ITSafe
CYBER SECURITY TRAINING

קורס בדיקות חוסן ופיתוח מאובטח

155 שעות

קורס בדיקות חוסן
ופיתוח מאובטח

בדיקת חדירה (הידועה בשם Penetration Testing או בקצרה PT) הינה תהליך מורכב המתבצע על ידי ההאקר על מנת לבדוק האם היישומים והשירותים של החברה פגיעים לליקויי אבטחה.

בדיקת חדירה הינה תהליך חשוב ביותר עבור ארגונים בארץ ובעולם ומתבצעת על ידי האקר מיומן אשר משתמש באותן השיטות בהן ישתמש ההאקר הזדוני, כדי לגלות האם הוא יכול לפגוע באפליקציות, אתרים או בתשתיות של החברה ולנצל ליקויי אבטחה על מנת לגרום לנזק. לאחר סיום הבדיקה ההאקר יספק דוח לחברה אשר יציג את כלל ליקויי האבטחה שאיתר וכמו כן פתרונות כיצד לתקן את ליקויי האבטחה האלו.

החברה יכולה לבקש מגוון רחב של בדיקות חוסן ולכן על ההאקר להיות בקיא במגוון רחב של תחומים, כגון: בדיקות חוסן ליישומי האינטרנט (האתרים והמערכות) של החברה, בדיקות חוסן לאפליקציות שמפתחת החברה הן לאנדרואיד והן לאייפון, בדיקות חוסן לתשתיות של החברה ברמה הרשתית ועוד.

עקב הידע הרב הנדרש לביצוע בדיקות חוסן והחוסר בתוכניות הכשרה מסודרות קיים מחסור רב בבודקי חוסן הן בארץ והן בעולם וכאן נכנס לתמונה קורס סייבר בדיקות חוסן ופיתוח מאובטח.

קורס בדיקות חוסן ופיתוח מאובטח הינו הקורס המקיף ביותר בתחום מבדקי החוסן המתבסס על מחקרים שביצעו מרצי הקורס תוך כדי עבודתם כבודקי חוסן / חוקרי סייבר בכירים בחברות בארץ.

במהלך הקורס המרצה יציג את הממצאים אשר מצא לאורך הקריירה שלו, ימקד את התלמיד ויפתח אצלו חשיבה יצירתית לצורך מבדקי חוסן. כך התלמיד יזכה לראות כיצד מתבצע מבדק חוסן על ידי מומחה בתחום.

ראש התחום והמרצה המוביל בקורסים הינו רומן זאיקין.

רומן זאיקין הינו מומחה באבטחת מידע וסייבר מחברת צ'ק פוינט ובעל מעל ל - 10 שנות ניסיון בתחום הסייבר. רומן חשף ביחד עם מומחי סייבר נוספים: ערן וקנין, דקלה ברדה ועודד ואנונו פרצות אבטחה רבות אצל חברות מוכרות ומשפיעות במשק העולמי כגון: WhatsApp, Facebook, Microsoft, LG, AliExpress, eBay, Skype, Telegram, ועוד.

רומן, הינו מחבר הספר "עולם אבטחת המידע וההאקינג" וסדרת הספרים "סייבר ובדיקות חוסן", מרצה בכנסים בין-לאומיים ובעל ניסיון הוראה רב והכשיר מעל ל - 1000 בוגרים במסלולי אבטחת מידע שונים.

בקורס זה תלמדו לעומק את נושא בדיקות החוסן, תפתחו אתרים ואפליקציות ותגישו דוחות מבדקי חוסן אשר ייבדקו על ידי מומחים בתחום.

קהל יעד

- מפתחים אשר רוצים לבצע הסבה מקצועית לתחום בדיקות החוסן או להעשיר את הידע שלהם בתחום.
- בודקי חוסן מתחילים שרוצים להשתפר בתחום בדיקות החוסן ולעלות מדרגה לשלב הבא.
- תלמידי מדעי המחשב/ הנדסת תוכנה מאוניברסיטאות/ מכללות שרוצים לשפר את הסיכויים שלהם לעבוד בתחום מבדקי חוסן.
- תלמידים שעברו קורסי סייבר בעבר ועדיין מרגישים שאינם מסוגלים לעבור ראיון עבודה בתחום בדיקות חוסן.
- כל מי שרוצה ללמוד לבצע בדיקת חוסן מקצועית מא' ועד ת' ובעל ניסיון מעשי בתחום טכנולוגי כגון ניהול רשת, DevOps ו - QA.

תנאי סף

קורס זה מכיל קטעי קוד רבים ותרגולים הכוללים קוד. על מנת להצליח בקורס ובמיוחד בבדיקות חוסן על התלמיד להכיר את הנושאים הבאים:

- יכולת הבנת קוד בסיסית כגון HTML ,JavaScript ,CSS.
- ניסיון תעסוקתי בתחום טכנולוגי כגון: ניהול רשת, פיתוח, DevOps, QA וכו'.
- יכולות טכניות ותשוקה לתחום אבטחת המידע וההאקינג.

משך הקורס

משך הקורס הינו 155 שעות אקדמיות המתקיימות במסגרת 31 מפגשים, פעם בשבוע בין השעות 17:40 ועד 21:30*.

חומר עזר

- מערכת סרטונים שבאה לעזור לתלמיד, אם תתקשו בנושא מסוים תוכלו לצפות בחומר של השיעור עד שתבינו אותו לעומק. את המערכת תוכלו למצוא בכתובת: platform.itsafe.co.il
- בקורס תתרגלו את כלל הנושאים על מערכת אתגרים מבוססת מחקרים אמיתיים שבוצעו על ידי המרצים של הקורס!
- בנוסף תקבלו את הספר - "סייבר ובדיקות חוסן ליישומי אינטרנט" כחומר עזר (ספר הנכתב על ידי רומן זאיקין).

בסיום הקורס

עם סיום הקורס התלמיד ידע לבצע בדיקת חוסן בצורה טובה ויסודית הכוללת כתיבת דו"ח בדיקת חוסן!

עבור תלמידים שהגישו את כל מטלות הקורס ועברו את הקורס בהצלחה עם ממוצע ציונים מעל ל - 85 תינתן עזרה בהשמה בתחום הסייבר ובדיקות החוסן.

* הלימודים אינם מתקיימים בחגים ומועדים. לוח חופשות יחולק בעת ההרשמה לקורס.

סילבוס קורס המבוא

30 שעות אקדמיות

01

HTML

- מבוא ל - HTML5
- הכרת השפה ומבנה התגים
- עבודה עם טפסים ותגים חיוניים למבדקי חוסן

02

CSS

- מבוא ל - CSS3
- עיצוב בסיסי
- עיצוב לפי tag, class, id
- עיצוב מתקדם ויכולות שימושיות למבדקי חוסן

03

JavaScript

- מבוא ל - JavaScript
- עבודה עם משתנים וסוגי משתנים
- תנאים
- לולאות
- פונקציות
- אובייקטים ותכנות מונחה עצמים
- עבודה עם Ajax
- שליטה על העמוד ועבודה עם ה - DOM
- שיטות הזרקת קוד

04

Bootstrap & JQuery

- מבוא ל - Bootstrap
- מבוא ל - jQuery
- עבודה עם Bootstrap
- עבודה עם JQuery בבדיקות חוסן

05

PHP

- מבוא ל - php7
- עבודה עם משתנים וסוגי משתנים
- תנאים
- לולאות
- פונקציות
- סרליזציה
- עבודה עם פרוטוקול ה - HTTP הכולל GET/POST/COOKIES
- ניהול זהות המשתמש SESSION
- שימוש ב - PDO וחיבור למסד הנתונים MySQL

06

MySQL

- מבוא ל - MySQL
- יצירת מסד נתונים
- יצירת טבלאות
- יצירת עמודות והגדרת הנתונים
- ביצוע פעולות על הנתונים

07

תרגול ופיתוח אתרים

- ביצוע הזרקת HTML
- ביצוע הזרקת CSS
- ביצוע הזרקת JavaScript
- פיתוח פורום בסיסי
- פיתוח בנק בסיסי
- עבודת הגשה

מודול בדיקות חוסן ליישומי אינטרנט ופיתוח מאובטח

50 שעות אקדמיות

01

מבוא וכלים

- למידת שיטת החשיבה של התוקף וחקירת מקרה - הזרקת תוכנה זדונית ל - Facebook
- הקמת סביבת מחקר ליישומי אינטרנט והכרות עם הכלים
- שימוש ב - Chrome Developer Tools רמה בסיסית
- שימוש ב - Chrome Developer Tools רמה מתקדמת
- עבודה בסיסית עם הכלי Burp Suite
- עבודה מתקדמת עם הכלי Burp Suite

02

ליקויי אבטחה מוכרים ו - OWASP TOP 10

- חקירת מקרה - הזרקת קוד לחנות ב-eBay
- 3 סוגי ה - XSS בסיסי (DOM, REFLECTED, STORED, BLINDXSS)
- CSS Injection
- XSS למתקדם והכרות עם SOP, CORS, JSONP
- CSP
- חקירת מקרה - הזרקת קוד ל - AliExpress
- Open Redirect
- CSRF ו - SSRF
- חקירת מקרה - השתלטות על חשבונות Snap Chat
- Cookies and Browser Storage
- הגנות ומעקפים
- Advance CSS injection
- חקירת מקרה - השתלטות על שואב האבק של LG וכל תשתית SmartThinQ
- Oauth2
- Using Components with known vulnerabilities
- Insecure Deserialization
- חקירת מקרה - מניפולציית הצ'ט של Facebook
- Security Misconfiguration
- מניפולציה על פרמטרים
- LFI/RFI/Path Traversal
- חקירת מקרה - השתלטות על חשבונות WhatsApp ו - Telegram
- Broken Access Control
- JWT
- Sensitive Data Exposure
- Broken Authentication
- Session Fixation
- Insufficient Anti Automation
- Injection
- Command Injection
- SQL Injection Basic
- SQL Injection Advance

03

מתודולוגיית הבדיקה וכתיבת דו"ח

- מתודולוגיית הבדיקה
- כתיבת דו"ח
- הגשת דו"ח ופרויקט

04

תחרות האקינג בין משתתפי הקורס

- תחרות האקינג וחלוקת פרסים שווים במיוחד לזוכים

"

במהלך הקורס המרצה יציג את הממצאים אשר מצא לאורך הקריירה שלו, ימקד את התלמיד ויפתח אצלו חשיבה יצירתית לצורך מבדקי חוסן.

מודול בדיקות חוסן ליישומי מובייל
(Android & iOS)

50 שעות אקדמיות

01

פיתוח אפליקציות

- **Android**
  - מבוא לפיתוח אפליקציה באנדרואיד
  - פיתוח אפליקציה בסיסית
- **iOS**
  - מבוא לפיתוח אפליקציה לאייפון
  - פיתוח אפליקציה בסיסית
- **תרגול בפיתוח אפליקציות**
  - פיתוח משחק בסיסי
  - עבודת הגשה

02

פיתוח הסביבה

- הקמת סביבת מחקר ליישומי מובייל והכרות עם הכלים
- עבודה עם adb
- עבודה עם apktool
- עבודה בסיסית עם הכלי Burp Suite בסביבת מובייל
- עבודה מתקדמת עם הכלי Burp Suite בסביבת מובייל

03

ליקויי אבטחה מוכרים ו - Mobile OWASP TOP 10

- Improper Platform Usage
  - שימוש לא נכון ב - API של מערכת ההפעלה
- Insecure Data Storage
  - סקירת Data Storages ומניפולציות
- Insecure Communication
  - תקשורת מבוססת Socketים (TCP/UDP)
  - תקשורת מבוססת HTTP/HTTPS
- Insecure Authentication
  - איתור ליקויי אבטחה בניהול הזהות של האפליקציה
- Insufficient Cryptography
- Insecure Authorization
- Untrusted Inputs
  - SQL Injections
  - Parameter Tampering
- Code Tampering
  - שכתוב אפליקציות וביצוע repackage
  - מעקף מנגנון SSL Pinning
- Reverse Engineering
  - Frida
  - Jadex and reverse engineering
- Extraneous Functionality
  - איתור פונקציונליות חבויה בקוד

04

מתודולוגיית הבדיקה וכתיבת דו"ח

- מתודולוגיית הבדיקה
- כתיבת דו"ח
- הגשת דו"ח ופרוייקט

"

בקורס זה תלמדו לעומק
את נושא בדיקות
החוסן, תפתחו אתרים
ואפליקציות ותגישו דוחות
מבדקי חוסן אשר ייבדקו
על ידי מומחים בתחום.

מודול בדיקות חוסן לתשתית ארגונית

25 שעות אקדמיות

01

תקשורת נתונים ופרוטוקולים

- התנהגות חבילות המידע ברשת LAN
- התנהגות חבילות המידע ברשת WAN
- מודל TCP/IP
- פורטים וסקוטים

02

פרוטוקולים

- פרוטוקולים בסיסיים שיש להכיר בעולם הרשתות
- היכרות עם סביבת דומיין של מייקרוסופט

03

ליקויי אבטחה והשתלטות על רשת ארגונית

- סריקת רשת ארגונית וניתוח התעבורה
- תכנון ההתקפה על הרשת הארגונית
- שימוש ב - Metasploit לצורך איתור ליקויי אבטחה וניצול ליקויי אבטחה.
- התקפת רשת ארגונית על סמך ניתוח התעבורה והתקפות מתקדמות
  - LLMNR
  - NBT-NS
  - MiTM
  - Pass the Hash
  - WPAD
- טכניקות לביצוע UAC Bypass
- טכניקות לביצוע Post Exploitation ו - Privilege Escalation

המחלקה העסקית לשירותך!

הכשרה מקצועית ומקיפה
עם המרצים המובילים בתעשייה

מיקום מרכזי בר"ג,
3 דקות מרכבת מרכז

כיתות לימוד ממוחשבות
חדישות ומרווחות

שירות בוטיק
ויחס אישי

טלפון: (054) 863-2232 www.itsafe.co.il support@itsafe.co.il
רחוב שוהם 5, מגדלי פז, קומה שלישית, מתחם הבורסה, רמת גן

ITSafe
CYBER SECURITY TRAINING