Web Basics 1

Web Server

- المواقع عباره عن شوية ملفات مرفوعه علي جهاز اسمه Server وكل سيرفر ليه ip وكل ip بيكون مربوط ب Domain معين
- الDomain اللي هو بيكون مثلا Facebook.com ده كده اسمه domain
- طبعا انا لما باجي افتح الموقع ده ببعت Request للسيرفر بقولو هاتلي الملفات دي فا انا عشان اوصل للملفات دي لازم انا والسيرفر نتعامل ببروتوكول معين اسمه HTTP اللي بيشتغلي علي بورت 80 او HTTPS اللي بيشتغل علي بورت 443
- البروتوكول عباره عن مجموعه من الخوارزميات او القواعد اللي بتحدد ازاي الأجهزه بيكلمو بعض يعني زي ما إحنا بنتكلم باللغة العربية أو الإنجليزية علشان نفهم بعض، الكمبيوترات وأجهزة الشبكة بتستخدم بروتوكولات علشان يتفقوا على طريقة تبادل البيانات
- اشهر انواع السيرفرات زي Apache , Nginx , IIS
- الApache بتشتغل علي ال Linux وال windows وال IIS بيشتغل علي Windows Server وال Nginx بيشتغل زي ال Apache برضو بس هو مستخدم اكتر فال Deep web وبرضه بيشتغل كـ Reverse Proxy وLoad Balancer وCache Server
- طبعا كل سيرفر بيكون فيه ثغرات وهنتعلم كل حاجه خاصه بيهم فيما بعد

HTTP Request

HTTP Parts

1. **Header**

- الهيدر ده اللي بيكون فيه المعلومات عن انا رايح لمين وجاي منين وعاوز ايه وكل الكلام ده

1. **Body**

- البادي او الPayload ده عباره بقي عن الحاجه اللي ببعتها
- عامل مثلا زي موظف البريد هو بيكون جاي من فرع مدينتك مثلا فا هو بيكون عارف هو جي من انهي فرع ورايح لفين اللي هو بيتك مثلا وبيوصلك الظرف مثلا اللي هو ال body

```
GET / HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/114.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
Origin: testphp.vulnweb.com
```

GET / HTTP/1.1

- الGET: نوع الريكويست (بيطلب بيانات من السيرفر)
-عارف انك لسه مش فاهم.....بص دا طلب GET يعني انا هنا بطلب بيانات من السيرفر يعني بالبلدي كده رايحله وايدي فاضيه فا الطبيعي مش هيكون مش body او Payload طب افرض مثلا لو ببعت طلب POST يعني بدي للسيرفر بيانات اه ساعتها الطلب ده هيكون فيه body لأني ببعت حاجه وده المستهدف اكتر من ال GET
- / : يعني الصفحة الرئيسية من الموقع
- الHTTP/1.1: إصدار البروتوكول المستخدم

Host

testphp.vulnweb.com → اسم الموقع اللي بيطلب منه

User-Agent

بيانات عن المتصفح ونظام التشغيل المستخدم (Mozilla/5.0 (X11; Linux x86_64; rv:109.0
(يعني أنت بتبعت الريكويست ده من Firefox على Linux 64-bit)

Accept

أنواع البيانات اللي المتصفح قابل يستقبلها

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp

Accept-Language

اللغة المفضلة للعرض

en-US,en;q=0.5

)يعني بالإنجليزي، ولو مش متاح، أي إنجليزي تاني(

Accept-Encoding

طرق الضغط اللي المتصفح يقبلها gzip, deflate, br
(يعني لو السيرفر ضاغط البيانات بأي واحدة من دول، المتصفح يعرف يفكها)

Connection

close → يعني يقفل الاتصال بعد ما الريكويست يخلص

Upgrade-Insecure-Requests

1 → يعني المتصفح بيطلب من السيرفر لو يقدر يحوّل الاتصال لـ HTTPS بدل HTTP

Origin

- ده عباره header فالrequest بيقول للسيرفر الطلب ده جاي منين
- حد هيجي يقولي طب ماهو فالريكويست اللي فوق مكتوب ان الorigin نفس الموقع وهو بقي الموقع هيبعت لنفسه؟
- اقولك لأ مش بالمعني الحرفي ده بص هقولك حاجه انا اصلا ممكن احط اكتر من دومين لنفس السيرفر بمعني اني ممكن مثلا
  test.com
  digital.gov
  local.ch
  كل دول مثلا يكون ليهم IP واحد وده اللي بيتعمل فعلا فا انا دلوقتي لو عاوز افتح test.com مش ممكن السيرفر يفتحلي local.ch بالغلط؟ اقولك اه بس ده لو في حالة مفيش الorigin هنا بقي مهمة الorigin يقول للسيرفر الطلب ده جاي من ال test.com والطلب نفسه فيه الhost اسم الموقع فا انت كده تمام ويفتحلك الموقع
- دا بيتم عن طريق (Cross-Origin Resource Sharing) CORS Policy يقرر هل يسمح أو يمنع

```
GET /data HTTP/1.1
Host: api.vulnweb.com
Origin: https://hacker.com
```

- شوف الطلب ده وقولي كده هل الطلب هيتم ولا لأ وليه
- وطبعا احنا كا هاكرز بنشوف اي طريقه نتخطي بيها الCORS دي عشان دي ممكن تودينا لثغره اسمها Host Header Injection
- في حاجه تانيه اسمها Referer ودي بيكون فيها انت كنت فاتح بيدج ايه فالموقع قبل ماتدخل علي البيدج دي

HTTP Request Methods

Method	الوظيفة
GET	بيطلب بيانات من السيرفر (من غير ما يغير حاجة)
POST	بيبعت بيانات للسيرفر (وبيستخدم غالبًا مع الفورم أو APIs)
PUT	بيعمل تحديث كامل (Replace) لبيانات موجودة
PATCH	بيعدل جزء من البيانات بس (Partial Update)
DELETE	بيطلب حذف بيانات من السيرفر
HEAD	زي GET بس بيرجع Headers من غير Body
OPTIONS	بيطلب من السيرفر يقوله إيه المسموح بيه من Methods على الريسورس
CONNECT	بيستخدم لإنشاء اتصال TCP/IP مباشر (غالبًا مع HTTPS Proxy)

Method	الوظيفة
TRACE	بيستخدم لاختبار وتتبع الريكويست وهو ماشي للسيرفر