**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 | לא הבנתי את ההבדל בין זה לשאלה הבאה |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | Num#{gli&&er}{"key":"value"}##  Num = מספר תלת ספרתי שספרת היחידות שלו היא 0 |
| פורמט כללי של תגובה | NUM#message{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** |
| אפשר לתת אינסוף לייקים | לתת לעצמו הרבה לייקים בלי צורך בהרבה פרופילים | **כן** | לשמור ממי ניתן כל לייק ואם מישהו מנסה לשלוח לייק עוד הפעם – לא לתת לו |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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** | **מוסיפה לייק** | |
| דוגמא אמיתית | 710#{gli&&er}{"glit\_id":17497,"user\_id":4291,"user\_screen\_name":"Eitan Turpaz","id":-1}## | |
| תפקיד הבקשה | להוסיף לייק לאיזשהו פוסט | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***Glit\_id*** | הID של הפוסט שרוצים לעשות לו לייק |
| ***User\_id*** | הID של המשתמש שנותן את הלייק |
| ***User\_screen\_name*** | השם של המשתמש שנותן את הלייק |
| ***Id*** | הID של נתינת הלייק או משהו, תמיד -1 |
|  |  |
|  |  |
|  |  |
|  |  |
| איך נראית התגובה | 715#Like publish approved{gli&&er}{"glit\_id":17497,"user\_id":4291,"user\_screen\_name":"Eitan Turpaz","id":107716,"date":"2021-06-30T20:43:53.062Z"}## | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| העברת ערך קטן מ1 בglit\_id או user\_id או העברת סוג משתנה לא נכון או כל דבר שקשור למבנה הבקשה בפרמטרים | **Tampring** | **לא הצליח** |
| העברת אקסטרה פרמטרים | **Tampring** | **לא הצליח** |
| העברת user\_id שונה מזה שאיתו התחברנו | **Spoofing** | **לא הצליח** |
| העברת user\_screen\_name שלא קשור לuser\_id (אם זה משנה בכלל) | **Spoofing** | **הצליח** |
| העברת מערך במקום מילון | **Tampring** | **לא הצליח** |
|  | Choose an item. |  |