وثيقة تعريف المادة

المقرر :أمن البيانات و التطبيقات

رمز المقرر: IWB404

ملخص:

يقدم محتوى المادة مقاربة لموضوع أمن المعلومات من منظور سوية التطبيقات بالتركيز على حقيقة أن الأمن كالسلسلة قوي بقوة أضعف حلقة في هذه السلسلة.

إن طبيعة و تنوع واختلاف معايير تطوير تطبيقات الوب والتقنيات التي يستخدمها المطورون يجعل من سوية التطبيقات من أكثر الأهداف عرضة للهجومات الموجهة إلى أنظمة المعلومات.

يركز المحتوى في هذه المادة على إعطاء الطالب فكرة نظرية و تطبيقية عن أكثر الهجومات شيوعاً والتي تؤثر على سوية التطبيقات مع التركيز على الذهنية و الإجرائية المستخدمة من قبل المخترقين في تنفيذ الهجوم إضافة إلى الأدوات المستخدمة لهذا الغرض.

يوفر المحتوى أمثلة تفصيلية لتمكين الطلاب من فهم كامل للنظرية و التطبيق كما يقدم أفكاراً عن أهم الطرق المتبعة في تطوير تطبيقات آمنة.

المخرجات التعليمية:

	المخرجات التعليمية	الجلسات	الوظيفة	الامتحان النهائي
LO1	إدراك مفهوم أمن سوية التطبيق و أهميته	S1 S2		👍
LO2	فهم إجرائية الاختراق المتبعة للتطبيقات و الذهنية التي يمتلكها المخترق عادة.	S3 S4 S5		👍
LO3	تفحص أنماط الاختراقات ضد التطبيقات و فهم نقاط الضعف و المتطلبات البدئية الواجب توافرها لنجاح الهجوم و طريقة تطبيق الهجومات والادوات المستخدمة لهذا الغرض	S6 S7-S8 S9-S10	👍	👍
LO4	تفحص مجموعة من المنهجيات الأكثر شيوعاً لتطوير تطبيقات الوب الآمنة	S11 S12	👍	👍

المحتوى

المحتوى المقدم في ملف PDF و المبني على كتاب (Web Application Security The Fast Guide) النسخة الأولى – 2017 للدكتور سامي خيمي.

- الأدوات و المراجع التي يزودها استاذ المادة كمراجع إضافية.

معايير التقييم و تغطية المحصلات:

المخرجات التعليمية	معايير التقييم و تغطية المحصلات
LO1	1. تعريف مفهوم أمن المعلومات و وصف نموذج أمن الطبقات و دور كل طبقة 2. وصف تقنيات الوب المختلفة و المستخدمة ضمن سوية التطبيق.
LO2	1. لخص مراحل إجرائية الاختراق مع التمييز بين الأنشطة المختلفة الواجب تطبيقها في كل مرحلة. 2. تفسير الطريقة التي يفكر بها المخترقون و دوافعهم.
LO3	1. تفسير الأنماط المختلفة للاختراق. 2. استخدام الأدوات بفعالية لإعادة توليد الهجوم لأهم أنواع الاختراقات.
LO4	1. مقارنة المنهجيات الأساسية لتطوير التطبيقات الآمنة

توليد الشواهد:

الطلاب في هذا المقرر مطالبون بتوليد مجموعة من الشواهد لإظهار تغطية شاملة لجميع المخرجات التعليمية. تتضمن الشواهد المطلوبة:

الوظيفة (25%)

في هذه الوظيفة يتم التركيز بشكل أساسي على :

1- توليد سيناريو لاختبار قدرة الطالب على فهم و تحليل و تحري وجود نقاط ضعف في تطبيق وربطه بطريقة الاختراق المناسبة.
2- توليد وثيقة أولية تظهر فهم الطالب للمنهجيات الأساسية بناء تطبيقات الوب الآمنة

الامتحان (75%):

يغطي هذا الشاهد معظم المخرجات التعليمية مع التركيز بشكل أساسي على سوية الحفظ والإدارك للمفاهيم.

الروابط:

يرتبط هذا المقرر بشكل رئيسي بمقرر تطوير تطبيقات الوب و المقرارات ذات العلاقة بهندسة البرمجيات و هندسة الوب كون المحتوى يناقش في أجزاء منه المنهجيات المختلفة لتطوير تطبيقات الوب الآمنة.

المصادر:

- محتوى المقرر على موودل كملف PDF
- كتاب Web Application security the fast guide تأليف الدكتور سامي خيمي النسخة الأولى 2017 - و العروض التقديمية الخاصة بالكتاب.
- المصادر الخاصة بالأدوات المستخدمة.
- الجلسات المتزامنة و المسجلة.

اللقاءات الافتراضية :

تقوم الجلسات الافتراضية بتغطية المقرر باستخدام مقاربتين:

- الحوار و النقاش لتشجيع الطلاب على تطوير إدراك متكامل لجميع المفاهيم.
- عرض عملي لبعض أهم الاختراقات و سيناريوهات تنفيذها و الأدوات المستخدمة.

مقترحات للقراءة

1. AKAMAI. (2014). *A Guide to multilayer web securty.*
2. Bryan Sullivan, V. L. (2012). MC Graw Hill.
3. Chandra, P. *Software Assurance maturity model.*
4. Christian S. Fötinger, W. Z. Understanding a hacker's mind –A psychological insight into the hijacking of identities.
5. Dafydd Stuttard, M. P. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition.* 2011: Wiley.
6. Gary McGraw, P. S.*BSIMM7.*
7. JOEL SCAMBRAY, V. L. (2011). *Hacking exposed web application.* MC Graw Hill.
8. Mark Curphey, J. S. (2003). *Improving Web Application Security: Threats and Countermeasures.*
9. OWASP. (2013). *OWASP top 10.*
10. Roger Meyer, C. C. (2008). *Detecting attacks on web application from log files.*
11. sheama, M. (2011). *Web application security for dummies.* Wiley.
12. Tom Brennan, J. J. (2015). *Top 10 Considerations For Incident Response.*
13. Xue, X. L. (2013). *A Survey on Web Application Security.*