**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 |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | <request\_number>#{gli&&er}{“key”:value}## |
| פורמט כללי של תגובה | <request\_number>#name{gli&&er}## |

**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** |
| החולשה הראשונה שנמצאה זה שכנגד חוקי האפליקציה ניתן באופציות של האפליקציה בדרך עקיפין לעשות יותר מלייק אחד לפוסט פר משתמש. | התוקף יכול לנצל זאת כך שהוא יכול לקבל הרבה לייקים לפוסט שהוא מעלה כנגד חוקי האפליקציה או שהוא יכול למכור אפשרות של "קניית לייקים" למשתמשים באפליקציה | **כן, השם שלו זה like.py והוא בתייקית הPOC** | ניתן לעשות מן עקרון הדגל לכל משתמש שהמפתחים יוסיפו כפרמטר שברגע שהמשתמש שולח בקשה ללייק הדגל הופך לtrue וכל עוד הוא על מצב זה לא ניתן לעשות לייק וברגע שהמשתמש מוריד את הלייק הפרמטר הופך לfalse . |
| החולשה השנייה היא שניתן באפליקציה לשנות את צבע הרקע של פוסט לצבע שאינו ברשימת האופציות ואת הצבע של הטקסט של הפוסט לצבע ששונה מצבע שחור | התוקף יכול לנצל את חולשה זו כדי לכתוב פוסטים בחשבונות של אנשים כך שלא יהיה ניתן לראותם וכך לשבש עמודים של אנשים אחרים ולהרוס אותם. | **כן, השם שלו זה post\_glit.py**  **והוא בתייקית הPOC** | ניתן לבנות כמו WHITE LIST של הצבעים המותרים לצבע הרקע של הפוסט ובנוסף לעשות שהצבע היחיד האפשרי לטקסט הוא שחור וברגע שמשתמש מכניס אפשרות שונה מ הרשימה הזו לעשות הודעת שגיאה ולא לעלות פוסט זה |
| החולשה השלישית היא שניתן לפי חיפוש בבר החיפוש למצוא פרטים איישים של משתמש משהו שלא ניתן למצוא בשימוש רגיל באפליקציה | התוקף דרך חולשה זו יכול לדעת פרטים על משתמשים כמו המייל של אותו משתמש או את האיי די של המשתמש וכך יכול להשתמש לעוד שימושים עם דברים אלה | **כן, השם שלו זה FindMailAndId.py**  **והוא בתייקית הPOC** | ניתן לעשות שהפרמטרים שיראו לעין בחיפוש בבר החיפוש הם פרמטרים שכבר ניתן לדעת לפי האפליקציה ולא פרמטרים שאינם גלוים לכולם |
| החולשה הרביעית היא אפשרות להגיב לגליט שמישהו העלה גם אם המישהו הוא עמוד פרטי שלא ניתן למצוא בחיפוש | הפורץ יכול לנצל זאת כדי להרוס עמודים פרטיים של משתמשים ואפילו יכול למכור שירות אשר מגיב לאנשים על עמוד פרטי תגובות לגליטים | **כן, השם שלו זה ReplyInPrivetMode.py**  **והוא בתייקית הPOC** | ניתן להוסיף בדיקה האם הID שכותב את התגובה והמקבל של התגובה הם חברים באפליקציה ואם לא לשלוח הודעת שגיאה ואם הם כן אז לאפשר לו לשלוח את התגובה |
| החולשה החמישית היא שיש אפשרות לשלוח בקשה חברות למשתמש וגם לאשר אותה בשמו של אותו משתמש וכך ניתן להיות חבר של כל משתמש גם ללא אישורו | הפורץ יכול לנצל את חולשה זו כדי להיות חבר של כל אחד מהמשתמשים גם אם הוא עמוד פרטי ולכתוב לו תגובות בעמוד ולראות מה שכול משתמש שהוא רוצה מעלה לגליטר | **כן, השם שלו זה friends.py**  **והוא בתייקית הPOC** | ניתן לעשות שלא ניתן לשלוח מאותו משתמש גם בקשה וגם אישור ובמידה וזה קורה יש להוציא הודעת שגיאה  ולחסום את האישור |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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** | **שליחת לייק** | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":38339,"user\_id":40995,"user\_screen\_name":"Ido ben zaken","id":-1}## | |
| תפקיד הבקשה | לשלוח לייק | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***glit\_id*** | הID של המשתמש שאנו עושים לו לייק |
| ***user\_id*** | הID של המשתמש שעוה את הלייק |
| ***user\_screen\_name*** | השם של המשתמש אשר עושה את הלייק |
| ***id*** | תמיד -1 |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":15917,"user\_id":40995,"user\_screen\_name":"Ido ben zaken","id":702292,"date":"2024-06-10T16:31:54.878Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| כתיבת ***glit\_id*** של משתמש אחר. | **Tampring** | **לא הצליח** |
| כתיבת ***user\_id*** של משתמש אחר. | **Tampring** | **לא הצליח** |
| **לשלוח יותר מלייק אחד** | **Tampring** | **הצליח** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

**נק כניסה שנייה**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | | | | |
| **מספר הבקשה** | **550** | | | | |
| **שם הבקשה בעברית** | **פרסום פוסט** | | | | |
| דוגמא אמיתית | 550#{gli&&er}{"feed\_owner\_id":40995,"publisher\_id":40995,"publisher\_screen\_name":"Ido ben zaken","publisher\_avatar":"im5","background\_color":"Teal","date":"2024-06-14T17:43:49.671Z","content":"bye","font\_color":"black","id":-1}## | | | | |
| תפקיד הבקשה | לשלוח לייק | | | | |
| תיאור פרמטרים | **שם** | **הסבר** | | | |
| feed\_owner\_id | הID של המשתמש שרוצה לפרסם את הפוסט | | | |
| publisher\_id | הID של המפרסם של הלייק | | | |
| publisher\_screen\_name | השם של המשתמש אשר מפרסם את הלייק | | | |
| publisher\_avatar | האייקון של המשתמש | | | |
|  | background\_color | צבע הרקע שבחר המשתמש לכיתוב | | | |
|  | date | תאריך פרסום הפוסט | | | |
|  | content | תוכן הפוסט | | | |
|  | font\_color | צבע הכיתוב שבו כתוב הפוסט | | | |
| איך נראית התגובה | 555#Glit publish approved{gli&&er}{"feed\_owner\_id":40995,"publisher\_id":40995,"publisher\_screen\_name":"Ido ben zaken","publisher\_avatar":"im5","background\_color":"Teal","date":"2024-06-14T17:43:49.671Z","content":"bye","font\_color":"black","id":41485}## | | | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | | |
|  | | | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| פרסום פוסט בשם מישהו אחר | | | **Spoofing** | **לא הצליח** |
| לשנות את צבע הרקע לצבע שאינו באופציות | | | **Tampring** | **הצליח** |
| לשנות את צבע הטקסט למשהו אחר משחור | | | **Tampring** | **הצליח** |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |

**נק כניסה שלישית**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | | | | |
| **מספר הבקשה** | | **300** | | | | |
| **שם הבקשה בעברית** | | **חיפוש בבר החיפוש** | | | | |
| דוגמא אמיתית | | 300#{gli&&er}{"search\_type":"SIMPLE","search\_entry":"i"}## | | | | |
| תפקיד הבקשה | | לחפש תווים או תו ולראות את כל האופציות הניתנות לנו | | | | |
| תיאור פרמטרים | | **שם** | **הסבר** | | | |
| search\_type | הסוג חיפוש שלנו | | | |
| search\_entry | החיפוש הוכנס באותה נקודת זמן | | | |
| איך נראית התגובה | | 305#Entities search result{gli&&er}[{"screen\_name":"Raz Nitzan","avatar":"im7","description":"Life is Good","privacy":"Public","id":5,"mail":"raz.nitzan@gmail.com"},{"screen\_name":"asa klein","avatar":"im7","description":"description\_data","privacy":"Public","id":7,"mail":"a@gmail.com"},{"screen\_name":"<h1>Shai</h1>","avatar":"im6","description":"<script>alert(\"haha\");</script>","privacy":"Public","id":9,"mail":"asd@123.com"},{"screen\_name":"Niv Dagan","avatar":"im5","description":"GFG","privacy":"Public","id":11,"mail":"hey@gmail.com"},{"screen\_name":"Tina S","avatar":"im7","description":":)","privacy":"Private","id":13,"mail":"waka@wakamail.com"}]##  החיפוש הוא כל האופציות המוצאות לנו ברשימה שאנו רואים ברגע שאנחנו מחפשים ופרטים על משתמשים אלה | | | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | | |
|  | | | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| קבלת פרטים של משתמשים שלא ניתן לראות | | | **Information Disclosure** | **הצליח** |
| שינוי מידע | | | **Other** | **לא הצליח** |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |

**נק כניסה רביעית**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | | | | |
| **מספר הבקשה** | | **650** | | | | |
| **שם הבקשה בעברית** | | **תגובה לפוסט** | | | | |
| דוגמא אמיתית | | 650#{gli&&er}{"glit\_id":41499,"user\_id":40995,"user\_screen\_name":"Ido ben zaken","id":-1,"content":"??","date":"2024-06-14T19:18:58.068Z"}## | | | | |
| תפקיד הבקשה | | לכתוב תגובה לפוסט קיים | | | | |
| תיאור פרמטרים | | **שם** | **הסבר** | | | |
| glit\_id | הID של המשתמש שאליו מופנת התגובה | | | |
| user\_id | הID של כותב התגובה | | | |
| publisher\_screen\_name | השם של המשתמש אשר מפרסם את הלייק | | | |
| id | תמיד -1 ולא משנה גם אם יהיה מספר אחר | | | |
|  | | content | תוכן התגובה | | | |
|  | | date | תאריך פרסום הפוסט | | | |
| איך נראית התגובה | | 655#Comment publish approved{gli&&er}{"glit\_id":41499,"user\_id":40995,"user\_screen\_name":"Ido ben zaken","id":12859,"date":"2024-06-14T19:18:58.068Z","content":"??"}## | | | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | | |
|  | | | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| פרסום תגובה בשם משתמש אחר | | | **Spoofing** | **לא הצליח** |
| שינוי הglit id וכך לכתוב תגובות לכל משתמש שרוצים גם אם הוא פרטי | | | **Tampring** | **הצליח** |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |

**נק כניסה חמישית**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | | | | |
| **מספר הבקשה** | | **410** | | | | |
| **שם הבקשה בעברית** | | **שליחת בקשה חברות** | | | | |
| דוגמא אמיתית | | 410#{gli&&er}[41678,3376]## | | | | |
| תפקיד הבקשה | | לשלוח בקשת חברות למשתמש | | | | |
| תיאור פרמטרים | | **שם** | **הסבר** | | | |
| המקום הראשון בסוגריים המרובעות | הID של המשתמש שיזם את שליחת בקשת החברות | | | |
| המקום השני בסוגריים המרובעות | הID של מקבל בקשת החברות | | | |
| איך נראית התגובה | | 415#Glance request is valid. A notification was sent to the user on session: USER\_NOT\_LOGGED\_ON\_WEBSITE{gli&&er}3376## | | | | |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | | | |
|  | | | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| התחזות למישהו שליחת בקשת חברות | | | **Spoofing** | **לא הצליח** |
| שליחת בקשת חברות וגם אישורה מאותו משתמש | | | **Tampring** | **הצליח** |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |

**נק כניסה שישית – לא הצליחה**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **מחקר נק' כניסה** | | | | | | |
| **מספר הבקשה** | | **200** | | | | |
| **שם הבקשה בעברית** | | **יציאה מהמערכת** | | | | |
| דוגמא אמיתית | | 200#{gli&&er}41678## | | | | |
| תפקיד הבקשה | | להתנתק מהמערכת | | | | |
| תיאור פרמטרים | | **שם** | **הסבר** | | | |
| המקום הראשון לאחר הסוגריים של הגליטר | הID של המשתמש שיזם את היציאה מהמערכת | | | |
| 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** |
| הוצאת מישהו מהמערכת | | | **Tampring** | **לא הצליח** |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |
|  | | | Choose an item. |  |