**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 | Stateful ,טקסטואלי |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | <NUMBER>#{gli&&er}{data:value,data:value}## |
| פורמט כללי של תגובה | <NUMBER>#command{gli&&er}{data:value,data:value}## |

**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** |
| ניתן לבצע לייק לגליט יותר מפעם אחת | תוקף יכול לגרום לכך שיהיה לגליט שהוא יבחר כמות בלתי מוגבלת של לייקים | **like.py** | בשרת יש לבדוק האם משתמש זה ביצע כבר לייק לגליט זה ואם כן להגביל את כמות הלייקים שיוכל לעשות לאחד |
| ניתן להעלות פוסט עם מידע בלתי חוקי שלא ניתן להעלות בצורה רגילה מהאפליקציה או האתר | תוקף יכול לזייף את תאריך פרסום הפוסט ובכך להסתיר את כך שהוא מעתיק לדוגמה פוסטים מאחרים או להשתמש בצבעים שעדיין לא יצאו באופן רשמי לאתר או תמונות שלא שלו | **post.py** | בשרת יש לבדוק האם המידע שהכנסת הוא חוקי, כלומר ייבדק האם התאריך הוא של היום והאם הצבע והתמונות הם חוקיים ושייכים למשתמש |
| ניתן להגיב על פוסטים באמצעות איזה שם שתבחר (כלומר ללא הזדהות אמיתית) ובנוסף ניתן לשנות את תאריך פרסום התגובה וניתן להגיב ללא הגבלה | תוקף מסוגל לנצל את זה שניתן להגיב ללא הגבלה כדי להציף את התגובות בספאם של פרסום לדוגמה, בנוסף הוא יכול לעשות זאת עם שם של מישהו אחר ותאריך לבחירתו | **comment.py** | ניתן לוודא שהשם אותו בחרת מתאים לuser שלך וכמו כן ניתן להגביל לתגובה אחת פעם בשנייה והמקסימום תגובות ממשתמש אחד הוא 10 |
| ניתן לתת לייק גם לפוסטים של עמודים פרטיים בעזרת ניחוש מזהה הפוסט שלהם ושליחת לייק אליו | **תוקף יכול לשלוח לייקים לאנשים שאינו אקראיים שאינו מכיר ובכך לגרום להם להכיר אותו כלומר פרסום או הטרדה ובמקרה של חשבון פרטי האדם יכול להיות מאוד מאוים איך הוא הגיע לפוסט שלו** | **Random**  **Like.py** | ניתן לבדוק האם מזהה הפוסט הוא של אדם פרטי ואם כן לחסום אותך מלשלוח לו לייק ובנוסף להגביל אותך בכמות לייקים בזמן מסויים |
| ניתן להגיב לפוסטים של אנשים פרטיים וכמו כן ניתן פשוט להגיב הודעה חוזרת על מלא פוסטים שונים ברנדומליות | **תוקף יכול לשלוח הודעה שיווקית כלשהי בצורה חוזרת לכל המשתמשים בכך שהיא תעבור על כל ה id הקיימים ותגיב להם על פוסטים כולל משתמשים פרטיים** | **Random**  **Comment.py** | ניתן להגביל את כמות התגובות שמשתמש יכול לעשות בזמן מסוים ולכמות משתמשים מסויימת וכמו כן לחסום את האופצייה של מישהו להגיב לאדם פרטי על פוסט |
| ניתן לצרף חברים ללא צורך באישורם | **תוקף יכול לגרום לכך שכל המשתמשים יהיו חברים שלו בעזרת בקשות אינסופיות על כל המשתמשים** | **Friend.py** | ניתן לאפשר אישור בקשת חברות רק אם המאשר שולח את הבקשה מהמשתמש שלו |
| ניתן לחפש משתמשים פרטיים ולקבל את הid של כלל המשתמשים לפי שם משתמש בלבד | **תוקף שמצא חולשה שבעזרתה הוא יכול לפגוע במשתמש לפי המזהה שלו כעת יכול גם לפי שם המשתמש ולכוון במי הוא רוצה לפגוע ובנוסף לכך הוא יוכל למצוא משתמשים פרטיים ובכך לפגוע בפרטיות** | **getID.py** | ניתן להוריד את האופציה של חיפוש WILDCARD וכמו כן לא למסור למשתמש מזהה של משתמש אחר. |
| ניתן לשלוח וואו (כמו לייק סודי) להיכן שאתה רוצה | **תוקף שמגלה את זה יהיה לו גישה לאופצייה שמוצגת באתר ואינה מתאפשרת למשתמשים אחרים כך שהוא יוכל למכור את הwows ולפגוע בחברה** | **Wow.py** | ניתן להוריד את האופצייה של wow בכלליות או לאפשר אותה רק למשתמשים מסוימים |
| ניתן לבצע וואו לגליט יותר מפעם אחת | תוקף יכול לגרום לכך שיהיה לגליט שהוא יבחר כמות בלתי מוגבלת של ואווז | **Wow.py** | בשרת יש לבדוק האם משתמש זה ביצע כבר וואו לגליט זה ואם כן להגביל את כמות הוואז שיוכל לעשות לאחד |
| ניתן להדפיס את המחסן של כל הבקשות האפשריות בעזרת בקשת 900 | **זה יכול להקל מאוד על התוקף למצוא חולשות בתכנה לדוגמה כך מצאתי את הוואו** | **commandBank.py** | ניתן למחוק פקודה זאת או להסתיר אותה במספר יותר גדול וקשה לניחוש |
| **אתגרים** | | | |
| ניתן לקבל פיד של משתמש בעזרת ה id שלו בלבד גם אם המשתמש פרטי | **תוקף יכול לראות את כל המידע שהעלת גם אם אתה אדם פרטי מה שמאוד פוגע בפרטיות המשתמש** | **printFeed.py** | ניתן לבדוק האם הזדהת בתור המשתמש אותו אתה מבקש לטעון |
| ניתן להיכנס למשתמש ללא צורך בסיסמה | **תוקף יכול להיכנס לאיזה משתמש שברצונו בעזרת שם משתמש בלבד** | **hackLogin.py** | ניתן לשנות כך שכאשר אתה טועה בסיסמה המערכת לא תחזיר לך את ה checksum |
| ניתן להשיג סיסמה של משתמש בעזרת הusername שלו והuser\_id בלבד | **תוקף יכול להיכנס לאיזה משתמש שברצונו מתי שהוא רוצה בעזרת הסיסמה ולעלות תכנים במקומו** | **Password.py** | ניתן לשנות את תהליך האימות כאשר אתה בודק מה הסיסמה שלך כך שבקוד יהיה שדה שהוא לגמרי אקראי ולא יהיה אפשר להצליח אותו בצורה קבועה |
| ניתן להשיג עוגייה של משתמש בעזרת הפרטי משתמש שלו – שם משתמש וסיסמה | **תוקף יכול לגנוב למשתמש את העוגייה אם הוא מממש את החולשה של הסיסמה** | **Cookie.py** | ניתן לשנות כך שלא יינתן פרטים על העוגייה בתשובה של השרת |

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** | **650** | |
| **שם הבקשה בעברית** | **לפרסם תגובה** | |
| דוגמא אמיתית | 650#{gli&&er}{"glit\_id":4564,"user\_id":854,"user\_screen\_name":"nativ 2.0","id":-1,"content":"hi","date":"2021-06-13T10:44:17.865Z"}## | |
| תפקיד הבקשה | פרסום תגובה עם תוכן ספציפי | |
| תיאור פרמטרים | **שם** | **הסבר** |
| glit\_id | מזהה הפוסט |
| user\_id | מזהה המשתמש שכותב תגובה |
| user\_screen\_name | השם המוצג ככותב התגובה |
| id | המזהה של הגליט (חייב להיות 1-) |
| content | תוכן התגובה |
| date | תאריך פרסום התגובה |
| איך נראית התגובה | 655#Comment publish approved{gli&&er}{"glit\_id":4564,"user\_id":854,"user\_screen\_name":"nativ 2.0","id" | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לפרסם אין סוף תגובות | **Other** | **הצליח** |
| להגיב לפוסט לא קיים | **Tampring** | **לא הצליח** |
| **להגיב למשתמש פרטי** | **Tampring** | **הצליח** |
| להגיב לא בשמי ובפרטים מזוייפים | **Spoofing** | **הצליח** |
| למחוק תגובה של אדם אחר | **Tampring** | **לא הצליח** |
| קבלת מזהה הפוסט | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **710** | |
| **שם הבקשה בעברית** | **הוספת לייק** | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":4499,"user\_id":366,"user\_screen\_name":"nativ kolisher","id":-1}## | |
| תפקיד הבקשה | הוספת לייק לפרסום ספציפי | |
| תיאור פרמטרים | **שם** | **הסבר** |
| glit\_id | המזהה של הגליט אליו מנסים לעשות לייק |
| user\_id | מזהה של המשתמש שעושה לייק |
| user\_screen\_name | השם של המשתמש שעושה לייק |
| id | המזהה של הגליט (חייב להיות 1-) |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":4499,"user\_id":366,"user\_screen\_name":"nativ kolisher","id":14141,"date":"2021-06-13T08:10:49.173Z"}## | |

|  |
| --- |
|  |
|  | | Choose an item. |  |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | |
|  | | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לעשות לייק לפוסט אינסוף פעמים | | **Other** | **הצליח** |
| לעשות לייק לפוסט לא קיים | | **Tampring** | **לא הצליח** |
| לעשות לייק לגליט של משתמש פרטי | | **Tampring** | **הצליח** |
| לעשות לייק לא בשמי | | **Spoofing** | **לא הצליח** |
| למחוק לייק של אדם אחר | | **Spoofing** | **לא הצליח** |
| השרת מחזיר את המזהה פוסט ו הודעה | | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **550** | |
| **שם הבקשה בעברית** | **לפרסם פוסט** | |
| דוגמא אמיתית | 550#{gli&&er}{"feed\_owner\_id":854,"publisher\_id":854,"publisher\_screen\_name":"nativ 2.0","publisher\_avatar":"im7","background\_color":"White","date":"2021-06-13T10:44:06.359Z","content":"hello","font\_color":"black","id":-1}## | |
| תפקיד הבקשה | פרסום פוסט עם תוכן ספציפי | |
| תיאור פרמטרים | **שם** | **הסבר** |
| feed\_owner\_id | המזהה של בעל העמוד בו הפוסט פורסם |
| publisher\_id":854 | המזהה של מפרסם הפוסט |
| publisher\_screen\_name | השם של יוצר הפוסט |
| publisher\_avatar | התמונה של יוצר הפוסט |
| background\_color | צבע רקע הפוסט |
| date | תאריך פרסום הפוסט |
| content | התוכן (מילים) המוצגים בפוסט |
| font\_color | צבע המילים המוצגות בפוסט |
|  | id | המזהה של הגליט (חייב להיות 1-) |
| איך נראית התגובה | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":854,"publisher\_id":854,"publisher\_screen\_name":"nativ 2.0","publisher\_avatar":"im7","background\_color":"White","date":"2021-06-13T10:44:06.359Z","content":"hello","font\_color":"black","id":4564}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| להעלות אין סוף פוסטים | **Other** | **הצליח** |
| להעלות פוסט ממשתמש לא שלי | **Spoofing** | **לא הצליח** |
| **לשנות את פרטי הפוסט לפרטים לא חוקיים** | **Tampring** | **הצליח** |
| קבלת המזהה של הפוסט | **Information Disclosure** | **הצליח** |

|  |
| --- |
| **מחקר נק' כניסה** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **350** | |
| **שם הבקשה בעברית** | **שינוי משתמש** | |
| דוגמא אמיתית | 350#{gli&&er}{"screen\_name":"nativ 1.0","avatar":"im6","description":"hello","privacy":"Private","id":366,"user\_name":"nativ","password":"123456","gender":"Undefined","mail":"321@gmail.com"}## | |
| תפקיד הבקשה | לשנות את הגדרות המשתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| screen\_name | השם המוצג |
| avatar | תמונה |
| description | תיאור |
| privacy | פרטיות |
| id | מזהה |
| user\_name | שם משתמש |
|  | password | סיסמה |
|  | gender | מין |
|  | mail | מייל |
| איך נראית התגובה | 355#User setting update approved{gli&&er}{"screen\_name":"nativ 1.0","avatar":"im6","description":"hello","privacy":"Private","id":366,"user\_name":"nativ","password":"123456","gender":"Undefined","mail":"321@gmail.com","date":"2021-06-13T16:59:01.573Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| שינוי הסיסמה | **Tampring** | **לא הצליח** |
| שינוי הפרטים עבור משתנה שונה | **Spoofing** | **לא הצליח** |
| **החזרת מידע עודף עבוד המשתמש** | **Information Disclosure** | **לא הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **500** | |
| **שם הבקשה בעברית** | **טעינת מסך הבית (הפיד)** | |
| דוגמא אמיתית | 500#{gli&&er}{"feed\_owner\_id":887,"end\_date":"2021-06-19T07:45:12.497Z","glit\_count":2}## | |
| תפקיד הבקשה | להציג את הפוסטים ותכנם של המשתמש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| feed\_owner\_id":887 | הid של המשתמש |
| end\_date | תאריך הטעינה |
| glit\_count | מספר הפוסטים להצגה |
| איך נראית התגובה | 505#Feed loading approved{gli&&er}{"glits":[{"feed\_owner\_id":887,"publisher\_id":887,"publisher\_screen\_name":"nativ 2.0","publisher\_avatar":"im2","background\_color":"Violet","date":"2021-06-19T04:44:40.000Z","content":"post 2","font\_color":"black","id":8386},{"feed\_owner\_id":887,"publisher\_id":887,"publisher\_screen\_name":"nativ 2.0","publisher\_avatar":"im2","background\_color":"White","date":"2021-06-19T04:44:25.000Z","content":"post 1","font\_color":"black","id":8385}],"commentsMap":{"gestureMap":{"8385":[{"glit\_id":8385,"user\_id":887,"user\_screen\_name":"nativ 2.0","id":3906,"date":"2021-06-19T04:44:32.000Z","content":"try1"}],"8386":[{"glit\_id":8386,"user\_id":887,"user\_screen\_name":"nativ 2.0","id":3907,"date":"2021-06-19T04:44:46.000Z","content":"try2"}]}},"likesMap":{"gestureMap":{"8385":[{"glit\_id":8385,"user\_id":887,"user\_screen\_name":"nativ 2.0","id":87605,"date":"2021-06-19T07:45:12.802Z"}],"8386":[{"glit\_id":8386,"user\_id":887,"user\_screen\_name":"nativ 2.0","id":87606,"date":"2021-06-19T07:45:12.802Z"}]}},"wowsMap":{"gestureMap":{"8385":[],"8386":[]}}}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| הצגת כל התוכן של משתמש אחר (גם אם הוא פרטי) | **Spoofing** | **הצליח** |
| הצגת מידע מיותר עבור המשתמש כגון מזהים | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **300** | |
| **שם הבקשה בעברית** | **בקשת חיפוש** | |
| דוגמא אמיתית | 300#{gli&&er}{"search\_type":"SIMPLE","search\_entry":"search321"}## | |
| תפקיד הבקשה | לחפש אדם ציבורי ולהגיע לעמוד שלו | |
| תיאור פרמטרים | **שם** | **הסבר** |
| search\_type | הסוג של החיפוש (SIMPLE – רגיל, WILDCARD-עובד גם על פרטיים, ID-מחפש לפי מזהה) |
| search\_entry | המשתמש אותו אתה מחפש |
| איך נראית התגובה | 305#Entities search result{gli&&er}[{"screen\_name":"search321","avatar":"im1","description":"hi","privacy":"Public","id":1584,"mail":"123@gmail.com"}]## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| קבלת ה id של המשתמש | **Information Disclosure** | **הצליח** |
| חיפוש משתמש פרטי | **Tampring** | **הצליח** |
| **חיפוש בשם מישהו אחר** | **Spoofing** | **לא הצליח** |
| קבלת פרטי ההתחברות של המשתמש | **Information Disclosure** | **לא הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **750** | |
| **שם הבקשה בעברית** | **הוספת wow** | |
| דוגמא אמיתית | 750#{gli&&er}{"glit\_id":8420,"user\_id":945,"user\_screen\_name":"nativ 6.0","id":-1}## | |
| תפקיד הבקשה | הוספת wow לפרסום ספציפי | |
| תיאור פרמטרים | **שם** | **הסבר** |
| glit\_id | המזהה של הגליט אליו מנסים לעשות וואו |
| user\_id | מזהה של המשתמש שעושה וואו |
| user\_screen\_name | השם של המשתמש שעושה וואו |
| id | המזהה של הגליט (חייב להיות 1-) |
| איך נראית התגובה | 755#Wow pulish approved{gli&&er}{"glit\_id":8420,"user\_id":945,"user\_screen\_name":"nativ 6.0","id":233,"date":"2021-06-19T21:00:10.567Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לעשות ווא לפוסט אינסוף פעמים | **Other** | **הצליח** |
| לעשות וואו לפוסט לא קיים | **Tampring** | **לא הצליח** |
| לעשות וואו לגליט של משתמש פרטי | **Tampring** | **הצליח** |
| לעשות וואו לא בשמי | **Spoofing** | **לא הצליח** |
| למחוק וואו של אדם אחר | **Spoofing** | **לא הצליח** |
| השרת מחזיר את המזהה פוסט ו הודעהע | **Information Disclosure** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **900** | |
| **שם הבקשה בעברית** | **בקשה להצגת כל הפקודות** | |
| דוגמא אמיתית | 900#{gli&&er}1## | |
| תפקיד הבקשה | להציג בפניי את כל באפשרויות שלי | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***אין פרפטרים*** | זהו פקודה יחידה ללא הדרים |
| איך נראית התגובה | 905#Protocol info response{gli&&er}"100:\tLogin Requests. Usage: [username, password]\n110:\tAuthentication response. Usage: <an integer number computed according to server's request>\n150:\tRegistration request. Usage: <registration data json object: user data + registration code>\n200:\tLogout request. Usage: <userId>\n300:\tSearch request\n310:\tLoad user details (info). Usage: <userId>\n320\tReturns the entities whose feed was visited by the given user. Usage: <userId>\n350:\tUpdate user setting. Usage: <updated user json object>\n400:\tGet glanceship status. Usage: [glanceship requester id, glanceship responder id]\n410:\tGlance request. Usage: [glanceship requester id, glanceship responder id]\n420:\tApprove a glance request. Usage: [glanceship requester id, glanceship responder id]\n430:\tRefuse a glance request. Usage: [glanceship requester id, glanceship responder id]\n440:\tLoad updates for user. Usage: <userId>\n500:\tLoad feed. Usage: [feed owner id, end date, glits count]\n550:\tPublish glit. Usage: <glit json object>\n650:\tPublish comment. Usage: <comment json object>\n710:\tPublish like. Usage: <like json object>\n720:\tDelete like. Usage: <like id>\n750:\tPublish Wow. Usage: <wow json object>\n760:\tDelete wow. Usage: <wow id>\n"##\n | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| קבלת כל הפקודות האפשריות ביניהם מוסתרות | **Tampring** | **הצליח** |
| קבלת מידע עבור האתר שלא הייתי אמור לגלות | **Information Disclosure** | **הצליח** |
| **קבלת מידע על המשתמשים** | **Information Disclosure** | **לא הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **400** | |
| **שם הבקשה בעברית** | **הוספת חבר** | |
| דוגמא אמיתית | 400#{gli&&er}[945,1584]## | |
| תפקיד הבקשה | לשלוח בקשת חברות | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***My\_id (האיבר הראשון ב [,]*** | המזהה של המשתמש ששולח את הבקשה |
| ***user\_id (האיבר השני ב [,]*** | המזהה של המשתמש שאליו שולחים את הבקשה |
| איך נראית התגובה | 405#Glanceship status response{gli&&er}{"requester\_user\_id":945,"responder\_user\_id":1584,"glanceship\_type":"Stranger"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| להוסיף חבר ללא אישורו | **Tampring** | **הצליח** |
| לקשר בין אנשים שאינם אתה | **Spoofing** | **לא הצליח** |
| **קבלת מידע עבור משתמש** | **Information Disclosure** | **לא הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** |  | |
| **שם הבקשה בעברית** |  | |
| דוגמא אמיתית |  | |
| תפקיד הבקשה |  | |
| תיאור פרמטרים | **שם** | **הסבר** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| איך נראית התגובה |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |