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 TCP/UDP	TCP
פורט	1336
מאפייני פרוטוקול	טקסטואלי, Stateful
פורמט **כללי** של בקשה (לא בקשה ספציפית!)	<NUMBER>#{gli&&er}{"data":value,"data",value}##
פורמט כללי של תגובה	<NUMBER>#Command name{gli&&er}{"data":value,"data",value}##

קראו למדריכ/ה לפני שאתם ממשיכים לשלב הבא!

2. 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**
מציאת כתובת מייל לפי שם משתמש	לגלות אימייל של משתמש ולפרוץ לו.	**כן**	שכשאשר מחפשים שם של מישהו, שהמייל לא יוצג שם, לפי דעתי זה גם לא שימושי.
מציאת סיסמא לפי שם משתמש	לגלות את הסיסמא ובעצם לגשת לחשבון הפרטי של המשתמש	**כן**	שהתוכנה תבדוק שהסיסמא שהוזנה תואמת לסיסמא של המשתמש ולא רק הצ'אקסם תואם. או שפשוט לא תחזיר את הצ'אקסם כאשר הסיסמא שגויה.
הוספת יותר מלייק אחד	להשיג הרבה לייקים ובכך להפוך למפורסם, או לתת לאנשים לייקים בתמורה לתשלום	**כן**	שלפני שמוסיפים לייק לבדוק אם המשתמש הזה כבר עשה לייק לפוסט
פרסום גליט בעבר	לפרסם על מישהו משהו שכאילו הוא אמר בעבר ולדפוק לו את החיים	**כן**	לבדוק את התאריך שהוא שווה לשל עכשיו
פרסום גליט עם צבע רקע שלא קיים	למכור לאנשים את האפשרות לפרסם גליט בצבע שלא קיים ובכך להפוך ל"נדירים"	**כן**	לוודא שהצבע נמצא ברשימת הצבעים האפשרית
יצירת משתמש עם קוד שקטן מ5 תווים	לא חושב שיש לו איך לנצל את זה	**כן**	לוודא שהקוד מתאים ל5 תווים
יצירת משתמש עם שם משתמש שארוך מההגבלה	יכול ליצור משתמש עם שם ארוך מאוד ולגרום לקריסת התוכנה	**כן**	לוודא שהאורך של השם לא ארוך מהמגבלה
יצירת שם משתמש עם שם שארוך מההגבלה	יכול ליצור משתמש עם שם ארוך מאוד ולגרום לקריסת התוכנה	**כן**	לוודא שהאורך של השם לא ארוך מהמגבלה

פרסום תגובה ללא שם	יכול לפרסם תגובות כאנונימי	**כן**	לוודא שיש שם לתגובה לפני שהיא מתפרסמת

3. 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 – גניבת כתובת מייל		
מספר הבקשה	**300**	
שם הבקשה בעברית	**חיפוש**	
דוגמא אמיתית	300#{glit&&er}{"search_type":SIMPLE, "search_entry":"dsadas"}	
תפקיד הבקשה	לחפש משתמש בחיפוש האפליקציה	
תיאור פרמטרים	**שם**	**הסבר**
	Search_type	סוג החיפוש
	Search_entry	שם הבן אדם אותו מחפשים (לא חייב להיות מדוייק)
איך נראית התגובה	305#Entities search result{gli&&er}[{"screen_name":"dadsasdsadasd","avatar":"im1","description":"dsadsa","privacy":"Public","id":2219,"mail":"dsadasd@gmail.com"},{"screen_name":"dsadsadasd","avatar":"im1","description":"dsadadasd","privacy":"Public","id":2243,"mail":"dsadsa@gmail.com"},{"screen_name":"dsadas","avatar":"im1","description":"asdasdf","privacy":"Public","id":7648,"mail":"asdas@gmail.com"}]##	

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**

חיפוש משתמש פרטי (Private)	**Tampring**	**הצליח**
שימוש בsearch_type שלא קיים	**Tampring**	**לא הצליח**
קבלת מייל למשתמש	**Information Disclosure**	**הצליח**

מחקר נק' כניסה – גניבת סיסמא		
מספר הבקשה	**100 + 110**	
שם הבקשה בעברית	**100 – ביצוע התחברות לשרת** **110 – שליחת הצ'אקסם**	
דוגמא אמיתית	100#{gli&&er}{"user_name":"admin_","password":"a","enable_push_notifications":true}## 110#{gli&&er}1658	
תפקיד הבקשה	100 – לבצע התחברות לשרת 110 – לשלוח את "אתגר" האבטחה (צ'אקסם)	
תיאור פרמטרים	**שם**	**הסבר**
	User_name	שם המשתמש
	Password	הסיסמא, לא חייבת להיות אמיתית (זה רק לביצוע הפעולה)
	Enable_push_notifications	לאפשר שליחת התראות / לא לאפשר
איך נראית התגובה	108#Illegal user login. Provided details do not match ascii checksum: 1658{gli&&er}{"type":"User Notification","header":"Login Failure","description":"Password doesn't match","userRecommendation":"Verify the provided password"}## 115#Authentication approved{gli&&er}{"screen_name":"admin_admin","avatar":"im2","description":"admin","privacy":"Public","id":10099,"user_name":"admin_","password":"adminadmin","gender":"Male","mail":"admin@gmail.com","date":"2022-06-21T11:56:17.927Z"}##	

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**
השגת סיסמא לפי שם משתמש	**Information Disclosure**	**הצליח**
השגת כל המידע על המשתמש בעזרת שם משתמש	**Information Disclosure**	**הצליח**

מחקר נק' כניסה – הוספת יותר מלייק אחד		
מספר הבקשה	**710**	
שם הבקשה בעברית	**הוספת לייק**	
דוגמא אמיתית	710#{gli&&er}{"glit_id":56558,"user_id":10099,"user_screen_name":"admin_admin","id":-1}##	
תפקיד הבקשה	להוסיף לייק לגליט	
תיאור פרמטרים	**שם**	**הסבר**
	Glit_id	האיידי של הגליט
	User_id	האיידי של המשתמש שמוסיף את הלייק
	User_screen_name	השם של המשתמש שמוסיף את הלייג
	id	המזהה של הגליט (-1)
איך נראית התגובה	715#Like publish approved{gli&&er}{"glit_id":56558,"user_id":10099,"user_screen_name":"admin_admin","id":486441,"date":"2022-07-02T18:41:20.798Z"}##	

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**

ביצוע לייק לגליט אחד יותר מפעם אחת	**Other**	**הצליח**
השרת מחזיר את ה-ID של ה-GLIT שהתווסף	**Information Disclosure**	**הצליח**

מחקר נק' כניסה – פרסום גליט בעבר		
מספר הבקשה	**550**	
שם הבקשה בעברית	**פרסום גליט**	
דוגמא אמיתית	550#{gli&&er}{"feed_owner_id":10099, "publisher_id":10099, "publisher_screen_name":"Ido's Program", "publisher_avatar":"im2","background_color":"Red","date":"2006-01-05T01:23:45.67Z","content":"A past message :)","font_color":"black","id":-1}##	
תפקיד הבקשה	להעלות גליט	
תיאור פרמטרים	**שם**	**הסבר**
	Feed_owner_id	האיידי של החשבון של הגליט
	Publisher_id	האיידי של המשתמש שמעלה את הגליט
	Publisher_screen_name	השם של המשתמש שמעלה את הגליט
	Publisher_avatar	התמונה של המפרסם
	Background_color	צבע רקע הגליט
	date	תאריך פרסום הגליט
	content	תוכן הגליט
	Font_color	צבע הגליט
	Id	המזהה של הגליט (-1)

איך נראית התגובה	555#Glit publish approved{gli&&er}{"feed_owner_id":10099,"publisher_id":10099,"publisher_screen_name":"Ido's Program","publisher_avatar":"im2","background_color":"Red","date":"2006-01-05T01:23:45.67Z","content":"A past message :)","font_color":"black","id":56602}##

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**
פרסום גליט בלי תאריך 00/00/0000	**Tampring**	**הצליח**
פרסום גליט בעבר	**Tampring**	**הצליח**

מחקר נק' כניסה – פרסום גליט עם צבע רקע אחר		
מספר הבקשה	**550**	
שם הבקשה בעברית	**פרסום גליט**	
דוגמא אמיתית	550#{gli&&er}{"feed_owner_id":10099, "publisher_id":10099, "publisher_screen_name":"Ido's Program", "publisher_avatar":"im2","background_color":"#92FF08","date":"2022-07-02T19:11:38.562Z","content":"What that color is ???","font_color":"black","id":-1}##	
תפקיד הבקשה	להעלות גליט	
תיאור פרמטרים	**שם**	**הסבר**
	Feed_owner_id	האיידי של החשבון של הגליט
	Publisher_id	האיידי של המשתמש שמעלה את הגליט
	Publisher_screen_name	השם של המשתמש שמעלה את הגליט
	Publisher_avatar	התמונה של המפרסם

	Background_color	צבע רקע הגליט
	date	תאריך פרסום הגליט
	content	תוכן הגליט
	Font_color	צבע הגליט
	Id	המזהה של הגליט (-1)
איך נראית התגובה	555#Glit publish approved{gli&&er}{"feed_owner_id":10099,"publisher_id":10099,"publisher_screen_name":"Ido's Program","publisher_avatar":"im2","background_color":"#92FF08","date":"2022-07-02T19:11:38.562Z","content":"What that color is ???","font_color":"black","id":56605}##	

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**
פרסום גליט עם צבע שלא קיים	**Tampring**	**הצליח**
פרסום גליט בלי צבע	**Tampring**	**הצליח**

מחקר נק' כניסה – יצירת משתמש עם קוד שקטן מ5 תווים		
מספר הבקשה	**105**	
שם הבקשה בעברית	**יצירת משתמש**	
דוגמא אמיתית	150#{gli&&er}{"registration_code":"123","user":{"screen_name":"D42RS4HLOP","avatar":"im2","description":"ddddd","privacy":"Public","id":-1,"user_name":"D42RS4HLOP","password":"123456","gender":"Male","mail":"idoo@ido.com"}}##	
תפקיד הבקשה	ליצור משתמש חדש	
תיאור פרמטרים	**שם**	**הסבר**

	Registration_code	הקוד של הרגיסטר
	user	פרטי החשבון, שם משתמש סיסמא אימייל וכו
איך נראית התגובה	155#User registration approved{gli&&er}{"screen_name":"CRDUPXX5W2","avatar":"im2","description":"ddddd","privacy":"Public","id":11964,"user_name":"CRDUPXX5W2","password":"123456","gender":"Male","mail":"idoo@ido.com"}##	

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**
יצירת חשבון עם קוד קטן	**Other**	**הצליח**

מחקר נק' כניסה – יצירת משתמש עם שם משתמש ארוך		
מספר הבקשה	**105**	
שם הבקשה בעברית	**יצירת משתמש**	
דוגמא אמיתית	150#{gli&&er}{"registration_code":"123456","user":{"screen_name":"2Z8V1T8JMC0B7HSRDK9P0TT672JQILPHSHSO1Q6E2IM27N4JTF56DCVF31T9LIB3BED94IV0IQFN8HQ5XD5UPBULT7NILA6FN0EF","avatar":"im2","description":"ddddd","privacy":"Public","id":-1,"user_name":"2O1WO","password":"123456","gender":"Male","mail":"idoo@ido.com"}}##	
תפקיד הבקשה	ליצור משתמש חדש	
תיאור פרמטרים	**שם**	**הסבר**
	Registration_code	הקוד של הרגיסטר
	user	פרטי החשבון, שם משתמש סיסמא אימייל וכו
איך נראית התגובה	155#User registration approved{gli&&er}{"screen_name":"2Z8V1T8JMC0B7HSRDK9P0TT672JQILPHSHSO1Q6E2IM27N4JTF56DCVF31T9LIB3BED94IV0IQFN8HQ5XD5UPBULT7NILA6FN0EF","avatar":"im2","description":"ddddd"	

	,"privacy":"Public","id":11968,"user_name":"2O1WO","password":"123456","gender":"Male","mail":"idoo@ido.com"}##

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**
יצירת חשבון עם שם משתמש ארוך מהמגבלה	**Other**	**הצליח**

מחקר נק' כניסה – יצירת משתמש עם שם ארוך		
מספר הבקשה	**105**	
שם הבקשה בעברית	**יצירת משתמש**	
דוגמא אמיתית	150#{gli&&er}{"registration_code":"123456","user":{"screen_name":"Idoooo","avatar":"im2","description":"ddddd","privacy":"Public","id":-1,"user_name":"3YV8P204D25XTQQSQ7MQ1WYDS3HRQ9JBAJI7VZRVG6W9EKFY1I6OEZITVHVV8PGX1X8S1JJZZMUI9BXZAKU44RPJS7AYCUXQ0YMQ","password":"123456","gender":"Male","mail":"idoo@ido.com"}}##	
תפקיד הבקשה	ליצור משתמש חדש	
תיאור פרמטרים	**שם**	**הסבר**
	Registration_code	הקוד של הרגיסטר
	user	פרטי החשבון, שם משתמש סיסמא אימייל וכו
איך נראית התגובה	155#User registration approved{gli&&er}{"screen_name":"Idoooo","avatar":"im2","description":"ddddd","privacy":"Public","id":11972,"user_name":"3YV8P204D25XTQQSQ7MQ1WYDS3HRQ9JBAJI7VZRVG6W9EKFY1I6OEZITVHVV8PGX1X8S1JJZZMUI9BXZAKU44RPJS7AYCUXQ0YMQ","password":"123456","gender":"Male","mail":"idoo@ido.com"}##	

תרחישי תקיפה לנק' כניסה תרחישים הקשורים לפרמטר ספציפי או לעצם הבקשה		
	סוג חולשה (STRIDE)	**הצליח / לא הצליח**
יצירת חשבון עם שם חשבון ארוך מהמגבלה	**Other**	**הצליח**