**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 | טקסטואלי, Stateful, מנגנון אותנטיקציה |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | REQUEST\_ID#{gli&&ter}{ header:value, header:value, header:value}## |
| פורמט כללי של תגובה | RESPOBSE\_ID#responseType{gli&&ter}}{header:value, header:value, header: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 לעלות פוסט עם פרמטרים שונים, לדוגמה: SCREEN\_NAME שונה או לשנות צבע של רקע כתב ותאריך . | SCREEN\_NAME  התוקף יכול לעלות פוסט מהמשתמש שלו אך יראו שזה ממשתמש אחר.  COLORS  התוקף יכול להסתיר תוכן פוגעני בכך שהוא משנה את צבע הכתב אן הרקע.  תאריך:  נגיד והתוקף נאשם בפשע חמור,  התוקף יכול לעלות פוסט בתאריך העבירה ובכך להוכיח שהוא עשה משהו באותו היום ולא אשם. | **כן** | בשביל לתקן את הבעיה עם הname\_SCREEN צריך לוודא שהID שממנו עולה הפוסט שווה לשם תחת אותו הID. בשביל לסגור את הבעיה עם צבע רקע וכתב פשוט לבדוק שהצבע ברשימה, או אפילו למחוק מהשרת את האפשרות להשתמש ב צבעים לא קיימים. בשביל התאריך צריך לבדוק מה התאריך באותו היום ואם הוא שווה לתאריך שהפוסט עולה |
| אין מנגונן שבודק האם המשתמש עשה LIKE\WOW על פוסט בID מסויים או לא. | **התוקף יכול לעשות אינסוף LIKES\WOWS**  **באותו הפוסט**  **בנוסף לכך להוריד LIKES\WOWS**  **שמשתמשים אחרים עשו לפוסט** | **כן** | **צריך לשמור את הid של המשתמש שעשה LIKE\WOW על פוסט ואז לבדוק האם משתמש עם ID X עשה לייק או לא ולאפשר רק אם לא** |
| ניתן לשנות את הפרמטרים של בקשת התגובה | **התוקף יכול לשנות את SCREEN\_NAME**  **ולעלות פוסט "בשם של משהו אחר"**  **או שהתוקף יכול לשנות תאריך** | **כן** | לוודא שהID שממנו עולה הפוסט שווה לשם תחת אותו הID. בשביל התאריך צריך לבדוק מה התאריך באותו היום ואם הוא שווה לתאריך שהפוסט עולה |
| יש בקשה שמביא הסטוריה של משתמשים | **התוקף יכול לראות הסטורייה של משתמשים אחרים** | **כן** | **או שלעשות את הפקודה הזאת למנהלים או למחוק אותה.** |
| דליפת מידע בFEED | **המשתמש יכול לקבל את כל הפרטים של FEED של משהו (גם של חשבון פרטי) ולראות דברים שאיננו אמור.**  **מעבר לכך המשתמש יכול לקבל את המזהים של כל לייק וwow**  **ולהשתמש בעובדה שלייק או וואו**  **לא קשורים למשתמש שפרסם אותו ובכך**  **להוריד את כל או חלק מהלייקים וואו למשתמשים** | **כן** | **לא לתת מידע על מזהים של לייקים וואו.**  **(לחולשה של הורדת לייקים וואו)**  **יש לקשר כל לייק וואו למזהה ולוודא שמי שמוריד את הלייק וואו הם המשתמשים עם אותו המזהה.** |
| הסיסמה והשם המשתמש נבדקים לפי הצאקסאם שלהם (הצאקסם חלש, (ערך האסקי של כל התווים) יש הרבה אפשרויות לאותו הצאקסם, ובתגובה להודעת כניסה השרת חושף את הצאקסם הנכון, וכאשר הסיסמה נכונה השרת חושף בהודעה את הסיסמה של המשתמש. | **התוקף יכול לדעת מה הצאקסאם של שם לעשות בקשת כניסה עם סיסמה לא נכונה לקבל את הצאקסם של הסיסמה והשם ביחד בגלל שיש לו את הצאקסם של השם אז הוא יכול לקבל גם את הצאקסם של סיסמה ולמצוא קומבינציה של תווים שמתאימה לאותו צאקסם לשלוח את זה לשרת ואז השרת עוד יחשוף לו את הסיסמה האמיתית** | **כן** | **קודם כל לא לחשוף את הסיסמה בהודעת תשובה ללוגאין אפילו אם הסיסמה נכונה, לעשות צאקסם חזק יותר, ולבדוק סיסמה לא לפי הצאקסם אלה לפי המחרוזת של הסיסמה עצמה כלומר עם הסיסמה "zzzzz" וה”ם שמשתמש “**  **Zzzzz” אז האקסם 1220**  **השרת לא יחליט אם הסיסמה נכונה לפי הצאקסם אלה ישווה את המחרוזת שהמשתמש מכניס לשם ולסיסמה (אפשר להשאיר את צאקסם כבדיקה נוספת)** |
| אין בדיקה שמשתמש אשר מאשר בקשת חברות הוא באמת המשתמש ששלחו לו בקשת חברות. | **התוקף יכול לשלוח בקשת חברות למשתמש ולשלוח בקשת אישור מהחשבון שלו וזה יעבוד. חולשה זו יכולה לאפשר לו לראות את העמוד של משתמשים פרטיים שרק חבריהם יכולים לראות אותם** | **כן** | **לבדוק שהמשתמש שמאשר בקשת חברות הוא המשתמש שקיבל אותה.** |

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** | | **550** | |
| **שם הבקשה בעברית** | | **לפרסם פוסט גליט** | |
| דוגמא אמיתית | | 550#{gli&&er}{"feed\_owner\_id":7792,"publisher\_id":7792,"publisher\_screen\_name":"natali1","publisher\_avatar":"im2","background\_color":"DarkOrange","date":"2022-06-03T13:26:17.437Z","content":"hiii","font\_color":"black","id":-1}## | |
| תפקיד הבקשה | | תפקיד הבקשה הוא לעלות פוסט גליט ספציפי ממשתמש ספציפי עם תוכן מסויים. | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| feed\_owner\_id | הID המזהה של FEED שבו יהיה הפוסט |
| publisher\_id | המזהה המפרסם |
| publisher\_screen\_name | השם שיוצג על המסך בפוסט בתור שם המפרסם |
| publisher\_avatar | תמונת הפרופיל |
| background\_color | צבע רקע של גליט |
| date | תאריך פרסום |
| content | התוכן של הפוט |
| font\_color | צבע פונט |
|  | | id | מזהה הבקשה |
| איך נראית התגובה | | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":7792,"publisher\_id":7792,"publisher\_screen\_name":"natali1","publisher\_avatar":"im2","background\_color":"DarkOrange","date":"2022-06-03T13:26:17.437Z","content":"hiii","font\_color":"black","id":7354}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לעלות פוסט בתור מישהו אחר (בלי לדעת את הסיסמה שלו) | **Spoofing** | **לא הצליח☹** |
| לזייף את התאריך של הפוסט למשל לאתמול או למחר | **Spoofing** | **הצליח** |
| לשים צבע רקע של פוסט שלו קיים בתפריט הצבעים | **Tampring** | **הצליח** |
| לשנות את הצבע של הFONT | **Tampring** | **הצליח** |
| לשנות את התמונה של המשתמש שרואים ליד הפוסט ואת השם | **Spoofing** | **הצליח** |
| לנסות להכניס את הפוסט לFEED של משהו אחר בלי להיות חברים (בחשבון פרטי רק חברים יכולים לעלות פוסטים) | **Tampring** | **הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **710** | |
| **שם הבקשה בעברית** | | **הוספת לייק לגליט** | |
| דוגמא אמיתית | | 710#{gli&&er}{"glit\_id":9794,"user\_id":8017,"user\_screen\_name":"natali2","id":-1}## | |
| תפקיד הבקשה | | **להוסיף לייק לגליט מסויים ממשתמש מסויים** | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| glit\_id | המזהה של הגליט שעליו נוסיף לייק |
| user\_id | מזהה של המשתמש ששם לייק |
| user\_screen\_name | מאיזה מסך שמו לייק |
| id | מזהה הבקשה |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לעשות יותר מלייק אחד על פוסט אחד מאותו המשתמש | **Spoofing** | **הצליח** |
| לקבל מידע על כל מי שם לייק על אותו הפוסט (שם ID וכו) | **Information Disclosure** | **הצליח** |
| שינוי user\_id לid אחר ובכך להוסיף לייק בתור משהו אחר | **Spoofing** | **לא הצליח** |
| להוסיף לייק לפני שמתחברים למשתמש | **Other** | **לא הצליח** |
| להוריד את glit\_id | **Tampring** | **לא הצליח** |
| להכניס ערכים לא הגיונים בשדות למשל אותיות בID | **Tampring** | **לא הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **650** | |
| **שם הבקשה בעברית** | | **לעלות תגובה לפוסט מסויים** | |
| דוגמא אמיתית | | 650#{gli&&er}{"glit\_id":9789,"user\_id":7792,"user\_screen\_name":"natali1","id":-1,"content":"test","date":"2022-06-06T10:30:41.048Z"}## | |
| תפקיד הבקשה | | **לעלות תגובה לפוסט מסויים מחשבון מסויים משם מסויים.** | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| glit\_id | הID של הגלית שעליו נרצה לעלות תגובה |
| "user\_id" | הID של המשתמש אשר מעלה את התגובה |
| ,"user\_screen\_name" | השם שיוצג על המסך בתור מי שהעלה את התגובה |
| id | ID |
| "content" | תוכן התגובה |
| "date" | תאריך שבו הועלתה התגובה |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לשנות את screen\_name וכך יראה כאילו משהו אחר הגיב | **Spoofing** | **הצליח** |
| לזייף את התאריך שבו הועלתה התגובה | **Spoofing** | **הצליח** |
| לפרסם תגובה לפני ההתחברות | **Other** | **לא הצליח** |
| לנסות להכניס תגובה ריקה | **Tampring** | **לא הצליח** |
| לנסות למחוק תגובות | **Tampring** | **לא עבד** |
| להכניס ערכים לא הגיונים בשדות למשל אותיות בglit\_ID | **Tampring** | **לא עבד** |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **100** | |
| **שם הבקשה בעברית** | | **להתחבר** | |
| דוגמא אמיתית | | 100#{gli&&er}{"user\_name":"natali2","password":"natali2","enable\_push\_notifications":true}## | |
| תפקיד הבקשה | | להתחבר עם שם וסיסמה לגליט | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| ***user\_name*** | שם המשתמש שאיתו נתחבר |
| ***password*** | סיסמה |
| ***enable\_push\_notificatoins*** | להפעיל התראות או לא |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| להתחבר למשתמש עם סיסמה לא נכונה | **Other** | **לא הצליח** |
| הבנתי שהמערכת משווה צאקסאם שם שם וסיסמה ולא את השם והסיסמה עצמם אז אפשר לנסות לגלות את הצא'ק הכולל בכך שנכניס שם של משתמש ואז נדע את הצאקסם של השם ואז גם של הסיסמה כי זה צאקסם כולל פחות השם המשתמש.  משם אפשר יהי לנסות למצוא סיסמה שהצאקסם שלה שהה לסיסמה המקורית ואז להכנס לחשבון | **Information Disclosure** | **הצליח** |
| אם נתחבר אם סיסמה מזויפת אך עובד בשרת יחזיר בתגובה להתחברות מוצלחת את הסיסמה המקורית של המשתמש | **Information Disclosure** | **הצליח** |
| לנסות להתחבר ללא שם או ללא סיסמה | **Tampring** | **לא עבד** |
| לעשות התחברות אחרי שכבר התחברנו | **Tampring** | **לא הצליח** |
| לשנות את הערך של enable\_push\_notifications למשהו לא הגיוני | **Tampring** | **לא הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **300** | |
| **שם הבקשה בעברית** | | **לחפש משתמש** | |
| דוגמא אמיתית | | 300#{gli&&er}{"search\_type":"SIMPLE","search\_entry":"natali16"}## | |
| תפקיד הבקשה | | לחפש משתמש | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| ***search\_type*** | סוג החיפוש שאותו נבצע |
| ***search\_entry*** | מה לחפש |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לנסות להכניס סוג חיפוש לק קיים (משם קיבלתי את כל הסוגי החיפושים: ID WILDCARD SYMPEL) | **Information Disclosure** | **הצליח** |
| לקבל מידע על משתמשים | **Information Disclosure** | **הצליח** |
| לחפש מידע על משתמש פרטי | **Information Disclosure** | **הצליח** |
| לשלוח בקשה ריקה (רק המזהה) | **Tampring** | **לא הצליח** |
|  | **Tampring** |  |
|  | **Tampring** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **500** | |
| **שם הבקשה בעברית** | | **לטעון FEED** | |
|  | | 500#{gli&&er}{"feed\_owner\_id":7792,"end\_date":"2022-06-07T20:24:06.108Z","glit\_count":2}## | |
| תפקיד הבקשה | | לקבל FEED של משהו | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| feed\_owner\_id | המזהה של FEED שאותו נרצה לטעון |
| "end\_date" | עד איזה תאריך להציג את הפובטים |
| "glit\_count" | כמות הפוסטים |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לטעון FEED של חשבון פרטי | **Information Disclosure** | **הצליח** |
| לקבל את כל הלייקים של פוסטים ןהמזהים שלהם, ואז אפשר יהי להוריד אותם לפי המזהה | **Information Disclosure** | **הצליח** |
| לקבל את כל WOW של פוסטים ןהמזהים שלהם, ואז אפשר יהי להוריד אותם לפי המזהה | **Information Disclosure** | **הצליח** |
| לשלוח בקשה ריקה (רק המזהה) | **Tampring** | **לא הצליח** |
|  | **Tampring** |  |
|  | **Tampring** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **720** | |
| **שם הבקשה בעברית** | | **להוריד LIKE** | |
|  | | 720#{gli&&er}50827## | |
| תפקיד הבקשה | | להוריד לייק תחת ID מסויים | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| מספר לפני ה## | מהזזה הLIKE |
|
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| למזהה לא קיים | **Tampring** | **לא הצליח** |
| להוריד לייק שידוע לי המזהה שלו אך לא אני שמתי | **Other** | **הצליח** |
|  | **Information Disclosure** |  |
|  | **Tampring** |  |
|  | **Tampring** |  |
|  | **Tampring** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **760** | |
| **שם הבקשה בעברית** | | **להוריד WOW** | |
|  | | 760#{gli&&er}827## | |
| תפקיד הבקשה | | להוריד לייק תחת ID מסויים | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| מספר לפני ה## | מהזזה הWOW |
|
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| להכניס מזהה לא קיים | **Tampring** | **לא הצליח** |
| להוריד WOW שידוע לי המזהה שלו אך לא אני שמתי | **Other** | **הצליח** |
|  | **Information Disclosure** |  |
|  | **Tampring** |  |
|  | **Tampring** |  |
|  | **Tampring** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **750** | |
| **שם הבקשה בעברית** | | **להוסיף WOW** | |
|  | | 750#{gli&&er}{"glit\_id": 9789, "user\_id": 8017, "user\_screen\_name": "natali2"}## | |
| תפקיד הבקשה | | להוריד 'WOW לפןסט מסויים | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| glit\_id | הפוסט שעליו נוסיף WOW |
|
| user\_id | מזהה המשתמש אשר מכניס WOW |
| user\_screen\_name" | שם שיוצג על המסך |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| להכניס מזהה של משהו אחר ובך להוסיף WOW ממנו | **Spoofing** | **לא הצליח** |
| להוסיף כמה WOW מאותו המשתמש | **Tampring** | **הצליח** |
| להוסיף USER\_ID לא הגיוני | **Tampring** | **לא הצליח** |
|  | **Tampring** |  |
|  | **Tampring** |  |
|  | **Tampring** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | |
| **מספר הבקשה** | | **320** | |
| **שם הבקשה בעברית** | | **לראות היסטוריה של משתמש** | |
|  | | 320#{gli&&er}7792## | |
| תפקיד הבקשה | | להציג את כל ההסטורית חיפוש של מתמש מסויים | |
| תיאור פרמטרים | | **שם** | **הסבר** |
| מספר לפני ה## | המזהה המשתמש שנראה את ההסטוריה שלו |
|
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |
| איך נראית התגובה | |  | |

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