ב״ה

תרגיל מספר 3 בקורס Web Application Security

1. מדוע Web Applications הם משמעותית פגיעים יותר (more vulnerable) מאשר Enterprise Applications שנבנו בטכנולוגית Client-Server? (מנה לפחות שלש סיבות והסבר אותם)
2. מה ההבדל העקרוני בין HTTP Basic Authentication ובין FORM Based Authentication? מתי יש צורך להצפין את ה HTTP Request Authentication?
3. הסבר את מנגנון ה Challenge-Response ? מה הסיבה לשימוש במנגנון של Challenge-Response בתהליך ה Authentication?
4. הסבר את הטכניקה המקובלת באפליקציות אינטרנט לניהול ה Session ואת אופני הישום שלה (היכן מועבר ה Session token), הסבר את היתרונות והחסרונות בכל אחד מאופני הישום. מדוע פרוטוקול ה HTTP אינו כולל session management מובנה?
5. הסבר את הטענה הבאה: ״ה session token של המשתמש מהווה למעשה את הסיסמא הזמנית של המשתמש״. מה מהמשמעות מבחינת אבטחת מידע של הטענה הנ״ל.
6. תאר שלש דרכים בהם מנסים תוקפים להשיג session token חוקי, ותאר את אמצעי ההגנה על מנת למנוע זאת (מהם אמצעי ההגנה כנגד כל אחת מההתקפות)
7. מה היא ההתקפת Cookie Poisoning? האם ההתקפה אפשרית רק על Persistent Cookie? כיצד ניתן להתגונן בפניה?
8. מדוע חשוב שהמשתמש יבצע logoff באופן מסודר? כיצד יש לסייע למשתמש על מנת שיבצע logoff מסודר? ומה נדרש לבצע בשרת/באפליקציה כאשר המשתמש בצע logoff?
9. הסבר את האופן שבו עובדת מערכת WebSSO על בסיס SAML Assertion? מה ההבדל בין אופן העבודה המתבסס על Push ובין אופן העבודה המתבסס על Pull? (השתמש בתסריט של Source first scenario)
10. תאר את תהליך ההזדהות ב OpenID? והסבר כיצד ניתן לבצע התקפת Phishing על משתמש המזדהה באמצעות OpenID?

את התרגיל יש להגיש מודפס עד לתאריך 30 למאי 2010.

בברכה

ד״ר דוד מובשוביץ