**Glitter: מחקר אבטחה**

במסמך זה נתעד את כל תהליך הבדיקות של שלב א', גם את הבדיקות שהניבו פרי וגם את אלו שלא – פשוט הכל! בסיום המסמך יש סיכום של כל החולשות שנמצאו ומוגשות. יחד עם המסמך יש להגיש את קבצי ה-py של הוכחות ההיתכנות.

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

| שם פרוטוקול | Glitter |
| --- | --- |
| מעל UDP/TCP | Tcp |
| פורט | 1336 (P.S: Nice Reference to 1337 ;) “Leet” ) |
| מאפייני פרוטוקול | Statefull and Textual |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | ProtocolNum#{gli&&er}{"condition1":"conditiontoit1","condition2":"conditiontoit2","condition3":"conditiontoit3"}## |
| פורמט כללי של תגובה | ProtocolNum#Smth Happened {gli&&er}{"condition1":"conditiontoit1","condition2":"conditiontoit2","condition3":"conditiontoit3"}## |

**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** | **קוד POC נכתב?** | **הצעה לפתרון** |
| User Can Find The Password of other person by looking up in password recheck message. | Hacker can Enter Other People account easily. | **yes** | Need another Indetification Approval to recheck the accounts password. |
| User Can Post Glits From Other Users Accounts Without Entering Them | **Hacker Can Make Some Disinformation by sending info from other account without them knowing.** | **yes** | Need another Indetification Approval to send the glit from account. |
| User can Know all the info for the account by only knowing its id. | **Hacker can Find the Email and other info of user without their knowing.** | **yes** | **Do info crypting and saving it in the backend side of the application.** |
| **I Can Find User id only by his Username** | **Hacker can Find the users id and by that do the third attack ive entered.** | **yes** | **Do info crypting and saving it in the backend side of the application.** |

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 שעצם הבקשה תהיה תקיפה?

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

| **מחקר נק' כניסה** | | |
| --- | --- | --- |
| **מספר הבקשה** | **100** | |
| **שם הבקשה בעברית** | **לוגין** | |
| דוגמא אמיתית | 100#{gli&&er}{"user\_name":"Pablik","password":"12345678","enable\_push\_notifications":true}## | |
| תפקיד הבקשה | To Make A Login Into An Account | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***user\_name*** | Username That you need to enter |
| ***password*** | Correct Password you need to enter to enter an account |
| ***Enable\_push\_***  ***notifications*** | An Option If I Want To Enable The push Notifications or not |
| איך נראית התגובה | 105#Login received. Please complete ascii checksum.{gli&&er}## | |

| **מחקר נק' כניסה** | | |
| --- | --- | --- |

| **מספר הבקשה** | **115** | |
| --- | --- | --- |
| **שם הבקשה בעברית** | **אישור של צקסאם** | |
| דוגמא אמיתית | 110#{gli&&er}1015## | |
| תפקיד הבקשה | To Send The Checksum That Was Asked | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***Number*** | Specific Number That Was Received After The Checksum Was Proceed. |
| איך נראית התגובה | 115#Authentication approved{gli&&er}{"screen\_name":"Pavel","avatar":"im1","description":"a","privacy":"Public","id":53076,"user\_name":"Pablik","password":"12345678","gender":"Male","mail":"pashazhernoklev@gmail.com","date":"2025-06-14T20:47:43.545Z"}## | |

| **מחקר נק' כניסה** | | |
| --- | --- | --- |
| **מספר הבקשה** | **310** | |
| **שם הבקשה בעברית** | **גילוי של ID של משתמש** | |
| דוגמא אמיתית | 310#{gli&&er}53076## | |
| תפקיד הבקשה | To Get the Id Of the Asked User | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***Number*** | Id Of The User |
| איך נראית התגובה | 315#Entity fetched succesfully{gli&&er}{"screen\_name":"Pavel","avatar":"im1","description":"a","privacy":"Public","id":53076}## | |

| **מחקר נק' כניסה** | | |
| --- | --- | --- |
| **מספר הבקשה** | **500** | |
| **שם הבקשה בעברית** | **התענה של פייד של משתמש** | |
| דוגמא אמיתית | 500#{gli&&er}{"feed\_owner\_id":53076,"end\_date":"2025-06-14T20:47:44.114Z","glit\_count":2}## | |
| תפקיד הבקשה | Loading Of The Feed of the chosen user | |
| תיאור פרמטרים | **שם** | **הסבר** |
| feed\_owner\_id | The Id Of Chosen User To open the exact profile we need |
| end\_date | To Show the date of the last activity was on the account? (not sure about this) |
| glit\_count | To show the amount of glits on the account |
| איך נראית התגובה | 505#Feed loading approved{gli&&er}{"glits":[{"feed\_owner\_id":53076,"publisher\_id":53076,"publisher\_screen\_name":"Pavel","publisher\_avatar":"im1","background\_color":"Violet","date":"2025-06-14T17:44:53.000Z","content":"purple","font\_color":"black","id":92784},{"feed\_owner\_id":53076,"publisher\_id":53076,"publisher\_screen\_name":"Pavel","publisher\_avatar":"im1","background\_color":"White","date":"2025-06-14T17:44:48.000Z","content":"ive entered smth to server","font\_color":"black","id":92783}],"commentsMap":{"gestureMap":{"92783":[],"92784":[]}},"likesMap":{"gestureMap":{"92783":[],"92784":[]}},"wowsMap":{"gestureMap":{"92783":[],"92784":[]}}}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| I Possibly can send Password Recheck Request to the Server And by that entering other account | **Spoofing** | **Possible** |
| Change The Parameters For The User Login To Wrong Ones | **Tampering** | **Impossible** |
| **I Can Find User id only by his Username** | **Info Disclosure** | **Possible** |
| I can send no info to the server | Tampering | **Impossible** |
|  | Choose an item. |  |
|  | Choose an item. |  |

\

\\

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
|  |  |  |
| Send checksum of other person while entering an account | **spoofing** | **impossible** |
|  |  |  |
|  |  |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| I Can Fetch user details by user ID. IDe | **Info Disclosure** | **Possible** |
|  |  |  |
|  |  |  |
|  |  |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| Send glit from other person without him knowing | **spoofing** | **possible** |
|  |  |  |
|  |  |  |
|  |  |  |
|  | Choose an item. |  |
|  | Choose an item. |  |