HTTP

6:37 PM Wednesday, July 3, 2024

(HTTP) Hypertext Transfer Protocol - הוא פרוטוקול תקשורת שנועד להעברת דפי HTML ואובייקטים כגון תמונות, קבצי קול, סרטונים וכ'ו... הפרוטוקול פועל בשכבת האפליקציה של מודל הOSI וIP/TCP (מודלים שמייצג את הדרך בהעברת הנתונים באינטרנט).

כיצד נוצרת התקשורת בHTTP? - התקשורת בHTTP נוצרת בין יצירת קשר בין צד השרת לצד הלקוח, באמצעות פרוטוקול UDP/TCP (TCP- העברת מידע באמצעות יצירת חיבור מקושר, משמע באשר נרצה לקבל מידע במלואו וללא טעויות משתמש בTCP לעומת UDP- פרוטוקול connectionless שאינו מצריך שכל המידע יגיע במלואו על מנת לא ליצור עיכובים, לדוגמא שיחות וידאו או ערוצי סטרימינג).

ראשית הלקוח יוצר חיבור לכתובת ה-IP ולפורט בו נמצא השרת, לאחר מכן נשלחת בקשה הכוללת את הכתובת של אובייקט המבוקש (כגון דף html) ופרטים נוספים על הבקשה והלקוח. השרת קורא את הבקשה מפענח אותה שול ללקוח תשובה בהתאם ומנתק את החיבור ללקוח בשהשליחה הסתיימה, או משאיר אותו פתוח לבקשות נוספות.

פרוטוקול HTTP הוא stateless protocol משמע, שכל בקשה עובדת בפני עצמה כך שבקשה קודמת שבוצעה איננה משפיעה על הבקשה הבאה שתבוצע. על מנת ליצור תקשורת בין הלקוח לשרת שמבוסס על היסטורית הבקשות בין השרת ללקוח נעשה שימוש בcookies. ברגע שאנו רוצים שהמשתמש לא ירצה בכל פעם שנכנס לאתר להקליד את הסיסמא, נעשה שימוש בcookies.

https הוא הפרוטוקול המאובטח של http - הוא מוסיף לדפדפן שכבת הצפנה כדי להגן על המידע המועבר בו, הhttps משמש בעיקר לפעולות של העברת כספים, העברת דואר אלקטרוני העברת מידע רגיש, אבטחה לחשבונות המשתמש, תקשורת בין משתמשים, זהות המשתמש והמידע המאוחסן עליו ועל ידו בשרתים.
חשוב להשתמש בhttps ברשתות לא מוצפנות משום שמשתמשים יכולים לבצע sniffing (לבדוק את המידע המועבר ברשת באמצעות כלים כמו wireshark,nmap וכו...) ולגלות מידע רגיש שנשלח ברשת .

שיטות בקשה בHTTP:

1. GET:
- משמש לקבלת או קריאת נתונים מהשרת.
- הפרמטרים של הבקשה נשלחים בתוך הURL כמחרוזת שאילתה.
- בקשות GET צריכות להיות Idempotency, כלומר בקשות חוזרות לא צריכות לשנות את מצב המשאב בשרת.

2. POST:
- משמש ליצירת משאבים חדשים בשרת.
- הנתונים של הבקשה נשלחים בגוף הבקשה, לא ב-URL.
- בקשות POST אינן Idempotency, כלומר בקשות חוזרות עשויות ליצור משאבים כפולים או לבצע פעולות מרובות.

3. PUT:
- משמש לעדכון משאב קיים בשרת או ליצירת משאב חדש אם הוא לא קיים.
- הנתונים של הבקשה נשלחים בגוף הבקשה.
- בקשות PUT הן Idempotency, כלומר בקשות חוזרות לא ישנו את מצב המשאב מעבר לבקשה הראשונית.
- אם המשאב לא קיים, PUT יכול ליצור אותו עם המזהה (ID) שסופק על ידי הלקוח.

4. PATCH:
- משמש לעדכון חלקי של משאב קיים בשרת.
- הנתונים של הבקשה נשלחים בגוף הבקשה, המכיל רק את השינויים שיש לבצע.
- בקשות PATCH אינן Idempotency, מכיוון שבקשות חוזרות משנות את המשאב בכל פעם.

5. DELETE:
- משמש למחיקת משאב קיים מהשרת.
- המזהה (ID) של המשאב שיש למחוק נשלח בדרך כלל כחלק מה-URL.
- בקשות DELETE הן Idempotency, כלומר בקשות חוזרות לא ישנו את מצב השרת מעבר לבקשה הראשונית.

- Uniform resource locator (URL)

זוהי כתובת מיוחדת לכל משאב שיש באינטרנט (כגון דפי HTML, CSS, תמונות וכ'ו...), הURL מחולק לכמה חלקים, כמה מהם הכרחיים וכמה אופציונליים.

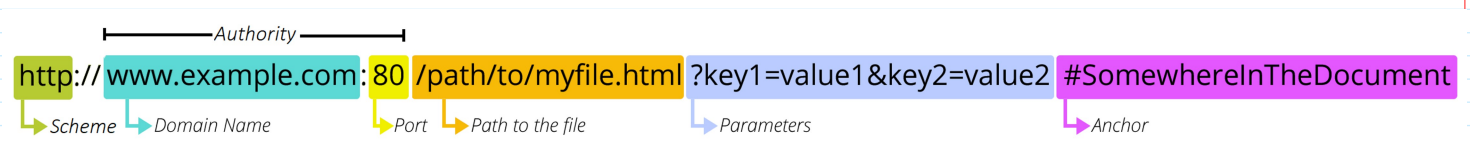
- Scheme
החלק הראשון של הURL זה הScheme ובו מצוין הפרוטוקול שהאתר משתמש בו. (http/https)

- Authority
החלק השני של הURL מופרד על ידי //: והוא מראה את הdomain name והport בו האתר משתמש מופרדים ב:
הdomain name מסמל על Web Server המבוקש, ובעוד כי הפורט מסמל באיזה "שער" השתמשנו על מנת לגשת למשאבים של השרת.

- Path to resource
על מנת לגשת למשאבים בWeb Server הURL משתמש בדרכים (PATH) בהם שמורים הקבצים הפיזיים בשרת.

- Parameters
פרמטרים מועברים ב-URL כדי להעביר נתונים נוספים לשרת כחלק מהבקשה.
הם מופרדים מכתובת ה-URL הבסיסית באמצעות סימן שאלה (?) ומוגדרים כזוגות המופרדים באמצעות סימן (&).
פרמטרים משמשים בדרך כלל להעברת נתוני שאילתה, פרמטרים של הדף ועוד.

- Anchor
Anchor משמשים לניווט בתוך דף אינטרנט ספציפי ולא מועברים לשרת כחלק מהבקשה.
הם מצוינים באמצעות סימן סולמית (#).
עוגנים שימושיים לקישור לחלקים ספציפיים של דף, כגון כותרות, פסקאות או רכיבים מסוימים
העוגנים מעובדים בצד הלקוח ואינם נשלחים לשרת כחלק מהבקשה.



סוגי שיטות בהן אפשר לפרוץ\לדלות מידע מאתר אינטרנט במידה והוא לא מאובטח מספיק -

- IDOR
מתן גישה לנתונים אישיים או מעבר לדפים שלמשתמש אין רשות להגיע אליהם באמצעות כתובת הURL.
לדוגמה, אם URL מכיל מזהה משתמש כמו https://example.com/userprofile?id=123, תוקף עשוי לנסות לשנות את ה-id כדי לגשת לפרופילים של משתמשים אחרים.

- File Inclusion
מתן גישה לתוקף לכלול ולהריץ קבצים (זדוניים) בשרת או לגשת לקבציים סודיים בשרת באמצעות כתובת הURL.

- SSRF (Server-Side Request Forgery)
גישה למשאבים פנימיים בשרת באמצעות פקודות HTTP.

- SQL Injection
התוקף יכול להזריק קטעי קוד SQL זדוניים שישנו את הלוגיקה של השאילתה המקורית, מה שיאפשר לו לעקוף אימות, לשנות נתונים או לחשוף מידע רגיש ממסד הנתונים.