بها مع السماح للروبوتات الشرعية) مثل محركات البحث، LetsEncrypt).
2. **القاعدة 2 :** تقوم بتصفية الروبوتات/المخترقين) مثل Yandex ، Baidu، (Python-requests ووكلاء المستخدم المشبوهين.
3. **القاعدة 3 :** تحظر الحركة المرورية من **ASNs** عالية الخطورة) مثل AWS ، (OVH ما لم يتم التحقق من شرعيتها.
4. **القاعدة 4 :** تحمي من هجمات **القوة الغاشمة**)مثل مسارات wp-login ، (wp-admin و **ASNs** الخبيثة.
5. **القاعدة 5 :** تحظر استغلالات **XML-RPC**، المسارات غير المصرح بها) مثل(wp-config ، والروبوتات العدوانية/الذكاء الاصطناعي.

وضع مكافحة الروبوتات:(Bot Fight Mode)

- يتحدى ويحظر الروبوتات الآلية، المخترقين، والتهديدات التلقائية.

حماية من هجمات:DDoS

- **حماية :HTTP DDoS** مفعلة دائمًا لتخفيف هجمات **طبقة التطبيقات**.

- **حماية شبكة SSL/من هجمات :DDoS** تمنع تلقائيًا هجمات **SYN floods**، **UDP reflection**، **استنفادSSL** ، والهجمات التي تنفذها **البوتنات**)مثل.(Mirai

التكامل مع:QUIC.cloud

- تم التكامل بأمان مع **Cloudflare**للتعامل مع **تحسين الصفحات والصور عبرCDN** ، مما يضمن تحسين الأداء دون المساس بالأمان.