

3/4

מבחן בקורס - אבטחת ישומים ברשת (Web Application Security)

סמסטר ב' - תש"ע

משך הבחינה: שעה וארבעים דקות

כל חומר עזר אסור בשימוש

יש לענות על 33 שאלות, כל שאלה שווה 3 נקודות, סה"כ 99 נקודות + נקודה בונוס

1. מפתח רצה לודא בדיקה ראשונית של הקוד של המשתמש בדפדפן וצורך זה הצפין באמצעות פונקציית Hash קריפטוגרפית את רשימת הקודים החוקיים וצרף אותה לקוד ה Javascript בדף ה HTML המכצע את בדיקת הקוד, האם זה בטוח כבדיקה ראשונית של הקוד?

- א. לא, כי לא מבצעים בדיקות בצד הדפדפן
- ב. לא, כי תמיד ניתן למנות על הקודים החוקיים ולהשוות לרשימת הקודים המוצפנים
- ג. כן, כל לא ניתן למנות על הקודים החוקיים
- ד. תלוי במרחב האפשרויות של הקודים החוקיים.

למה ב Web application לא ניתן להתבסס על Client-Side Validation?
 א. כי המפתחים של Web applications אינם יודעים לממש Client-Side Validation
 ב. כי קל לתוקף לבטל את המימוש של ה Client-Side Validation ע"י שינוי הקוד שרץ בדפדפן
 ג. כי קל לתוקף לשנות את ה HTTP request ששולח הדפדפן ל Web server
 ד. תשובות ב' וג' נכונות

3. באיזה מוד של NAT כל כתובת חיצונית רואה את השרת ברשת הפנימית בכתובת IP אחרת?

- א. Full Cone
- ב. Restricted Cone
- ג. Port Restricted Cone
- ד. Symmetric NAT

4. מה ההבדל העקרוני בין Packet Filter ובין NAT?
 א. NAT מסתיר את הכתובות של הרשת הפנימית וה Packet Filter מבקר את הגישה לכתובות ברשת הפנימית

- ב. ה NAT מסתיר את הכתובות של הרשת החיצונית וה Packet Filter מבקר את הגישה לכתובות ברשת החיצונית
- ג. ה NAT מתאים לפרוטוקול ה UDP וה Packet Filter לפרוטוקול ה TCP
- ד. ה NAT מקביל ל Statefull Packet Filter

5. מנגנון ה Challenge-Response הוא

- א. מנגנון Access-Control
- ב. מנגנון Auditing
- ג. צורה של חתימה דיגיטלית
- ד. אופן מאובטח להעברת סיסמא ברשת

6. איזה התקפה מהווה איום ישיר על ה Availability של המערכת?

6/6

- א. ההאזנה לתקשורת
- ב. שינוי תוכן ההודעה
- ג. התקפת Denial-of-Service
- ד. התחזות למשתמש אחר

7. כאשר הגדרת התבניות (Patterns and Signatures) עליהם מבוסס זיהוי ההתקפות במנגנון מסוג Negative Security Logic היא מאד מדויקת אזי

לדיוק הציון גבוה לא אוקי \Rightarrow
- מבוסס על אירועי אכיזה
- לא מבוסס על אירועי חיסיון

- א. הסיכוי ל False Negative גבוה
- ב. הסיכוי ל False Positive גבוה
- ג. תשובות א' וב' נכונות
- ד. כל התשובות לא נכונות

8. מה הוא המנגנון המאפשר להבטיח את שלמות המידע (Data Integrity) כאשר המידע נייח?

- א. Authorization and Access Control
- ב. Encryption
- ג. Auditing
- ד. Authentication

9. מה הוא Vulnerability?

- א. סיכון למערכת מאירוע אבטחת מידע
- ב. נזק אפשרי למערכת מאירוע אבטחת מידע
- ג. פגיעות במערכת שיכולה לאפשר התקפה על המערכת
- ד. התקפה על המערכת שיכולה לגרום נזק למערכת

10. ב Web SSO המבוסס על SAML במודל ה PULL

- א. ה Assertion חייב להיות חתום בחתימה דיגיטלית כי הוא עובר דרך הדפדפן של המשתמש
- ב. ה Assertion לא חייב להיות חתום כי הוא עובר דרך הדפדפן של המשתמש
- ג. ה Artifact חייב להיות חתום בחתימה דיגיטלית כי הוא עובר דרך הדפדפן של המשתמש
- ד. ה Artifact לא חייב להיות חתום כי הוא אינו מכיל את ה Assertion עצמו

11. מה מבין שיטות ההזדהות הבאות עונה על ההגדרה של Strong Authentication?

- א. שימוש בסיסמא הנשלחת באמצעות ה SMS
- ב. שימוש בסיסמא סטטית בשילוב בסיסמא המיוצרת ע"י התקן ליצור סיסמאות חד פעמיות (OTP Token)
- ג. סיסמא חד פעמית המיוצרת ע"י התקן ליצור סיסמאות חד פעמיות (OTP Token)
- ד. סיסמא סטטית הנשלחת באמצעות מנגנון של Challenge Response

12. איזה מבין הבדיקות הבאות אינה מסוג Positive Security Logic?

- א. בדיקה שהאורך של הפרמטר הוא בטווח האורך החוקי שהוגדר
- ב. בדיקה שהערך של הפרמטר הוא הערך שנשלח למשתמש כ Hidden Parameter
- ג. בדיקה שהערך של הפרמטר אינו כולל מחרוזת שידועה כמשתמשת להתקפת SQL Injection
- ד. בדיקה שהערך של הפרמטר מכיל רק אותיות וספרות

13. מה הכוונה בדרישה ל Second Preimange resistance מפונקציית Hash קריפטוגרפית?

- א. אשקשה למצוא שתי הודעות M ו M' שחישוב פונקציית ה Hash עליהם נותן אותה תוצאה
- ב. אשקשה לחשב את פונקציית ה Hash בהנתן הודעה M

X/Y

13. שבהנתן הודעה M קשה למצוא הודעה M' שחישוב פונקציה ה Hash עליה יתן אותה תוצאה כמו חישוב ה Hash על פונקציה M
ד. שקשה למצוא את הודעה M בהנתן ערכה של פונקציה ה Hash על M

14. מי הוא ה Certificate Authority?

א. הגורם המנפיק Digital certificates

ב. הגורם הבודק את ה Digital Certificates

ג. הגורם לו הונפק ה Digital Certificate

ד. הגורם המיצר את ה Public key המופיע ב Digital Certificate

15. אי טיפול נכון בהודעות שגיאה הוא

א. Risk

ב. Vulnerability

ג. Attack

ד. כל התשובות אינם נכונות

16. איזה Vulnerability מנצלת התקפת Phishing?

א. את חוסר ההבנה של המשתמש והאמון של המשתמש בהודעות דואל (Social Hacking)

ב. את העובדה שהאפליקציה לא משתמשת ב HTTP Digest Authentication

ג. את העובדה שהאפליקציה לא מבצעת Input Validation כנדרש

ד. את העובדה שהאפליקציה רצה על שרת שלא הוקשח כהלכה

17. איזה מנגנון יכול למנוע XSRF/CSRF כאשר האפליקציה חשופה ל XSS?

א. Client-side Input Validation

ב. Server-Side Input Validation

ג. Output Encoding

ד. כאשר אפליקציה חשופה ל XSS אין מנגנון שיכול למנוע התקפת XSRF/CSRF

18. איזה התקפה מנצלת את העובדה שה SessionID שנמצא ב Cookie נשלח אוטומטית ע"י הדפדפן?

א. התקפת XSS

ב. התקפת XSRF/CSRF

ג. התקפת SQL Injection

ד. התקפת Hidden Parameter Manipulation

19. איזה מנגנון/דרישת אבטחת מידע לא מספק ה SSL?

א. Data Integrity

ב. Data Confidentiality

ג. Non-repudiation

ד. Server Authentication

20. ההבדל בין Statefull firewall ובין Stateless Firewall בא לידי ביטוי?

א. הן בתעבורת TCP והן בתעבורת UDP

ב. רק בתעבורת UDP כי בא אין משמעות ל Connection State

ג. רק בתעבורת TCP כי בא מופיע ה SYN BIT ב TCP Header

ד. רק בתעבורת TCP כי בא יש Connections ובא אפשר לשייך Packet ל Connection



21. ההגדרה של Positive Security Logic היא

- א. מה שמזוהה כהתקפה צריך למנוע
- ב. רק מה שהוגדר כחוקי יאופשר ע"י המערכת
- ג. רק מה שהוגדר כלא חוקי ימנע ע"י המערכת
- ד. התנהגות נורמטיבית תוגדר כחיובית

22. מה כולל ה SSL Cipher Spec?

- א. את אלגוריתם החתימה הדיגיטלית האסימטרית של ה Digital Certificate
- ב. את אלגוריתם החתימה הדיגיטלית הסימטרית ואת אלגוריתם ההצפנה הסימטרית
- ג. את אלגוריתם ההצפנה האסימטרית, את אלגוריתם ההצפנה הסימטרית, ואת אלגוריתם החתימה הדיגיטלית הסימטרית
- ד. את אלגוריתם ההצפנה האסימטרית, את אלגוריתם ההצפנה הסימטרית, ואת אלגוריתם החתימה הדיגיטלית האסימטרית

23. לצורך איזה מנגנון 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
- ג. Access-control
- ד. Output encoding

24. בפרוטוקול ה SSL למה משמש ה Server Write MAC Key?

- א. להצפנת המידע מה Server ל Client
- ב. להצפנת המידע מה Client ל Server
- ג. לחתימה דיגיטלית סימטרית על המידע מה Client ל Server
- ד. לחתימה דיגיטלית אסימטרית על המידע מה Client ל Server

25. איזה מבין ההתקפות הבאות מאפשרת לגנוב SessionID מהדפדפן של במשתמש?

- א. התקפת XSS
- ב. התקפת Forceful Browsing
- ג. התקפת SQL Injection
- ד. התקפת Hidden Parameter Manipulation

26. מדוע פרוטוקול ה OpenID חשוף להתקפת Phishing?

- א. הוא לא חשוף יותר מפרוטוקולים אחרים
- ב. כי בקשת ההזדהות ששולח ה RP (Relying Party) ל OP (OpenID Provider) עוברת דרך הדפדפן
- ג. כי התשובה ששולח ה OP ל RP עוברת דרך הדפדפן
- ד. כי ההפניה של המשתמש ל OP לצורך ההזדהות נעשת ע"י ה RP

27. ב HTTP Digest Authentication מי בודק את שם המשתמש והסיסמא שהזין המשתמש?

- א. ה Web application
- ב. הדפדפן Web browser
- ג. ה Web server
- ד. שכבת ה SSL

28. איזה מהטענות הבאות ביחס לקשר בין Authentication ל Authorization אינה נכונה?

4/6

- א. שני המנגנונים נחוצים על מנת לישם מדיניות של Access-control
- ב. Authentication מבוסס על Authorization
- ג. Authentication מבוסס על Authentication
- ד. Authentication הוא סוג של Authorization

29. כמה פעולות חישוב של Hash קריפטוגרפי מבוצעות בחישוב ה Response ב HTTP Digest Authentication על פי RFC 2069 כאשר הדפדפן שולח בשם אותו משתמש לשרת בקשה לאותו URI באותו אתר?

- א. אחת
- ב. שתיים
- ג. שלוש
- ד. ארבע

30. כיצד ה Firewall יודע שה Packet הוא בקשה לפתוח TCP Connection?

- א. הוא לא יודע, כי אין אינדיקציה ב TCP Header
- ב. הוא יודע על פי ה SYN ביט שדולק ב TCP Header
- ג. הוא יודע על פי ה ACK ביט שדולק ב TCP Header
- ד. הוא יודע על פי ה SYN ביט וה ACK ביט שדולקים ב TCP Header

31. למה יש צורך ב Web application במנגנון של Session management?

- א. זה לא יחודי ל Web application אלא נכון גם ל Client-server application
- ב. כי HTTP הוא Request-Response protocol
- ג. כי HTTP הוא Stateless protocol
- ד. כי ל Web server יש מגבלות במימוש פרוטוקול ה HTTP

איזה מבין ההתקפות הבאות מטרתה לשלוח לאפליקציה פקודות בשמו של המותקף?

- א. התקפת XSS
- ב. התקפת XSRF/CSRF
- ג. התקפת SQL Injection
- ד. התקפת Hidden Parameter Manipulation

33. מה היא התקפת Cookie poisoning?

- א. התקפה שבה התוקף גונב את ה SessionID שנמצא ב Cookie
- ב. התקפה שבה התוקף משנה את ערכו של ה Cookie שנשמר בדפדפן
- ג. התקפה שבה התוקף משנה ב Web server את ערכו של Cookie שנשלח לדפדפן
- ד. התקפה שבה התוקף משנה את ערכו של ה Cookie שנשמר בבסיס הנתונים בשרת

34. באיזה פרוטוקול SSL נעשה שימוש בחתימה דיגיטלית סימטרית?

- א. SSL Record Protocol
- ב. SSL Handshake Protocol
- ג. SSL Change Cipher Spec Protocol
- ד. SSL Alert Protocol

35. על מנת להגן על גבתי ה Artifact בפני תוקף שישתמש בו על מנת להתחזות למשתמש אזי:

- א. יש להצפין ב SSL את התקשורת בין הדפדפן של המשתמש ובין ה SAML Identity Provider
- ב. יש להצפין ב SSL את התקשורת בין הדפדפן של השתמש ובין ה Relying Party SAML

ג. יש להצפין ב SSL את התקשורת בין ה SAML Identity Provider ובין ה Relying SAML Party תשובות א' וב' נכונות

4/4

36. איזה מנגנון אבטחת מידע יחודי למניעת Stored and Reflected XSS?
א. Client-side Input Validation
ב. Server-Side Input Validation
ג. Access-Control
ד. Output Encoding

37. האם Firewall שמגן על אתר Web ברשת הפנימית יכול לחסום Incoming TCP Connections?
א. כן, וזה מומלץ על מנת לשפר את אבטחת המידע של האתר
ב. כן, כי ממילא בקשת ה HTTP נשלחת בפרוטוקול UDP
ג. לא מכיוון שבקשת ה HTTP נשלחת בפרוטוקול TCP ע"י דפדפן שנמצא ברשת החיצונית
ד. תשובות א' וב' נכונות

38. מה ההבדל בין Stream Cipher ל Block Cipher?
א. Stream Cipher הוא סוג של הצפנה סימטרית ו Block Cipher הוא סוג של הצפנה אסימטרית
ב. Stream Cipher מותאם להצפנה של ביטים ו Block Cipher מותאם להצפנה של בתים (Bytes)
ג. Stream Cipher מצפין כל ביט בפני עצמו ו Block Cipher מצפין בלוק של ביטים יחד
ד. Stream Cipher מותאם לשימוש במפתחות קצרים ו Block Cipher מותאם לשימוש במפתחות ארוכים

39. משה רוצה להעביר קובץ בעל רמת סודיות גבוהה לשלמה ללא שנפגשו ביניהם, מה יעשה?
א. משה יצפין את המידע במפתח הציבורי שלו ואת המפתח הציבורי שלו יצפין במפתח הציבורי של שלמה
ב. משה יגריל מפתח אקראי ובאמצעותו יצפין את הקובץ בהצפנה סימטרית ואת המפתח האקראי יצפין באמצעות המפתח הפרטי של משה ויצרף לקובץ המוצפן
ג. משה יגריל מפתח אקראי ובאמצעותו יצפין את הקובץ בהצפנה אסימטרית ואת המפתח האקראי יצפין באמצעות המפתח הציבורי של שלמה ויצרף לקובץ המוצפן
ד. משה יגריל מפתח אקראי ובאמצעותו יצפין את הקובץ בהצפנה סימטרית ואת המפתח האקראי יצפין באמצעות המפתח הפרטי של שלמה ויצרף לקובץ המוצפן

40. באמצעות מה בודק הדפדפן את החתימה הדיגיטלית שב Digital Certificate שנשלח אליו ע"י האתר אליו פנה הדפדפן?
א. באמצעות ה Public Key של האתר שאליו פנה הדפדפן
ב. באמצעות ה Public Key של הדפדפן
ג. באמצעות ה Public Key של ה Certificate Authority שהנפיק את ה Digital Certificate של האתר ונמצא ב Digital Certificate של ה Certificate Authority שהנפיק את ה Digital Certificate שנשלח אליו האתר
ד. באמצעות ה Private Key של ה Certificate Authority שהנפיק את ה Digital Certificate של האתר ונמצא ב Digital Certificate של ה Certificate Authority שהנפיק את ה Digital Certificate שנשלח אליו האתר

בהצלחה