**Glitter: מחקר אבטחה**

במסמך זה נתעד את כל תהליך הבדיקות של נק' הכניסה, גם את הבדיקות שהניבו פרי וגם את אלו שלא – פשוט הכל! בסיום המסמך יש לעדכן סיכום של כל החולשות שמצאנו.

**Ip = 54.187.16.171**

1. **חלק א' – מחקר פרוטוקול כללי**השתמשו בכלי המחקר הרגילים שלנו כדי לאסוף מאפיינים כלליים על הפרוטוקול.

|  |  |
| --- | --- |
| שם פרוטוקול | Glitter |
| מעל UDP/TCP | TCP |
| פורט | 1336 |
| מאפייני פרוטוקול | טקסטואלי |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | 550#{gli&&er}{"feed\_owner\_id":id user,"publisher\_id":id user,"publisher\_screen\_name":"Name","publisher\_avatar":"im6","background\_color":"White","date":"update dateTtime.419Z","content":"text from user","font\_color":"black","id":-1}## |
| פורמט כללי של תגובה | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":id,"publisher\_id":id,"publisher\_screen\_name":"Name ","publisher\_avatar":"im6","background\_color":"White","date":"date Ttime.419Z","content":"text","font\_color":"black","id":325}## |

1. **חלק ב' - סיכום חולשות**

יש למלא חלק זה תוך כדי מילוי של חלק ג'. אם אתם בסייקל הראשון בכיתה – **דלגו על הטבלה** ועברו לחלק ג' כעת.

|  |  |  |
| --- | --- | --- |
| **חולשות שנמצאו** | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **הצעה לפתרון** |
| אפשר לעשות יותר מלייק אחד | פירסום שקרי | Counter בקוד של התוכנה שיספור שכמות הלייקים לא תעלה על אחד |
| רואים את ה ID בהסנפות | ID בעזרת ה  יהיה ניתן להשיג פרטים אישים | שהתוכנה עצמה תצפין את הכתובות האלה |
| אפשר לראות בהסנפה אימיילים של משתמשים אחרים | גישה לפרטים אישיים | שימוש ב cookies |
| אפשר לראות התכתבויות של משתמשים אחרים | גישה לפרטים אישיים | מסנג'ר פרטי של הודעות בנפרד מעמוד הבית של המשתמש |
| יצירת משתמשים זהים לחלוטין | התחזות לאנשים | שלא תהיה אפשרות לפרטים זהים – גם סיסמאות וגם שמות משתמש ובנוסף כל כמה זמן לבקש מהמשתמש לשנות סיסמה. |
|  |  |  |
|  |  |  |

1. **חלק ג' – מחקר נק' כניסה**השתמשו בטבלה הבאה בתור תבנית – שכפלו אותה עבור כל נק' כניסה שאתם חוקרים.   
   נק' כניסה היא בקשה ספציפית בפרוטוקול.  
   זכרו לשאול את עצמכם את השאלות הבאות:  
   - איזו דרך יש לתקוף כל פרמטר בפני עצמו?  
   - איזו דרך יש שתזמון הבקשה מהווה תקיפה?

**יש לשכפל את 2 הטבלאות האלה עבור כל נק' כניסה**

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **קוד הבקשה** | **710** | | |
| **שם הבקשה בעברית** | **לייק** | | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":370,"user\_id":12376,"user\_screen\_name":"Naama biton","id":-1}## | | |
| תפקיד הבקשה | הוספת לייק | | |
| תיאור פרמטרים | **שם** | **הסבר** | |
| ***Glit\_id*** | תעודת זיהוי של מי שפרסם את הגליט | |
| user\_id | תעודת זיהוי של מי שעשה לייק | |
| user\_screen\_name | שם של מי שעשה לייק | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":370,"user\_id":12376,"user\_screen\_name":"Naama biton","id":156,"date":"2022-11-23T18:34:26.198Z"}## | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | |
| **תיאור התרחיש נתתי כמה לייקים לאותו פוסט וזה עבד** | | | **הצליח /**  **לא הצליח** |
| לתת לייק אחד | | | **הצליח** |
| לתת שני לייקים | | | **הצליח** |
| לתת שלושה לייקים | | | **לא הצליח** |
|  | | |  |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **קוד הבקשה** | **דולף מכמה מקומות למשל מ 710** | |
| **שם הבקשה בעברית** | **כל בקשה** | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":370,"user\_id":12376,"user\_screen\_name":"Naama biton","id":-1}## | |
| תפקיד הבקשה | תלוי בקשה | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***User\_id*** | הid של המשתמש |
| ***שאר הפרמטרים תלויים בבקשה.*** |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":370,"user\_id":12376,"user\_screen\_name":"Naama biton","id":156,"date":"2022-11-23T18:34:26.198Z"}## | |

|  |  |  |  |
| --- | --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | |
| **תיאור התרחיש כל תרחיש רואים אות ה ID בהסנפה.** | | | **הצליח /**  **לא הצליח** |
| לשלוח גליט | | | **הצליח** |
| לעשות לייק | | | **הצליח** |
| התכתבות | | | **הצליח** |
| חיפוש משתמש | | | **הצליח** |
| **מחקר נק' כניסה** | | | |
| **קוד הבקשה** | **300 או 320** | | |
| **שם הבקשה בעברית** | **חיפוש משתמשים** | | |
| דוגמא אמיתית | 300#{gli&&er}{"search\_type":"SIMPLE","search\_entry":"th"}## | | |
| תפקיד הבקשה | חיפוש חברים ע"מ להוסיף אותם לחברים | | |
| תיאור פרמטרים | **שם** | **הסבר** | |
| search\_entry | השם משתמש שאנחנו מחפשים | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
| איך נראית התגובה | 305#Entities search result{gli&&er}[{"screen\_name":"theMangoProphet","avatar":"im8","description":"all hail the great mango!","privacy":"Public","id":15,"mail":"itsik1231995@gmail.com"},{"screen\_name":"The Imposter","avatar":"im6","description":"a","privacy":"Public","id":22,"mail":"SUS@gmail.co"},{"screen\_name":"cj the gangsta","avatar":"im8","description":"fuck off <3","privacy":"Public","id":195,"mail":"b@gmail.com"},{"screen\_name":"Oren The king","avatar":"im1","description":"\"Motto\"","privacy":"Public","id":233,"mail":"oren1430@gmail.com"},{"screen\_name":"mark the kingggggg","avatar":"im6","description":"\"","privacy":"Public","id":333,"mail":"marktheking@gmail.com"}]## | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | |
| **תיאור התרחיש** | | | **הצליח /**  **לא הצליח** |
| search\_entry | | | **הצליח** |
|  | | |  |
|  | | |  |
|  | | |  |
| **מחקר נק' כניסה** | | | |
| **קוד הבקשה** | **500** | | |
| **שם הבקשה בעברית** | **כניסה לפרופיל של משתמש** | | |
| דוגמא אמיתית | 500#{gli&&er}{"feed\_owner\_id":12453,"end\_date":"2022-11-27T18:25:52.947Z","glit\_count":2}## | | |
| תפקיד הבקשה | להיכנס לפרופיל של משתמש | | |
| תיאור פרמטרים | **שם** | **הסבר** | |
| feed\_owner\_id | ה ID של המשתמש שאליו נכנסו בפרופיל | |
| end\_date | תאריך כניסה אחרון | |
| glit\_count | מספר הגליטים שנמצאים בעמוד של המשתמש | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
| איך נראית התגובה | 505#Feed loading approved{gli&&er}{"glits":[{"feed\_owner\_id":12453,"publisher\_id":12437,"publisher\_screen\_name":"thequeen","publisher\_avatar":"im1","background\_color":"White","date":"2022-11-23T15:51:09.000Z","content":"hiiii","font\_color":"black","id":390}],"commentsMap":{"gestureMap":{"390":[]}},"likesMap":{"gestureMap":{"390":[]}},"wowsMap":{"gestureMap":{"390":[]}}}## | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | |
| **תיאור התרחיש כניסה לעמוד של המשתמש** | | | **הצליח /**  **לא הצליח** |
| לראות שיחות עם משתמשים אחרים עמוד המשתמש | | | **הצליח** |
|  | | |  |
|  | | |  |
|  | | |  |
| **מחקר נק' כניסה** | | | |
| **קוד הבקשה** | **150** | | |
| **שם הבקשה בעברית** | **פתיחת משתמש חדש** | | |
| דוגמא אמיתית | 150#{gli&&er}{"registration\_code":"n2346","user":{"screen\_name":"nnaanananna","avatar":"im1","description":"nanana"," privacy":"Public ","id":-1,"user\_name":"nannananana","password":"123456","gender":"Undefined","mail":"nanananana@gmail.com"}}## | | |
| תפקיד הבקשה | פתיחת משתמש זהה למשתמש קיים - התחזות | | |
| /תיאור פרמטרים | **שם** | **הסבר** | |
| registration\_code | קוד הרשמה | |
| screen\_name***.*** | השם שיופיע בפרופיל המשתמש | |
| description | תיאור המשתמש | |
| privacy":"Public | משתמש פרטי/ ציבורי | |
| id | ה id של המשתמש | |
| user\_name | שם המשתמש | |
| password" | סיסמת המשתמש | |
| mail | אימייל המשתמש | |
| איך נראית התגובה | 155#User registration approved{gli&&er}{"screen\_name":"nnaanananna","avatar":"im1","description":"nanana","privacy":"Public","id":12569,"user\_name":"nannananana","password":"123456","gender":"Undefined","mail":"nanananana@gmail.com"}## | | |

|  |  |
| --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | |
| **תיאור התרחיש התחזות למשתמש אחר** | **הצליח /**  **לא הצליח** |
| לחקות את השם שבפרופיל | **הצליח** |
| לחקות את הסיסמה | **הצליח** |
| לחקות את ה ID | **הצליח** |
| לחקות גם תמונהדדד | **הצליח** |