

اختبار

SQL Injection

١. الوصف: لديك صفحة تسجيل دخول تحتوي على الحقليين التاليين: اسم المستخدم وكلمة المرور. في الشيفرة الخلفية، يتم تنفيذ الاستعلام التالي للتحقق من صحة المستخدم:

```
SELECT * FROM users WHERE username = '$username' AND password = '$password';
```

المهمة:

- اشرح لماذا هذه الشيفرة عرضة لـ SQL Injection.
- اقترح طريقة لإصلاحها.

اشرح لماذا هذه الشيفرة عرضة لـ SQL Injection:

عندما يتم إدخال البيانات بدون التحقق منها، يمكن للمهاجم إدخال أكواد SQL في حقول المدخلات مثل اسم المستخدم وكلمة المرور، مما يتيح له تعديل الاستعلام ليصل إلى بيانات غير مصرح له بالوصول إليها وهذا يسمح له بتخطي عملية التحقق من الهوية أو الوصول إلى بيانات المستخدمين الآخرين كما أن كلمة المرور الموجودة هي من كلمات المرور الشائعة والسهل تخمينها.

اقترح طريقة لإصلاحها:

الحل استخدام استعلامات معدة مسبقاً (Prepared Statements) والتي تقوم بفصل مدخلات المستخدم عن الاستعلام، مما يمنع إدخال أوامر ضارة. بالإضافة إلى ذلك، من المهم التحقق من المدخلات والتأكد من أنها تتبع الشكل المتوقع للبيانات.

XSS

١. الوصف: لديك صفحة تعرض تعليقات المستخدمين دون تنقية المدخلات. يمكن لأي مستخدم إدخال تعليق يحتوي على شيفرة: JavaScript

```
<div><?php echo $comment; ?></div>
```

المهمة:

- اشرح لماذا هذه الشيفرة عرضة لـ XSS.
- اقترح طريقة لإصلاحها.

اشرح لماذا هذه الشيفرة عرضة لـ XSS:

صفحة التعليقات تسمح بعرض المدخلات دون تنقية، وهذا يسمح لأي مستخدم بإدخال شيفرة JavaScript يمكن أن تنفذ هذه الشفرة في متصفحات المستخدمين الآخرين الذين يعرضون التعليقات. هذا يعرض المستخدمين لهجمات XSS، حيث يمكن للمهاجم سرقة ملفات تعريف الارتباط (Cookies) الخاصة بهم أو تنفيذ إجراءات غير مرغوبة.

اقترح طريقة لإصلاحها:

الحل الأفضل هو تنقية (Sanitize) المدخلات بشكل شامل لمنع أي شيفرات JavaScript أو HTML غير مرغوبة من التنفيذ. كما يمكن استخدام مكتبات تعقيم مخصصة تزيل أو تمنع الأكواد الضارة لضمان أمان البيانات المعروضة.

CSRF

١. الوصف: لديك نموذج لتغيير كلمة المرور يتم إرساله عبر طلب POST

```
<form method="POST" action="change_password.php">
  <input type="password" name="new_password">
  <input type="submit" value="Change Password">
</form>
```

المهمة:

- اشرح لماذا هذا النموذج عرضة لـ CSRF.
- اقترح طريقة لإصلاحها.

اشرح لماذا هذا النموذج عرضة لـ CSRF:

إن نموذج تغيير كلمة المرور يتم إرساله عبر طلب POST دون حماية من هجمات CSRF، يمكن للمهاجم إرسال طلب نيابة عن المستخدم إلى الخادم لتغيير كلمة المرور، طالما أن المستخدم قد سجل الدخول مسبقاً، مما يتيح تنفيذ الإجراء الضار بدون علم المستخدم.

اقترح طريقة لإصلاحها:

يمكن حماية النموذج عن طريق إضافة رموز مميزة (CSRF Tokens)، بحيث يتم التحقق من صحة الطلب قبل تنفيذه للتأكد من أنه صادر من مصدر موثوق. كما يفضل تنفيذ الطلبات الحساسة عبر طرق آمنة (مثل HTTPS) وطلب المصادقة الإضافية عند الحاجة.