ITSAFE

POWERED BY CYSOURCE

מסלול

בודק חוסן

CYSOURCE

מסלול בודק חוסן

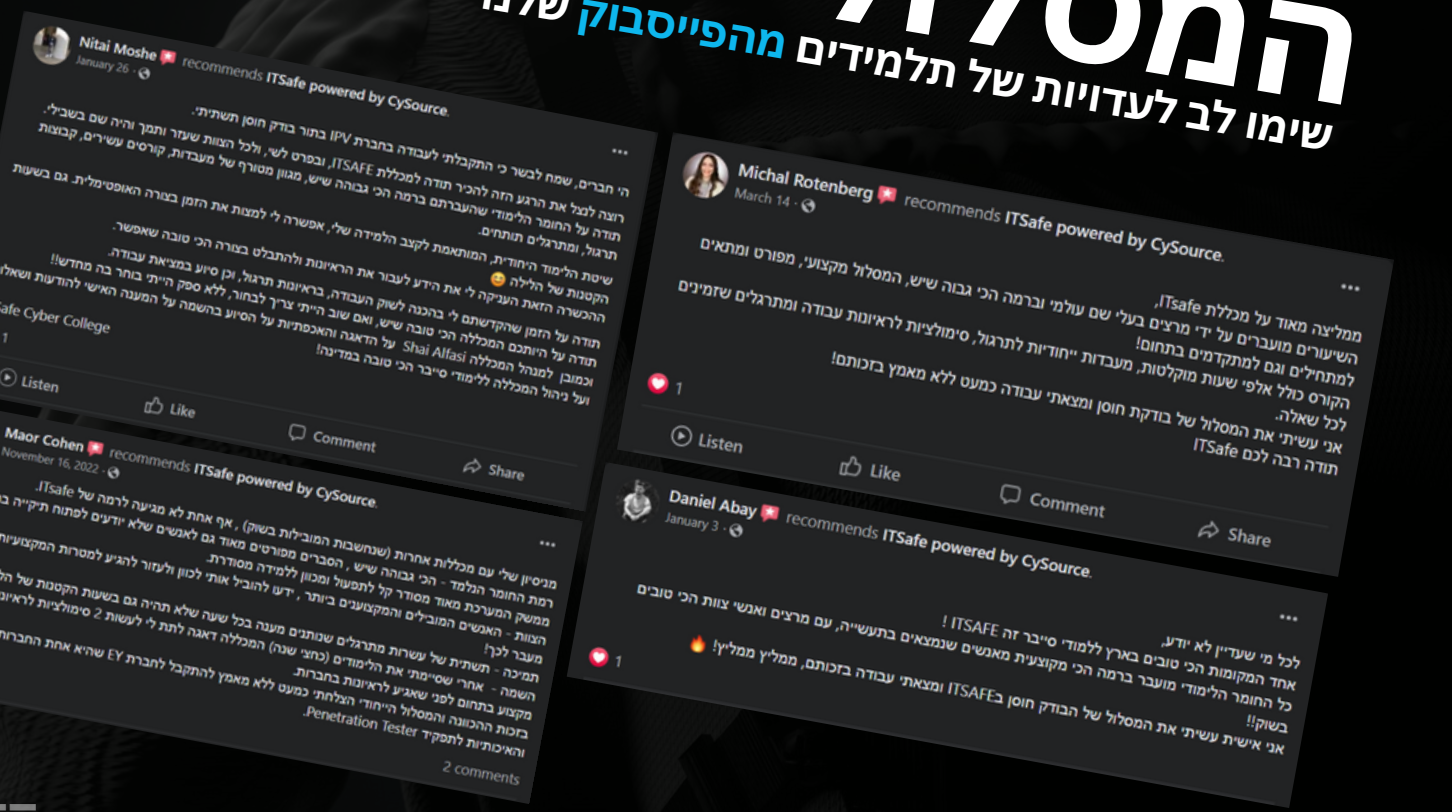
התפתחות תעשיית ההייטק העולמית והמעבר לשירותים דיגיטליים הובילו לגידול במתקפות סייבר הרסניות ברחבי העולם ואיתם גם הגידול בכוח אדם איכותי שיאייש את החזית הטכנולוגית בענף הסייבר.

בדיקות חוסן או בלועזית **Penetration Testing** או בקצרה **PT**, הינו תהליך מורכב המתבצע על מנת לאמוד את החוסן של הנכסים הדיגיטליים השונים כגון שרתים,תחנות עבודה, אפליקציות וכיו"ב. תהליך של בדיקת החוסן הינו הכרחי לכל ארגון על מנת לאתר ולחשוף חולשות ופגיעויות אשר עלולות לסכן את ההמשכיות העסקית והמידע ולגרום נזק רב, מקצוע בודק חוסן הינו מהמקצועות המבוקשים ביותר בענף הסייבר ומגלם בתוכו הזדמנויות קריירה מגוונות, תפקידו של בודק חוסן הוא להשתמש בטכניקות וכלים על מנת לחפש את אותן חולשות אבטחה על מנת לסגור אותן ולהקשיח את ההגנה של הארגון על ידי תקיפה מתואמת וידועה מראש.

אנו גאים להציג בפניכם את מסלול בודק חוסן של **ITSAFE** אשר מספק את כל הידע והניסיון הנדרש בצורה הוליסטית על מנת להכשיר למקצוע בודק חוסן.

המסלול שלנו, עובד!

שימו לב לעדויות של תלמידים מהפייסבוק שלנו



מבוא והיכרות עם תקשורת | 2 שעות תוכן | מבחן

1.היכרות והבנה בסיסית של מהי רשת

- עקרונות תקשורת בסיסיים
- חוקי תקשורת בסיסיים
- סוגי רשתות:
  - PAN
  - LAN
  - WLAN
  - CAN
  - WAN
- היכרות עם Client Server
- היכרות עם Peer2Peer
- היכרות עם פרוטוקולי תקשורת ותפקידם
  - Web Protocol
  - SMTP protocol
  - FTP protocol
- מודל שבע השכבות (OSI)
  - שכבת האפליקציה
  - שכבת הפרזנטציה
  - שכבת הסשן
  - שכבת התעבורה
  - שכבת הרשת
  - שכבת המידע
  - שכבה פיזית

2.היכרות עם ציודי תקשורת

- HUB
- Switch
- Router

3.היכרות עם מודל TCP/IP

- פרוטוקולי TCP/UDP
- היכרות עם פורטים
- היכרות עם סוקטים

ITSAFE
POWERED BY CYSOURCE

לינוקס Essentials | 7.5 שעות תוכן | 25 שעות תירגול | מבחן

1.מבוא ללינוקס

- דברי פתיחה ודגשים ללמידה
- ההיסטוריה של לינוקס
- היכרות עם הפצות לינוקס
- מבוא לוירטואליזציה
- הכנה לוירטואליזציה
- ישום וירטואליזציה עם VirtualBox
- התקנת סביבת Ubuntu Server
- עזרי למידה

2. פקודות ועבודה בסיסית

- היכרות עם Linux Shell
- פקודות ניווט
- פקודות Listing
- עבודה עם ספריות
- עבודה עם כתבנים
- אופרטורים
- פקודות חיפוש
- עבודה עם grep
- התקנת חבילות בלינוקס
- פקודות דחיסה וארכיון
- Wildcard & Globbing

3. מערכת הקבצים של לינוקס

- היכרות עם FHS
- root
- bin
- etc
- sbin
- usr
- var
- dev
- lib
- mnt
- opt
- proc
- Environment Variable
- Hard Links & Soft Links
- introduction to bash scripting

4.שירותים ולוגים

- היכרות עם Apache2
- היכרות עם Nginx
- Nginx & Apache2 Reverse Proxy
- UFW
- FTP
- SSH
- SCP
- Auth Log
- Access Log

5. תקשורת ופקודות Troubleshooting

- Network Identification
- החלפת כתובת IP זמנית
- היכרות עם DHCP
- קביעת כתובת IP סטטית
- היכרות עם DNS
- עבודה עם Netstat
- Ps & Top
- Kill
- Df & Du
- עבודה עם Tcpdump

6. הרשאות, משתמשים וקבוצות

- מבוא להרשאות, משתמשים וקבוצות
- יצירת משתמשים וסוגי משתמשים
- היכרות והבנה של קובץ passwd
- היכרות והבנה של קובץ shadow
- היכרות עם sudo
- היכרות עם קבוצות
- יצירת קבוצות
- הוספת משתמשים לקבוצות
- היכרות עם הרשאות
- Chown & Chmod
- הרשאות נומריות
- מבחן קורס

ITSAFE
POWERED BY CYSOURCE

פיתוח בפייתון | 13 שעות תוכן | 40 שעות תירגול | פרוייקט גמר

1.היכרות עם פייתון

- דברי פתיחה
- מהי שפת פייתון
- משתנים
- עבודה עם טקסט
- עבודה עם מספרים
- קלט ופלט
- עבודה עם תנאים (if,else,elif)
- עבודה עם רשימות (tuple,list,set)
- שילוב תנאים עם רשימות
- תרגילים

2. מילונים לולאות ופונקציות

- עבודה עם מבנה נתונים Dictionary
- יצירת רשימה דינמית
- לולאות (For,while)
- לולאות (Continue,Break,Pass,Else)
- לולאות ומילונים
- פונקציות בסיסיות
- פונקציות החזרת ערך
- פונקציות kwarg & argv
- תרגילים

3. ניהול שגיאות ופיתוח מקבילי

- עבודה עם קבצים
- ניהול שגיאות בסיסי
- ניהול שגיאות מתקדם
- Try,Except,Else,Finally
- מודולים
- פעולות על מערכת ההפעלה
- פיתוח מקבילי Threads
- ניהול Threads
- סנכרון בסיסי בין Threads
- עבודה עם Process
- תרגילים

4. תקשורת וקומפילציה

- תקשורת נתונים
- עבודה עם חבילות מידע
- פיתוח Socket בסיסי
- פיתוח Socket מתקדם
- פיתוח כלי סריקת רשת
- שרת-לקוח בפייתון
- תקשורת מרובת משתתפים
- תקשורת בתכנות מקבילי
- פעולות מרוחקות
- TCP Vs UDP
- קומפילציה לקובץ Exe
- תירגול

5. פיתוח מונחה עצמים

- פיתוח מונחה עצמים
- שימוש בסיסי במחלקה Class
- שימוש מתקדם במחלקה Class
- מתודות מחלקה
- ניהול מחלקות יעיל
- הורשת מחלקות
- מחלקות Vs פונקציות
- תרגילים

6. צד שרת צד לקוח

- ניתוח חבילות מידע מאתרים
- שליחת SMS באמצעות פייתון
- אוטומציות בדפדפן ו Selenium
- צד שרת בסיסי Flask
- Flask ב-Fullstack
- תקשורת ומסד נתונים ב-Flask
- פיתוח אתר ב-Flask
- תרגילים

7. פיתוח גרפי

- פיתוח תוכנה גרפית בפייתון (GUI)
- היכרות עם Tkinter
- השמשה של Tkinter
- פיתוח מבוסס HTML ופייתון
- פיתוח באמצעות Eal
- פיתוח מבוסס Material Design
- פיתוח משחק נחש את המילה
- פיתוח כלי סריקת רשת
- תרגילים

ITSAFE
POWERED BY CYSOURCE

בדיקות חוסן תשתית | 15 שעות תוכן | 110 שעות תירגול | פרוייקט גמר

1.הקמת סביבת מעבדות

- וירטואליזציה עם VirtualBox
- טעינת Kali Linux
- טעינת Windows
- טעינת Metasploitable2

2. היכרות עם עולם בדיקות החוסן

- טרמינולוגיה בעולם התקיפה
- סוגי בדיקות תשתית
- תהליכי סריקה וזיהוי פגיעויות
- השגת שליטה וחשיבותה
- אחיזות על מכונה נתקפת

3. אבני יסוד בתקיפה

- מימוש תקשורת Reverse Shell
- מימוש תקשורת Bind Shell
- האזנה בפרוטוקולי TCP/UDP
- העברת קבצים Netcat
- סריקות בסיסיות Netcat
- היכרות עם Wireshark
- פילטרים ב-Wireshark
- חילוץ מידע מקבצי PCAP

4. איסוף מידע פאסיבי ואקטיבי

- Google Dorks
- איסוף ואיתור כתובות מיילים
- איסוף מידע פאסיבי OpenSource
- DNS Enumeration
- תקשורת מול שרתי DNS
- כלי מחקר מול שרתי DNS
- DNS Forward Lookup
- DNS Reverse Lookup

5. סריקת פורטים

- לחיצת יד משולשת ותקשורת TCP
- סריקות UDP
- טעויות נפוצות בסריקות פורטים
- סריקות פורטים ע"י NMAP
- סריקות מתקדמות NMAP NSE
- עקיפות Firewalls
- זיהוי מערכות הפעלה
- Service Enumeration

6. היכרות ועבודה עם Metasploit

- היכרות עם Metasploit
- מודולים ב-Metasploit
- היכרות עם Payloads
- היכרות עם Auxiliaries
- היכרות עם Exploits
- תקיפת FTP עם חולשת RCE
- SMB Windows Brute Force
- Hydra Brute Force
- פרופילי סיסמאות
- Enumeration Tactics
- הזרקות Shellcode
- מעבר בין תהליכים
- תקיפות Wordpress & Drupal
- LFI/RFI
- Log injections
- Environ&Fuzzing
- Remote Code Execution
- Command Injections
- סוסים טרויאנים Msfvenom
- שליטה ב-Meterpreter
- Tomcat
- Backdooring
- AdvanceMeterpreter
- Keylogging
- Download/Upload Functions
- SMTP Enumeration

7. העברת קבצים

- העברת קבצים באמצעות פייתון
- העברת קבצים ב-Windows ע"י Powershell
- העברת קבצים בין Windows ל- Linux ע"י FTP
- העברת קבצים באמצעות שרת SMB
- שיטות נוספות להעברת קבצים

8. הסלמת הרשאות Windows

- UAC Bypass - User Interaction
- UAC Bypass - No User Interaction
- PE Suggester
- Patch enumeration
- Unquoted Path
- Insecure Service
- Zero Click PE

9. הסלמת הרשאות Linux

- Basic Enumerations
- Kernel Exploits
- suid Exploitation
- Sudo Abuse
- Word Writable
- CronTab PE
- Sensitive Files
- Http Methods

10. חקר חולשות

- היכרות עם x86
- היכרות והבנה של תהליכי זיכרון
- זיכרון של בינארי
- CPU Registers
- BufferOverflow Introduction
- OlyDBG Introduction
- Overflowing the buffer
- Fuzzing
- Dealing with crash
- EIP Control
- Shellcode space locating
- Bad Charactars
- Execution flow redirection
- Return Address
- Shellccoding with Metasploit
- Getting a shell

11. סיסמאות

- הזדהות Challenge Response
- גיבוב LM/NTLM
- SAM
- Password Flow
- Mimikatz
- Hash extraction SamDump
- Hash extraction SecretDump
- SecretDump Remoting
- Password cracking Hashcat/John
- Pass the hash
- Reponder & LLMNR intro
- Responder to capture NTLMv2

ITSAFE
POWERED BY CYSOURCE

הסלמת הרשאות לינוקס | 2 שעות תוכן | 20 שעות תירגול | פרוייקט גמר

1. Linux Refresher
- Users
- Files & Directories
- File Permissions
- Special Permissions
- View Permissions
- Real, Effective, Saved GUID

2. Spawning root shells
- Rootbash Suid
- Custom Executable
- MSFvenom
- Native Reverse Shell

3. Tools
- Linux Smart Enumeration
- LinEnum
- LinuxPrivChecker
- BeRoot
- UnixPrivEscCheck
- Enumerating Kernel Exploits
- Compiling & Exploitation Kernel
- SSH Port Forwarding

4. Service Exploits & Permissions
- Service Running As Root
- Enumerating Program Versions
- Mysql Manipulating & Exploiting
- etc/shadow/
- Hash Cracking
- etc/passwd/
- Mkpasswd
- Openssl
- Backups
- SSH Keys

5. Sudo
- Useful commands
- Knows Passwords
- Shell Escape
- Abusing Intended functionality
- Environment Variables
- LD Preload
- Limitations
- LD Library Path

6. Cron Jobs
- File Permissions
- etc/crontab/
- Bash Reverse shells
- Path Environment Variable
- Wild Cards
- Wild Cards & File Names
- Checkpoint's

7. SetUID/SetGID Exploit Techniques
- ?What is SUID/SGID
- Finding SUID/SGID Files
- Shell Escape Sequences
- LD Preload & LD Library Path
- Known Exploits
- Shared Object injection
- Strings, Strace, Ltrace
- Abusing Shell Features
- Debugging with PS4

8. Password Keys & NFS
- History files
- Config files
- SSH Keys
- NFS
- Useful commands
- Root Squashing
- Mounting NFS
- Manipulating NFS

ITSAFE
POWERED BY CYSOURCE

הסלמת הרשאות ווינדוס | 2 שעות תוכן | 20 שעות תירגול | פרוייקט גמר

Introduction & Lab Setup.1

- Windows10
- Kali Linux
- Groups & Members in Windows
- ACL's, Services, Registry, Directories

Must Known Tools.2

- PowerUP
- SharpUP
- SeatBelt
- winPEAS
- Accesschk
- JuicyPotato
- Procmon

Spawn a shell & Kernel .3 Exploits

- Reverse Shell Over MSFvenom
- Netcat
- Psexec to System
- Manual Kernel Enumeration
- Automatic Kernel Enumeration

Service Exploits .4

- Insecure Properties
  - Enumeration & Exploitation
- Unquoted Path
  - Enumeration & Exploitation
- Weak Registry Permissions
  - Enumeration & Exploitation
- Insecure Service executables
  - Enumeration & Exploitation
- DLL Hijacking

Registry Exploits.5

- Manual Registry Enumeration
- Automatic Registry Enumeration
- Registry Explotiation
- Query Registry Services
- Manual AIE Enumeration
- Automatic AIE Enumeration
- AIE Exploitation

Passwords.6

- Manual Password Enumeration
- Automatic Password Enumeration
- Query Registry Passwords Store
- Saved Creds man & auto Enum
- Configurations Files
- Recursive Configuration Files
- SAM & System locations
- SAM & System Hash Dump
- SAM & System Hash Crack
- PTH-Winexe

Scheduled Tasks .7

- Manual Schduled Tasks Enum
- Scheduled Tasks Exploitation

Insecure GUI Apps .8

- Insecure GUI Apps Enumeration
- Insecure GUI Apps Exploitation
- Startup Apps Enumeration
- Startup Apps Exploitation

Insecure GUI Apps .9

- Vulnerability Research Wan
- Vulnerability Research winPEAS

ITSAFE
POWERED BY CYSOURCE

מבוא לבדיקות חוסן Web | 11 שעות תוכן | 60 שעות תירגול | פרוייקט גמר

HTML.1

- Introduction to HTML
  - What is HTML ?
  - Purpose of HTML
  - HTML syntax
- HTML Elements
  - HTML tags and attributes
  - HTML structure and hierarchy
  - Block-level and inline-level elements
  - Semantic HTML
- Document Structure
  - HTML document structure
  - Head and body sections
- Text Formatting
  - Text formatting tags
  - Heading tags
  - Paragraph tags
  - Lists
- Links and Images
  - Anchor tags and href attribute
  - Image tags and src attribute
  - Image formats
- Tables
  - Table tags
  - Table structure
  - Table cells and rows
- Forms
  - Form tags
  - Input types and attributes
  - Submit buttons

CSS.2

- Introduction to CSS
  - What is CSS
  - Purpose of CSS
  - CSS syntax
  - Inline, internal, and external styles
- CSS Selectors
  - CSS selector types
  - Selector specificity
  - Selector combinations
  - Pseudo-classes and pseudo-elements
- Box Model and Layout
  - Box model
  - .Margin, border, padding
  - .Display property
  - Float and clear
  - Positioning
- Colors and Backgrounds
  - Color models
  - Color properties
  - Background properties
- Responsive Design
  - Responsive units
  - Flexbox
- CSS and HTML
  - Linking CSS and HTML
  - Styling HTML elements
  - Advanced CSS selectors

JavaScript.3

- Introduction to JavaScript
  - What is JavaScript
  - Purpose of JavaScript
  - JavaScript syntax
  - Inline, internal, and external scripts
- Variables and Data Types
  - Variables
  - Data types
  - Type coercion
- Operators and Expressions
  - Arithmetic operators
  - Comparison operators
  - Logical operators
  - Conditional statements
- Functions
  - Function definition and invocation
  - Parameters and arguments
  - Return statement
- Arrays and Objects
  - Array definition and manipulation
  - Object definition and manipulation
  - Properties and methods
  - JSON format
- Loops and Iteration
  - For loop
  - While loop
  - Do-while loop
  - Array iteration methods
- DOM Manipulation
  - Introduction to the DOM
  - DOM traversal and manipulation
  - Event handling
- AJAX and Fetch API
  - Introduction to AJAX
  - Fetch API
  - JSON data format
- Error Handling and Debugging
  - Common JavaScript errors
  - Debugging tools
- ES6 Features
  - .let and const keywords
  - Arrow functions
  - Template literals
- jQuery
  - Introduction to jQuery
  - Ajax with jQuery

SQL.4

- Introduction to SQL
  - ?What is SQL
  - Purpose of SQL
  - SQL syntax
  - SQL data types
- Creating Tables
  - Creating tables
  - Defining columns
  - Setting primary keys
  - Defining data types
- Inserting Data
  - Inserting data into tables
  - Using INSERT statement
  - Using VALUES keyword
- Reading Data
  - Reading data from tables
  - Using SELECT statement
  - Filtering data with WHERE clause
  - Sorting data with ORDER BY clause
- Updating Data
  - Updating data in tables
  - Using UPDATE statement
  - Modifying data with SET clause
  - Filtering data with WHERE clause
- Deleting Data
  - Deleting data from tables
  - Using DELETE statement
  - Filtering data with WHERE clause

ITSAFE
POWERED BY CYSOURCE

מבוא לבדיקות חוסן Web | 11 שעות תוכן | 60 שעות תירגול | פרוייקט גמר

PHP.5

- Introduction to PHP
  - What is PHP
  - Purpose of PHP
  - PHP syntax
  - Inline, internal, and external scripts
- Variables and Data Types
  - Variables
  - Data types
  - Type coercion
  - Scope
- Operators and Expressions
  - Arithmetic operators
  - Comparison operators
  - Logical operators
  - Conditional statements
- Functions
  - Function definition and invocation
  - Parameters and arguments
  - Return statement
- Arrays and Objects
  - Array definition and manipulation
  - Object definition and manipulation
  - Properties and methods
  - JSON format
- Control Structures
  - If/else statements
  - Switch statements
  - Loops (for, while, do-while)
  - Break and continue statements
- Forms and User Input
  - Handling form data
  - Retrieving user input with GET and POST
  - Sanitizing and validating user input
  - Session handling
- Cookies
  - Introduction to cookies
  - Setting and retrieving cookies
  - Deleting cookies
- Database Connectivity
  - Introduction to database connectivity
  - Connecting to databases
  - Executing SQL queries
  - Retrieving and manipulating data
  - Prepared statements
- PHP and HTML
  - Embedding PHP in HTML
  - Using PHP to generate HTML content

BASIC CRUD application.6

- Using html, CSS, js, SQL and php to:
  - Read data from DB
  - Update data into tables and columns
  - Inserting data into DB
  - Deleting data from DB

Complete web application.7

- Using html, CSS, js, SQL and php to:
  - Create Login and register mechanism
  - Creating pagination
  - Updating user profile
  - Session in PHP

ITSAFE
POWERED BY CYSOURCE

בדיקות חוסן Web | 10 שעות תוכן | 110 שעות תירגול | פרוייקט גמר

1.ניתוח קוד וזיהוי ליקויי אבטחה

- דרכי חשיבה
- חקירת מקרה: Facebook messenger
- הקמת סביבת מחקר
- בסיס Chrome Developer tools
- מתקדם Chrome Developer tools
- בסיס BurpSuite
- מתקדם BurpSuite

2.חולשות ו OWASP Top 10

- חקירת מקרה: הזרקת קוד Ebay
- Xss (Reflected,Stored,Dom)
- Css Injection
- Advanced Xss
- Sop,Cors,Jsonp
- CSP
- חקירת מקרה: הזרקת קוד AliExpress
- OpenRedirect
- SSRF&CSRF
- חקירת מקרה: השתלטות על חשבון SnapChat
- Storage Browser and Cookies
- Advanced CSS Injection
- חקירת מקרה: השתלטות על שואב LG
- SmartThinq
- Oauth2
- Components Known Vulnerabilities
- חקירת מקרה: Facebook chat
- Security Misconfigurations
- מניפולציה על פרמטרים
- LFI/RFI/Path traversal
- חקירת מקרה: ATO Whatsaap & Telegram
- Broken Access Control
- JWT
- Sensitive Data Exposure
- Broken Authentication
- Session Fixation
- Insufficient Anti Authomation
- Command injection
- SQL Injection Basic
- SQL Injection Advanced

3.מתודולוגיית בדיקה וכתיבת דו"ח

- הגשת דוחות ופרוייקטים
- כתיבת דו"ח PT
- מתודולוגיית בדיקה

ITSAFE
POWERED BY CYSOURCE

בדיקות חוסן Mobile | 9 שעות תוכן | 30 שעות תירגול | פרוייקט גמר

1.מבוא לבדיקות חוסן Mobile

- מבוא לפיתוח אפליקציות אנדרואיד
- היכרות עם מערכת ההפעלה
- היכרות עם סוגי אפליקציות
- Web App
- Hybrid App
- Native App
- הגדרת סביבת מחקר ופיתוח
- Android Studio
- Genymotion
- מבנה של אפליקציית WebApp

2.ניתוח אפליקציות Native

- מבנה אפליקציות Native
- Android Building Blocks
- Manifest File
- Activity
- Views
- Fragments
- Intent
- Content Provider
- Broadcast Receiver

3.ניתוח אפליקציות Hybrid

- התקנת Plugin ב-Cordova
- יצירת אפליקציית Cordova
- הגדרת סביבת פיתוח ב-Cordova
- מבנה Hybrid Apps
- פיתוח אפליקציה ב
  - HTML,CSS,JS
- Native Storage
- SQLite
- Local Notifications
- פרוייקט הגשה

4. ליקויי אבטחה בפיתוח

- Android App Sandbox
- תהליכים באנדרואיד
- קבצים ונתיבים Structure File
- Working With Adb
- Importer Platform Usage
- Exposed Application Interface
- LogCat
- Drozer

5.חולשות אבטחה בתקשורת ואחסון

- Insecure Data Storage
- Attacking Shared Preferences
- Attacking SQLite Database
- Attacking Data On Sdcard
- Insecure Communication
- Snigging Android Traffic
- Using BurpSuite
- HTTPS And BurpSuite
- Bypass SSL Pinning

6.חולשות במנגנוני הזדהות והרשאות

- Insecure Authentication
- Using BurpSuite Repeater
- Using BurpSuite Intruder
- Insufficient Cryptography
- Attacking Custom Encryption
- App Reverse Engineering - Jadx
- Insecure Authorization Bypass
- Insecure Pernission Bypass
- Facebook Messenger cast study
- Demo Of Mobile PT Report

7.ניתוח קוד סטטי ודינמי

- Client Code Quality
- Google Maps Case Study
- Pro Guard
- Code Temparing
- Frida Dynamic Instrumentation
- Repackaging

8. ניתוח קוד ומציאת חולשות

- App Reverse Engineering
- Dji Drone Hacking Case Study
- Root Detection
- LG Gome Hack Case Study
- Extraneous Funcionality
- Debug Enabled Apps
- Hack Apps Via Backup
- סיכום קורס

ITSAFE
POWERED BY CYSOURCE

ITSAFE
POWERED BY CYSOURCE
www.ITSAFE.co.il