Dor Erlich 19.05.2024

CybErlich

SQL Injection

CyberSecurity Analyst
Incident Responder
SIEM Content Developer
Python Developer

Companies I worked with:

See Secure consulting
Citadel
TripleP (CyCube.io)
Pagaya Technologies
MyHeritage

SIEM:
Azure Sentinel
Splunk
Qradar
FortiSiem
McAfee ESM

CrowdStrike, AWS, Perception Point, Symantec DLP, End-Point Protector, Wiz, Ermetic, etc

SQL Injection

מתקפת SQL Injection היא תקיפה בה התוקף מנצל פרצה באפליקציה\אתר הקורבן בכדי להזריק קוד SQL על מנת למשוך מידע, לשנות מידע, למחוק מידע וכדומה

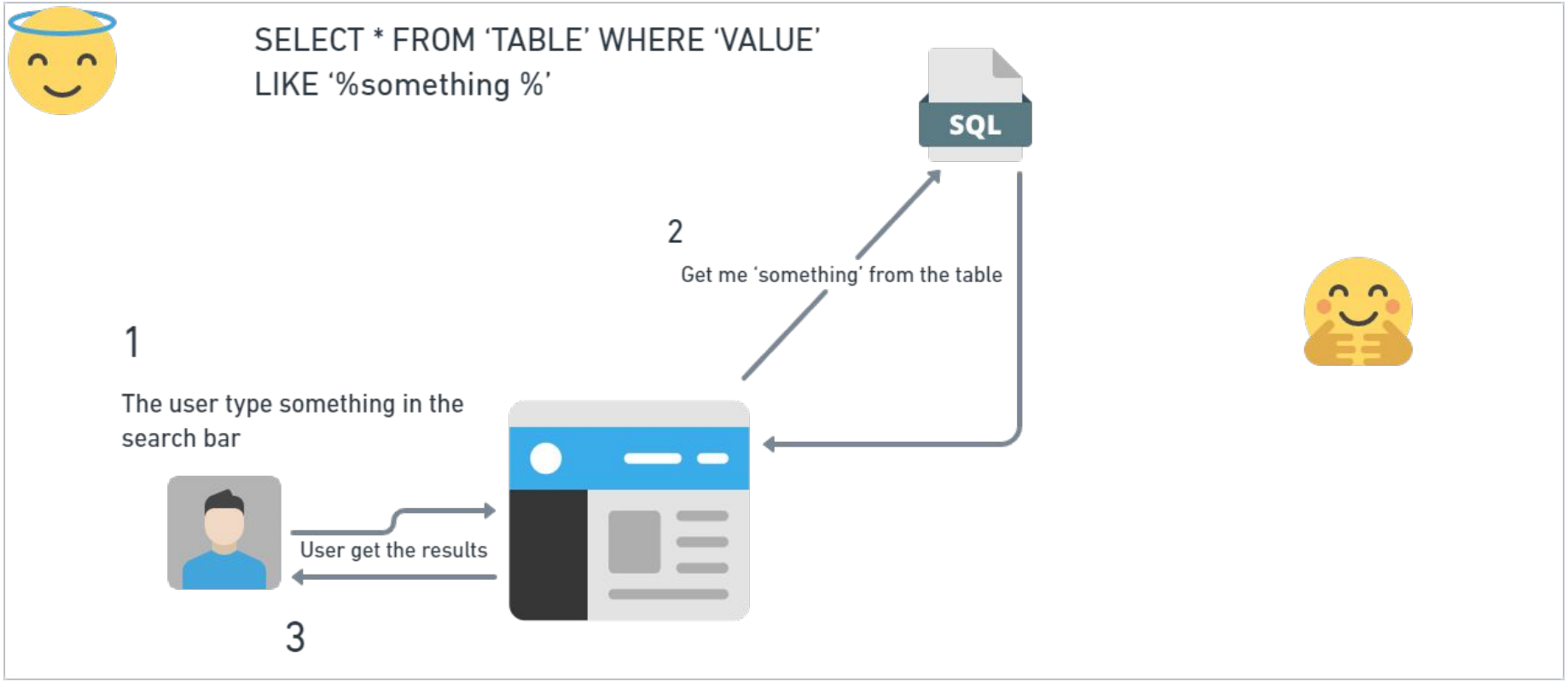
בדרך כלל, הזרקות קוד יתבצעו כאשר האתר מאפשר למשתמשים להכניס INPUT כלשהו, כדי לקבל תוצאות (כמו במקרה של חיפוש מוצר וכדומה)
דוגמא נפוצה שקיימת, המשתנה שאליו הלקוח כותב יהיה מוקף בגרש (')‚ התוקף יוצא מנקודת הנחה זו, מכניס גרש לתוך המשתנה, שהמשמעות הלוגית שלו היא סיום הערך שהוכנס בINPUT (שמשם ואילך נכתב קוד), מכניס את הקוד שברצונו להזריק, ומסיים עם – או # כדי להשאיר את שאר הקוד המקורי שנכתב כהערה ולא כקוד עם משמעות לוגית

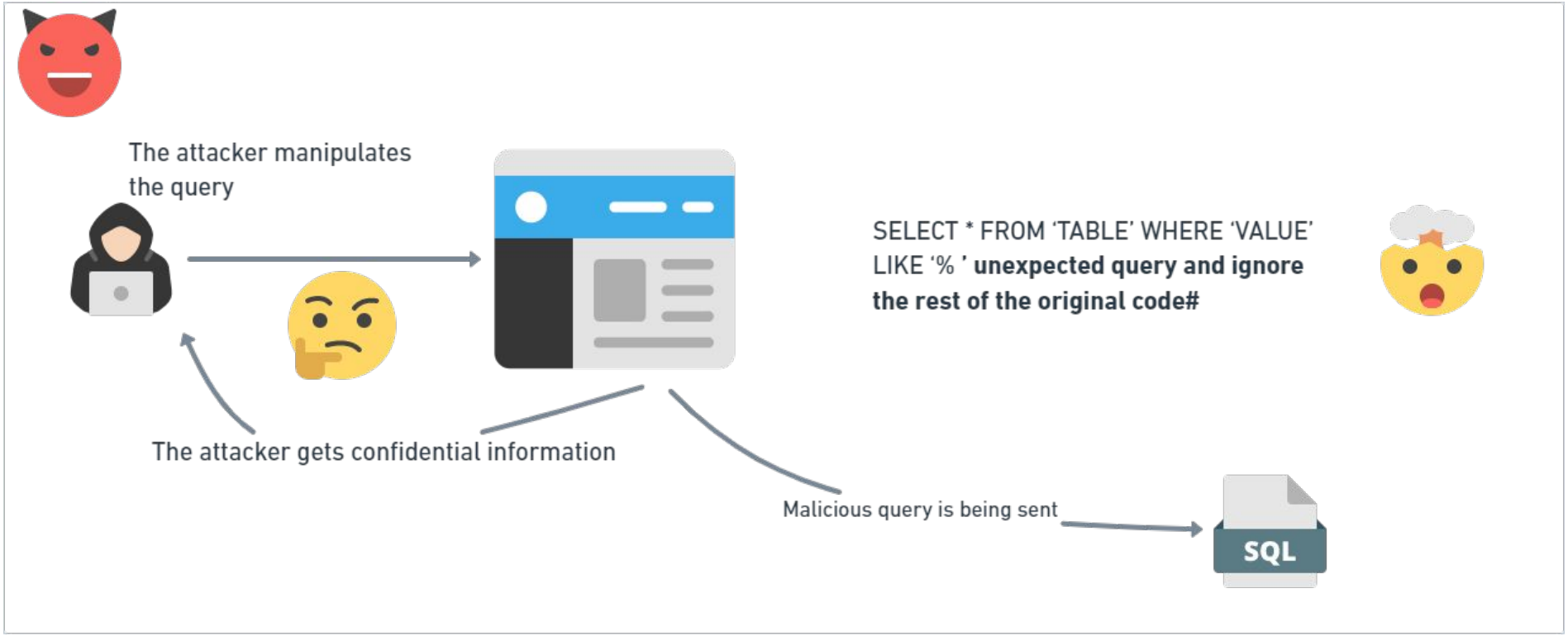
לדוגמא,

SELECT * FROM ‘MOVIES’ WHERE ‘NAME’ LIKE ‘%**INPUT**%’

התוקף יכול לכתוב ב Input קוד כדי לשאוב מידע רגיש לדוגמא שימוש בUnion

‘ union select username, password, id from users #


SELECT * FROM 'TABLE' WHERE 'VALUE'
LIKE '%something %'
SQL
2
Get me 'something' from the table
1
The user type something in the search bar
User get the results
3


The attacker manipulates the query
SELECT * FROM 'TABLE' WHERE 'VALUE' LIKE '% ' unexpected query and ignore the rest of the original code#
The attacker gets confidential information
Malicious query is being sent
SQL

דרכי התגוננות

WAF

מערכת זיהוי וחסימה של מתקפות רשת

Input validation

החלפה אוטומטית של תווים כדי לשלול מהם את המשמעות הלוגית

Least privileges principle

הגבלת שימוש של יוזרים לטבלה ספציפית

Data masking

הגבלת תגובה שלילית ל'אין תוצאות' - לא להראות שגיאות מערכת