סייבר ובדיקות חוסן ליישומי אינטרנט

רומן זאיקין

תוכן עניינים

מבוא

על המחבר

רומן זאיקין הינו מומחה באבטחת מידע וסייבר מחברת צ'ק פוינט וראש תחום מסלול אבטחת המידע וסייבר ב-HackerU מזה מעל ל-5 שנים, אשר חשף ביחד עם מומחי סייבר נוספים: ערן וקנין, דקלה ברדה ועודד ואנונו פרצות אבטחה רבות אצל חברות מוכרות ומשפיעות במשק העולמי כגון: Facebook, WhatsApp, Telegram, Skype, eBay, AliExpress, LG, Microsoft ועוד...

כותב הספר "עולם אבטחת המידע וההאקינג" ובעל מעל ל-10 שנות ניסיון בתחום אבטחת מידע וסייבר.

מרצה בכנסים בין-לאומיים ובעל ניסיון הוראה רב, הכשיר מעל ל-1000 בוגרים במסלולי ההכשרה של HackerU; לינוקס, ניהול רשתות, סייבר ואבטחת מידע, אשר השתלבו בחברות גדולות ומשפיעות. קיבל למעלה מ-15 הסמכות בתחום ניהול רשתות, לינוקס ואבטחת מידע.

בספר זה יציג רומן את תחום בדיקות החוסן בעולם הסייבר וילמד כיצד לבצע בדיקת חוסן ולמצוא פרצות אבטחה ולהתגונן מפניהם ביישומי אינטרנט.

הספר, "סייבר ובדיקות חוסן ליישומי אינטרנט", הוא הראשון בסדרת הספרים – "סייבר ובדיקות חוסן".

מהי מטרת הספר?

בשנים האחרונות אנו רואים מחסור במומחי סייבר ובודקי חוסן בתעשיית הסייבר. האיומים הולכים וגדלים ובמקביל פרצות אבטחה רבות מתגלות.

מטרת סדרת הספרים "סייבר ובדיקות חוסן" היא ללמד אותך, חוקר אבטחת המידע (ההאקר) המתחיל, כיצד לבצע בדיקת חוסן ראויה וכיצד לאתר ליקויי אבטחה ופרצות במערכות שונות ומגוונות.

בספר תלמד לבצע בדיקות חוסן ליישומי אינטרנט, ותקבל את הכלים להמשיך ולהתפתח בתחום.

מהשקפתו של רומן, תחום הסייבר הוא עקומת למידה אינסופית. בפרקי זמן קצרים יחסית של שבוע אפשר למצוא עשרות מערכות חדשות, סביבות חדשות וטכניקות חדשות ולכן עליכם להשאר עם היד על הדופק ולהכניס את הלמידה לחלק מהשגרה היומית שלכם.

כדי להצליח בעולם הזה עליך להכיר את היסודות ואת התחום על בוריו ומשם לצמוח ולגדול. בהצלחה לכולם!

מהי בדיקת חוסן?

אם בעבר חברות היו מחזיקות שרתים ומחשבים רבים בבית העסק ללא כל חיבור לאינטרנט, העסקים היו פחות מקוונים ורכישת מוצרים בחנויות המקוונות הייתה פחות פופולרית, כיום התמונה שונה לחלוטין. ניתן לראות מעבר חד לשירותי הענן. יותר ויותר עסקים עוברים לשירותים המקוונים ולאפליקציות. הרכישה באינטרנט נכנסה לסדר היום.

כיום כל בית עסק שמחזיק מידע רגיש על לקוחותיו מהווה מטרה לתוקפים פוטנציאליים, ועליו להגן על המידע שנמצא בחזקתו.

האקרים ממדינות עוינות או גופי פשיעה קיברנטיים רק מחפשים מטרות קלות. וכאן אתם נכנסים לתמונה כבודקי חוסן.

בדיקת חוסן היא בעצם בדיקת נכסי הארגון על ידי מומחה אבטחת מידע, אשר מנסה לפרוץ לנכסים של הארגון באותן שיטות שבהן משתמשים ההאקרים הזדוניים.

בתום הבדיקה מספק הבודק לארגון דוח מפורט של כלל הממצאים שמצא, בתוספת רמת סיכון ולפעמים גם סבירות לניצול הממצא.

הבודק מספק בנוסף המלצות לתיקון הממצאים ואף לעתים מבצע בדיקה חוזרת לאחר שהממצאים תוקנו. בדיקה זו נקראת תיקוף ממצאים.

אם בית העסק מקפיד ברגולציית בדיקות החוסן, הסכנה הנשקפת לנכסי הארגון קטנה באופן משמעותי.

כפי שניתן לראות, מומחי אבטחת המידע, ההאקרים בעלי הכובע הלבן, חיוניים עד מאוד בתקופה זו. והצורך בהאקרים עולה בקצב אקספוננציאלי.

אילו סוגי בדיקות חוסן קיימות?

כעיקרון, בתחום שלנו הלקוח בוחר את סוג בדיקת החוסן הרלוונטית לבית העסק שלו, והיא יכולה לכלול אחת מסוגי הבדיקות הבאות:

- בדיקת חוסן לאתר החברה.
- בדיקת חוסן לתוכנה ספציפית שהחברה מפתחת.
- בדיקת חוסן לאפליקציית האנדרואיד או האייפון של החברה.
- בדיקת חוסן לרשת הארגונית של החברה וניסיון השתלטות על הרשת הארגונית.
- בדיקת חוסן הכוללת הנדסת אנוש (social engineering).
- בדיקת חוסן ספציפית על מנת לבדוק מערכת או חלק ספציפי במערכת.

בנוסף לבדיקת החוסן, הלקוח יכול לקבוע תנאים נוספים לבדיקה. תנאי הבדיקה יכולים להתחלק ל-3 סוגים:

- **White Box** – בדיקה אשר במהלכה הלקוח מוסר מידע מפורט לבודק ולעתים אף מוסר קטעי קוד. בעת הבדיקה מקבל הבודק לפעמים גם איש קשר בתוך החברה לצורך מענה על שאלות שיכולות לצוץ במהלכה. את הבדיקה מבצעים מתוך החברה או מחוץ לרשת, בהתאם לבקשת הלקוח.

- **Gray Box** – בדיקה אשר במהלכה הלקוח מוסר מידע חלקי לבודק, ובעצם בוחר אילו נתונים למסור לבודק ואילו נתונים הוא מצפה מהבודק להבין בעצמו.

- **Black Box** – בדיקה אשר במהלכה לבודק אין כל ידע קודם על המערכת, ומרבית הבדיקה נעשית מחוץ לרשת הארגונית. כלומר, הבודק מבצע את הבדיקה מתוך חברת בודקי החוסן שהוא מועסק בה ולא מתוך הארגון שאותו הוא בודק.

מתוקף תפקידי כחוקר אבטחת מידע ובודק חוסן, ביצעתי כל אחת מבדיקות החוסן המפורטות מעלה פעמים רבות עבור ארגונים שונים בארץ ובעולם.

כמו כן, מניסיוני בתחום נוכחתי לדעת שכמות בדיקות החוסן ליישומי אינטרנט רבה פי כמה וכמה מבדיקות חוסן אחרות.

לרוב, החברות המספקות שירותי בדיקות חוסן מבצעות בדיקות חוסן לאתרים, ולכן בחרתי להוציא את הספר הראשון בסדרת ספרי בדיקות החוסן דווקא בנושא זה.

סדרת הספרים "סייבר ובדיקות חוסן" תכלול את הספרים הבאים:

- סייבר ובדיקות חוסן ליישומי אינטרנט
- סייבר ובדיקות חוסן ליישומי מובייל
- סייבר ובדיקות חוסן לרשתות ארגוניות
- סייבר הנדסה לאחור וניצול חולשות

אתיקה

אנו שומעים כל הזמן בחדשות על פרצות אבטחה, החל מהתקפות דיוג והונאות ועד לגניבת מאגרי מידע וחשבונות בנק.

האקרים זדוניים יעשו הכל כדי להתעשר, ובתקופה האחרונה אנו עדים לכך שחבורות האקרים מתאגדות ומתפקדות ממש כחברה לכל דבר, שמטרתה היחידה היא להתעשר על חשבון המשתמש התמים.

אבל האם ידעתם שיש האקרים בעלי כוונות טובות עם אותה רמת כישורים? אלה ההאקרים האתיים, מומחי אבטחת המידע או ההאקרים בעלי "הכובע הלבן".

נתחיל בהגדרות, מה זה פריצה אתית?

ההאקר האתי (הידוע גם כהאקר בעל הכובע הלבן) הוא מומחה אבטחת המידע האולטימטיבי. האקרים אתיים יודעים כיצד למצוא ולנצל ליקויי אבטחה וחולשות במערכות השונות - בדיוק כמו האקר זדוני או האקר בעל "הכובע השחור".

למעשה, שניהם משתמשים באותם כישורים. עם זאת, ההאקר האתי משתמש במיומנויות אלו באופן לגיטימי כדין כדי לנסות למצוא ליקויי אבטחה ולתקן אותם לפני שההאקרים הזדוניים יצליחו להגיע למידע זה.

בספר זה אלמד אתכם להיות האקרים אתיים. אתם תלמדו לבצע מבדקי חוסן לאתרים ולהגיש דוח מסודר עם ממצאי בדיקותיכם.

אך לאילו אתרים מותר לפרוץ? באילו אתרים מותר לבצע בדיקת חוסן?

בתחום שלנו, אם לא קיבלתם אישור מפורש לבצע בדיקת חוסן על אתר כלשהו, אל תעשו זאת.

חברות המספקות את שירות בדיקות החדירה ישמחו להעסיק אתכם. לחלופין יש המון תוכניות הנקראות bug bounty המאפשרות לכם לפרוץ לאתרים ולאתר ליקויי אבטחה בזמנכם הפנוי ולקבל תשלום על כך.

Bug Bounty

תוכנית bug bounty היא יוזמה הפונה לקהילת ההאקרים שמטרתה מציאת פרצות אבטחה באתרים. לאחר מכן ניתן לקבל תגמולים עבור הגילוי והדיווח על הממצאים.

תפקידן של תוכניות bug bounty הוא להעלות את רמת אבטחת המידע של הארגון, ובכך לצמצם את הסיכוי לפרצת אבטחה על ידי ההאקרים הזדוניים.

ספקי תוכנה רבים ואתרי אינטרנט מפעילים תוכניות bug bounty, ומוכנים לשלם תגמולים לחוקרים אשר ימצאו וידווחו על פרצות אבטחה במערכות שלהם.

בדוחות שהחוקרים שולחים לחברה חובה לתעד את התהליך ולתת את כל המידע הדרוש, על מנת שמנהלי אבטחת המידע של אותה חברה יוכלו לשחזר את הבאג שנמצא.

בדרך כלל, סכומי התשלומים תלויים בכמה פקטורים, כגון: גודל הארגון, הקושי לפרוץ את המערכת ועוצמת ההשפעה על משתמשי המערכת כתוצאה מליקוי האבטחה שמצאתם.

הסכומים יכולים לנוע מ-50 דולרים ואף להגיע למיליוני דולרים.

כדי למצוא תוכניות כאלו ולבדוק כמה תקבלו על כל ליקוי אבטחה שתדווחו, אני ממליץ לכם להירשם ל-2 האתרים הבאים:

https://www.hackerone.com/

https://www.bugcrowd.com

כאשר תגיעו לרמות גבוהות יותר של אבחון פרצות אבטחה, תוכלו גם להתחיל לחפש חולשות שנקראות Zero Days.

Zero Day

כאשר מדברים על Zero Day או בשמו השני 0-day, הכוונה היא לליקוי אבטחה שיוצרי המערכת לא מכירים אלא רק החוקרים שמצאו את הליקוי הזה.

בדרך כלל, כשחוקרי אבטחה מגלים ליקוי אבטחה הם מדווחים עליו לחברה כדי שיתקנו אותו וזאת כדי שהם יוכלו לפרסם מאמר המסביר על המחקר שלהם וממצאיו.

הספירה מתחילה ביום שהחוקר מדווח לחברה. במחשבים סופרים מ-0, ולכן זהו בעצם יום 0. מכאן הגיע השם 0-Day. היום שלאחר מכן נקרא One Day שהוא מסוכן לא פחות מ-Zero Day.

יום לאחר שמתגלה חולשת Zero Day לא כל החברות מספיקות לעדכן את השירותים שלהם, וכך מנצלים ההאקרים את חולשת ה-One Day כדי לפרוץ לארגונים. משום שליקוי האבטחה כבר דווח, הפרצה נקראת One Day.

ברגע שחוקר מוצא ליקוי אבטחה קריטי ולא מדווח לחברה הוא בעצם מחזיק ב-Zero Day, וחברות רבות ישלמו סכומי עתק כדי לקנות אותו מהם, לדוגמה חברת Zerodium ואחרות:

https://zerodium.com/

יסודות לבדיקת חוסן לאתרים

טרם נתחיל לצלול אל עולם הסייבר ובדיקות החוסן לאתרים, עליכם להכיר את היסודות ואת אבני הדרך.

אני מאמין שלפני שמתחילים לפרוץ משהו, עלינו להבין איך לבנות אותו. לדעתי יהיה קשה מאוד לפרוץ אתר אם אינכם יודעים לבנות אתר.

איך תמצאו ליקוי אבטחה ובאמת תבינו מה מתרחש מאחורי הקלעים, אם אינכם יודעים לבנות צד שרת וצד לקוח?

כדי להצליח בבדיקת חוסן ולבצע אותה על הצד הטוב ביותר, עליכם להבין איך בונים את המערכת בצורה הטובה ביותר. ככל שתכירו סביבות וטכנולוגיות רבות יותר, כך יהיה לכם קל יותר להתמודד עמן.

במידה והנכם בקיאים כבר בשפת צד שרת ובשפת צד לקוח, אתם יכולים לדלג על החלק של היסודות ולעבור לחלק של הקמת סביבת הבדיקות.