|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **710** | |
| **שם הבקשה בעברית** | **הוספת לייק** | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":1663,"user\_id":408,"user\_screen\_name":"Ivan ","id":-1}## | |
| תפקיד הבקשה | להוסיף לייק לגליט מסויים | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***glit\_id*** | מזהה של הגליט שעליו עושים לייק |
| ***user\_id*** | מזהה של המשתמש שעושה לייק |
| ***user\_screen\_name*** | שם המשתמש העושה לייק |
| ***id*** | מזהה של הגליט |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":1663,"user\_id":408,"user\_screen\_name":"Ivan ","id":104983,"date":"2020-06-23T04:07:39.666Z"}## | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **חולשות שנמצאו** | | | | |
| **הסבר על החולשה שנמצאה** | | **כיצד תוקף יכול לנצל זאת** | **סקריפט POC מצורף** | **הצעה לפתרון** |
| אפשר לעשות לייק לגליט לא קיים | | אפשר ליצור גליטים ככה | [**liker.py**](https://github.com/mixelburg/Final-Project/blob/master/liker.py) | בדיקת תקינות הקלט |
| להשות לייק לגליט של משהו שהוא לא חבר שלי | | אפשר לשים לייק למשתמש פרטי | [**liker.py**](https://github.com/mixelburg/Final-Project/blob/master/liker.py) | בדיקת תקינות הקלט |
| לנשות לעשות לייק לגליט יותר מפעם אחת | | אפשר לשים הרבה לייקים | [**liker.py**](https://github.com/mixelburg/Final-Project/blob/master/liker.py) | בדיקת תקינות הקלט |
| אפשר לעשות לייק לגליט בשם אחר | | אפשר לשים הרבה לייקים אם שמות שונות | [**liker.py**](https://github.com/mixelburg/Final-Project/blob/master/liker.py) | בדיקת תקינות הקלט |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לעשות לייק בשמ אחר (user\_screen\_name) | **Spoofing** | **הצליח** |
| לעשות לייק לגליט לא קיים | **Tampring** | **הצליח** |
| לעשות לייק לפני להתחברנו | **Tampring** | **לא הצליח** |
| להשות לייק לגליט של משהו שהוא לא חבר שלי | **Tampring** | **הצליח** |
| לנשות לעשות לייק לגליט יותר מפעם אחת | **Tampring** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **720** | |
| **שם הבקשה בעברית** | **מחיקת לייק** | |
| דוגמא אמיתית | 720#{gli&&er}<like\_id>## | |
| תפקיד הבקשה | למחוק לייק לגליט מסויים | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***like\_id*** | מזהה לייק |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":1663,"user\_id":408,"user\_screen\_name":"Ivan ","id":104983,"date":"2020-06-23T04:07:39.666Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| למחוק יותר מלייק אחד | **Tampring** | **הצליח** |
| למחוק לייק של משהו אחר | **Spoofing** | **הצליח** |
| למחוק לייק לגליט של משתמש פרטי | **Tampring** | **הצליח** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **חולשות שנמצאו** | | | | |
| **הסבר על החולשה שנמצאה** | | **כיצד תוקף יכול לנצל זאת** | **סקריפט POC מצורף** | **הצעה לפתרון** |
| אפשר למחוק יותר מלייק אחד | | למחוק לייקים | [**liker.py**](https://github.com/mixelburg/Final-Project/blob/master/liker.py) | בדיקת תקינות הקלט |
| אפשר למחוק לייק של משהו אחר | | למחוק לייקים | [**liker.py**](https://github.com/mixelburg/Final-Project/blob/master/liker.py) | בדיקת תקינות הקלט |
| אפשר למחוק לייק לגליט של משתמש פרטי | | למחוק לייקים | [**liker.py**](https://github.com/mixelburg/Final-Project/blob/master/liker.py) | בדיקת תקינות הקלט |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **650** | |
| **שם הבקשה בעברית** | **הוספת comment** | |
| דוגמא אמיתית | 650#{gli&&er}{"glit\_id":1663,"user\_id":408,"user\_screen\_name":"Ivan ","id":-1,"content":"why not","date":"2020-06-23T06:29:00.751Z"}## | |
| תפקיד הבקשה | **הוספת comment** | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***glit\_id*** | מזהה של הגליט שעליו עושים לייק |
| ***user\_id*** | מזהה של המשתמש שעושה לייק |
| ***user\_screen\_name*** | שם המשתמש העושה לייק |
| ***id*** | מזהה של הגליט |
| ***content*** | טקסט |
| ***date*** | תאריך |
| איך נראית התגובה | 655#Comment publish approved{gli&&er}{"glit\_id":1663,"user\_id":408,"user\_screen\_name":"Ivan ","id":1411,"date":"2020-06-23T10:45:33.820Z","content":"test"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לעשות comment בשם משהו אחר | **Spoofing** | **הצליח** |
| לעשות comment לגליט פרטי | **Tampring** | **הצליח** |
| לעשות comment בתאריך אחר | **Tampring** | **הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **סקריפט POC מצורף** | **הצעה לפתרון** |
| אפשר לעשות comment בשם משהו אחר | לעשות comment בשם משהו אחר | [**comment.py**](https://github.com/mixelburg/Final-Project/blob/master/comment.py) | לבדוק שם |
| אפשר לעשות comment לגליט פרטי | לעשות comment לגליט פרטי | [**comment.py**](https://github.com/mixelburg/Final-Project/blob/master/comment.py) | לבדוק האם גליט פרטי |
| אפשר לעשות comment בתאריך אחר | לעשות comment בתאריך אחר | [**comment.py**](https://github.com/mixelburg/Final-Project/blob/master/comment.py) | לבדוק תאריך |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **550** | |
| **שם הבקשה בעברית** | **הוספת גליט** | |
| דוגמא אמיתית | 550#{gli&&er}{"feed\_owner\_id":408,"publisher\_id":408,"publisher\_screen\_name":"Ivan","publisher\_avatar":"im7","background\_color":"Teal","date":"2020-06-25T11:58:44.508Z","content":"testing","font\_color":"black","id":-1}## | |
| תפקיד הבקשה | להוסיף גליט | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***feed\_owner\_id*** | מזהה המשתמש שלו עושים גליט |
| ***publisher\_id*** | מזהה המשתמש העושה גליט |
| ***publisher\_screen\_name*** | שם משתמש העושה גליט |
| ***publisher\_avatar*** | תמונה של המשתמש העושה גליט |
| ***backgroung\_color*** | צבע של גליט |
| ***date*** | תאריך |
| ***content*** | טקסט |
| ***font\_color*** | צבע אותיות |
| איך נראית התגובה | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":408,"publisher\_id":408,"publisher\_screen\_name":"Ivan ","publisher\_avatar":"im7","background\_color":"Teal","date":"2020-06-25T11:58:44.508Z","content":"testing","font\_color":"black","id":4601}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לעשות גליט למשתמש פרטי | **Tampring** | **הצליח** |
| לעשות גליט אם שם שונה | **Tampring** | **הצליח** |
| לעשות גליט אם תמונה שונה | **Tampring** | **הצליח** |
| לעשות גליט אם צבע אותיות שונה | **Tampring** | **הצליח** |
| תאריך לא נכון | **Tampring** | **הצליח** |
| לעשות גליט אם צבע לא קיים | **Tampring** | **הצליח** |
| לעשות גליט אם HTML | **Tampring** | **הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **סקריפט POC מצורף** | **הצעה לפתרון** |
| אפשר לעשות גליט למשתמש פרטי | לעשות גליט למשתמש פרטי | [**post.py**](https://github.com/mixelburg/Final-Project/blob/master/post.py) | לבדוק האם יש לך זכות לעשות גליט למשתמם |
| לעשות גליט אם שם שונה | לעשות גליט אם שם שונה | [**post.py**](https://github.com/mixelburg/Final-Project/blob/master/post.py) | לבדות האם שם נכון |
| לעשות גליט אם תמונה שונה | לעשות גליט אם תמונה שונה | [**post.py**](https://github.com/mixelburg/Final-Project/blob/master/post.py) | לבדוק תמונה |
| לעשות גליט אם צבע אותיות שונה | לעשות גליט אם צבע אותיות שונה | [**post.py**](https://github.com/mixelburg/Final-Project/blob/master/post.py) | לא לתת לשנות צבע |
| לעשות גליט אם צבע לא קיים | לעשות גליט אם צבע לא קיים | [**post.py**](https://github.com/mixelburg/Final-Project/blob/master/post.py) | לבדוק האם צבע קיים |
| תאריך לא נכון | לעשות לגיט אם תאריך לא נכון | [**post.py**](https://github.com/mixelburg/Final-Project/blob/master/post.py) | לבדוק תאריך |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **500** | |
| **שם הבקשה בעברית** | **להראות גליטים** | |
| דוגמא אמיתית | 500#{gli&&er}{"feed\_owner\_id":408,"end\_date":"2020-06-25T05:34:04.000Z","glit\_count":2}## | |
| תפקיד הבקשה | להראות גליטים | |
|  | ***feed\_owner\_id*** | שם משתמש |
| ***end\_date*** | תאריך הסוף |
| ***glit\_count*** | כמות הגליטים |
| איך נראית התגובה | 505#Feed loading approved{gli&&er}{"glits":[{"feed\_owner\_id":408,"publisher\_id":408,"publisher\_screen\_name":"Ivan ","publisher\_avatar":"im7","background\_color":"Red","date":"2020-06-25T05:02:38.000Z","content":"some text","font\_color":"black","id":4428},{"feed\_owner\_id":408,"publisher\_id":408,"publisher\_screen\_name":"Ivan | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לראות גליטים של משתמש פרטי | **Information Disclosure** | **הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **סקריפט POC מצורף** | **הצעה לפתרון** |
| אפשר לראות גליטים של משתמש פרטי | לראות גליטים של משתמש פרטי | [**feed.py**](https://github.com/mixelburg/Final-Project/blob/master/feed.py) | לבדוק האם יש לך זכות לראות גליטים של משתמם פרטי |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **300** | |
| **שם הבקשה בעברית** | **חיפוס לפי שם** | |
| דוגמא אמיתית | 300#{gli&&er}"s"## | |
| תפקיד הבקשה | חיפוס לפי שם | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***""*** | data |
| איך נראית התגובה | 305#Entities search result{gli&&er}[{"screen\_name":"Stephen Nadel","avatar":"im1","description":"Feels good to be a gangster","privacy":"Public","id":12,"mail":"sgddb@gmail.com"},{"screen\_name":"noamselig","avatar":"im6","description":"Gil is the best ?????","privacy":"Private","id":13,"mail":"noamselig@gmail.com"},{"screen\_name":"sd","avatar":"im8","description":"hi","privacy":"Public","id":15,"mail":"eitan@pelech.ort.org.il"},{"screen\_name":"testing\_user\_1\_full","avatar":"im1","description":"4","privacy":"Public","id":21,"mail":"vixic96774@lexu4g.com"},{"screen\_name":"Osher Berger","avatar":"im5","description":"Alla hu akbar","privacy":"Public","id":23,"mail":"osherberger31@gmail.com"}]## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לקבל מידע של משתמשים פרטיים | **Information Disclosure** | **הצליח** |
| לקבל מידע שאתה לא אמור לקבל | **Information Disclosure** | **הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **סקריפט POC מצורף** | **הצעה לפתרון** |
| אפשר לקבל מידע של משתמשים פרטיים | לקבל מידע של משתמשים פרטיים | [**search.py**](https://github.com/mixelburg/Final-Project/blob/master/search.py) | לא לתת מידע |
| אפשר לקבל מידע שאתה לא אמור לקבל | לקבל מידע שאתה לא אמור לקבל | [**search.py**](https://github.com/mixelburg/Final-Project/blob/master/search.py) | לא לתת מידע |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **410** | |
| **שם הבקשה בעברית** | **שליחת בקשת תצוגה** | |
| דוגמא אמיתית | 410#{gli&&er}[408,406]## | |
| תפקיד הבקשה | שליחת בקשת תצוגה | |
|  | ***[,]*** | מזהה של משתמש ראשון ושני |
| איך נראית התגובה | 415#Glance request is valid. A notification was sent to the user on session: 25062020.b287c358565022150250d6ee39e7098a.1310.25062020{gli&&er}406## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לשלוח למשתמש לא קיים | **Tampring** | **לא הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **400** | |
| **שם הבקשה בעברית** | **בדיקת מצב** | |
| דוגמא אמיתית | 400#{gli&&er}[408,406]## | |
| תפקיד הבקשה | בדיקת מצב | |
|  | ***[,]*** | מזהה של משתמש ראשון ושני |
| איך נראית התגובה | 405#Glanceship status response{gli&&er}{"requester\_user\_id":408,"responder\_user\_id":406,"glanceship\_type":"Stranger"}## | |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **310** | |
| **שם הבקשה בעברית** | **בדיקת משתמש** | |
| דוגמא אמיתית | 310#{gli&&er}406## | |
| תפקיד הבקשה | בדיקת משתמש | |
|  | ***{406}*** | מזהה של משתמש |
| איך נראית התגובה | 315#Entity fetched succesfully{gli&&er}{"screen\_name":"Ido Malachi","avatar":"im8","description":"Hakuna Matate","privacy":"Private","id":406}## | |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **350** | |
| **שם הבקשה בעברית** | **שינוי הגדרות** | |
| דוגמא אמיתית | 350#{gli&&er}{"screen\_name":"Ivan ","avatar":"im2","description":"hello world","privacy":"Public","id":408,"user\_name":"mixelburg","password":"qweASDzxc90","gender":"Male","mail":"tester@gmail.com"}## | |
| תפקיד הבקשה | שינוי הגדרות | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***screen\_name*** | שם משתמש |
| ***avatar*** | תמונה |
| ***description*** | תיאור |
| ***privacy*** | סטטוס |
| ***id*** | מזהה משתמש |
| ***user\_name*** | שם משתמש |
| ***password*** | סיסמה |
| ***gender*** | מין |
|  | ***mail*** | mail@ |
| איך נראית התגובה | 355#User setting update approved{gli&&er}{"screen\_name":"Ivan ","avatar":"im2","description":"hello world","privacy":"Public","id":408,"user\_name":"mixelburg","password":"qweASDzxc90","gender":"Male","mail":"tester@gmail.com","date":"2020-06-26T08:46:27.551Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לשנות את מה שאתה לא אמור לשנות | **Tampring** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **200** | |
| **שם הבקשה בעברית** | **יציאה** | |
| דוגמא אמיתית | 200#{gli&&er}408## | |
| תפקיד הבקשה | יציאה | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***<408>*** | מזהה משתמש |
| איך נראית התגובה | 205#User logout approved{gli&&er}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לצאת עם מזהה אחר | **Tampring** | **לא הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **750** | |
| **שם הבקשה בעברית** | **הוספת wow** | |
| דוגמא אמיתית | 750#{gli&&er}{"glit\_id":100,"user\_id":408,"user\_screen\_name":"screen\_name"}## | |
| תפקיד הבקשה | **הוספת wow** | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***glit\_id*** | מזהה גליט |
| ***user\_id*** | מזהה משתמש |
| ***user\_screen\_name*** | שם משתמש |
| איך נראית התגובה | 755#Wow pulish approved{gli&&er}{"glit\_id":100,"user\_id":408,"user\_screen\_name":"screen\_name","id":12507,"date":"2020-07-04T16:31:27.508Z"}## | |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **760** | |
| **שם הבקשה בעברית** | **מחיקת wow** | |
| דוגמא אמיתית | 760#{gli&&er}<wow\_id>## | |
| תפקיד הבקשה | **מחיקת wow** | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***wow\_id*** | מזהה wow |
| איך נראית התגובה | 765#Unwow publish approved{gli&&er}{"glit\_id":6448,"user\_id":1608,"id":972,"date":"2020-07-04T16:42:11.331Z"}## | |