**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 STATEFULL |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | מספר בקשה#{גליטר}#{שדות בקשה} |
| פורמט כללי של תגובה | מספר תשובה #{גליטר}#{שדות תשובה} |

אייפי: 54.187.16.171

**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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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** | **710** | |
| **שם הבקשה בעברית** | **לייק לגליט** | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":46,"user\_id":38,"user\_screen\_name":"user1","id":-1}## | |
| תפקיד הבקשה | לתת לייק לגליט ספציפי | |
| תיאור פרמטרים | **שם** | **הסבר** |
| glit\_id | מספר מזהה לגליט שלו נתתי לייק |
| user\_id | מספר מזהה של המשתמש שנותן את הלייק |
| user\_screen\_name | שם תצוגת המשתמש שנתן את הלייק |
| id | מספר מזהה לבקשה (תמיד -1) |
|  |  |
|  |  |
|  |  |
|  |  |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":46,"user\_id":38,"user\_screen\_name":" user 1","id":107,"date":"2021-06-06T15:17:50.710Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לתת לייק יותר מפעם אחת | **Other** | **הצליח** |
| לשלוח בקשת לייק לפני התחברות | **Tampring** | **לא הצליח** |
| **לשים user id של משתמש אחר ולזייף בקשות לייק** | **Spoofing** | **לא הצליח** |
| לעשות לייק לגליט לא קיים | **Tampring** | **הצליח** |
| לעשות לייק למשתמש פרטי שאני לא עוקבת אחריו | **Tampring** | **הצליח** |
|  | Choose an item. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **קוד POC נכתב?** | **הצעה לפתרון** |
| לתת לייק יותר מפעם אחת | התוקף יכול לתת לייקים למרות שהוא כבר עשה לייק יכול להוסיף לעצמו המון לייקים | לא | לבדוק האם על הגליטר שמנסים לעשות לו לייק יש כבר לייק מה אותו user\_id |
| לעשות לייק למשתמש פרטי שאני לא עוקבת אחריו | התוקף יכול לשנות את הגליט איידי לגליט איידי של משתמש שהוא לא עוקב אחריו ולעשות לייקים לגליטים שלו, יוכל להתשמש בזה כדי להספים לייקים למשתמש אחר שלא בהכרח רצה את זה | כן | לבדוק האם הuser עוקב אחרי הגליט ואם אותו גליט פרטי, אם הגליט פרטי והמשתמש לא עוקב אחריו לחסום את האופציה ללייק |
| לעשות לייק לגליט לא קיים | הגליטר פותח גליט חדש דרך היוזר שניסה לעשות לייק לגליט לא קיים, יכול לגרום ליצירה רבה מדי של גליטים וקריסת השרת | לא | לבדוק האם הגליט אכן קיים ואם לא אז לא לתת אפשרות לעשות לגליט הזה לייק |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **420** | |
| **שם הבקשה בעברית** | **אישור בקשת חברות ספציפית** | |
| דוגמא אמיתית | 420#{gli&&er}[188,38]## | |
| תפקיד הבקשה | לאשר חברות ספציפית של משתמש שביקש הצעת חברות | |
| תיאור פרמטרים | **שם** | **הסבר** |
| [129,99] | מספר ראשון ID של שולח הבקשה מספר שני ID של מי שנשלחה לו הבקשה |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| איך נראית התגובה | 425#Glance response is valid. A notification was sent to the user{gli&&er}38## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| לאשר בקשה שנשלחה ממני למשתמש בלי להיות מחובר למשתמש הזה | **Spoofing** | **הצליח** |
| לאשר בקשת חברות בלי שהייתה קיימת לפני | **Tampring** | **לא הצליח** |
| **לאשר בקשת חברות קיימת של 2 משתמשים אחרים שאתה לא אחד מהם** | **Spoofing** | **הצליח** |
| לאשר בקשת חברות ללא התחברות לשרת | **Other** | **לא הצליח** |
| לאשר בקשת חברות עם id זהה גם של שולח הבקשה וגם של מבקש הבקשה (למשל 300,300) | **Tampring** | **לא הצליח** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **חולשות שנמצאו** | | | | | | | | | |
| **הסבר על החולשה שנמצאה** | | | **כיצד תוקף יכול לנצל זאת** | | **קוד POC נכתב?** | | **הצעה לפתרון** | | |
| לאשר בקשה שנשלחה ממני למשתמש בלי להיות מחובר למשתמש הזה | | | אפשר לשלוח בקשות חברות לאנשים בגליטר ואתה יכול לאשר את אותם בקשות בין אם הבן אדם ששלחת לו רוצה לאשר את הבקשה ובין אם לא, יכול להשיג מידע על גליטים שלא בהכרח רצית שאותו תוקף יראה | | כן | | לבדוק האם המשתמש שמאשר את הבקשה הוא באמת המשתמש שאמור לאשר אותה אם כן אז לאשר את הבקשה ואם לא אז לא לאפשר את הבקשה הזאת | | |
| **לאשר בקשת חברות קיימת של 2 משתמשים אחרים שאתה לא אחד מהם** | | | יכול לאשר בקשות בין אנשים שאחד מהם לפחות לא רצה לעקוב או שהבן אדם השני יעקוב אחריו, יכול לחשוף בני אדם לגליטים שהם לא אמורים לראות כי יש סיבה שאדם לא מאשר עוקב של אדם אחר | | כן (קוד זהה לשל הפרצה לפני) | | לבדוק שמי שמאשר את הבקשה זה אכן הבן אדם שאחראי על העמוד | | |
|  | | |  | |  | |  | | |
|  | | |  | |  | |  | | |
| **מחקר נק' כניסה** | | | | | | | |
|  | **300** | | | | | | |
| **שם הבקשה בעברית** | **חיפוש גליטר** | | | | | | |
| דוגמא אמיתית | 300#{gli&&er}{"search\_type":"WILDCARD","search\_entry":"us"}##  300#{gli&&er}{"search\_type":"SIMPLE","search\_entry":" user "}## | | | | | | |
| תפקיד הבקשה | לחפש גליטר (ספציפי או מספר גליטים במקביל) | | | | | | |
| תיאור פרמטרים | **שם** | | **הסבר** | | | | |
| search\_type | | איזה סוג חיפוש אנחנו רוצים לבצע מבין 3 אופציות  ID SIMPLE WILDCARD | | | | |
| search\_entry | | מה אנחנו מחפשים | | | | |
|  | |  | | | | |
|  | |  | | | | |
|  | |  | | | | |
|  | |  | | | | |
|  | |  | | | | |
|  | |  | | | | |
|  | |  | | | | |
| איך נראית התגובה | 305#Entities search result{gli&&er}[{"screen\_name":"Sharon","avatar":"im1","description":"Blabal","privacy":"Public","id":8,"mail":"1235@gmail.com"},{"screen\_name":" user 1","avatar":"im2","description":"motto","privacy":"Private","id":38,"mail":"something@gmail.com"},{"screen\_name":"shahaf bodarem","avatar":"im8","description":":(","privacy":"Public","id":44,"mail":"shahaf@gmail.com"},{"screen\_name":"mor\_sh","avatar":"im1","description":"hello","privacy":"Public","id":55,"mail":"mor@gmail.com"},{"screen\_name":"shem badoy","avatar":"im7","description":"dodo farok the king","privacy":"Public","id":56,"mail":"bibihameleh@gmail.com"}]## | | | | | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | | | | | |
|  | | | | | **סוג חולשה  (STRIDE)** | | **הצליח /**  **לא הצליח** |
| לקבל מידע על משתמש ספציפי | | | | | **Information Disclosure** | | **הצליח** |
| לקבל מידע על מספר משתתפים שמכילים אותם תווים (למשל חלק מהמשתתפים שמכילים no בתחילת השם) | | | | | **Information Disclosure** | | **הצליח** |
| לבצע חיפוש מבלי להתחבר לשרת | | | | | **Other** | | **לא הצליח** |
| אם מישהו מחפש אותך אתה מקבל מהשרת את המידע על הID של המשתמש | | | | | **Information Disclosure** | | **הצליח** |
| לבצע חיפוש מ search\_type לא קיים | | | | | **Tampring** | | **לא הצליח** |
|  | | | | | Choose an item. | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **קוד POC נכתב?** | **הצעה לפתרון** |
| לקבל מידע על משתמש ספציפי | הוא יכול לחפש שם של משתמש בחיפוש ולנצל את זה כדי להשיג מידע עליו כמו אימייל וuser ID ולנצל את שניהם לתקיפות נוספות | כן | לבדוק האם יש למשתמש הרשאות מסויימות או להוסיף הרשאות לאנשים שכן אמורים לקבל מידע על ID ואימייל ולא לתת את המידע לכל משתמש שמחפש את המידע הזה |
| לקבל מידע על מספר משתתפים שמכילים אותם תווים (למשל חלק מהמשתתפים שמכילים no בתחילת השם) | יכול לקבל מידע על כמה משתמשים כמו אימייל וid במקביל ושוב, לנצל את המידע שקיבל למתקפות נוספות | כן (אותו קוד כמו חולשה לפני רק לא מחפשים שם מלא) | לבדוק האם יש למשתמש הרשאות מסויימות או להוסיף הרשאות לאנשים שכן אמורים לקבל מידע על ID ואימייל ולא לתת את המידע לכל משתמש שמחפש את המידע הזה |
| אם מישהו מחפש אותך אתה מקבל מהשרת את המידע על הID של המשתמש | **בעזרת זה ניתן להשיג ID של משתמשים ולדעת למי שייך אותו ID כיוון שמקבלים גם את שם המשתמש, יכו להשתמש בנתונים האלה לתקיפות נוספות על משתמשים** | **לא** | **אם מעבירים מידע על אדם שחיפש אותך אז להעביר רק את שם המשתמש ולא את הID של אותו אדם** |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **650** | |
| **שם הבקשה בעברית** | **תגובה לגליט** | |
| דוגמא אמיתית | 650#{gli&&er}{"glit\_id":367,"user\_id":38,"user\_screen\_name":" user 1","id":-1,"content":"hiii","date":"2021-06-08T16:37:36.531Z"}## | |
| תפקיד הבקשה | להגיב לגליט ספציפי | |
| תיאור פרמטרים | **שם** | **הסבר** |
| glit\_id | מספר מזהה לגליט שעליו מגיבים |
| user\_id | מספר מזהה למפרסם התגבוה על הגליט |
| user\_screen\_name | השם של מפרסם התגובה על הגליט |
| id | מזהה מספר לבקשה |
| content | הודעה שאתה רוצה לשלוח |
| date | זמן פרסום התגובה |
|  |  |
|  |  |
|  |  |
| איך נראית התגובה | 655#Comment publish approved{gli&&er}{"glit\_id":367,"user\_id":38,"user\_screen\_name":" user1","id":612,"date":"2021-06-08T16:37:36.531Z ","content":"hiiii"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| להגיב על שמו של משתמש אחר | **Spoofing** | **לא הצליח** |
| להגיב על גליט לא קיים | **Tampring** | **הצליח** |
| **להגיב לגליט של בן אדם שאני לא עוקבת אחריו בשימוש בglit id** | **Tampring** | **הצליח** |
| להגיב על גליט בלי להתחבר לשרת | **Other** | **לא הצליח** |
| למחוק תגובה על גליט | **Tampring** | **לא הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **קוד POC נכתב?** | **הצעה לפתרון** |
| להגיב על גליט לא קיים | כאשר מגיבים על גליט לא קיים נוצר הגליט בחשבון של אותו משתמש שיכול להיות שהוא בכלל לא רצה את היצירה של הגליט הזה. ניתן לנצל את החולשה הזאת כדי ליצור גליטים רבים ובכך להקריס את השרת | לא | לתת אפשרות להגיב רק על גליטים קיימים, אם הגליט לא קיים יש להציג שגיאה למשתמש |
| **להגיב לגליט של בן אדם שאתה לא עוקב אחריו בשימוש בglit id** | תוקף יכול להשתמש בזה כדי להגיב המון תגובות אצל אנשים שלא אישרו את הבקשה שלו או שלא רצו שיעקוב אחריהם ויכול להרוס לאנשים את הגליטר שלהם | כן | לבדוק האם האדם שמנסים להגיב לו הוא עמוד פרטי ולבדוק האם האדם שמנסה להגיב לו עוקב אחריו, אם לא לא לתת אופציה להגיב על גליטים. |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **550** | |
| **שם הבקשה בעברית** | **יצירת גליט** | |
| דוגמא אמיתית | 550#{gli&&er}{"feed\_owner\_id":99,"publisher\_id":99,"publisher\_screen\_name":" user2","publisher\_avatar":"im1","background\_color":"White","date":"2021-06-11T09:49:16.078Z","content":"hello","font\_color":"black","id":-1}## | |
| תפקיד הבקשה | ליצור גליט חדש | |
| תיאור פרמטרים | **שם** | **הסבר** |
| feed\_owner\_id | ID של בעל עמוד הגליטר |
| publisher\_id | ID של מפרסם הגליט |
| publisher\_screen\_name | איך קוראים ליוצר הגליט |
| publisher\_avatar | התמונה בחשבון של מפרסם הגליט |
| background\_color | הרקע של הגליט שפורסם |
| date | תאריך פרסום הגליט |
| content | מה נכתב בגליט הספציפי שפורסם |
| font\_color | צבע הכתב |
| id | מספר מזהה לבקשה |
| איך נראית התגובה | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":99,"publisher\_id":99,"publisher\_screen\_name":"userCheck","publisher\_avatar":"im1","background\_color":"White","date":"2021-06-11T09:49:16.078Z ","content":" hello ","font\_color":"black","id":1375}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| יצירה של כמות גליטים בלתי מוגבלת במקביל | **Other** | **לא הצליח** |
| פרסום גליט אצל אדם אחר מבלי להיות חבר של אותו משתמש אם העמוד פרטי | **Tampring** | **הצליח** |
| יצירת גליט בחשבון של אדם אחר מבלי להיות מחובר לחשבון של אדם זה ולפרסם על שמם של משתמשים אחרים בעזרת זיוף תמונה ושם | **Spoofing** | **הצליח** |
| יצירת גליט מבלי להתחבר לשרת | **Tampring** | **לא הצליח** |
| יצירת גליט בחשבון של אדם אחר מבלי להיות מחובר לחשבון של אדם זה דרך זיוף כל הפרטים של אותו משתמש | **Spoofing** | **לא הצליח** |
| פרסום גליט בחשבון שלא קיים | **Tampring** | **לא הצליח** |

|  |  |  |  |
| --- | --- | --- | --- |
| **חולשות שנמצאו** | | | |
| **הסבר על החולשה שנמצאה** | **כיצד תוקף יכול לנצל זאת** | **קוד POC נכתב?** | **הצעה לפתרון** |
| יצירת גליט בחשבון של אדם אחר מבלי להיות מחובר לחשבון של אדם זה ולפרסם על שמם של משתמשים אחרים בעזרת זיוף תמונה ושם | יכול לפרסם כל גליט שירצה בעמוד של אדם אחר ועל שמו של כל אדם שירצה (בעזרת שינוי התמונה ושם המשתמש של מפרסם הגליט) | לא | לבדוק האם השם שעל שמו פירסמו גליט הוא השם בעל ה publisher\_id הזה (לבדוק את ה publisher\_id) |
| פרסום גליט אצל אדם אחר מבלי להיות חבר של אותו משתמש אם העמוד פרטי | אם העמוד פרטי זה אומר שמנהל העמוד רוצה שרק לאנשים שפציפיים תיהיה גישה לעמוד ופרסום הגליטים שלו, תוקף יכול לנצל את הפירצה הזאת לפרסום גליטים אצל אדם שהוא לא עוקב אחריו ובכך לזייף גליטים בשמו של אותו משתמש או בשמם אל משתמשים אחרים | כן | לבדוק האם העמוד פרטי ואם כן לבדוק האם המשתמש עוקב אחרי אותו עמוד שבו הוא רוצה לפרסם גליט מסויים |