**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 | TEXT טקסטואלי סייטפול |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | CODE{NUMBER}#DATA## |
| פורמט כללי של תגובה | {NUMBER}CODE#DATA |

**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** |
| כאשר מחפשים משתמש השרת שולח הצעות למשתמשים אך גם את כל המידע עליהם כולל הID שלהם והמייל. | לקבל מידע על כל המשתמשים שרוצה | **כן** | לתקן את שליחת ההצעות לשמות בלבד. |
| כאשר כותבים פוסט, שינוי זמן השליחה לזמן בעתיד בעבר | **העברת מידע בעבר או בהווה** | **כן** | **למחוק את שליחת הפרטים שלא רצוים** |
| כאשר כותבים תגובה לגליט ניתן לשנות את תצוגת שם המשתמש ובעצם להתחזות למשהו אחר | **התחזות למשהו אחר** | **כן** | **שלא יהיה ניתן ששם המשתמש ושם תצוגת המשתמש יהו שונים** |
| כאשר עושים לייקים מהירים , הם נחשבים למרות שאמור להיות ניתן רק אחד | **זיוף כמות לייקים** | **כן** | **שיהיה אופציה רק ללייק אחד** |
| כאשר מתחברים למשתמש מקבלים מידע על כל המשתמשים שנכנסו לפיד שלך | **ניצול המידע על המשתמשים האחרים** | **כן** | **המשתמש יקבל רק את השמות שלהם עם האווטר שלהם** |
| נתיב באתר אובייקט משתמש | **חיפוש אדם על פי ID** | **כן** | **לא לאפשר למשתמש אחר לעשות זו על משתמש אחר** |
| אתגר הפרטיות חיפוש | **לקבל מידע על משתמשים** | **כן** | **לא לאפשר למשתמש לעשות זו על משתמש אחר** |
| כאשר נכנסים לפיד של משהו אחר התוכנה מחזירה את הקשר בין המשתמשים | **לדעת את הקשר בין משתמשים אחרים** | **כן** | **לאפשר אך ורק את האופציה לשלוח קשר בינך לבין משתמש אחר** |
| קבלת מידע על משתמש | לקבל מידע על משתמש אחר | **כן** | **לא לאפשר לחפש משתמשים אחרים כך** |
| כאשר נכנסים לחשבון מקבלים עדכון על הודעות בפיד | **לקבל מידע על משתמש אחר** | **כן** | **לא לאפשר לקבל מידע על פיד של משהו אחר כך** |
| אתגר הפרטיות – בזמן הבקשה לחיפוש מופיע הבקשה להיסטורית החיפוש אאפשר לשנות את למשהו אחר | **לקבל את המידע על היסטורית חיפוש של משתמשים** | **כן** | **לאפשר לדעת את היסטורית החיפוש שלך בלבד** |
| אתגר הכניסה – המערכת לא בודקת את הסיסמה אלה רק אם היא מתאימה בגודל האסקי שלה לכן ניתן לרשום כל סיסמה שמתאימה בגודל וזה יעבוד בגלל שאנחנו מקבלים את גודל הצאקסאמ של כל ניתן להוריד את הצאקסאמ של השם משתמש | **להכנס למשתמש אחר** | **כן** | **לא לשלוח את אורך הצאקסאמ לשמתמש אם טעה וגם לבדוק את הסיסמה** |
| אתגר XRSF – השתלת קישור לאדם שהוא עושה פעולות אצלו במחשב | **גרימה לפעולות בלתי רצוניות** | **כן** | **לבטל את האופציה לשים קישורים מוסתרים** |
| אתגר סיסמה – באיפוס הסיסמה ניתן לראות דפוס חוזר של המילה באמצע ובצדדים זה רק מספר התאריך ובכך לקבל את סיסמת המשתמש בשניה המילה באמצע הינה הID אלפבת לאנגלית עם גימטריה | **לקבל את סיסמת המשתמש** | **כן** | **לשנות את המנגנון למשהו אחר שאינו קל להבנה** |

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** | **300** | |
| **שם הבקשה בעברית** | **חיפוש** | |
| דוגמא אמיתית | **300#{gli&&er}{"search\_type":"SIMPLE","search\_entry":"m"}##** | |
| תפקיד הבקשה | חיפוש משתמשים | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **search\_type** | סוג חיפוש |
| **search\_entry** | מידע רצוי |
| איך נראית התגובה | 305#Entities search result{gli&&er}[{"screen\_name":"omg@bro.com","avatar":"im5","description":"omg@bro.com","privacy":"Public","id":4,"mail":"omg@bro.com"},{"screen\_name":"omri savra","avatar":"im2","description":"alert(1);","privacy":"Public","id":14,"mail":"yoyo@gmail.com"},{"screen\_name":"theMangoProphet","avatar":"im8","description":"all hail the great mango!","privacy":"Public","id":15,"mail":"itsik1231995@gmail.com"},{"screen\_name":"omri savra","avatar":"im1","description":"hello world","privacy":"Public","id":20,"mail":"yoyo@gmail.com"},{"screen\_name":"The Imposter","avatar":"im6","description":"a","privacy":"Public","id":22,"mail":"SUS@gmail.co"}]## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לרשום **search\_type מחיקת ערך** | **Tampering** | **לא הצליח** |
| **search\_entry מחקת ערך** | **Tampering** | **לא הצליח** |
| **קבלת מידע על המשתמש מייל ID וכל המידע על המתמש הרצוי בעזרת החיפוש של כל דבר.** | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **650** | |
| **שם הבקשה בעברית** | **תגובה לפוסט** | |
| דוגמא אמיתית | **650#{gli&&er}{"glit\_id":51979,"user\_id":43264,"user\_screen\_name":"the king","id":-1,"content":"tomoro","date":"2024-06-22T13:31:56.769Z"}##** | |
| תפקיד הבקשה | כתיבת תגובה לגליט | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **glit\_id** | מספר זיהוי משתמש של הפוסט |
| **user\_id** | מספר זיהוי של המשתמש |
| **user\_screen\_name** | שם תצוגה |
| **id** | מספר זיהוי הודעה |
| **content** | תוכן תגובה |
| **date** | תאריך |
|  |  |
|  |  |
| איך נראית התגובה | 655#Comment publish approved{gli&&er}{"glit\_id":51979,"user\_id":43264,"user\_screen\_name":"the king","id":16517,"date":"2024-06-22T13:31:56.769Z","content":"tomoro"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| שינוי תוכן **user\_screen\_name ולהתחזות למשהו אחר** | **Spoofing** | **הצליח** |
| **מחיקת תוכן התגובה** | **Tampering** | **לא הצליח** |
| **מחיקת מספר זיהוי** | **Information Disclosure** | **לא הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **550** | |
| **שם הבקשה בעברית** | **כתיבת גליט** | |
| דוגמא אמיתית | **550#{gli&&er}{"feed\_owner\_id":43264,"publisher\_id":43264,"publisher\_screen\_name":"dorian the king","publisher\_avatar":"im1","background\_color":"White","date":"2024-06-22T13:47:11.485Z","content":"than","font\_color":"black","id":-1}##** | |
| תפקיד הבקשה | כניסה למשתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **feed\_owner\_id** | מספר זיהוי משתמש של הפוסט |
| **publisher\_id** | מספר זיהוי של המשתמש |
| **publisher\_screen\_name** | שם תצוגה |
| **publisher\_avatar** | אווטר |
| **background\_color** | צבע רקע |
| **date** | תאריך |
| **content** | תוכן |
| **font\_color**  **id** | פונט  זהות |
| איך נראית התגובה | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":43264,"publisher\_id":43264,"publisher\_screen\_name":"dorian the king","publisher\_avatar":"im1","background\_color":"White","date":"2024-06-22T13:47:11.485Z","content":"than","font\_color":"black","id":52058}## | |

**תרחישי תקיפה לנק' כניסה**

תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| שינוי תוכן **user\_screen\_name ולהתחזות למשהו אחר** | **Spoofing** | **לא הצליח** |
| **מחיקת תוכן התגובה** | **Tampering** | **לא הצליח** |
| **שינוי זמן שליחת הודעה** | **Tampering** | **הצליח** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **710** | |
| **שם הבקשה בעברית** | **לייק להודעה** | |
| דוגמא אמיתית | **710#{gli&&er}{"glit\_id":52058,"user\_id":43264,"user\_screen\_name":"dorian the king","id":-1}##** | |
| תפקיד הבקשה | לעשות לייק | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **glit\_id** | מספר זיהוי |
| **user\_id** | מספר זיהוי |
| **user\_screen\_name** | שם תצוגה |
| **id** | מספר הודעה |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":52058,"user\_id":43264,"user\_screen\_name":"dorian the king","id":1015203,"date":"2024-06-22T14:36:21.002Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
| **מחיקת תוכן התגובה** | **Tampering** | **לא הצליח** |
| **שליחת יותר מהודעה אחת של לייק** | **other** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **500** | |
| **שם הבקשה בעברית** | **כניסה לפיד** | |
| דוגמא אמיתית | **500#{gli&&er}{"feed\_owner\_id":43264,"end\_date":"2024-06-23T13:51:35.369Z","glit\_count":2}##** | |
| תפקיד הבקשה | כניסה לפיד | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **end\_date** | תאריך |
| **feed\_owner\_id** | מספר זיהוי של בעל פיד |
| **glit\_count** | מספר גילטים |
| איך נראית התגובה | 505#Feed loading approved{gli&&er}{"glits":[{"feed\_owner\_id":43264,"publisher\_id":44130,"publisher\_screen\_name":"noam cohen","publisher\_avatar":"im1","background\_color":"Gold","date":"2024-06-22T15:19:15.000Z","content":"vfd","font\_color":"black","id":52654},{"feed\_owner\_id":43264,"publisher\_id":44130,"publisher\_screen\_name":"noam cohen","publisher\_avatar":"im1","background\_color":"White","date":"2024-06-22T15:18:31.000Z","content":"vsv","font\_color":"black","id":52653}],"commentsMap":{"gestureMap":{"52653":[{"glit\_id":52653,"user\_id":44130,"user\_screen\_name":"noam cohen","id":16687,"date":"2024-06-22T15:18:35.000Z","content":"fdfs"}],"52654":[{"glit\_id":52654,"user\_id":44130,"user\_screen\_name":"noam cohen","id":16688,"date":"2024-06-22T15:20:21.000Z","content":"hallo"},{"glit\_id":52654,"user\_id":44130,"user\_screen\_name":"noam cohen","id":16692,"date":"2024-06-22T15:20:21.000Z","content":"hallo"},{"glit\_id":52654,"user\_id":44130,"user\_screen\_name":"noam cohen","id":16693,"date":"2019-06-22T15:20:21.000Z","content":"hallo"}]}},"likesMap":{"gestureMap":{"52653":[],"52654":[]}},"wowsMap":{"gestureMap":{"52653":[],"52654":[]}}}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
| **מחיקת תאריך** | **Tampering** | **לא הצליח** |
| **שליחת הבקשה** | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **410** | |
| **שם הבקשה בעברית** | **פולו** | |
| דוגמא אמיתית | 410#{gli&&er}[43264,5]## | |
| תפקיד הבקשה | פולו לחבר | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **glit\_id** | מספר זיהוי משתמש של הפוסט |
| **user\_id** | מספר זיהוי של המשתמש |
| איך נראית התגובה | 415#Glance request is valid. A notification was sent to the user on session: USER\_NOT\_LOGGED\_ON\_WEBSITE{gli&&er}5## | |

|  |  |  |
| --- | --- | --- |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
| **מחיקת מספר זיהוי שני** | **Spoofing** | **לא הצליח** |
| **שליחת הבקשה מאותו מספר לאותו מספר** | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **get** | |
| **שם הבקשה בעברית** | **בקשה** | |
| דוגמא אמיתית | https://glitter.org.il/entity/19847 | |
| תפקיד הבקשה | קבלת אובייקט משתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **id** | מספר זיהוי משתמש |
| cookies | מספר זיהוי של המשתמש |
| איך נראית התגובה | {"screen\_name":"melach ew","avatar":"im8","description":"QWERTYUIUHGFDFGHJ","privacy":"Public","id":19847} | |

|  |  |  |
| --- | --- | --- |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
| **מחיקת cookies** | **Spoofing** | **לא הצליח** |
| **שליחת הבקשה מאותו עם מספר של משהו אחר** | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **400** | |
| **שם הבקשה בעברית** | **קשר** | |
| דוגמא אמיתית | **"400#{gli&&er}[2,1]##"** | |
| תפקיד הבקשה | קבלת מידע על הקשר בין האנשים | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **id** | מספר זיהוי משתמש |
| id | מספר זיהוי של המשתמש |
| איך נראית התגובה | 405#Glanceship status response{gli&&er}{"requester\_user\_id":43264,"responder\_user\_id":42833,"glanceship\_type":"Pending"}## | |

|  |  |  |
| --- | --- | --- |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
| **שליחת הבקשה מאותו עם מספר של משהו אחר** | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **440** | |
| **שם הבקשה בעברית** | **הודעות חדשות בפיד** | |
| דוגמא אמיתית | **"440#{gli&&er}44822##"** | |
| תפקיד הבקשה | קבלת מידע על גליטים בפיד | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **id** | מספר זיהוי משתמש |
|  |  |
| איך נראית התגובה | 445#Updates load approved{gli&&er}{"glanceRequests":[{"initiator":{"screen\_name":"dorianTheKing","avatar":"im1","description":"b","privacy":"Public","id":43264}},{"initiator":{"screen\_name":"ori cohen","avatar":"im1","description":"ani gever","privacy":"Public","id":43453}},{"initiator":{"screen\_name":"noamcohen","avatar":"im1","description":"br","privacy":"Public","id":45985}}],"pushUpdates":[]}## | |

|  |  |  |
| --- | --- | --- |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
|  |  |  |
| **שליחת הבקשה עם מספר של משהו אחר** | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **310** | |
| **שם הבקשה בעברית** | **משתמש** | |
| דוגמא אמיתית | **310#{gli&&er}43264##** | |
| תפקיד הבקשה | קבלת מידע על משתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| **id** | מספר זיהוי משתמש |
|  |  |
| איך נראית התגובה | 315#Entity fetched succesfully{gli&&er}{"screen\_name":"dorianTheKing","avatar":"im1","description":"b","privacy":"Public","id":43264}## | |

|  |  |  |
| --- | --- | --- |
| data | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| מחיקת מספר זיהוי | **Spoofing** | **לא הצליח** |
|  |  |  |
| **שליחת הבקשה עם מספר של משהו אחר** | **Information Disclosure** | **הצליח** |