ב"ה

מבחן בקורס – בנית ישומים מאובטחים (Building Secure Applications)

סמסטר א' – תשע"ד, מועד ב'

משך הבחינה: שעה וחצי, כל חומר עזר אסור בשימוש

יש לענות על 33 מתוך 35 השאלות

(מי שיענה על יותר מ 33 שאלות יבדקו 33 השאלות הראשונות שענה עליהם)

1. איזה מבין ההתקפות הבאות מנצלת טעות (Vulnerability) של המפתח?
   א. Insecure direct Object reference
   ב. SQL Injection attack
   ג. Dictionary attack
   ד. תשובות א' וב' נכונות – התשובה הנכונה
   ה. תשובות א' ב' וג' נכונות

2. האזנה לאינפורמציה המועברת ברשת היא:
   א. Vulnerability שיכול להיות מנוצל לפגיעה בסודיות המידע
   ב. Vulnerability שיכול להיות מנוצל לפגיעה בשלמות המידע
   ג. Attack - התקפה שפוגעת בסודיות המידע – התשובה הנכונה
   ד. Attack – התקפה שפוגעת בשלמות המידע
   ה. כל התשובות נכונות

3. איזה מנגנון מאפשר לגלות שתוכן הקובץ שונה ע"י גורם שאינו מורשה?
   א. Read Access Control
   ב. Write Access Control
   ג. Digital Signature – התשובה הנכונה
   ד. Encryption

4. איזה התקפה מהווה איום ישיר על ה Availability של האפליקציה
   א. ההאזנה לתקשורת בין רכיבי האפליקציה
   ב. שינוי תוכן ההודעה שנשלחת ע"י המשתמש
   ג. התקפה הגורמת לאפליקציה להכנס ללואה אינסופית – התשובה הנכונה
   ד. התחזות למשתמש אחר

5. באיזה תפיסת אבטחת מידע יתכן False Positive בהנחה שהמנגנון מקונפג באופן מדויק?
   א. ב Positive Security Logic
   ב. Negative Security Logic – התשובה הנכונה
   ג. ב Positive Security Logic וב Negative Security Logic
   ד. אף אחת מהתשובות לעיל אינה נכונה

6. מדוע ה Network Firewall אינו מגן בפני התקפות ברמת האפליקציה:
   א. כי הוא אינו חלק אינטגרלי מהאפליקציה
   ב. כי הוא מישם Negative Security Logic
   ג. **כי הוא בודק את ה Packet רק ברמת פרוטוקול התקשורת ולא את התוכן האפליקטיבי של Packet – התשובה הנכונה**
   ד. כי הוא מישם Positive Security Logic

7. מה היחס בין אורך המפתח ההצפנה ובין רמת הסודיות של המידע שמספק אלגוריתם ההצפנה?
   א. הטענה "כל שהמפתח ארוך יותר רמת הסודיות שמספק אלגוריתם ההצפנה גבוהה יותר" נכונה תמיד
   ב. **הסודיות של המידע תלויה הן באורכו של המפתח ההצפנה והן בחוזקו של אלגוריתם ההצפנה – התשובה הנכונה**
   ג. הסודיות של המידע תלויה רק בחוזקו של אלגוריתם ההצפנה ואינה תלויה כלל באורך המפתח
   ד. כאשר אלגוריתם ההצפנה אינו שביר אין חשיבות לאורכו של המפתח

8. מה היחס בין מוד ECB למוד CBC?
   א. ECB בטוח יותר מאשר CBC
   ב. **CBC בטוח יותר מאפשר ECB – התשובה הנכונה**
   ג. ECB משמש להצפנה ו CBC לחתימה דיגיטלית
   ד. ECB משמש להצפנה סימטרית ו CBC להצפנה אסימטרית

9. ההבדל העקרוני בין הצפנה סימטרית להצפנה אסימטרית הוא:
   א. שהצפנה סימטרית מתאימה ל Stream Cipher והצפנה אסימטרית ל Block Cipher
   ב. **שבהצפנה סימטרית אותו מפתח משמש גם להצפנה וגם לפענוח ובהצפנה אסימטרית מפתח אחד משמש להצפנה והמפתח האחר לפענוח – התשובה הנכונה**
   ג. שבהצפנה סימטרית יש להשתמש מפתחות הצפנה ארוכים יותר לעומת מפתחות ההצפנה שבהם נעשה שימוש בהצפנה אסימטרית
   ד. שבהצפנה סימטרית אותו אלגוריתם משמש גם להצפנה וגם לפענוח ובהצפנה אסימטרית אלגוריתם אחד משמש להצפנה והאחר לפענוח
   ה. שהצפנה סימטרית מתאימה לשמירה על שלמות המידע והצפנה אסימטרית על סודיות המידע
   ו. תשובות ב' וג' נכונות

10. N אנשים מעונינים ליצור ערוצי תקשורת מאובטחים בינהם לכמה מפתחות יזדקקו בהצפנה סימטרית ובהצפנה אסימטרית?
   א. ל 2N מפתחות הן בהצפנה סימטרית והן בהצפנה אסימטרית
   ב. ל N מפתחות בהצפנה סימטרית ול 2N מפתחות בהצפנה אסימטרית (N מפתחות ציבוריים ו N מפתחות פרטיים)
   ג. **ל N(N-1)/2 מפתחות בהצפנה סימטרית ל 2N מפתחות בהצפנה אסימטרית (N מפתחות ציבוריים ו N מפתחות פרטיים) – התשובה הנכונה**
   ד. ל N(N-1)/2 מפתחות בהצפנה סימטרית ל N^2 מפתחות בהצפנה אסימטרית (N מפתחות פרטיים ו N(N-1) מפתחות ציבוריים)

11. באיזה מבין מודי ההצפנה הבאים ביט הסתר תלוי רק בביט הגלוי המקביל לו?
    א. Stream Cipher
    ב. Block Cipher in CTR mode
    ג. Block Cipher in CBC mode
    ד. **תשובות א' וב' נכונות – התשובה הנכונה**

12. באיזה מהאלגוריתמים הבאים ניתן למקבל (לחשב במקביל) את פענוח ההודעה המוצפנת?
    א. AES in ECB mode
    ב. AES in CBC mode
    ג. AES in CTR mode
    ד. תשובות א' וב' נכונות
    ה. תשובות א' וג' נכונות
    ו. תשובות ב' וג' נכונות
    ז. **כל התשובות נכונות – התשובה הנכונה**

13. ב XML Encryption ה CipherData element יכול להכיל:
    א. רק את התוכן המוצפן
    ב. רק Reference לתוכן המוצפן
    ג. גם תוכן המוצפן וגם מצביע לתוכן המוצפן
    ד. **או את התוכן המוצפן או מצביע לתוכן המוצפן – התשובה הנכונה**

14. ב XML Encryption כאשר ה EncryptionMethod הוא אלגוריתם הצפנה אסימטרית למה יכול לשמש ה KeyInfo Element בתוך ה ה EncryptedData element
    א. להעביר את שם הקוד של המפתח הפרטי שבו השתמשו להצפנת ה CipherData
    ב. להעביר את המפתח הציבורי התואם למפתח הפרטי שבו השתמשו להצפנת ה CipherData
    ג. **להעביר את המפתח הציבורי שבו השתמשו להצפנת ה CipherData – התשובה הנכונה**
    ד. תשובות א' וג' נכונות

15. מה הכוונה בדרישה ל Second Preimange resistance מפונקצית Hash קריפטוגרפית?
    א. שקשה למצוא שתי הודעות M ו M' שחישוב פונקצית ה Hash עליהם נותן אותה תוצאה
    ב. שקשה לחשב את פונקצית ה Hash בהנתן הודעה M
    ג. **שבהנתן הודעה M קשה למצוא הודעה M' שחישוב פונקצית ה Hash עליה יתן אותה תוצאה כמו חישוב ה Hash על הודעה M – התשובה הנכונה**
    ד. שקשה למצוא את הודעה M בהנתן ערכה של פונקצית ה Hash על M

16. חתימה דיגיטלית על תוכן הודעה M יכולה להיות מבוססת על:
    א. הצפנה סימטרית של ה Hash הקריפטוגרפי של הודעה M
    ב. הצפנה סימטרית של תוכן ההודעה וערך ה Hash הקריפטוגרפי של הודעה M
    ג. חישוב פונקצית HMAC על ההודעה M בשילוב מפתח סודי סימטרי
    ד. תשובות א' וב' נכונות
    ה. **תשובות א', ב' וג' נכונות – התשובה הנכונה**

17. איזה אלמנט **<u>אינו</u>** חלק מה SignedInfo element ב XML Digital Signature?
    א. **Key Info – התשובה הנכונה**
    ב. SignatureMethod
    ג. CanocalizationMethod
    ד. Reference elements

18. מה היחס בין Transform ובין Canocalization ב XML Digital Signatures?
    א. Transform זה סוג של Caonocalization
    ב. **Canocalization זה סוג של Transform – התשובה הנכונה**
    ג. אין קשר בין Transform ובין Canocalization
    ד. הם זהים

19. ב Java Crypto API כאשר ב getInstance לא מצוין שמו של ה Provider אזי ה JRE? (בחר את התשובה המדויקת ביותר)
    א. יבחר את ה Provider שמוגדר כ Default ב Java Security File
    ב. יבחר את ה Provider הראשון ברשימה שמופיעה ב Java Security File שמספק ישום ל engine class המבוקש
    ג. **יבחר את ה Provider הראשון ברשימה שמופיעה ב Java Security File שמספק ישום לאלגוריתם המבוקש עבור engine class – התשובה הנכונה**
    ד. יבחר את ה Provider שמספק את הישום המהיר ביותר לאלגוריתם המבוקש עבור engine class מתוך הרשימה שמופיעה ב Java Security File
    ה. יבחר את ה Provider שמספק את הישום המאובטח ביותר לאלגוריתם המבוקש עבור engine class מתוך הרשימה שמופיעה ב Java Security File

20. ב Java Crypto API מה הם המצבים (States) האפשריים ל Signature engine class ?
    א. Uninitialized
    ב. Digest calculation
    ג. Sign
    ד. Verify
    ה. **תשובות א' ג' וד' נכונות – התשובה הנכונה**
    ו. תשובות ב' ג' וד' נכונות
    ז. תשובות א' ב' ג' וד' נכונות

21. לאיזה התקפה אפשרית נחשף שרת המממש מנגנון של Challenge-Response כתוצאה מכך שהוא שומר את ה Challenge שנשלח למשתמש בתהליך ה Authentication (במידה ולא יממש אמצעי הגנה מתאימים)?
    א. להתקפת Replay
    ב. **להתקפת DoS/DDoS (Distributed Denial of Service) – התשובה הנכונה**
    ג. התקפת MITM (Man In The Middle)
    ד. התוקף יכול לפענח מתוך ה Response את הסיסמא של המשתמש

22. מה הוא מנגנון ההצפנה שמונע התקפת Replay על סיסמא סטטית המועברת ברשת
א. הצפנת הסיסמא ע"י מפתח הצפנה סימטרי
ב. הצפנת הסיסמא ע"י מפתח הפרטי של ה Client בהצפנה אסימטרית
ג. **שימוש במנגנון Challenge Response – התשובה הנכונה**
ד. תשובות א' וב'
ה. תשובות ב' וג'
ו. תשובות א' ב' וג'

23. באיזה שיטת הזדהות (Authentication Method) הסיסמאות של המשתמשים לא נשמרות בשרת?
א. Challenge-Response המבוסס על הצפנה אסימטרית
ב. Lampert's Hash
ג. הזדהות באמצעות כרטיס בינגו וסיסמא סטטית
ד. **תשובות א' וב' נכונות – התשובה הנכונה**
ה. תשובות א' ג' נכונות
ו. תשובות א' ב' וג' נכונות

24. מה תפקידו של ה Salt בהגנה על הסיסמאות הסטטיות הנשמרות בקובץ Etc/password במערכות Unix/Linux
א. הוא משמש להצפנת הקובץ בהצפנה סימטרית
ב. הוא משמש למניעת מניה מלאה על הסיסמא המוצפנת
ג. הוא משמש למניעת מניה מלאה על הסיסמא באמצעות טבלאות של סיסמאות מוצפנות מוכנות מראש (Pre computed dictionary attack)
ד. הוא מונע מצב שבו ניתן יהיה לאתר משתמשים שבחרו סיסמאות זהות
ה. תשובות ב' וג' נכונות
ו. **תשובות ג' וד' נכונות – התשובה הנכונה**
ז. תשובות ב' ג' וד' נכונות

25. מה מבין שיטות ההזדהות הבאות עונה על ההגדרה של Strong Authentication?
א. **שימוש בסיסמא סטטית בשיתוף סיסמא הנבנת ע"י ערכים מכרטיס בינגו – התשובה הנכונה**
ב. שימוש בסיסמא חד פעמית הנשלחת באמצעות ה SMS
ג. סיסמא המיוצרת ע"י Challenge-Response Token
ד. סיסמא סטטית הנשלחת באמצעות מנגנון של Lampert's Hash

26. איזה מבין ה Authentication tokens הבאים אינו דורש חיבור למחשב?
א. Smartcard
ב. Time Based OTP Token
ג. USB based Token
ד. סיסמא חד פעמית (OTP) הנשלחת באמצעות SMS
ה. תשובות א' וב' נכונות
ו. **תשובות ב' וד' נכונות – התשובה הנכונה**
ז. תשובות ג' וד' נכונות

27. במודל ה ACL איזה מבין המשפטים הבאים נכון?
א. **ACL של Object מתקבל מעמודה ב Access Control Matrix שניקו ממנה את התאים הריקים – התשובה הנכונה**
ב. ACL של Subject מתקבל מעמודה ב Access Control Matrix שניקו ממנה את התאים הריקים
ג. ACL של Object מתקבל משורה ב Access Control Matrix שניקו ממנה את התאים הריקים
ד. ACL של Subject מתקבל משורה ב Access Control Matrix שניקו ממנה את התאים הריקים

28. כאשר משתמש מחליף תפקיד בארגון ויש לעדכן את הרשאות ה Access Control שלו לאוביקטים במערכת:
א. קל לבצע זאת יותר במודל ה ACL מאשר במודל ה Capabilities
ב. **קשה לבצע זאת יותר במודל ה ACL מאשר במודל ה Capabilities – התשובה הנכונה**
ג. בשני המודלים זה קל לביצוע
ד. בשני המודלים זה קשה לביצוע

29. השימוש בקבוצות של משתמשים (Groups) בא להקל על הניהול של ההרשאות:
א. **במודל ה ACL – התשובה הנכונה**
ב. במודל ה Capabilities
ג. במודל ה MAC
ד. במודל ה RBAC

30. במודל ה RBAC אזי ה Role הוא?
א. אוסף של משתמשים
ב. **אוסף של הרשאות לבצע פעולות על אוביקטים – התשובה הנכונה**
ג. אוסף של אוביקטים בעלי הרשאות זהות
ד. אף תשובה אינה נכונה

31. איזה מבין שיטות ה Access-Control הבאות היא המותאמת ביותר לניהול הרשאות מבוזר ?
א. **DAC – התשובה הנכונה**
ב. MAC
ג. RBAC
ד. תשובות א' וב' נכונות
ה. תשובות א' וג' נכונות
ו. אף אחת מהשיטות לעיל

32. על מנת להבטיח שלא בוצע Hidden Parameter Tampering נדרש:
א. לבצע Input validation based on Negative security logic על ערך הפרמטר
ב. לבצע Format validation על ערך הפרמטר
ג. **לבדוק שהערך שהתקבל מהדפדפן הוא אחד מהערכים (או הערך) שנשלח בדף ה Web לדפדפן – התשובה הנכונה**
ד. לבדוק שהערך של הפרמטר אינו כולל תו שאופיני להתקפת SQL Injection

33. לצורך איזה מנגנון אבטחת מידע יש צורך ב canocalization?
א. Input validation that is based on positive security logic
ב. **Input validation that is based on negative security logic – התשובה הנכונה**
ג. Access-control
ד. Challenge-Response

34. מה הדרכים למנוע התקפת Injection attacks?
א. שימוש ב Authentication Factor טוב יותר
ב. Input validation
ג. צמצום ההרשאות של האפליקציה
ד. תשובות א' וג' נכונות
ה. **תשובות ב' וג' נכונות – התשובה הנכונה**
ו. תשובות א' ב' וג' נכונות

35. איזה מבין המצבים הבאים היא דוגמא ל Insecure Direct Object Reference?
א. שילוב של RecordID בבסיס הנתונים ב URL של בקשת ה HTTP
ב. שילוב של אינדקס לטבלת המרה כ Hidden Parameter ב FORM
ג. שילוב של מספר ת.ז. של המשתמש כ Hidden Parameter ב FORM
ד. תשובות א' וב' נכונות
ה. **תשובות א' וג' נכונות – התשובה הנכונה**
ו. תשובות א' ב' וג' נכונות

בהצלחה