**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 |
| מאפייני פרוטוקול | פרוטוקול טקסטואלי, סטייטפול |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | [Message ID]#{gli&&er}[Values]## |
| פורמט כללי של תגובה | [Message ID]#Info{gli&&er}[Values]## |

**קראו למדריכ/ה לפני שאתם ממשיכים לשלב הבא!**

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** | **קוד POC נכתב?** | **הצעה לפתרון** |
| משתמש יכול לעשות לייק לפוסט שעשה לו כבר לייק ובכך להוסיף כמות לייקים כרצונו | להוסיף כמות לייקים בלתי מוגבלת ובכך להפוך ל "מפורסם", או שאולי הוא יכול למכור לייקים לאנשים תמורת תשלום | **כן** | הוספת מנגון שיוודא אם המשתמש כבר עשה לייק לפוסט |
| אפשרות להשיג user id של משתמש | ה user id של משתמש כלשהו עלול להיות מידע רגיש, מכוון שבעזרתו התוכנה יודעת עם איזה משתמש היא מדברת, אז השגתו עלולה להוביל לפריצות יותר רציניות שדורשות התחזות | **כן** | כאשר שולחים בקשות שיש בהן user id, אפשר להצפין אותו במקום להשאיר אותו חשוף. |
| אפשרות להשיג מייל של משתמש | השגת מייל של משתמש היא דבר רגיש ובכך התוקף יכול למצוא עליו דברים | **כן** | פשוט לא לשלוח את המייל בתוך הבקשה, אין לזה שימוש. |
| אפשרות להשיג סיסמה של משתמש לפי ניסיון התחברות כושל | לגלות את הסיסמה של אותו חשבון ובכך להשתמש במשתמש שלו ללא אישור | **כן** | שמתי שמתחברים, יהיה מנגון שמוודא שהסיסמה באמת תואמת ולא רק ה checksum |
| **אפשרות להתחבר לחשבון רק עם שם משתמש (אתגר)**  *דיי חופף אני יודע, אבל בכל זאת הפרדתי כי אחד זה כביכול חולשה ואחד זה אתגר* | **להתחבר לחשבון לא שלו ללא רשות** | **כן** | **שמתי שמתחברים, יהיה מנגון שמוודא שהסיסמה באמת תואמת ולא רק ה checksum** |
| אפשרות לעלות פוסטים בצבעים מיוחדים | תוקף יכול לעלות פוסטים "נדירים" וגם למכור את האפשרות לעלות אותם לאנשים אחרים בתשלום | **כן** | לוודא שהצבע שמעלים איתו פוסט באמת קיים באפשרויות הניתנות למשתמש |
| משתמש יכול לאשר בקשת חברות שנועדה למשתמש אחר | תוקף יכול לאשר בקשת חברות אשר נשלחה לעמוד פרטי, ובכך לראות את תוכן העמוד שלו בלי רשותו. | **כן** | לוודא שבקשת האישור חברות מתבצעת על ידי המשתמש שאליו נועדה הבקשה. |
| משתמש יכול להגיב על פוסט של משתמש פרטי | תוקף יכול להטריד / להציק למשתמשים פרטיים, ולגרום לבהלה כאשר אנשים לא מבינים איך למשתמש שהם לא מכירים יש "גישה" לעמוד שלהם. | **כן** | לוודא שהמשתמש שמגיב על פוסט מורשה לעשות זאת |
| קיימת האפשרות שמשתמש יעדכן את שמו לשם ארוך יותר מהמגבלה המותרת. | תוקף יכול לפגוע בחווית המשתמש בכך שהשם שלו כל כך ארוך שזה הורס את ה ui (יש סיבה שיש מגבלה), שם מאוד ארוך יכול לבזבז משאבים מהשרת, ובנוסף לכך בשילוב עם הפרצה שאפשר למצוא סיסמה של משתמש ולהכנס לחשבון שלו, תוקף יכול לעשות זאת לחשבון מסויים ולשנות את השם שלו לשם ארוך מהמגבלה, ובכך לאיש המקורי לא תהיה גישה אליו (שמתחברים למשתמש יש גם מגבלת אורך) | **כן** | לוודא את אורך השם לא רק באפליקציה אלא גם אצל השרת. |
| קיימת האפשרות ליצור משתמש עם שם ארוך מהמגבלה המותרת. | כמו מקודם, תוקף יכול לפגוע בחווית המשתמש בכך שהשם שלו כל כך ארוך שזה הורס את ה ui (יש סיבה שיש מגבלה), ושם מאוד ארוך יכול לבזבז משאבים מהשרת. | **כן** | לוודא את אורך השם לא רק באפליקציה אלא גם אצל השרת. |
| קיימת האפשרות לגשת לתוך הקיר של עמוד פרטי ולראות את הפוסטים / תגובות שלו. | תוקף יכול לצפות בפוסטים של עמוד פרטי בלי רשותו, מה שפוגע בפרטיות שלו. | **כן** | לוודא שהמשתמש שמנסה לגשת לאותו עמוד מורשה לעשות זו. |
| **קיימת האפשרות להשיג סיסמא של משתמש לפי השחזור סיסמא (אתגר)** | **תוקף יכול לגנוב את הסיסמא האישית של הבן אדם ובכך להכנס לחשבון שלו בלי אישור** | **כן** | **להשקיע קצת יותר בקוד איפוס, שלא יהיה לו דפוס מוגדר מראש או תבנית מסויימת שאפשר לפצח אותה.** |
| **קיימת האפשרות להשגת cookieשל משתמש. (אתגר)** | **תוקף יכול לגנוב את ה cookie ובכך להתחזות לבן אדם.** | **כן** | **לא להעביר את ה cookie בתשובה של השרת, אין בזה שום טעם ושימוש וזה סתם חסר היגיון.** |
| **קיימת האפשרות לראות את היסטוריית החיפוש של משתמש מסויים (אתגר)** | **תוקף יכול לפגוע בפרטיות של הבן אדם, ובמקרים מסויימים אולי אפילו לאיים על אותו משתמש שהוא יפיץ את זה.** | **כן** | **לוודא שמי ששולח את הבקשה של הטעינת היסטורייה באמת תואם את ה id שנשלח כפרמטר.** |
| **אפשרות להעלאת פוסט עם קישור זדוני שגורם למשתמש הלוחץ עליו לעלות פוסט בניגוד לרצוניו. (אתגר)** | **תוקף יכול לנצל את זה ולגרום לבן אדם הלוחץ על הקישור להלחץ ולחשוב שפרצו לו לחשבון.** | **כן** | **אפשר לעשות מאגר של קישורים מסויימים שאסור להכניס לפוסט, ולוודא שהפוסט "נקי".** |

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 - בקשת הלייק** | | |
| --- | --- | --- |
| **מספר הבקשה** | **710** | |
| **שם הבקשה בעברית** | **לייק לפוסט** | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":86616,"user\_id":51648,"user\_screen\_name":"guy molnar","id":-1}## | |
| תפקיד הבקשה | הוספת לייק לפוסט | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***glit\_id*** | מספר מזהה של פוסט |
| ***user\_id*** | מספר מזהה של החשבון שנותן את הלייק |
| ***user\_screen\_name*** | השם של המשתמש הנותן את הלייק |
| ***id*** | מזהה לייק |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":86616,"user\_id":51648,"user\_screen\_name":"guy molnar","id":1085836,"date":"2025-06-10T11:34:42.355Z"}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| הכנסת glit\_id לא קיים | Tampering | **לא הצליח** |
| העברת פרמטרים נוספים ולא רצויים | Tampering | **לא הצליח** |
| שליחת הבקשה שוב גם אם כבר המשתמש עשה לייק על הפוסט | Tampering | **הצליח** |
| הכנסת user id של משתמש אחר | Spoofing | **לא הצליח** |
| הכנסת user\_screen\_name לא תואם ל user id | Spoofing | **לא הצליח** |
| ביצוע הפעולה לפני התחברות | Other | **לא הצליח** |

| **מחקר נק' כניסה - חיפוש משתמש** | | |
| --- | --- | --- |
| **מספר הבקשה** | **300** | |
| **שם הבקשה בעברית** | **חיפוש משתמש** | |
| דוגמא אמיתית | 300#{gli&&er}{"search\_type":"SIMPLE","search\_entry":"guymolnar"}## | |
| תפקיד הבקשה | חיפוש משתמש בתיבת החיפוש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***search\_type*** | סוג החיפוש |
| ***search\_entry*** | התוכן שהוכנס לתוך תיבת החיפוש |
| איך נראית התגובה | 305#Entities search result{gli&&er}[{"screen\_name":"guymolnar","avatar":"im8","description":"ds","privacy":"Public","id":52002,"mail":"guymolnar2000@gmail.com"}]## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| שינוי סוג הבקשה | Tampering | **לא הצליח** |
| העברת פרמטרים נוספים ולא רצויים | Tampering | **לא הצליח** |
| הכנסת שם של משתמש אחר וקבלת ה id שלו | Information Disclosure | **הצליח** |
| הכנסת שם משתמש לא קיים | Tampering | **לא הצליח** |
| הכנסתת שם של משתמש אחר וקבלת האימייל שלו | Information Disclosure | **הצליח** |
| ביצוע הפעולה לפני התחברות | Other | **לא הצליח** |

| **מחקר נק' כניסה - התחברות משתמש** | | |
| --- | --- | --- |
| **מספר הבקשה** | **100, 110** | |
| **שם הבקשה בעברית** | **התחברות לתוך משתמש, ואישור ההתחברות באמצעות checksum** | |
| דוגמא אמיתית | 100#{gli&&er}{"user\_name":"guymo","password":"123","enable\_push\_notifications":true}##  110#{gli&&er}711## | |
| תפקיד הבקשה | חיבור לתוך משתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***user\_name*** | שם המשתמש |
| ***password*** | סיסמה |
|  | ***enable\_push\_notifications*** | הפעלת התראות או לא |
| איך נראית התגובה | 105#Login received. Please complete ascii checksum.{gli&&er}##  או במצב שההתחברות שגויה:  108#Illegal user login. Provided details do not match ascii checksum: 711{gli&&er}{"type":"User Notification","header":"Login Failure","description":"Password doesn't match","userRecommendation":"Verify the provided password"}##  115#Authentication approved{gli&&er}{"screen\_name":"guy molnar","avatar":"im1","description":"ds","privacy":"Public","id":51648,"user\_name":"guymo","password":"123","gender":"Male","mail":"guy@gmail.com","date":"2025-06-11T18:16:32.977Z"}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| העברת פרמטרים נוספים ולא רצויים | Tampering | **לא הצליח** |
| הכנסת סיסמה כך שסכום האסקי שלה ושל השם משתמש שווה לסכום הדרוש להכנס ובכך למצוא פרטים אישיים על המשתמש | Information Disclosure, Spoofing | **הצליח** |
| **הכנסת סיסמה כך שסכום האסקי שלה ושל השם משתמש שווה לסכום הדרוש להכנס תגרום להתחברות למשתמש (אתגר)** | Spoofing | **הצליח** |
| הכנסת שם משתמש לא קיים | Tampering | **לא הצליח** |
| ביצוע הפעולה אחרי שמתחברים כבר | Other | **לא הצליח** |

| **מחקר נק' כניסה - שליחת פוסט** | | |
| --- | --- | --- |
| **מספר הבקשה** | **550** | |
| **שם הבקשה בעברית** | **שליחת פוסט** | |
| דוגמא אמיתית | 550#{gli&&er}{"feed\_owner\_id":51648,"publisher\_id":51648,"publisher\_screen\_name":"guy molnar","publisher\_avatar":"im1","background\_color":"Violet","date":"2025-06-14T11:21:03.607Z","content":"pink","font\_color":"black","id":-1}## | |
| תפקיד הבקשה | העלאת פוסט | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***feed\_owner\_id*** | מזהה ה "קיר" בו מעלים את הפוסט |
| ***publisher\_id*** | מזהה המשתמש שמעלה את הפוסט |
| ***user\_screen\_name*** | השם המוצג של מי שמעלה את הפוסט |
| ***pblisher\_avatar*** | האוואטר / תמונה של מי שמעלה את הפוסט |
|  | ***background\_color*** | הצבע של הפוסט (הרקע) |
|  | ***date*** | תאריך הפצת הפוסט |
|  | ***content*** | תוכן הפוסט |
|  | ***font\_color*** | צבע הטקסט |
|  | ***id*** | מזהה פוסט |
| איך נראית התגובה | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":51648,"publisher\_id":51648,"publisher\_screen\_name":"guy molnar","publisher\_avatar":"im1","background\_color":"Violet","date":"2025-06-14T11:21:03.607Z","content":"pink","font\_color":"black","id":90542}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| הכנסת תאריך מהעתיד | Tampering | **לא הצליח** |
| הנכסת publisher\_screen\_name מזוייף | Spoofing | **לא הצליח** |
| הכנסת publisher\_avatar לא תואם למשתמש | Spoofing | **לא הצליח** |
| הכנסת font\_color שונה כרצוננו | Tampering | **הצליח** |
| הכנסת backgrounnd\_color שלא באפשרויות המוצגות למשתמש | Tampering | **הצליח** |
| ביצוע הפעולה לפני התחברות | Other | **לא הצליח** |

| **מחקר נק' כניסה - אישור בקשת חברות** | | |
| --- | --- | --- |

| **מספר הבקשה** | **420** | |
| --- | --- | --- |
| **שם הבקשה בעברית** | **אישור בקשת חברות** | |
| דוגמא אמיתית | 420#{gli&&er}[51648,52859]## | |
| תפקיד הבקשה | אישור בקשת חברות | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***אינדקס ראשון*** | מזהה המשתמש ששלח את בקשת החברות |
| ***אינדקס שני*** | מזהה המשתמש שאליו נשלחה הבקשה |

| איך נראית התגובה | 425#Glance response is valid. A notification was sent to the user{gli&&er}51648## | |
| --- | --- | --- |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לאשר בקשת חברות מצד המבקש כאשר המשתמש אליו נועדה הבקשה לא אישר אותה עדיין | Tampering | **הצליח** |

| **מחקר נק' כניסה - תגובה על גליט** | | |
| --- | --- | --- |
| **מספר הבקשה** | **650** | |
| **שם הבקשה בעברית** | **תגובה על פוסט** | |
| דוגמא אמיתית | 650#{gli&&er}{"glit\_id":91909,"user\_id":51648,"user\_screen\_name":"guymolnar","id":-1,"content":"dsa","date":"2025-06-17T14:33:31.208Z"}## | |
| תפקיד הבקשה | שליחת תגובה על פוסט | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***glit\_id*** | מזהה פוסט / גליט |
| ***user id*** | מזהה המשתמש המפרסם את התגובה |
|  | ***user\_screen\_name*** | השם של המשתמש שמפרסם את התגובה |
|  | ***id*** | מזהה תגובה |
|  | ***content*** | תוכן התגובה |
|  | ***date*** | תאריך פרסום התגובה |
| איך נראית התגובה | 655#Comment publish approved{gli&&er}{"glit\_id":95331,"user\_id":51648,"user\_screen\_name":"guy molnar","id":30641,"date":"2025-06-18T12:21:31.967Z","content":"wah"}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לפרסם תגובה על גליט של משתמש פרטי | Tampering | **הצליח** |
| לפרסם תגובה בשם אנונימי / שונה | Spoofing | **לא הצליח** |
| לשנות את ה User id למישהו אחר | Spoofing | **לא הצליח** |
| ביצוע הפעולה לפני התחברות | Other | **לא הצליח** |

| **מחקר נק' כניסה - עדכון פרטי משתמש** | | |
| --- | --- | --- |
| **מספר הבקשה** | **350** | |
| **שם הבקשה בעברית** | **עדכון פרטי משתמש** | |
| דוגמא אמיתית | 350#{gli&&er}{"screen\_name":"guymor","avatar":"im1","description":"ds","privacy":"Public","id":51648,"user\_name":"guymo","password":"123","gender":"Male","mail":"guy@gmail.com"}## | |
| תפקיד הבקשה | לעדכן את הפרטים של משתמש מסויים | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***screen\_name*** | השם של המשתמש |
| ***avatar*** | התמונה / אווטאר של המשתמש |
|  | ***description*** | התיאור של המשתמש |
|  | ***privacy*** | פרטיות המשתמש (ציבורי או פרטי) |
|  | ***id*** | מזהה המשתמש |
|  | ***user\_name*** | שם המשתמש של המשתמש |
|  | ***password*** | סיסמת המשתמש |
|  | ***gender*** | מין המשתמש |
|  | ***mail*** | האימייל של המשתמש |
| איך נראית התגובה | 355#User setting update approved{gli&&er}{"screen\_name":"guymor","avatar":"im1","description":"ds","privacy":"Public","id":51648,"user\_name":"guymo","password":"123","gender":"Male","mail":"guy@gmail.com","date":"2025-06-20T12:10:05.726Z"}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לשנות סיסמה | Tampering | **לא הצליח** |
| למחוק פרמטרים | Tampering | **לא הצליח** |
| לשנות user id | Tampering | **לא הצליח** |
| שינוי השם לשם ארוך יותר מהמגבלה | Tampering | **הצליח** |

| **מחקר נק' כניסה - יצירת משתמש** | | |
| --- | --- | --- |
| **מספר הבקשה** | **150** | |
| **שם הבקשה בעברית** | **יצירת משתמש חדש** | |
| דוגמא אמיתית | 150#{gli&&er}{"registration\_code":"12345","user":{"screen\_name":"HelloPaulHowAreYou?","avatar":"im1","description":"ds","privacy":"Public","id":-1,"user\_name":"HelloPaulHowAreYou?","password":"123","gender":"Male","mail":"2@d.gfd"}}## | |
| תפקיד הבקשה | יצירת משתמש חדש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***registration\_code*** | קוד התחברות משתמש |
| ***screen\_name*** | השם של המשתמש |
| ***avatar*** | התמונה / אווטאר של המשתמש |
|  | ***description*** | התיאור של המשתמש |
|  | ***privacy*** | פרטיות המשתמש (ציבורי או פרטי) |
|  | ***id*** | מזהה המשתמש |
|  | ***user\_name*** | שם המשתמש של המשתמש |
|  | ***password*** | סיסמת המשתמש |
|  | ***gender*** | מין המשתמש |
|  | ***mail*** | האימייל של המשתמש |
| איך נראית התגובה | 155#User registration approved{gli&&er}{"screen\_name":"HelloPaulHowAreYou?","avatar":"im1","description":"ds","privacy":"Public","id":55154,"user\_name":"HelloPaulHowAreYou?","password":"123","gender":"Male","mail":"2@d.gfd"}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לשים סיסמה ריקה | Tampering | **לא הצליח** |
| למחוק פרמטרים | Tampering | **לא הצליח** |
| לשים user id קיים | Tampering | **לא הצליח** |
| שינוי השם לשם ארוך יותר מהמגבלה | Tampering | **הצליח** |

| **מחקר נק' כניסה - כניסה לעמוד** | | |
| --- | --- | --- |
| **מספר הבקשה** | **500** | |
| **שם הבקשה בעברית** | **טעינת קיר משתמש** | |
| דוגמא אמיתית | 500#{gli&&er}{"feed\_owner\_id":52377,"end\_date":"2025-06-20T13:25:43.074Z","glit\_count":2}## | |
| תפקיד הבקשה | כניסה / טעינה לקיר (Feed) של משתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***feed\_owner\_id*** | מזהה המשתמש אליו שייך הקיר |
| ***end\_date*** | התאריך |
|  | ***glit\_count*** | כמות הפוסטים להציג |
| איך נראית התגובה | 505#Feed loading approved{gli&&er}{"glits":[{"feed\_owner\_id":52377,"publisher\_id":52377,"publisher\_screen\_name":"lebron","publisher\_avatar":"im8","background\_color":"White","date":"2025-06-20T06:50:07.000Z","content":"hii","font\_color":"black","id":98025},{"feed\_owner\_id":52377,"publisher\_id":52377,"publisher\_screen\_name":"lebron","publisher\_avatar":"im8","background\_color":"White","date":"2025-06-20T06:50:07.000Z","content":"hii","font\_color":"black","id":98029}],"commentsMap":{"gestureMap":{"98025":[],"98029":[]}},"likesMap":{"gestureMap":{"98025":[],"98029":[]}},"wowsMap":{"gestureMap":{"98025":[],"98029":[]}}}## | |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לשים feed\_owner\_id של משתמש פרטי וקבלת תוכן העמוד שלו | Tampering / Information Disclosure | **הצליח** |
| למחוק פרמטרים | Tampering | **לא הצליח** |
| לשים user id לא קיים | Tampering | **לא הצליח** |

| **מחקר נק' כניסה - שליחת בקשת חברות** | | |
| --- | --- | --- |

| **מספר הבקשה** | **410** | |
| --- | --- | --- |
| **שם הבקשה בעברית** | **שליחת בקשת חברות** | |
| דוגמא אמיתית | 410#{gli&&er}[51648,52859]## | |
| תפקיד הבקשה | שליחת בקשת חברות | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***אינדקס ראשון*** | מזהה המשתמש ששלח את בקשת החברות |
| ***אינדקס שני*** | מזהה המשתמש שאליו נשלחה הבקשה |

| איך נראית התגובה | 415#Glance request is valid. A notification was sent to the user on session: 26062025.c33f89a76175d1eab1a43b7cb6f693ca.1632.26062025{gli&&er}22654## | |
| --- | --- | --- |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| **קבלת ה cookie של המשתמש אליו שלחנו את הבקשה בתשובת השרת (אתגר)** | Information Disclosure | **הצליח** |

| **מחקר נק' כניסה - שכחת סיסמא?** | | |
| --- | --- | --- |

| **מספר הבקשה** | **אין (בקשה דרך הווב)** | |
| --- | --- | --- |
| **שם הבקשה בעברית** | **שחזור סיסמא** | |
| דוגמא אמיתית | POST /password-recovery-code-request/  “guymor”  POST /password-recovery-code-verification/  “guymor”,  “1106FCAAC1700” | |
| תפקיד הבקשה | לשחזר סיסמא אם שכחת | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***פרמטר ראשון / בקשה ראשונה*** | שם המשתמש ששכחנו את הסיסמא אליו |
| ***פרמטר ראשון / בקשה שנייה*** | שם המשתמש ששכחנו את הסיסמא אליו |
|  | ***פרמטר שני / בקשה שנייה*** | קוד שחזור הסיסמא המורכב מהתאריך היום, מזהה המשתמש בגימטריה והשעה שנשלח לאימייל של המשתמש |

| איך נראית התגובה | 123 | |
| --- | --- | --- |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| **לשים שם משתמש לא שלנו, ואז לשלוח בפרמטר הבקשה את קוד שחזור הסיסמא שנשלח לאימייל שלו באמצעות מזהה המשתמש שלו (אתגר)** | Information Disclosure | **הצליח** |

| **מחקר נק' כניסה - טעינת היסטורית חיפוש** | | |
| --- | --- | --- |

| **מספר הבקשה** | **אין (בקשה דרך הווב)** | |
| --- | --- | --- |
| **שם הבקשה בעברית** | **טעינת היסטוריית חיפוש** | |
| דוגמא אמיתית | GET /history/22654 | |
| תפקיד הבקשה | לטעון את היסטוריית החיפוש עבור משתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***פרמטר ראשון*** | מזהה המשתמש שנטען עבוריו ההיסטורייה |

| איך נראית התגובה | {"screen\_name":"guymo","avatar":"im1","description":"ds","privacy":"Public","id":22211},{"screen\_name":"guymor","avatar":"im1","description":"12","privacy":"Public","id":22654} | |
| --- | --- | --- |

| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| --- | --- | --- |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| **לשים מזהה משתמש שונה (לא שלנו), ובכך לראות את ההיסטוריית חיפוש הפרטית שלו וקבלת פרטים על פעולות שעשה שלא אמורות להיות חשופות לנו. (אתגר)** | Information Disclosure | **הצליח** |

**לא כל כך בטוח איך אני אמור לתעד את ה xss אז אני פשוט אכתוב מה זה ומה עשיתי**

**העלאת פוסט זדוני, עם קישור שמוביל להעלאת פוסט בעמוד שלחץ הקישור, עם כיתוב שהמשתמש בוחר (HACKED לדוגמא)**

**please donate to our sick little brother.. <a href='/glit?id=-1&feed\_owner\_id=-1&publisher\_id=-1&publisher\_screen\_name=hacker&publisher\_avatar=im1&background\_color=Black&date=2025-06-28T12:50:41.392Z&content=HACKED!&font\_color=white'>Link for donations</a>"**