**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** | **לא** | **שיהיה אופציה רק ללייק אחד** |
|  |  |  |  |

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** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

| **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** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

| **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}## | |

| 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"}## | |

| 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** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |