**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 |  |
| פורט |  |
| מאפייני פרוטוקול |  |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) |  |
| פורמט כללי של תגובה |  |

**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** |  | |
| **שם הבקשה בעברית** |  | |
| דוגמא אמיתית |  | |
| תפקיד הבקשה |  | |
| תיאור פרמטרים | **שם** | **הסבר** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| איך נראית התגובה |  | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |