**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 | http |
| פורט | 80 |
| מאפייני פרוטוקול | User\_id, user\_screen\_name, id, publisher\_avatar |
| פורמט **כללי** של בקשה (לא בקשה ספציפית!) | GET >> Headers POST >> Headers >> Data |
| פורמט כללי של תגובה | 200 OK // 500 ERROR |

**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 לשלוח את הפקטה של הלייקים שוב ושוב כמה שרוצים ומספר הלייקים לאותו פוסט יגדל כל הזמן עד שנפסיק לשלוח | כמות לייקים אין סופית | **כן** | לבדוק באותו פוסט אם user id שמנסה לעשות לייק קיים כבר אז לא לתת לו לעשות עוד לייקים |
| כאשר אנו שולחים פוסט מופיע באחד מן השדות את צבע הפוסט בצד של הלקוח | אפשר לשנות את צבע הפוסט לאיזה צבע שנבחר גם אם הוא לא הופיע בפלטת הצבעים שבאתר | **כן** | לבדוק שאכן הצבע של הפוסט הוא אחד מתוך שמונת הצבעים ואם לא תופיע הודעת שגיאה |
| כאשר אנו שולחים פוסט מופיע באחד מן השדות את צבע הכתב בצד של הלקוח | ניתן לשנות את צבע הכתב לאיזה צבע שנבחר למרות שאין אפשרות כזאת באתר והצבע אמור להיות תמיד שחור | **כן** | לבדוק באתר שהכתב של הפוסט הוא תמיד שחור וכאשר מישהו ירשום כתב אחר יופיע שגיאה |
| שאנחנו שולחים פוסט או תגובה באחד מן השדות ניתן לראות את התאריך | התוקף יכול לשנות את התאריך לאיזה תאריך שבא לו | **כן** | לבדוק שהתאריך הוא של היום לפני שהאתר מעלה את הפוסט סופית |
| כאשר מעלים פוסט אז באחד משדות ההודעה מופיע את שם התמונה | התוקף יכול לשנות את התמונה שלו וכך להתחזות למישהו אחר | **כן** | להוריד את החלק הזה מתוך ההודעה ולדאוג שלא יהיו leaks ככה לא יוכלו לשנות זאת |
| כשאנחנו טוענים פוסטים חדשים  אז יש שדה של בעל הפיד | התוקף יכול לשנות את האיידי ולטעון פוסטים של מישהו אחר | **כן** | להעלים את זה מהצד של המשתמש ולוודא שהפוסטים הם של אותו משתמש שביקש אותם |
| כשטוענים פוסטים חדשים יש שדה של מספר הפוסטים | התוקף יכול טעון כמה פוסטים שהוא רוצה שנוגד את הרצונות של האתר | **כן** | לעשות מנגנון שלא נותן לעלות יותר מ – 2 פוסטים בפעם אחת ולנסות להוריד את זה מהצד של הלקוח |
| כאשר מעלים פוסט אז אפשר לראות את השדה עם תוכן ההודעה | התוקף יכול להעלות את תוכן הפוסט איך שבא לו בלי סינון של שפה לא נהותה לדוגמא ובנוסף הוא יכול לעשות קרוס סייט סכריפטינג ולעלות קישורים תוכן מודגש (בולד) | **כן** | צריך לחסום אפשרות של קרוס סייט סקריפטינג ובנוסף להוסיף בוט שיעבור על כל הפוסטים שנגיד עלו כל החצי שעה האחרונה והוא יבדוק אם יש פוסטים עם שפה לא נהותה ויוריד אותם |
| עשיתי את אתגר הקוקי וגיליתי שיש נוסחה שאפשר להשתמש בה בשביל לעשות זאת | התוקף יכול לקחת רק את השם של הבן אדם ולגלות עליו את הקוקי וזה מפחיד כי הוא יכול לעשות עם זה המון דברים | **כן** | להצפין בצורה יותר טובה את הקוקי |

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** | **200** | |
| **שם הבקשה בעברית** | **להעלות פוסט** | |
| דוגמא אמיתית | GET http://cyber.glitter.org.il/glit?id=1-&feed\_owner\_id=240&publisher\_id=240&publisher\_screen\_name=admin&publisher\_avatar=im8&background\_color=Gold&date=2022-06-06T14:01:17.157Z &content=%D7%9C%D7%9D%D7%9C%D7%9D&font\_color=black HTTP/1.1 | |
| תפקיד הבקשה | העלת פוסט | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***id*** | אישור הודעה של האתר |
| ***Feed\_owner\_id*** | המספר המזהה של מי שדף זה שייך לו |
| ***Publisher\_id*** | המספר המזהה של מפרסם ההודעה |
| ***Publisher\_screen\_name*** | השם שמוצג לכולם בתור מפרסם ההודעה |
| ***Publisher\_avatar*** | התמונה של מפרסם ההודעה |
| ***Background\_color*** | הצבע של הפוסט |
| ***date*** | התאריך של הפוסט |
| ***Font\_color*** | צבע הכתב בפוסט |
| איך נראית התגובה | 200 OK | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| **Id - למחוק** | **Information Disclosure** | **לא הצליח** |
| ***Feed\_owner\_id של מישהו אחר*** | **Spoofing** | **הצליח** |
| ***Publisher\_id של מישהו אחר*** | **Spoofing** | **הצליח** |
| ***Publisher\_screen\_name של מישהו רנדומלי*** | **Spoofing** | **הצליח** |
| ***Publisher\_avatar – לשנות את התמונה*** | **Information Disclosure** | **הצליח** |
| ***Background\_color שונה ממה שקיים בפלטת הצבעים*** | **Tampring** | **הצליח** |
| ***Date שונה מהיום - לדוגמה לפני מאה שנה*** | **Tampring** | **הצליח** |
| ***Font\_color שונה משחור*** | **Tampring** | **הצליח** |

|  |  |  |
| --- | --- | --- |
| **מחקר נק' כניסה** | | |
| **מספר הבקשה** | **200** | |
| **שם הבקשה בעברית** | **לייק** | |
| דוגמא אמיתית | POST http://cyber.glitter.org.il/likes/ HTTP/1.1  "}glit\_id":35102,"user\_id":240,"user\_screen\_name":"admin","id":-1{ | |
| תפקיד הבקשה | לעשות לייק | |
| תיאור פרמטרים | **שם** | **הסבר** |
| ***Glit\_id*** | מספר מזהה של הפוסט |
| ***User\_id*** | מספר מזהה של המשתמש שנותן לייק |
| ***User\_screen\_name*** | שם של מי שנותן לייק |
| ***id*** | אישור של האתר |
| איך נראית התגובה | 200 OK | |

|  |  |  |
| --- | --- | --- |
| **תרחישי תקיפה לנק' כניסה**  תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה | | |
|  | **סוג חולשה  (STRIDE)** | **הצליח /**  **לא הצליח** |
| **Id - למחוק** | **Information Disclosure** | **לא הצליח** |
| ***Glit\_id – לשנות לאחד אחר*** | **Tampring** | **הצליח** |
| ***User\_id של מישהו אחר*** | **Spoofing** | **לא הצליח** |
| ***User\_screen\_name של מישהו אחר*** | **Spoofing** | **לא הצליח** |