

עריכה לשונית: יובל שקלים
עימוד: כרמית בן ימיני
עיצוב העטיפה: אלה רסקין
הפקה: אורלי לוי

אוריון הוצאת ספרים
www.orion-books.co.il
03-5030822
ת"ד 5330 חולון 5815202

© כל הזכויות שמורות

אין להעתיק, לשכפל, לצלם, להקליט, לתרגם, להפיץ או לאחסן ספר זה או קטעים ממנו בשום צורה שהיא (מכנית, אופטית, אלקטרונית או אחרת). שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מן המחברים וההוצאה.

נדפס בישראל 2023

עודד ואנונו • רומן זאיקין • דיקלה ברדה

סייבר והאקינג בעולם הבלוקצ'יין והקריפטו



תוכן העניינים

9	מבוא
9	על המחברים
11	למה כתבנו את הספר?
11	מהי מטרת הספר?
12	בלוקצ'יין פרספקטיבה אישית
13	תודות
15	מה זה בלוקצ'יין?
17	אז איך זה עובד?
18	אז מה זה בעצם בלוק?
19	מה זה hash?
22	ריכוזיות לעומת ביזוריות
22	מהי רשת ריכוזית?
24	יתרונות של רשת מבוזרת בעולם הבלוקצ'יין
25	אלגוריתם קונצזוס
25	שיטות עבודה באלגוריתם קונצזוס
26	הוכחת עבודה (PoW) Proof of Work
32	רמת קושי של כרייה
32	חסרונות של הוכחת עבודה
32	יתרונות של הוכחת עבודה
33	מערכת הוכחת החזקה (PoS) Proof Of Stake
34	יתרונות של הוכחת החזקה/הימור
35	חסרונות של הוכחת החזקה/הימור
36	הבדלי אבטחה בין PoW ל-PoS
36	סוגי התקפות הקיימות בשיטות העבודה PoS/PoW
37	DoS Attack
38	Sybil Attacks

40.....	Selfish Mining Attack
40.....	Bribe Attack
41.....	אז איך ההתקפה נעשית?
41.....	Proof of History – הוכחת היסטוריה
45.....	יתרונות של הוכחת היסטוריה
45.....	חסרונות של הוכחת היסטוריה
46	מטבעות קריפטוגרפים
49.....	Bitcoin
51.....	ההבדל בין coin ל-token (בין מטבע לאסימון)
53.....	Tokens types
55.....	מטבע יציב – Stablecoins
59.....	ארנקים
61.....	התקפות על ארנקים
65	L1/L2 – שכבה ראשונה ושנייה
65.....	L1 – שכבה ראשונה
66.....	L2 – שכבה שנייה
67	Defi – פיננסיות מבוזרת
68.....	אז איך זה בדיוק עובד?
71	Oracle
73	Bridges – גשרים
75.....	סוגי גשרים
76.....	התקפות על גשרים
85	Exchanges – בורסות קריפטו
85.....	בורסה ריכוזית
86.....	בורסה מבוזרת
86.....	ההבדל בין DEX ל-CEX
88	DAO – ארגון אוטונומי מבוזר
88.....	אז איך זה עובד בדיוק?
89.....	פרצת ה-DAO
93.....	ICO

94.....	STO
95.....	IEO
96	Web 3.0
97.....	Web 1.0
97.....	Web 2.0
97.....	Web 3.0
100.....	Upgrades Bitcoin
100.....	BIP 340 – Schnorr Signatures
100.....	BIP 341 Taproot
101.....	BIP 342 Tapscript
102.....	Lightning Network
103.....	Metaverse
106.....	אז איך בעצם מגיעים לעולם הדיגיטלי הזה?
107	Ethereum
109.....	EVM – מכונה וירטואלית
112	ERC-20
114	ERC-721
115	NFT's
115.....	Non Fungible Token או בקיצור NFT
116.....	OpenSea attack
121.....	Rarible attack
127	Smart contracts
129.....	סוגי חוזים
133	solidity פיתוח חוזים חכמים באמצעות
153.....	solidity משתנים וסוגי משתנים בשפת
158.....	solidity פונקציות ונראות בשפת
168.....	solidity תנאים בשפת
172.....	solidity שימוש ב-modifier בשפת
176.....	solidity עבודה עם טקסט ואזורי זיכרון בשפת

181.....	solidity	לוגים ושמירת אירועים בשפת
191.....	solidity	פעולות העברת כספים בשפת
199.....	solidity	ניהול שגיאות בשפת
203.....	solidity	לולאות בשפת
203.....	for	לולאת
208.....	while	לולאת
211.....	solidity	עבודה עם ממשקים ותקשורת חוזה לחוזה בשפת

221 dApps TOP 10

224.....	המתודולוגיה שמאחרי המודל
224.....	הגדרת הסביבה לצורך מחקר בלוקצ'יין
227.....	brownie של
228.....	ניתוח חוזה וניצול ליקויי אבטחה
244.....	איתור ליקויי אבטחה
246.....	D01 — Flash Loan Attack
277.....	D02 — Smart Contract Insecure Design
280.....	DO3 — Client-Side Code Injections
287.....	D04 — Reentrancy
298.....	D05 — Broken Access Control
314.....	D06 — Arithmetic Overflows
330.....	D07 — Randomness & Cryptographic Failures
347.....	D08 — Front-Running
354.....	D09 — Denial of Service
368.....	D10 — Information Disclosure

מבוא

על המחברים

מחברי הספר עורד ואנונו, רומן זאיקין ודיקלה ברדה הם מומחי אבטחת מידע וסייבר מחטיבת המחקר של חברת הסייבר צ'ק פוינט ולכל אחד מהם מעל ל-15 שנות ניסיון בתחום הסייבר.

השלושה מרצים בכנסי סייבר בין-לאומיים כגון RSA, Defcon, BlackHat, HiTB ועוד.

עורד ואנונו בעל ניסיון של כ-20 שנה בעולם הסייבר והינו ראש מחקר חולשות מוצרים בצ'ק פוינט. עורד מוביל צוותי מחקר חולשות אשר חשפו לאורך השנים עשרות חולשות בטכנולוגיות נפוצות. הוא מרצה באקדמיה ובכנסים ברחבי הגלובס על עולם הסייבר ההתקפי דרך עולם המחקר, מקדיש זמן לעבוד עם סטארטאפים צעירים על חדשנות טכנולוגית, ובעל 4 פטנטים בתחום הגנת הסייבר.

רומן זאיקין הוא מומחה באבטחת מידע וסייבר בחברת צ'ק פוינט, אשר חשף יחד עם דיקלה ברדה פרצות אבטחה רבות אצל חברות מוכרות ומשפיעות במשק העולמי כגון DJI, Telegram, WhatsApp, Facebook, OpenSea, Rarible, Skype, Atlassian, LG, eBay, Amazon ועוד רבות נוספות.

זאיקין כתב את הספר "עולם אבטחת המידע וההאקינג" ואת סדרת הספרים "סייבר ובדיקות חוסן", כמו כן זאיקין בעל למעלה מ-15 שנות ניסיון בתחום הסייבר.

דיקלה ברדה, מומחית אבטחת מידע בעולם ה-web והבלוקצ'יין בחברת הסייבר צ'ק פוינט, מעל 15 שנים ניסיון, במשך השנים חשפה ביחד עם רומן זאיקין פרצות אבטחה רבות אצל חברות טכנולוגיה מובילות. בשנים האחרונות חוקרת את עולם הבלוקצ'יין, בעיקר מנתחת פרצות שקורות בעולם החוזים החכמים.

ביחד עם רומן זאיקין ועודד ואנונו פירסמה פרצות אבטחה שנמצאו בפלטפורמות הבלוקצ'יין OpenSea ו-Rarible, בזמנה החופשי מפתחת כלי מחקר ומשתתפת בתוכניות Bug Bounty.

בספר זה יציגו עודד, רומן ודיקלה את תחום הבלוקצ'יין מנקודת מבטם של ההאקר, חוקר הסייבר, והטכנולוגיה העובדת מאחורי הקלעים ברשת.

בפרק הראשון נלמד מה זה בלוקצ'יין, נצלול ונבין את הטכנולוגיה והפרוטוקולים הקיימים בעולם זה.

בפרק השני נלמד מה היא שפת הקוד סולידיטי, כיצד עובדת הטכנולוגיה ברמת הביטים והבייטים. נתרגל כיצד לבנות חוזה חכם מהקוד ועד הטמעה ברשת הבלוקצ'יין.

בפרק השלישי נלמד ונתרגל לאתר ליקויי אבטחה בעולם הבלוקצ'יין ואיך האקרים ניצלו אותם בהתקפות על חוזים חכמים.

לאורך כל הספר ישנם קטעי קוד, תרגילים, אתגרים, ומעבדות אשר ילמדו וילוו אותך צעד אחר צעד.