سيكيورتي ١٥١

The Arab's Guide to Becoming in Cyber Secuirty

Mohamed Adel

بسم الله الرحمن الرحيم
اللهم صلي وسلم على سيدنا محمد

تم تصميم هذا الكتاب وكتابته ذاتيًا

About the Author

Twitter:
https://x.com/MohamedAdelitss

Github:
https://github.com/MohamedAdel-itsme

About the book

الكتاب ده اتعمل بسبب أن معظم المصادر العربية الموجودة في المجال ده هي كورسات مدفوعة

و أن كانت مجانية فا هي مش كاملة (و انا اقصد هنا "مش كاملة" انها توصلك لمستوي كويس من المعرفه)

و انا دورت كتير اوي على مصادر و فعلا لقيت اكتر حاجه المصادر العربية مفتقدها هي الكتب فا دا كان دافع اساسي اني اعمل الكتاب ده.

الكتاب ده هينقل فكرك من شخص ما يعرف يعني ايه security لشخص يعرف غالبية ال technologies في الـ security

Who is this book for

الكتاب ده لاي شخص عايز يدخل مجال الـ Cyber security في اي تخصص في الـ Cyber Security سواء كان pentesting or Soc or incident response .
لأنك في الكتاب ده هتتعلم اساسيات ال security و اساسيات اخري عشان تدخلك عالم الـ Cyber security

أو أي شخص عايز يبدأ في الـ bug bounty و عايز يبدا يتعلم اساسيات ال security وازاي ال firewall بيشتغل و ازاي بيتم تشفير البيانات و انواع ال malwares و ازاي بيعملو design لل network عشان تكون secure .

Prerequisites

ايه هي الحاجات الي المفروض تكون مذاكرها و عارفها قبل ما تبدا تقرا الكتاب ده ؟

1-network Basics :

محتاج تكون عارف اساسيات ال network كويس و يعني ايه ip و يعني dns و يعني ايه dhcp و الخ.....

و انصحك بكورس network + و انصحك بلاش ccna عشان advanced جدا علي اللي انت محتاجه لكن لو هتخصص في ال Network penetration testing فا خده طبعا .

2-Operating system basics :

محتاج تعرف أساسيات نظام التشغيل زي windows و linux و تكون عارف تتعامل مع ال cmd في الويندوز و عارف يعني ايه registry و ملفات نظام الويندوز بتتكون من ايه و كذلك في الـ linux محتاج تعرف تتعامل مع الـ terminal و تعرف شويه commands أساسية و تعرف ملفات نظام التشغيل بيتكون من ايه .

How to study this book

طيب ازاي تبدأ تذاكر الكتاب و ازاي متنساش اللي ذاكرته و تطبق عليه كمان ؟؟

الكتاب مقسم عندك ل عشر اجزاء كل جزء بيتكلم عن حاجه معينه
و هتلاقي كل الاجزاء في ال table of content و ديه ال page الي جايه .

طيب هتبدا انك تقرا كل chapter (جزء) و تبدأ انك تدور علي برنامج تكتب فيه الـ notes بتاعتك يعني تبدأ تلخص كل جزء قريته في الكتاب اي حاجه تقراها تبدأ انك تلخصها في الـ notes بتاعتك و عندك برامج كتيرة ممكن تكتب الـ notes بتاعتك فيها زي notion أو obsidian كده اتاكد ان المعلومة الي انت ذاكرتها مش هتنساها ابدا و هتكون فامها 100% .

Table of content :

CHAPTER ONE

Security fundamental

—----------

قبل ما نبدأ تأكد انك قرات كل الصفحات قبل ما تبدأ في الكتاب ,
عشان فيه حاجات مهمه زي انك ازاي تذاكر الكتاب ,
و ايه المتطلبات الي انت محتاجها عشان تبدا تقرا الكتاب ده ,
و الكتاب ده ل مين بظبط .
ف قبل ما تبدأ تأكد انك قريت كل الصفحات اللي قبل الصفحه ديه
----------—

قبل ما تبدا تتعلم ازاي تخترق جهاز أو شبكة المفروض تتعلم ازاي تحمي الجهاز ده اصلا او الشبكة عشان تبقي عارف طرق الحماية الي المفروض تتخطاها.

في الـ chapter ده هتتعلم اساسيات ال Security و يعني ايه اصلا cyber security و ايه الفرق ما بينه و ال security و انواع ال firewall و ازاي اصلا بيشتغل . و ازاي بيتم تشفير البيانات و انواع ال malwares و ازاي تحمي الشبكة بتاعتك كمان .

1-The Difference between information security and cyber security

—----------

1-Information Security:

نيجي عند مفهوم مهم جدا هو ال information security

ال information Security هو المجال اللي بيحمي أي بيانات وانا اقصد هنا أي بيانات حرفيا يعني اذا كانت digital أو بيانات ورقية او اي يكن البيانات ديه فين أو على ايه . و المجال ده بيتفرع منه مجالات كتيرة زي الـ cyber security و هنيجي دلوقتي نتكلم عليه.

2-Cyber security :

- ال cyber security زي ما قلنا هو فرع من فروع مجال ال information security و الـ cyber security هو المجال الي فيه بنحمي أي digital assets . طيب يعني ايه digital assets(يعني اي حاجه ديجيتال ليها قيمه يعني اذا كان computers او كاميرات او سيرفرات).

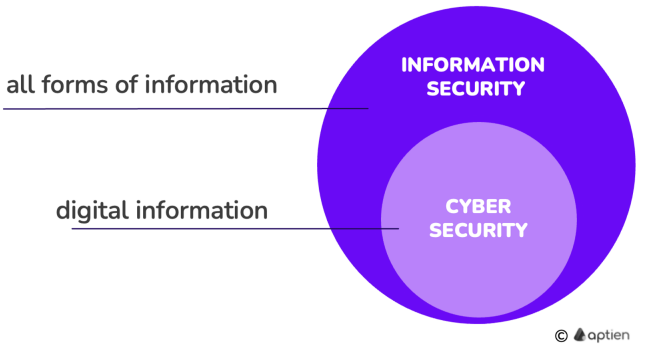
- طيب ايه فكره انهم يسمو المجال cyber security ؟

تعالى كده نقسم الكلمتين تلاقيها cyber و security

و cyber يعني اي حاجه ديجيتال متوصلين مع بعض او حتا لو مش متصلين . زي سيرفرات او computers .

و ال security يعني حمايه .

لما تيجي تجمعهم مع بعض يطلع لك حمايه اي digital assets زي ما قلنا فوق .



و دى صورة

بتوضح لك الموضوع شويه .

- طيب حاليا هتكلم عن تخصصات الي في cyber secuirty و هتكلم علي اشهرهم و هما الـ blue team and red team (لو انت عارفهم ممكن تعمل skip للنقطه ديه)

Blue team :

و ده الفريق الدفاعي الي بيدافع و الي بيحمي الشبكه و الاجهزه و اي assets عوما و فيه تخصصات كتير في ال blue Team زي ال Soc

ال soc team هما الي بيراقبو الانظمه و الشبكه و يشوفو اي حاجه malicious (ضارة) و يلقطوها و عموما احنا في الكتاب ده ملناش دعوه بيهم.

Red Team :

ده هو الفريق الهجومي و اللي بيعمل هجوم علي الشبكه او الاجهزه عشان يعرفو نقاط الضعف الي في الشبكه او الانظمة و في ال red Teaming فيه فروع كتيرة زي الـ web pentest او ال network pentest او ال api pentest

و عموما في الكتاب ده انا بجهزك عشان تكون jr pentester يعني عارف غالبية التولز و الـ Basics Techniques في الاختراق و بعد كده تقدر تروح اي تخصص انت عايزه .

2-CIA Triad

—----------

التلاته اللي هقولهم دلوقتي هما الثلاث مبادئ الاساسية في الـ information security .

و بيتقال عليهم الـ CIA Triad يعني ده المثلث الي بيكون فيه التلات حاجات الاساسيه الي بيحققوا information secuirty لازم يكونوا متحققين عشان تحقق ال information security عشان تأمن المعلومات من السرقه او الاتاك او اي حاجه مش كويسه

1-(C): confidentiality(السريه):

هي انك تحمي الداتا بتاعتك من ال data exfiltration يعني تسريب البيانات .

يعني انك تحدد مين ليه access على الداتا .

مين يشوفها بمعني اصح

يعني باختصار هديك مثال : نقول دلوقتي ان فيه فايل علي السيرفر و الفايل ده عشان نطبق عليه ال confidentiality لازم تحدد صلاحيات كل شخص على الفايل ده يعني تحدد مين يقدر يشوف الملف و مين ميقدرش يشوفه و كده انت حققت السريه و محدش يقدر يسرب البيانات و ديه أول مبدأ من مبادئ أمن المعلومات

2-(I): integrity:(السلامه):

هي انك تحمي الداتا بتاعتك من التعديل يعني مش اي حد يعمل modify للداتا بتاعتك

يعني باختصار هديك مثال :

نقول دلوقتي ان فيه فايل علي السيرفر و الفايل ده عشان نطبق عليه ال integrity لازم تحدد صلاحيات كل شخص على الفايل ده مين يقدر يعدل على الملف و مين ميقدرش و كدا انت حققت السلامه و محدش unauthorized (ملهوش صلاحية) يقدر يعدل على الملف

3-(A) Availability(الإتاحة):

هي انك تحمي الداتا بتاعتك من التلف او انها تكون مش موجوده او التعطيل زي مثلا ال dos attack او ال ddos attack

اهم حاجه ان تكون الداتا متاحة طوال الوقت

يعني باختصار هديك مثال :

نقول دلوقتي ان فيه فايل علي السيرفر و الفايل ده عشان نطبق عليه ال availability لازم تحدد صلاحيات كل شخص على الفايل ده يعني تحدد مين يقدر يمسح الملف و مين ميقدرش يمسحه و كده انت حققت السريه و محدش يقدر يسرب البيانات و ديه أول مبدأ من مبادئ أمن المعلومات

3-Basics cyber security terminologies

—----------

دلوقتي هتعرف اهم و اشهر مصطلحات هتسمعها في المجال و لازم تكون عارفها

1-vulnerability :

ال vulnerability بالعربي يعني ثغرة .

ال exploit بالعربي يعني استغلال .

ال vulnerability (أو الثغرة بالمعنى العربي) هي نقطة الضعف اللي الهاكر بيستغلها و يقدر يعمل منها exploit للثغرة يعني استغلال للثغرة اللي اكتشفها .

هديك مثال :

عندنا شركة مش منزلة antivirus علي اجهزتها فا بالتالي الهاكر يقدر يعمل exploit للثغرة ديه (الثغرة هنا انهم مش منزلين antivirus) فا بالتالي الهاكر يقدر يخترقها بسهولة ب اي نوع من انواع malware زي ان هو يبعتلها virus مثلا و هنشرح انواع ال malware قدام

2-Threat :

ال Threat هي التهديد الي حصل بعد ما الهاكر عمل exploit لل vulnerability

يعني خلينا متفقين ان مفيش تهديد عندنا في النظام غير لما يكون فيه ثغرة و شخص يستغلها

يعني لو فيه ثغرة و محدش لسه استغلها يبقى احنا كدا لسه معندناش تهديد

Threat = vulnerability + exploit

و هنا هيجي ل مصطلح مشهور اسمه ال threat actor الي هو ممثل التهديد الي هو الهاكر يعني .

لان الهاكر هو الي مثل التهديد ده و هو الي استغل الثغرة .

ومعلومة كمان ال Threat actor مش لازم يجي من برة الشبكه ممكن يجي من جوه كمان يعني لو انتم شركة ممكن يكون شغال معاكم .

3-Risk :

ال Risk (او الخطر بالعربي) يعني هو الخطر اللي ممكن يحصل لما يكون فيه threat و بيكون ليه تأثير .

Risk = Threat + impact

لان ممكن يكون فيه threat بس ميكونش فيه خطر .

يعني هديك مثال :

دلوقتي نقول ان احنا عندنا system و ال system ده كان فيه ثغرة و حد استغلها و عرف يخترق النظام يعني دلوقتي عندنا threat بس ال threat actor ده (الي هو الهاكر يعني) اخترق ب يوزر عادي مش admin يعني كده مش هيعرف يعمل حاجه في النظام يعني مش هيعرف يمسح ولا يعمل اي حاجه

يعني كده مفيش Risk بس لو دخل ب حاجه زي ال admin كده يبقي فيه Risk لان هو يقدر يمسح و يخرب و يعمل كل حاجة

4-Categories of threat actors:

هنتكلم دلوقتي عن تصنيفات ال threat actors

و خلينا متفقين ان الشخص الي بيخترقك الي هو ال Threat actor ده مش لازم يكون هاكر ممكن عادي يكون شخص اخترقك بدون قصد .

هتقولي ازاي بدون قصد يعني ؟؟

يعني ممكن يكون شخص من جوه الشركة معاه فلاشة و يكون فيها virus و هو ميعرفش و يحطها و ال virus يشتغل عادي و خلاص الشخص الي حط الفلاشة هو الي بقى قدام الشركة ان هو ال Threat actor .

بس احنا هنتكلم عن تصنيف واحد بس هو ال hacker و انواعه كمان

Types of Hackers :

- black hat:

ده هكر بيخترق و بيبقى ملوش اذن انه يعمل اي حاجة و في الغالب بيكون عايز يخرب حاجه لان عادي ممكن يكون penetration tester الي شغال و يكون ليه اذن بس الـ Black hat ملهومش اذن و بيخترقو اختراق غير قانوني

- white hat:

ده هاكر بيخترق بس بيكون ليه اذن من الشركة زي مثلا ال bug hunters دول الي بيكتشفو الثغرات علي المواقع و بيكون ليهم اذن علي المواقع الي بيعملو pentest عليها

- gray hacker :

ده هاكر بيخترق و مش بيكون ليه اذن انو يخترق بس مش شرير

يعني هو بيبقي ملوش اذن انو يخترق بس مش هيئذيك يعني ممكن انو يكتشف ثغرة في الموقع بتاعك و ميكونش ليه اذن انه يكتشف بس هو اكتشف و راح بلغها ليك الثغرة ديه و مراحش عمل بيها حاجة مش كويسة.

يعني من الاخر هو مبيكونش ليه اذن انه يخترق بس غرضه كويس

- **script kiddy:**

دول اطفال الهاكرز مبيبقاش ليهم هدف معين

يعني ممكن مثلا يكون حد بيتعلم tool معينة و يقوم يروح علي موقعك و يجرب عليها

هو هنا ملوش اذن و ملوش غرض أصلا . هو بس بيجرب ال tool

5-APT (advanced persistent threat) :

ال APT بالعربي يعني (التهديدات المستمرة المتقدمة)

ال APT هي هجمات بيعملوها الدول على بعض بس مش شرط الدول . ممكن شركات كبيرة على بعض .

بس في الاغلب بتبقا دول و هدفهم انهم يقعدو أكبر فترة مخترقين النظام ويتجسسون على كل حاجة .

يعني بتكون فيه دوله عندها فريق كبير من الهاكرز بيعملو attack علي دوله تانيه بس الاختراق ده بيكون مستمر وممكن الدولة الي بتهجم تقعد مخترقة الدولة الثانية لسنين من غير ما حد يكتشفها .

4- social engineering

—----------

ال Social engineering بالعربي يعني (الهندسة الاجتماعية)

باختصار شديد ال Social engineering هي التلاعب بالبشر

يعني انت بدل ما هتخترق جهاز أو شبكة . أنت هنا هتخترق البشر يعني هتتلاعب بالناس بمعني اصح .

هديك مثال صغير :

دلوقتي انا مثلا بعتلك mail و بنقول ان احنا شركة و محتاجين ناس تشتغل من البيت براتب كبير جدا و عشان تعرف باقي تفاصيل العمل تفتح اللينك اللي موجود في اللينك .

و اول ما تفتح اللينك تلاقي موبايلك بقي معمولة hack

و بياناتك كلها اتسرقت .

هنا هو تلاعب بيك و خدعك بمجرد انو قالك الراتب كبير و عشان تعرف باقي التفاصيل تفتح اللينك .

كده انا شرحتلك يعني ايه Social engineering .

دلوقتي هنشرح اهم طريقة بيستخدموها في ال social engineering و هيا ال phishing

phishing :

هو الاصتياد و هوا انك تخدع شخص و تفهمه انك شركة مهمه او تنتحل اسم شركة او اسم موقع معين و تعمل زية بظبط عشان بس تخدع الشخص و تخليه يدخل بياناته و تسرقها عن طريق بقا لينك او برنامج فيه malware او الخ....

هديك مثال :

دلوقتي فيه هاكر عايز عن طريق ال phishing يسرق الباسورد بتاعك الي انت مسجل بيه في موقع معين

فا عشان يعمل كده قادمو طريقتين :

اول طريقة انو يدخل علي الموقع ده و يفضل يدخل باسوردات عشوائيين

تاني طريقة إنه يستخدم الـ phishing و يعمل موقع شبه اللي انت مسجل فيه بالظبط،

و يبعتلك اللينك و يقولك سجل فيه.

و اللينك ده بقى فيه الموقع المزور.

فبالتالي، أول ما تدخل اليوزر نيم و الباسورد، هيتبعت للهاكر اليوزر نيم و

لأن هو مبرمج الموقع المزور على كده: إن أول ما تسجل فيه يتبعت له اليوزر نيم و الباسورد.

و أول ما البيانات تتبعت له، هو يدخل اليوزر نيم والباسورد في الموقع الحقيقي،

و كده يبقى الهاكر سرق الحساب بتاعك عن طريق ال phishing.

كده انا شرحتلك يعني ايه phishing دلوقتي بقا هقولك انواع ال phishing لان ليه اكتر من كذا نوع

- vishing:

هو phishing عن طريق الصوت يعني مكالمة

نفس الي بيحصل بظبط في ال phishing هيحصل بس بالصوت عشان كده سموه vishing . مثلا ان حد يكلمك و يبدا يقولك لو سمحت الفيزا بتاعت حضرتك اتوقفت لازم تيدنا البيانات و كدا ده اشهر مثال ممكن اقولهولك

- **spear phishing:**

هو فيشنيج موجه لشخص معين و هنا طالما موجه لشخص معين يبقي الرساله الي جايالك او الايميل الي جايلك فيه معلومات عنك زي اسمك مثلا

- **whaling :**

هو spear phishing يعني موجه لاشخاص معينة بس هنا بيبقا للناس الي شغالين في position كبير في الشركات زي CEO مثلا .

عشان بيبقا اغلبية الاشخاص الي شغالين في ال positions زي ديه بيبقو كبار في السن و مش عارفين كتير في التكنولوجيا فا نسبه ان ال phishing ينجح بتبقي كبيرة .

5-Malware Types

—----------

اولا كده يعني ايه malware ؟؟؟

malware اختصار لكلمة malicious software و بالعربي يعني اي برمجية ضارة .

اي برنامج او كود او اي سوفت وير ضار فا هو اسمه malware .

----------—

Malware types

عندنا انواع كتيرة من ال malware و منها :

1-virus :

هو برمجيه خبيثه بتندمج مع الفايلات و بتحتاج انك تشغلها (يعني تدوس علي الفايل ده و تشغله) و بعد كده بتبدا أنها تنتشر بين الملفات ال executable الي عندك في النظام .

(executable يعني ملفات قابلة للتشغيل , لان فيه ملفات غير قابلة للتشغيل زي الصورة او ملف تكست او اي بيانات , لكن انا اقصد هنا executable انها ملف فيه كود بيتنفذ زي exe او bash او bat)

مثال :

دلوقتي حد عطاك فلاشة و انت قمت فاتح الفلاشة و لقيت فيه فايل ,

و الفايل ده كان فيه virus الي هو كود خبيث جواه الفايل , و اول ما فتحت الفايل

ال virus بدا يشتغل و ينشر الاكواد الخبيثة جوه كل ملف عندك في النظام و كده هو ضامن انك لو مسحت الفايل الي فيه الفلاشة , كده كده الكود هيشتغل تاني لانه حاطه في كل ملفات النظام الي عندك بمجرد انك بس تشغل اي ملف زي اي ملف exe ال كود الخبيث هيشتغل تاني .

طيب ايه هدف الشخص اللي بيعمل virus ده ؟؟؟

ال virus هدفه التخريب و او التعديل او سرقة بيانات وبعتها لشخص اخر او تبطئ الجهاز

2-Worm :

الـ Worm هو كود خبيث يقدر يدخل جهازك و يتنفذ لوحده من غير ما يدمج نفسه مع اي ملف و من غير ما انت تشغله , عكس الـ virus كان بيحتاج فايل يندمج معاه و محتاج ان انت تشغل الفايل ده.

طيب هتقولي ازاي يعني هيدخل لوحده و ازاي هيتنفذ من غير ما اشغله ؟؟

ده بسبب الثغرات اللي بتبقي موجوده في الجهاز

هديك مثال :

فيه ثغرة اسمها eternal blue ms17-010 ودية ثغرة موجودة في بروتوكول smb v1 في انظمة windows 7 و ما قبلها وفيه version من windows 10 اتصاب و كمان versions من windows server اتصابو بالثغرة ديه .

الثغرة ديه كانت بتخليك تقدر تتحكم في ال memory بتاعتك الجهاز لو ال smbv1 مفتوح و متصاب بالثغرة و تقدر تنفذ اي اكواد خبيثة و تروح تتنفذ فى memory في أي processes . و كمان بعد ما يخترق النظام يقدر يروح للاجهزه التانيه اللي موجوده في الشبكة لو فاتحيين ال smb v1 و مصاب .

عشان كده ال malware ده اتسمى ب worm الي هوا دودة بالعربي عشان بينتشر و يقدر يدخل علي كل الاجهزة . و كده الكود الخبيث اتنفذ من غير ما يندمج مع فايل او انك تشغله.

3-Trojan :

ال trojan ده (الي هو حصان طروادة بالعربي) . ده malware بس متخفي .

طب يعني ايه؟؟

يعني ال malware ده بيخفي نفسه عن طريق انو بيدمج الاكواد الخبيثة في اي ملف زي صورة مثلا او ملف pdf و الملفات دول بيبانو طبعيين جدا بس اول ما تفتحهم الصورة او ال pdf يفتحو عادي و يظهرو البيانات الي جواهم بس في الخلفية فيه اكواد خبيثة بتتنفذ .

و عشان كمان الضحية ميحسش ان فيه حاجه ضارة يقوم مغير الامتداد بتاع الملف عشان الهاكر لما بيدمج الصورة او ال pdf في كود خبيث مبيبقاش بنفس امتداد ال صورة او ال pdf . بيبقى ب امتداد تاني فا بيعمل حاجه اسمها extension spoofing عشان بس يبان من برة انو بامتداد pdf أو صورة .

و في غالبية ال trojan الكود الخبيث اللي بيبقي موجود جوه الملف بيبقى backdoor و الـ backdoor ده يعني باب خلفي , يعني انو بيفتح port عندك علي الجهاز و يعمل اتصال من ال port ده و ياخد shell . او يعمل reverse shell و ديه حاجة advanced هنتعرف عليا قدام.

4-PUPs:

هي بتبقي برامج تنزل بدون علمك و انت بتنزل برنامج تاني يعني مثلا و انت بتنزل متصفح تلاقي فيه برنامج تاني نزل مع المتصفح بدون علمك و ده بيتسمي ب

Grayware يعني هوا مش malware يعني غرضة انو مش يأذيك بس هو هنا نزل برنامج بدون علمك

5-spyware:

هو مالوير الغرض بتاعه انو يتجسس عليك يعني مثلا يفتح ميكرفون ياخد سكرين شوت يفتح الكاميرا .

6-keylogger:

هو malware غرضه انو يسجل اي حاجة بتتكتب من الكيبورد بتاعك و يسجلها و يبعتها للهاكر . و يقدر من الموضوع ده انه يسرق باسورداتك او اي حاجة اي بتكتبها .

7-Backdoor

هو malware بيفتح باب خلفي للهاكر و من أشهر الحاجات ان الهاكر يفتح بورت علي جهازك مثلا و يدخل من عليه و ياخد shell كامل و ده اسمه Blind shell او ممكن يعمل reverse shell يعني بدل ما يفتح بورت علي جهازك يقوم هو مخليك متصل علي بورت مفتوح عند جهاز الهاكر عشان بس لو الطريقه الاولي منفعتش و ال firewall منعه . و كده كده قدام هنستعمل ال reverse shell كتير جدا لما نوصل ل ال system pentest.

8-ransomware:

ده malware بيشفر كل بيانات جهازك و ممكن يطلب فدية عشان يفكها و ممكن لا . مثلا زي malware اسمه wanna cry ال malware ده بيستغل ثغرة اسمها

eternal blue الي كنت شارحها و بيقوم داخل و مشفر كل الملفات و طالب فلوس و اول ما الفلوس تتبعت للهاكر البيانات المشفرة تتفك .

6-cryptographic

—----------

ال cryptographic او علم اخفاء البيانات بالعربي .

يعني علم اخفاء البيانات بدل ما يخلي الكلمه طبيعية و ممكن اي حد يفهمها , هنا في علم اخفاء البيانات احنا بنخلي الكلمة ديه محدش يعرف يفهمها و كمان ممكن ميعرفش يرجعها لاصلها في بعض من طرق اخفاء البيانات .

مثال :

Life (دى كلمة عادية جدا) :

و الكلمة العادية ديه بتتسمى هنا بإسم plaintext و الاسم ده بيعبر عن ايه text باين و ممكن حد يفهمه .

63bd7065ef1e165a04255d4048836ce126dfe2b6a0777722ad3a5c6013129d19 (ديه شوية حروف و ارقام بعد ما عملت طريقة من طرق علم اخفاء البيانات) :

هنا ده بقا اسمو ciphertext و الاسم ده بيعبر عن اي text معمولة cryptographic .

علم اخفاء البيانات هيا processes بتتعمل ب شوية algorithms عشان بس يخفو البيانات و في شوية طرق بيتعمل عمل بيها اخفاء البيانات من حيث ان محدش يعرف يقرا الكلام ده غير الي مسموح له فقط .

و كلمة algorithms يعني خوارزميات بالعربي . يعني شوية طرق معقدة بتطبق بقا الطرق المعقدة ديه علي اي plaintext و تحولة ل ciphertext

---

دلوقتي هنشرح طرق اخفاء البيانات :

1-Hash :

الهاش هو من ابسط طرق ال cryptograohic .

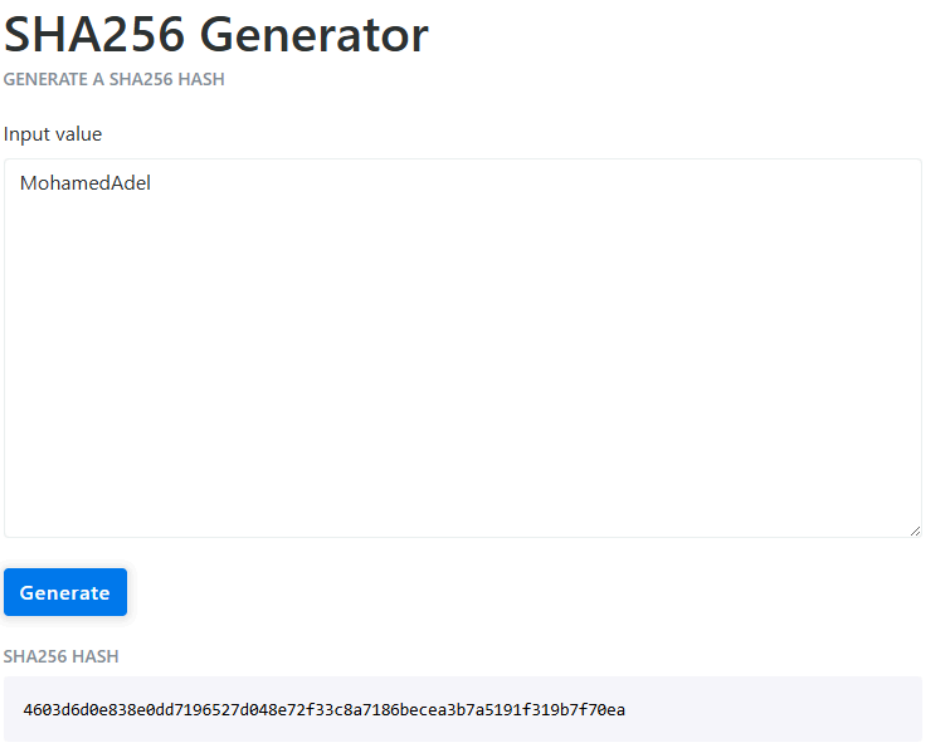
- طب ايه هيا فايدة الهاش او بيستخدم في ايه ؟؟

ال hash بيستخدم عشان يتاكدو من ان البيانات متعملش فيها حاجة او اتغيرت لان لو البيانات اتغيرت و اتعمل عليها نفس algorithm الهاش هتطلع ب output مختلفة .

هديك مثال :

فيه algorithm اسمها sha256 و ديه خوارزمية بيتعمل بيها ال hash . و دلوقتي انا دخلتلها كلمة mohamed و طبقت عليه الخوارزمية و قامت مطلعالي ال ciphertext .

لكن لو دلوقتي غيرنا كلمة mohamed ال output هيتغير .



هنا ال ciphertext اتغير و هنا انت كدا تاكدت ان ال hash بيستخدم في التأكد ان البيانات متغيرتش .

هديك مثال تاني لاستخدامات ال hash :

دلوقتي احنا عندنا ملفات كتيرة في النظام بتاعنا و عايزين نعرف اذا كان الملفات ديه بيتعدل عليها او لا .

فا نقوم جايبين كل الملفات ديه و عاملين لها hash .

و بعد فترة نرجع نعمل hash للملفات تاني اللي على النظام و نقارنها ب ال hash القديم اللي كنا عاملينو . لو لقيناه فيه تعديل في الهاش يبقا الملفات اتعدل عليها .

ده مثال بسيط جدا علي ال hash و هديك امثلة واقعية اكتر دلوقتي بس لما نشرح خواص ال hash

---

- خصائص الـ hash :

1-طول ثابت (fixed length) :

أن ال output الي بيطلع بعد ما تعمل للبيانات هاش دايما ال ciphertext بيكون length ثابت مبيتغيرش .

يعني دلوقتي نيجي عند algorithm زي sha256 . ديه خوارزمية و الخوارزمية ديه بتطلع length واحد بس يعني طول واحد بس .

لكن لو روحنا علي خوارزمية زي md5 هنلاقيها بتطلع length تاني بس برده ثابت مش بيتغير .

و الاتنين دول اللي هما md5 و sha256 هما خوارزميات من خوارزميات ال hash .

هديك مثال :

sha256 Algorithm output length :

```
4603d6d0e838e0dd7196527d048e72f33c8a7186becea3b7a5191f319b7f70ea
```

```
1fb4b2f38bfae06a8809300f32dba3e1a7199e1304891f215057e57b5ea56164
```

```
C3550d493d34109fbe21f2cf15c8c8018e12ba88d08113312152d1a69d80da38
```

MD5 algorithm output length :

447b12a9afc903a49461e85a4246ae9a

33fec996d517a93d07564c9a897bf7a6

a70a265793c10302729b243a9e73e4e9

لو لاحظت دلوقتى ان كل algorithm بتطلع طول مختلف عن التاني بس اهم حاجة ان ال algorithm الواحدة الطول بتاعها ثابت مش بيتغير .

2-اتجاه واحد (One way) :

دايما تلاقي في طرق زي التشفير او اي يكن , تلاقيه دايما بيتفك ب مفتاح ده لو انت كنت عارف يعني الموضوع ده , يعني بيرجع تاني لاصله لو كان معموله تشفير .

لكن في ال hash ال ciphertext هو one way يعني اي text معمولة cryptographic ب الهاش , مينفعش ترجعو تاني ل plaintext يعني للتكتست الاصلي , عشان هو one way يعني اتجاه واحد مينفعش يرجع تاني للاصلي زي ما كان .

- هنا بقا هديك آخر مثال في استخدامات الهاش و المثال ده هيكون حقيقي و ده استخدام ال hash الحقيقي في الشركات :

اكبر إستخدم لل hash في الشركات و المواقع هيا انهم بيحفظو الباسوردات في الداتا بيز معمولها hash .

طيب ليه بيعملو كده؟؟

عشان الباسوردات ديه لو اتسربت محدش يعرف يعمل بيها حاجة لان ال hash زي ما قولتلك هو one way يعني مبيرجعش ل اصله تاني فا بالتالي حتى الباسوردات اللي اتسربت محدش هينتفع بيها .

طيب ازاي بيعملوا check علي الباسورد الي بدخلو في الموقع و الباسوردات في الداتا بيز معمولها hash ؟؟

انت اول ما بدخل الباسورد بتاعك في الموقع بيقوم الباسورد ده معمولة hash و متقارن ب ال hash الي في الداتا بيز و لو زيه يبقى هتدخل الاكونت بتاعك ولو مش زيه يبقى مش هتدخل .

و كده يبقى انت عرفت كل حاجه عن ال hash .

2-Encryption :

التشفير هي طريقة من طرق ال cryptographic من حيث أنك تخزن البيانات او ترسلها و محدش يعرف يفهمها او يرجعها ل اصلها غير الي معاه مفتاح فك التشفير و هنيجي لموضوع المفاتيح ده بعد شوية .

- طيب ال encryption بيستخدم في ايه ؟؟

ال encryption عكس ال hash , يعني في ال encryption تقدر ترجع النص زي ما كان بس لو معاك المفتاح .

و من استخدام التشفير هي ارسال البيانات بشكل آمن . يعني ايه؟؟

يعني دلوقتي أنت لما تسجل في موقع معين انت المفروض بتدخل ايميل و باسورد , و بعد كده الايميل و الباسورد دول بيتباعو للسيرفر .

فا ممكن و هما بيتباعو للسيرفر , حد يقوم شايفهم عادي لو بيعمل حاجه زي ال

man in the middle attack و ده أتاك بيخليك تتنصت على أى بيانات بتترسل عن طريق ال network يعني اي packet بتطلع من جهازك لو مش متشفرة , الهاكر الي معاك في الشبكه ممكن يشوف البيانات ديه او حتى ال isp ممكن كمان يشوف بياناتك لو مش متشفرة .

فا هنا كان لازم نعمل encryption بحيث البيانات الي بتترسل تبقي متشفرة و السيرفر اللي رايحله البيانات يبقي معاه مفتاح التشفير .

و كده يبقي انا اديتك مثال كويس تفهم بيه استخدام ال encryption ,

طبعا غير انه بيستخدم في تخزين البيانات عشان لو البيانات اتسربت محدش يعرف يفكها غير الي معاه المفتاح.

عندنا نوعين من ال encryption هما :

1-Symmetric encryption :

هنا عملية التشفير و فك التشفير بتم عن طريق مفتاح واحد فقط الي هو ال private key و المفتاح الخاص ده بيتشفر بيه و بيفك بيه التشفير كمان فا هنا بقا ظهرت المشكله .

المشكلة ان انت لما تعمل connection مع موقع مثلا فا انت المفروض بتطلب ال key عشان تشفر البيانات فا المشكلة هنا مفيش غير مفتاح واحد فقط الي هو الـ private key , فا يقوم السيرفر بعتلك ال private key الي هتتشفر بيه البيانات و اول ما البيانات توصل للسيرفر, السيرفر يفك التشفير ب نفس المفتاح الي هو ال private key .

طب ايه المشكله؟؟

المشكلة هنا ان لو حد عمل man in the middle اتاك و عرف يشوف ال packets الي بتتبعت و الي جايه من السيرفر هيعرف يشوف ال private key لان انت اول ما بتكونكت مع السيرفر هو بيبعتلك المفتاح فا بالتالي لو الهاكر عرف ياخد المفتاح ,

هيعرف يفك التشفير . و كدا اصلا اكن مفيش تشفير من أساسه . فا كان لازم نحل مشكلة ان التشفير و فك التشفير بيحصل ب نفس المفتاح .

عشان كده اخترعو طريقة تانيه و ديه الي هشرحها دلوقتي .

2-Asymmetric encryption:

التشفير ده بيتم عن طريق مفتاحين اسمهم ال pair key .

و هنا السيرفر الي انت بتعمل connect بيه هو الي بيولد pair key يعني مفتاحين ,

واحد private و ده بتاع السيرفر بس و هو الي بيفك بيه و , واحد public و ده انت الي بتشفر بيه .

و كدا المشكلة الي كانت في Symmetric encryption اتحلت لان بقا فيه مفتاحين , واحد يتفك بيه و واحد يتشفر بيه .

هديك مثال :

دلوقتي انا فتحت موقع معين , ف سيرفر الموقع اول ما عملت connect بيه اداني المفتاح ال public بتاعه عشان اشفر بيه و اول ما اشفر بيه و ابعتله السيرفر يفك التشفير ب ال private key و المفتاح ده مبيبقاش مع حد ابدا غير السيرفر .

و كده الهاكر مش هيعرف يسرق ال private key .

معلومة اضافيه كمان :

ان ال encryption ال length بتاعه بيتغير علي طول يعني مش length ثابت زي ال hash .

هديك اختبار صغير :

هديك private key و جملة متشفرة و تفكها ب algorithm ال rsa 2048 bit:

Ciphertext :

```
MhacSbOmvd2J3ybbUbimBGuLB9crk3a4opyMR//5hhAfm9dTWJI9TR3o0tmZu
DE131uDw0GSNU1MZWmthTQFCj+pvdljUgXQ/kbYLCu7z7pNPy3U9jEn2hVdkC
6nYmvnYMM+mJmH69rx47FbfX2/18ZSpGjr9spm/+7qC2A4T8r8E8NCgHPtyWw
KYPh1a5Y1RrXDmemM+br1IJ03BUS/tY46qeRHGPmEolwU4m5oXxneyu346371
```

```
Di8fsyP8if0mlo3Qym9P3xzbaYuIw5onKoYMNqtE5jv2aC0OpO9AsOUZCjVtR
FiVm42onf6j2yZQ3jTvoaXqsRlqhfkKHPXUFA==
```

Private key :

```
-----BEGIN RSA PRIVATE KEY-----

MIIEuwIBADANBgkqhkiG9w0BAQEFAASCBKUwggShAgEAAoIBAQCVBzojZqufJ
XZr6gbFZdA27aLhOulxCWP6vXsKlKulNuJLDpNHQrgIEj8kilRz0Dnp1F0KDA
kvOLldV2vOySP5nBgCtce/U5CVR3cRXHL0ljPCA/NoFw/5grC4OyJrudTRK7s
MT/N5cloUOPlL1BXzltSt4bLNEN1NqZyJYnldOWvQA/IBP79FyxWPXN/ySUpV
w0t67+c7jSQeT+QxlFeQFeRhn9AMvdtBdC6afE1H1kQ2A5IUiqUlWrShJBHxg
HvbEYteU7iYME6B5t6osFMbsH2WUpltaCtDfUnXoLs+lFPcVcEnsOxAHwwPrj
e1xGmRcYmwWrUQnHbxuAiIPUGlAgMBAAECgf8Xdb7+Bt7KSGhCYXtI/j4Vmrm
JVNZq21xhz6V1Ub7mwz0Pk7vOyMuWE0lDxByHUfNljyJJjDUZIFTaqZub2EFR
ifQ9rCzfPmIEUSIgf+0yYHLFZNnS1c6UXxgMTtxpGPGBL0ePjwZ4MW6WWftLD
jGZpws6VDO34TyO46Rz/CYe02DyfNYFl84H6YEyb3afh5RAcEv3azdxmZOxwd
3XEEeGRKE3F8hRx1y3uVsOqsQ+hRdLSBXWbvc+lCSlN7/079/I1WCeR7KChxf
eVeaqEIknOw0EcoIn26H4H1OeYhWjZ7vJIdFSgLVzTDb/yg7FdXkbfnwAdkVd
lo7e9S48QZsCgYEAwXinbU7N7M8kYpKuXPAY+bjqpNDFR0QgfCaW9En7DXHjH
iPFO2HnxCaVeVJ1oxUW+fR16p6yYc2WZ2GlgYHy1GuRxBt4fEtZZwr2BSX0jQ
ZoN5sNISKqRapohNOcPCa/sk+VNtIAfchlSeXi71S50AWjvVbazSGi27XFrv/
kFQMCgYEAxTF2CMQMA9wuaeB6CfEU/D638jmhhYY/bEq4jNMUZseBMvkawQ4t
3pd2stvkNeDjRlsjEMmTosS+qdbtwsfvSKYUqli5eBOCZeaPN4bDZWn7YkMQl
NvKCkThV36OUn2IlOcsgl3RRDRZbG0aU22kC3evW/BkIO326kN4Dp5Y6jcCgY
EAv9qCxQ15fVSocyubxsO9MJ4j6U6x4wr238ZwuU1HrLx8CV5Vbp6W81eDsGy
KBS+bukCmUgQPRpdVh604L6YKhIUrZnoLT850mI8xCkfqK5Ln9ARIz8wNZ8ol
nVouuyN9wzfR8yvqmtEHSHG0SbsOC/AbwF2J2hN56UBnCTPuHLsCgYBz57uiM
WGCj1O0pd31o/+auF60gI1hB2SWCWFqXNNcCh310ReZq/ToJgz92mPMC3BrNT
xqLKGbhZswBwXffFc4U25IJjh1zLnTnW5Gy+5j2KSKwDKp3HpoCM6O9/M9p02
```

```
1gB/YTL6pIUACjCpyKTrIBsRK/QRNmrGMRrX1mbtXhwKBgCQGMNRkOOB09RZC
w4aT9YO70vap4GZlOHCv1JgSaoIeaea4stDI2obTEag9JLVQs9XyWz+zVMVYC
Wfmjgc3bCU5dnGv6ZuFa/Vgx2tWb32R67npZfmT/b/8u6iVRpmLS7eNUPjFvw
xbXQvNk542Gn2KmiRpgzope54dE09JXF6l

-----END RSA PRIVATE KEY-----
```

3-PKI (public key infrastructure):

ديه اخر طريقة في ال cryptographic هشرحها بإذن الله .

ال public key infrastructure بالعربي يعني (البنية التحتيه اللي بتدير المفاتيح العامة) , هو عبارة عن نظام كامل اتعمل عشان يعمل كل الحاجات الي هقولها دلوقتي .

بس خلينا نسأل نفسنا سؤال ,

ليه اصلا فيه طريقة تالتة في ال cryptographic ؟؟

طيب عشان نفهم ليه الطريقة ديه اتعملت , لازم نفهم ايه المشكلة الي حلها ال pki :

المشكلة ان انت لما كنت بتيجي تعمل connect علي موقع معين و يديك ال public key , انت هنا مش ضامن ان ال public key ده جاي من الموقع , مهو ممكن يكون فيه هاكر عدل في ال packet و غير ال public key والبيانات بتتبعت ليك ,

و كدا لو الهاكر ضامن ان البيانات الي هتتشفر . هتتشفر ب ال public key الي هو مدهولك و كدا هو ممكن يفكو عادي لان هو معاه الـ private key .

و ديه هيا المشكلة و كان لازم يبقي ليها حل و نتاكد ان ال public key ده هو مفتاح جاي من الموقع نفسه . عشان كدا ال pki اسمو بالعربي البنية التحتية لادارة المفاتيح العامة .

طيب عشان الناس تضمن ان الموقع ده امان و المفاتيح ديه جاية من الموقع مش من حد تاني لازم الموقع يكون معاه شهادة تضمن ان الموقع ده امان , و الشهادة ديه بتكون فيها ال public key و كذا معلومات تانية و الشهاده ديه بتكون موثوقة من جهات مشهورة و مضمونة .

و هنشرح دلوقتي ازاي الموقع بيعمل الشهاده بتاعته . و ازاي احنا بنتاكد ان الشهاده ديه امان و مش مزورة , لان عادي ممكن الهاكر يزورها .

1- RA (Registration authority) :

ديه منظمة التسجيل الي صاحب الموقع بيبعتلها طلب شهادة و فيه معلومات الموقع و ال public key و كذا معلومات تانية , و الطلب ده اسمه :

csr (certificate signing request) , و ده الطلب الي في كل معلومات الموقع زي ما قلنا و فيه ال public key و كمان بيتاكدو ان انت صاحب الموقع عشان مش اي حد معاه معلومات عن الموقع يروح يعمل طلب شهادة .

و بعد كده منظمه التسجيل تروح تبعت الطلب ده ل ال CA عشان توقع على الطلب و تطلعلك الشهاده . و هنشرح ايه هيا منظمة ال CA .

2-CA (certificate authority) :

ديه الجهة (او المنظمة يعني) الي بتوقع علي ال csr الي هوا طلب التسجيل الي جاي من RA الي هيا جهة التسجيل . و كمان بعد ما توقع علي الطلب تصدر لك الشهادة .

و فيه نوعين من ال CA :

- Single CA :

و ديه ca منفردة لوحدوها يعني مفيش حد تحتها يعني كده سيرفر لوحده هو الي شايل كل الحمل و هوا الي بيوقع علي كل الشهادات . و ديه مشكلته ان لو السيرفر ده وقع , كده مش هيبقي فيه شهادات بتطلع بس الشهادات الي طلعت خلاص بتبقي شغالة عادي . بس لو اخترق ديه مشكلة اكبر بكتير اوي , لان الهاكر هيبقي معاه ال private key و كمان ال CA ديه مش هتبقي معتمدة لان مش هينفع نعتمد شهادات من شركة مخترقة اصلا .

فا كان الحل ان احنا نعمل ال Hierarchical CA و ده هنشرحة دلوقتي .

- Hierarchical CA :

ديه بتبقي CA بس بشكل هرمي يعني فيها CA root و intermediate ca .

يعني ca رئيسية و ca فرعية .

و ال CA الفرعيين شغالين طول الوقت و بيصدرو شهادات و الرئيسية اوفلاين عشان ميحصلش عليها اختراق و لو حصل اختراق علي ال intermediate هتتشال عادي من ال root و تعمل واحدة جديدة و ترجع كل الشهادات تاني عادي بس اهم حاجة ال root ميحصلش عليها اختراق . بتفتح وقت الضرورة بس وقت ما مثلا تمضي علي ca فرعية لان لازم كل ال ca الفرعين يكونو معاهم شاهادات من ال root .

المهم ان بعد ما الطلب csr يتقبل من ال ca و تطلع الشهادة للموقع .

بعد كده ال ca تروح ل جهة اسمها VA تروح و تديها ال certificate وهقولك ليه دلوقتي .

3-VA (verification authority) :

هي الجهة (او المنظمة يعني) الي بتتاكد من الشهادة الى السيرفر بعاتهالك , الشهادة ديه لسا صالحة ولا لا , لان ممكن الشهادة تكون منتهية الصلاحية . و فيه بروتوكول بيعمل الموضوع ده . ان هو بيبعت رقم الشهادة ل ال va و يتحقق اذا كان لسا شغالة ولا لا .

طيب هيجي دلوقتي في دماغ حد سؤال :

دلوقتي مش ممكن الهاكر يغير في ال شهادة عادي و يغير في ال public key برده , مهو كده احنا معملناش حاجة ؟؟؟

هقولك لا مش هينفع .

لان الشهادة ديه بيبقا فيها حاجة اسمها توقيع ,

و هنشرح التوقيع ده بيتكون من ايه دلوقتي . بس قبل ما نشرح التوقيع , لازم تعرف ان ال ca بيبقا عنده public key و private key بتوعه هو بيشفر بيهم .

التوقيع ده بيتكون من :

مجموع بيانات الشهاده زي ال public key بتاع الموقع و اسم الموقع و الخ...

و بيقوم عامل ل مجموع بيانات الشهادة hash يعني بيعمل لكل ده hash و عاملها بعد كده تشفير ل ال hash ده ب ال private key بتاعه . الي هوا ال private key بتاع ال ca .

و كده اتعمل التوقيع .

طيب و بعد ما الشهادة توصل ل المتصفح يقوم المتصفح جامع كل بيانات الشهادة و يقوم عاملها hash .

و بعد كده يقوم واخد التوقيع بتاع الشهادة و فاكه ب ال public key بتاع ال CA نفسه و ياخد ال hash منه .

و يبدا يقارن ال hash بتاع البيانات بتاع الشهادة و ال hash اللي جاي من ال ca و لو مش هو يبقي البيانات الي في الشهادة ديه اتعدلت .

7-Network security

—----------

عشان تحمي اي network فيه طرق كتيرة جدا . بس الي هقولهم دلوقتي هما أشهر طرق لحماية ال network .

1-Firewall :

ال firewall بالعربي يعني جدار الحماية .

ال firewall مهمته انو يحمي الشبكة بتاعتك عن طريق انك بتحددلو مين يدخل الشبكه بتاعتك و يبعتلك packets و مين ميقدرش . و ال firewall ده ممكن يكون سوفت وير و ينزل علي اي vm او ممكن يكون هارد وير .

عن طريق انو بيفلتر ال packets و يشوف حاجة اسمها access control list , و ديه زي ليست كده فيها كل ال ip الي يقدرو يدخلو الشبكة بتاعتك و كمان فيها مين ال ip الي يقدر يطلع برة الشبكة و يقدر يفتح انترنت من جوه الشركة كمان .

هديك مثال :

دلوقتي نقول انك عندك شركة و عايز تحدد مواقع معينة بس الموظفين يدخلو عليها و مش عايزيهم يعرفو يدخلو علي مواقع تانية .

فا هنا انت بتقوم رايح جايب ال firewall و تقوم حاطط في ال access control list كل ال ip الي انت عايزهم يقدرو يعملو connect عليها .
يعني لو انت حاطط في ال access control list ال ip بتاع facebook , هيقدرو يخشو عليها عادي , بس لو مش حاطه مش هيعرفو .

مثال تاني :

لو انت عايز موظفين معينين بس هما الي يدخلو علي النت وقتيها بتحدد ال ip بتاع اجهزتهم و تحطو في ال access control list و كدا يقدرو يخرجو علي الشبكة الخارجية عادي . و باقي الموظفين لا .

ال firewall يقدر يشتغل بطريقتين :

1-stateless operation:

هنا ال firewall بيشتغل كا الاتي :
لو انت دلوقتي حبيت تطلع و تعمل connect عليه موقع جوجل لو انت مسموحلك و موجود في ال access control list هخليك تتواصل مع جوجل عادي و يطلعك علي شبكة النت عادي . بس لما جوجل يرد عليك مش هيرضي يخليه يوصلك . يعني ال

packet الي جاية من جوجل مش هتوصلك عشان جوجل مش مسموحلة انو يدخل شبكتك و يبعتلك packets .

2-stateful operation :

هنا ال firewall بيشتغل كا الاتي :

لو انت دلوقتي حبيت تطلع و تعمل connect علي موقع جوجل لو انت مسموحلك و موجود في ال access control list هخليك تتواصل مع جوجل عادي و يطلعك علي شبكة النت عادي . و لما جوجل يرد عليك هيرضي عادي . يعني ال packet الي جاية من جوجل هتوصلك .

كده في ال statful الي انت عملت connect عليه يوصلك عادي . بس في ال stateless , لا عشان لازم يكون الي انت عملت connect عليه , هو كمان مسموحلة انو يرد عليك و يبعتلك packets .

2-IDS (intrusion detection system):

ال ids ممكن يكون هاردوير او سوفت وير .

طيب بيعمل ايه ؟؟؟

ال ids هو بيعمل detection لاي حاجة malicious (يعني بالعربي ال ids هو عباره انو بيكتشف اي packet داخلة النيتورك فيها حاجة ضارة) .

بس ال ids بيكتشف بس , بس مش بيمنع .

يعني هو بيكتشف و بيديك انذار ان فيه حاجة ضارة دخلت ال network بتاعتك بس مش بيمنع الحاجة الضارة ديه , هو بس يديك انذار و انت اتصرف .

طيب هو بيكتشف ازاي ان فيه حاجة ضارة ؟؟؟

عن طريق طريقتين :

- **signature based detection:**

بيعمل detection عن طريق الـ signature database .

ديه داتا بيز بتكون جاية مع الـ ids بيكون فيها حاجة اسمها signature يعني بصمات , البصمات ديه بتكون بصمة لأي حاجة ضارة ,

أي packet بتعدي على الـ ids بيقوم مقارن البيانات الي في ال packet ب ال signature الي عنده في الداتا بيز , لو وجد ان فيه حاجة ضارة و مطابقه للبصمة يبقي هيديك انذار علي طول .

- **behavior based detection:**

الطريقة التانية اللي بيعمل detection بيها هي السلوك ,

يعني لو لقا سلوك مشبوه زي مثلا ال brute force , يعني واحد بيحاول قاعد يجرب باسوردات بسرعه جدا فا يقوم الـ ids عامل انذار علي طول .

3-IPS (intrusion prevention system):

ال ips ممكن يكون هاردوير او سوفت وير .

ال ips هو زي ال ids بظبط يعني بيكتشف ال packets الي فيها حاجاة ضارة و بيقوم عامل انذار .

بس مش كده و بس . هنا هو حل مشكلة ال ids . هو ان ال ids كان بيكتشف بس .

لكن ال ips حل المشكلة و بقا بيكتشف و بيمنع كمان .

4-WAF (Web application firewall) :

ال waf هو firewall بس متخصص في هجمات ال web application .

زي مثلا انو يقدر يكتشف ال sql injection او xss او rce .

و هو زي باقي ال firewall يعني عنده signature database بيقارن منها ال packet الي جيالة ب ال داتا بيز الي عندة .

5-Siem solution :

ال siem solution ممكن يكون هاردوير او سوفت وير .

ال siem solution هو اختصار ل

(Security Information and Event Management solution) .

طيب هو بيعمل ايه بظبط؟؟؟

هو مهمته انو بيجمع كل ال logs بتاعت كل الاجهزة الي في الشبكة و يبدا انو يربط كل الاحداث ببعض و يكتشف اي حاجة مشبوهة او ضارة .

طيب يعني ايه logs ؟؟

Logs ديه يعني السجلات , يعني اي حاجة بتتعمل علي الجهاز بتاعك بتتحط في حاجة اسمها log .

فا الي بيعمله ال siem solution انو بيجمع كل ال logs بتاعت الاجهزة و يربط ببعض .

هديك مثال :

لو هكر دخلت علي الشبكة بتاعتك و بدا يدخل علي الاجهزة كلها , واحدة ورا التانية و يبدا يعمل حاجات ضارة .

هنا ال siem solution معاه ال logs بتاعت كل الاجهزة و هيبدا يحث ان فيه حاجة غلط و يديك انذار .

6-soar (Security Orchestration, Automation, and Response،) :

ال soar ممكن يكون هاردوير او سوفت وير .

طب ايه اللي بيعمله ؟؟؟

هو بيكمل الي بيعمله ال siem solution يعني ال siem بعد ما يعمل detection و يقوم عامل إنذار , يقوم ال soar واخد ال انذار و يقوم فاحص المعلومات الي في ال الانذار , و لو فيه خطر يقوم عامل action علي طول و مانع الحاجة الضارة اللي بتحصل .

و كده الحمدلله تم شرح ال Security fundamental

CHAPTER TWO

Web fundamental

في ال chapter ده , هنشرح الـ web basics الي لازم تكون عارفها قبل ما تبدأ في الـ penetration testing .

يعني هنشرح حاجات زي ال cookies و ال http request و ال response بيتكونو من ايه .

و هنشرح اساسيات ال burp suite عشان هتستعمله في الـ web penetration testing . فا انت كا junior لازم تكون عارف برنامج زي ال burp suite .

1-The Difference between website and web application

—----------

1-Website :

ال website هو موقع static بيعرضلك معلومات فقط , يعني مينفعش تتفاعل معاه و تكتب كومنت او تنزل بوست او اي تفاعلات لان هو static يعني صفحه مبتتغيرش .

هشرحلك بتفصيل اكتر :

ال website هو موقع بيبقا صفحات static بس , يعني صفحات ثابته مبتتغيرش , زي كده لما تعمل صفحه ب ال html و تحط فيها شوية معلومات و تقوم ناشرها علي النت , هو ده بقا ال website .

و في اغلب ال websites مبيبقاش ليهم database , لانهم مش محتاجين database لانها مجرد صفحات html .

زي كدا موقع wikipedia و اي مواقع شخصية زي انك بتعرض فيها معلومات عنك ده برده website .

2-Web application :

الـ web app هو ويب تفاعلي , يعني هنا في الـ web app تقدر تكتب كومنت و يظهر تقدر تعمل لايك او شير او تعمل login لانه ويب dynamic يعني متغير مش ثابت .

و ال web application بيبقا فيها داتا بيز , غير ال website اللي مكنش فيها غير صفحات ثابتة فيها شوية معلومات .

و في الاغلب تلاقي ان الـ web app دايما بيقدم خدمة معينة زي مثلا التواصل زي واتساب و الخ... من الخدمات اللي بتقدمها الـ web apps , عكس ال website الي بيعرض لك صفحه ثانيه فيها شوية معلومات.

2-Client side and Server Side

—----------

لما تيجي تفتح اي موقع او تفتح connection مع اي سيرفر , لازم يكون فيه طرفين و هما :

1-Client side :

ال client side هو الطرف بتاعك انت ك user الي بيفتح اتصال مع السيرفر بتاع الموقع من ال Browser بتاعك .

يعني هنا ال client side هو ال Broswer بتاعك , عشان ال Brwoser هوا البرنامج الي بيفتح اتصال من جهازك مع ال سيرفر بتاع الموقع .

- دلوقتي انت بعد ما تفتح connection مع سيرفر الموقع , ايه الي بيظهرلك في ال client side ؟؟

بيظهرلك في ال browser المحتوى بتاع الموقع و اللي بيبقا مكتوب بلغات زي html و css و javascript .

فا كدا خلاصه الموضوع :

ال client side هي النحية بتاعتك انت كا يوزر و الي بيظهرلك فيها محتوي الموقع في ال Broswer بتاعك . و المحتوي ده بيبقا مكتوب فيه لغات زي html و css و js .

2-Server side :

من الناحية التانية هو السيرفر، وده ببساطة هو الجهاز أو الكمبيوتر اللي عليه الموقع اللي انت بتفتحه من المتصفح.

و السيرفر ده بيبقا فيه حاجتين :

1-web server software :

ال web server software هو البرنامج اللي بيستقبل الطلبات الي انت بتبعتها للسيرفر , اللي هيا اسمها (http request و ديه هنشرحها قدام) .

بعد ما البرنامج يستقبل الطلبات الي انت بتبعتها للسيرفر , بيقوم رادد عليك بحاجة اسمها http response و فيها المحتوي الي بيظهرلك , و زي ما قلنا المحتوي اللي بيظهرلك ده بيكون مكتوب بلغات زي html و css و javascript .

و فيه امثلة كتيرة ل ال web server software :

زي apache و iis

2-the website :

تاني حاجة السيرفر بيكون حاملها هو الموقع نفسه .

الموقع كله ب ال database بتاعته و اكواد ال backend بتاعت الموقع , و اكواد ال backend ديه هيا الاكواد الي بتعالج البيانات الي انت بتحطها في الموقع عشان مثلا انها تبدا تضيف البيانات ديه في الداتا بيز او تحذفها و الخ....

هديك مثال علي ال server side :

دلوقتي نعتبر انت فتحت موقع جوجل و سجلت الدخول ب ايميل و باسورد , فا اول ما تفتح الموقع , المتصفح بتاعك بيبعت ل السيرفر بتاع جوجل حاجة اسمها http request .

و من ناحية السيرفرات بتاعك جوجل فيه حاجة اسمها ال web server software الي هي مثلا حاجة زي apache . و apache ده يستقبل ال http request الي انت بعته و يديه ل ال backend .

فا يقوم ال backend الي هي ممكن تكون مكتوبة بحاجه زي php .

يقوم ال backend متحقق من البيانات الي انت دخلتها .

و بعد كده ال web server software يبعتلك http response فيه المحتوي الي المفروض يظهر لك بعد تسجيل الدخول لو الايميل و الباسورد صحيح.

و كده ابقا شرحتلك ايه اللي بيحصل في الـ server side .

3-HTTP Protocol Basics

—----------

اولا كده خلينا نشرح ايه هو بروتوكول الـ http :

بروتوكول الـ http هو البروتوكول اللي بيستخدم إرسال واستقبال البيانات بين المتصفح و السيرفر .

زي انك مثلا تفتح موقع جوجل , فا ال http مسؤال انه يبعت الطلب ده لسيرفر جوجل و برده مسؤول انه يبعت الرد من السيرفر ليك عشان يعرض لك صفحه جوجل.

- طيب دلوقتي هييجي سؤال في دماغك و تقول آمال ال https ده يبقا ايه و ليه مش بيستخدم في إرسال واستقبال طلبات الويب ؟؟

عشان نفهم ال https صح , لازم نفهم هو عبارة عن ايه :

ال https عبارة عن بروتوكولين في بعض , يعني مش بروتوكول واحد مستقل بذاته , والبروتوكولين هما ال http و الـ ssl/tls ,

و ال ssl/tls هو البروتوكول المسئول عن انو يجيب ال certificate من السيرفر و يشفر الاتصال والبيانات عبر الـ public key الي بياخدها من الشهادة .

فا كده ال http هو بروتوكول شغال فوق ال ssl/tls , يعني ال ssl/tls يشفر الاتصال بينك و بين السيرفر و طلبات الـ http تتبعت جوه القناة المشفرة ديه .

و خلينا متفقين علي ان اي HTTP Message بتبقى فيها حاجتين اساسين

Headers and Body

و هنشرح كل ده دلوقتي في ال HTTP Request و ال Response .

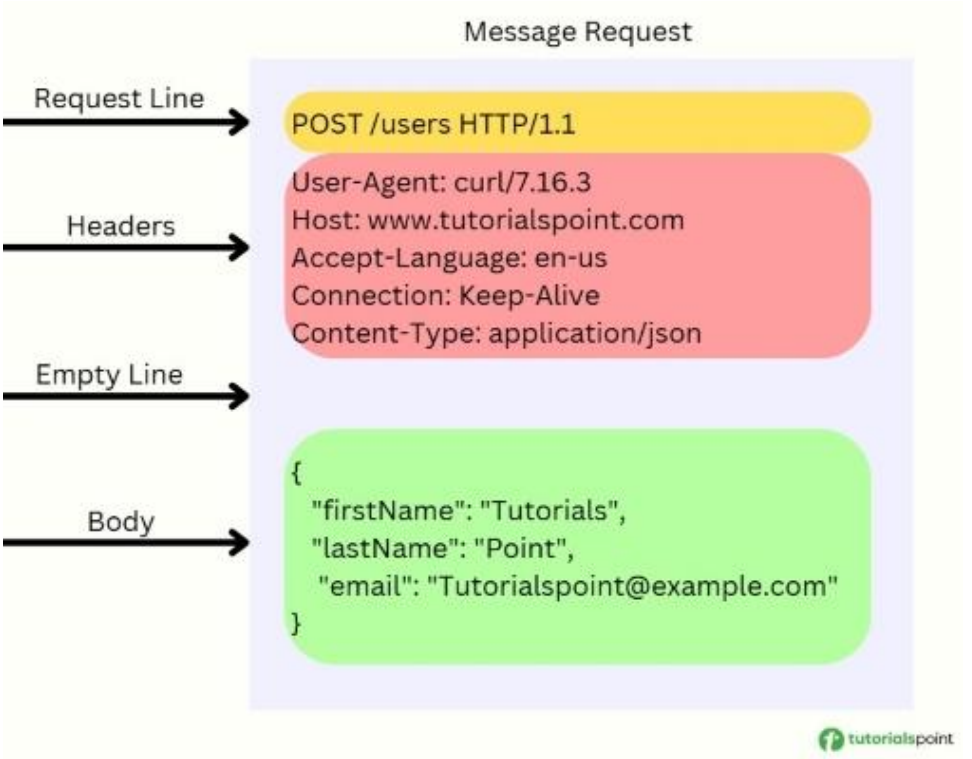
4-HTTP Request

—----------

ال http request هو الطلب الي بيتبعت لسيرفر الموقع عشان يعرض صفحه معينه او يضيف بيانات و الخ...

HTTP Request components :

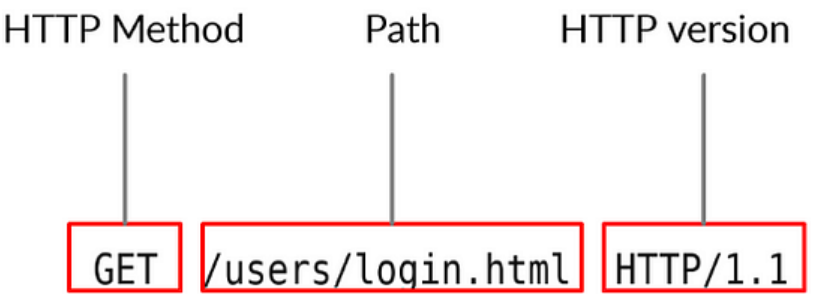
هنشرح دلوقتي ايه هو شكل ال http request ده و بيتكون من ايه :



1-Request line :

اول سطر في ال http request هو ال Request line ,

ال Request line ده بيوصف الطلب بتاعك , و غرض الطلب ايه , و الطلب ده رايح فين في الموقع بضبط . و هنشرح كل حاجة دلوقتي بالتفصيل .



- HTTP Method :

ال http method هي اول حاجة بتتكتب في الـ request line , و هي اللي بتحدد نوع الطلب ده ايه وايه العملية المطلوب السيرفر يعملها .

لان الطلب بيبقى ليه كذا نوع مش نوع واحد او عملية واحدة السيرفر بينفذها و خلاص .

و من انواع الطلبات :

GET: لعرض البيانات (زي انك تعرض صفحه معينه في الموقع زي صفحه ال login)

POST : لارسال البيانات (زي انك تبعت للسيرفر معلومات تسجيل الدخول زي الايميل و الباسورد)

و فيه انواع كتير من الطلبات بس دول اشهر انواع الطلبات .

- Path :

هنا انت بتحدد المكان اللي انت عايز تروحه في الموقع , زي انك تروح صفحه ال login او الصفحه الاساسية للموقع (the root page) / , او انك تروح صفحه او مكان في الموقع فا هنا بيتحدد في ال path

- HTTP version :

هنا المتصفح بيحدد ال http version اللي بيستعمله عشان السيرفر يفهم هيتعامل معاه ازاي لان كل version و ليه تعامل خاص .

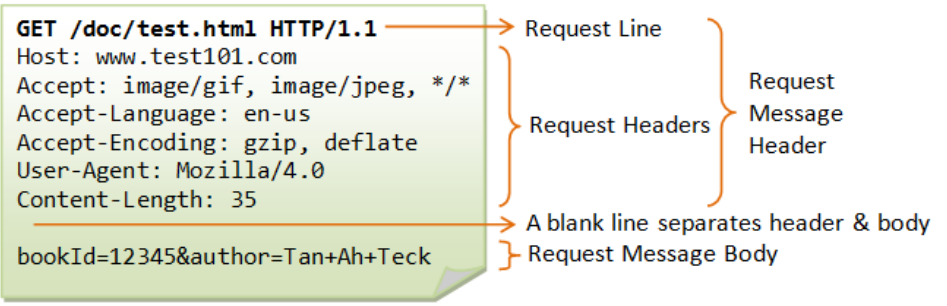
و كده ال Request line اتشرح و فهمت ان هو اللي بيشرح الطلب بتاعك و رايح فين و عايز ايه بظبط .

2-Headers :

تاني حاجة عندنا في ال HTTP Request هيا ال Headers . و ال Headers دول (اللي هما الرؤوس بالعربي) دول عبارة عن معلومات بتتحط في ال HTTP Request عشان تنظم الاتصال بين ال client و السيرفر و توضح الطلب اكتر .

زي مثلا Header اسمه Accept و الهيدر ده بيحدد للسيرفر ايه نوع البيانات اللي المتصفح بيقبلها , و كده السيرفر مش هيبعت نوع بيانات المتصفح مبيقبلهاش .

ده بس كان مثال عشان تفهم ازاي ال Header بتنظم الاتصال و البيانات اللي ما بين الـ client و السيرفر .



- Host :

ال host هيدر بيحدد ال domain اللي انت رايحلة .

هتقولي دلوقتي طب مهو كده كده الطلب موجه للموقع , طب ليه كاتبين اسم ال موقع (اللي هو ال domain يعني) ؟؟؟

هقولك الطلب مش موجه للموقع , الطلب بيتوجه للسيرفر اللي فيه الموقع , و السيرفر ده بيبقا فيه اكتر من موقع مش موقع واحد فا لازم تحدد له ال domain اللي انت موجه الطلب ده ليه .

- User Agent :

هيدر ال user agent هو الهيدر اللي بيتكتب فيه اسم المتصفح بتاعك و ال version اللي بتستخدمه و ال operating system بتاعك .

طيب ال header ده ليه بيتكتب ؟؟

عشان ممكن السيرفر بيحدد انه يظهر لك حاجة معينة ل operating system معين أو Browser .

- Accept :

الهيدر ده بيحدد أنواع البيانات اللي بيقبلها المتصفح لان ممكن السيرفر يبعت نوع المتصفح مش بيقبله .

فا هنا المتصفح بيحط انواع البيانات اللي بيقبلها و السيرفر يختار منها

مثال :

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

ديه انواع البيانات اللي المتصفح بيقبلها و السيرفر يقدر يبعتها ليه .

- Accept language :

هنا المتصفح بيقول للسيرفر ايه اللغه اللي عايز يستقبلها

- Accept encoding :

هنا المتصفح بيقول للسيرفر ايه نوع الضغط اللي بيقبلو , عشان البيانات لما بتتبعت من المتصفح للسيرفر او العكس , البيانات بتتضغط عشان لما تتبعت عن طريق ال Network تبقا سريعة .

فا المتصفح بيقول للسيرفر نوع الضغط اللي بيقبلو علشان لما البيانات توصل للمتصفح يعرف يفكها . و انا اقصد البيانات اللي بتبقي في ال body , و هنشرح بعد شوية ال body .

3-empty line :

تالت حاجة في ال Request بتبتقا فاصل بيفصل ما بين ال Headers و ال Body و الفاصل ده بيبقا موجود اذا كان في ال Request او ال Response .

4-Body :

اخر حاجة في ال HTTP request هوا ال body .

و ال Body ده لو فيه بيانات بتتبعت بتتحط في ال body .

يعني ال body اللي بيتحط فيها البيانات اللي بتتبعت .

و ال body دايما تلاقيه في نوع الطلب ال post , عشان ال post ده نوع بيرسل بيانات فا بالتالي يبقا فيه body , لكن في حاجه زي ال get مش هتلاقي body عشان ال get بيعرض صفحه فا بالتالي مش هيبقي فيه محتوي يبعتو يعني . هو مجرد بيطلب ان يتعرضلو صفحه .

مثال :

شخص عايز يفتح جوجل فا بالتالي مفيش اي بيانات هتتبعت , يعني مفيش body .

يعني نوع الطلب هنا GET .

ده كان مثال بسيط اوي عشان بس الموضوع يوضح شوية .

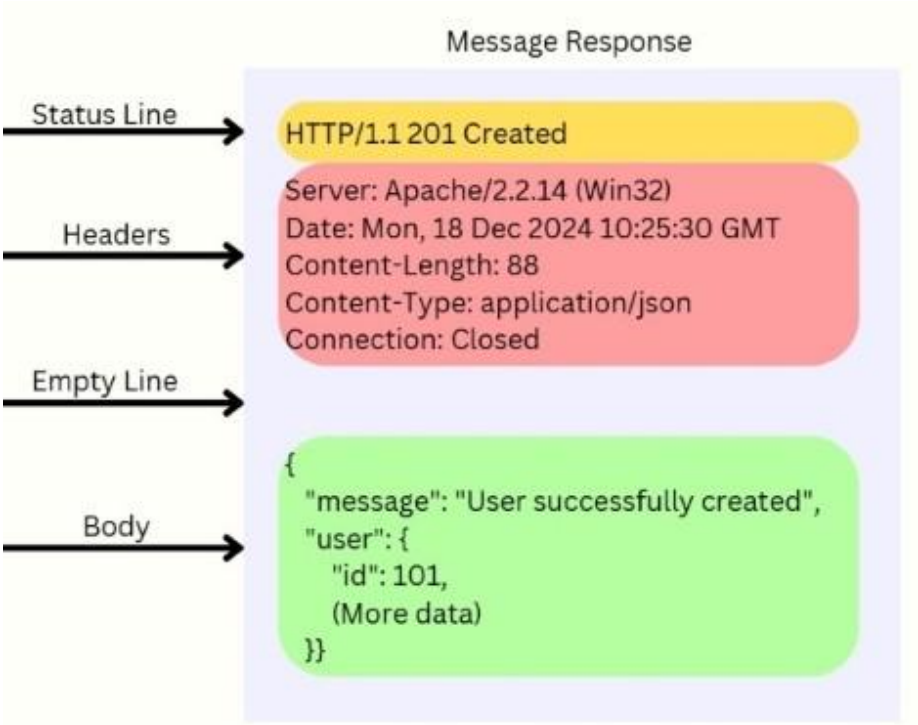
5-HTTP Response

—----------

ال HTTP Response هو الرد اللي بيجي من السيرفر ليك.

HTTP Response components :

دلوقتي هنشرح ال HTTP Response بيتكون من ايه و شكله بيبقا عامل ازاي .



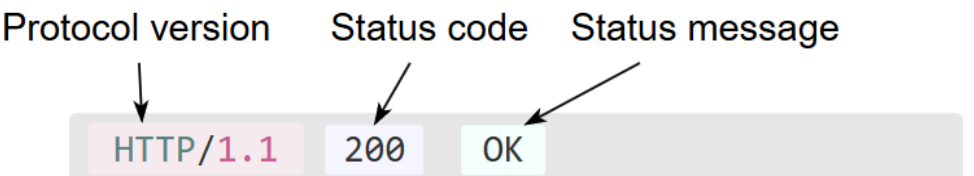
1-Status line :

نعتبر دلوقتي انك بعت HTTP Request ل موقع جوجل و عايز تعرض صفحه جوجل الرئيسية . فا الطلب اللي انت بعته لجوجل ده , جوجل هيبدأ يشوف المسار اللي انت رايحله (ال path يعني) و هيبدا يرد عليك .

طب هيبدا يرد ب ايه ؟؟

هيرد ب حالات (ال status يعني).

يعني ممكن المسار اللي انت رايحله ده مش موجود في جوجل اصلا فا يبدا جوجل يبعتلك في ال Response رقم 404 , يعني الصفحه ديه مش موجوده . و الرقم ده بيدل علي حالة الرد . اذا كان موجود او مش مسموح ليك وقتها هيكون فيه رقم تاني . و في كل حالة رقم مختلف .



- Protocol Version :

اول حاجة بتتكتب في ال status line هو ال Protocol version اللي السيرفر رد عليك بيه

- Status code:

تاني حاجة بتتكتب في ال status line هو ال status code .

ال status code هي اللي بتعبر عن حالة ال response اللي جالك ايه .

يعني مثلا لو كانت الصفحه اللي انت رايحلها في الموقه مش موجود هيديك رقم 404 .

او مثلا مش مسموح ليك تدخل الصفحه ديه فا قوتيها هيديك كود 403 .

و كل رقم و من دول بيدل علي حالة معينة .

- Status message :

هنا هو بيوصف الكود اللي كتبناه قبليه يعني مثلا لو الكود 200 يعني كدا العملية نجحت . فا كده هيكتبلك ok .

و لو الكود 404 , فا هيكتبلك في ال status message , هيكتبلك not found .

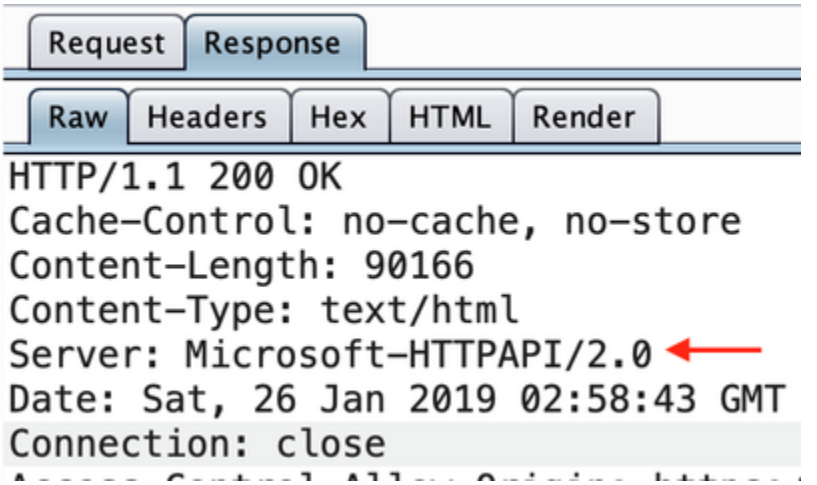
هيا هيا بس بتعبر عن الكود بس ب نص .

2-Headers :

- Server :

Header ال server هو الهيدر اللي بيتكتب فيه اسم ال operating system و ال web server software زي apache .

و فيه مواقع بتحط اسم ال operating system وفيه مواقع لا بسبب الخصوصية .



- Date :

الهدر ده بيبعت الوقت و التاريخ اللي اتبعت فيه ال Response .

- Cash control :

انت لما تبعت Request لاي سيرفر , ال Response اللي بيجيلك ممكن تلاقي بيتخزن لفترة معينة , و ممكن يتخزن في السيرفر او المتصفح .

طيب ليه اصلا بيتخزن ؟؟

عشان انت لو رجعت بعت نفس ال Request مرة تانية ميرجعش السيرفر يعمل نفس العملية بتاعتو تاني .

يعني لو ال response متخزن في المتصفح بتاعك وقتيها مش هتبقي مضطر ان الريكويست يتبعت للسيرفر تاني و ياخد وقت , (ده يعني لو بعتى نفس الريكويست)

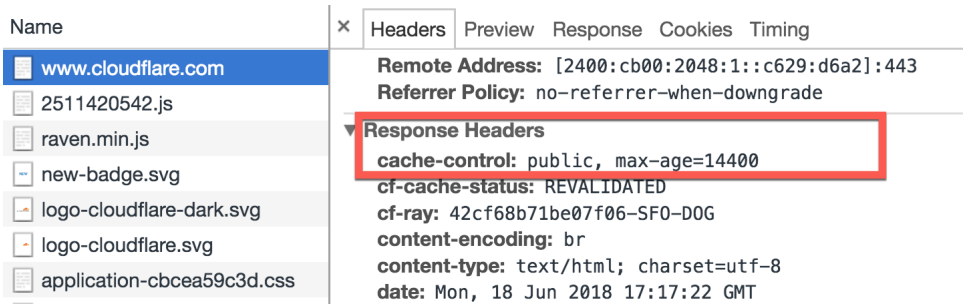
لكن لو متخزن في السيرفر , فا وقتيها هيتبعت للسيرفر بس السيرفر مش هيعمل نفس العملية تاني لان ال Response هنا متخزن عنده .

مثال :

انت دلوقتي فتحت صفحه جوجل , فا جوجل بعت ال Response بتاعه و قام مخزنه في المتصفح بتاعك . فا بعد شوية انت تقفل صفحه جوجل و تفتحها تاني و تلاقيها اتفتحت بسرعه جدا و مش بتاخد وقت .

عشان هيا اصلا متبعتش للسيرفر تاني , هيا اتخزن عندك في المتصفح .

و لو كان ال Repsonse متخزن في السيرفر فا هو هيتبعت للسيرفر بس السيرفر مش هيرجع يعمل نفس العملية تاني .



هنا مكتوب في ال cach control انو public , و معني public هنا ان ال Response اللي اتبعتلك اتخزن في السيرفر و بقي متاح للجميع ان ياخد ال Response ده , و كده السيرفر اي request شبه اللي انت بعت اتبعت تاني للسيرفر من اي حد , وقتا السيرفر مش هيضطر انه يعمل العملية تاني و هيبعتله ال Response علي طول.

- Content type :

ده بيبقا فيه نوع البيانات اللي اتبعتلك في ال body . يعني لو كان ال body كان مكتوب ب json فا يبقي ال content type json .

- Content encoding :

ده نوع الضغط اللي اتضغط بيه ال body .

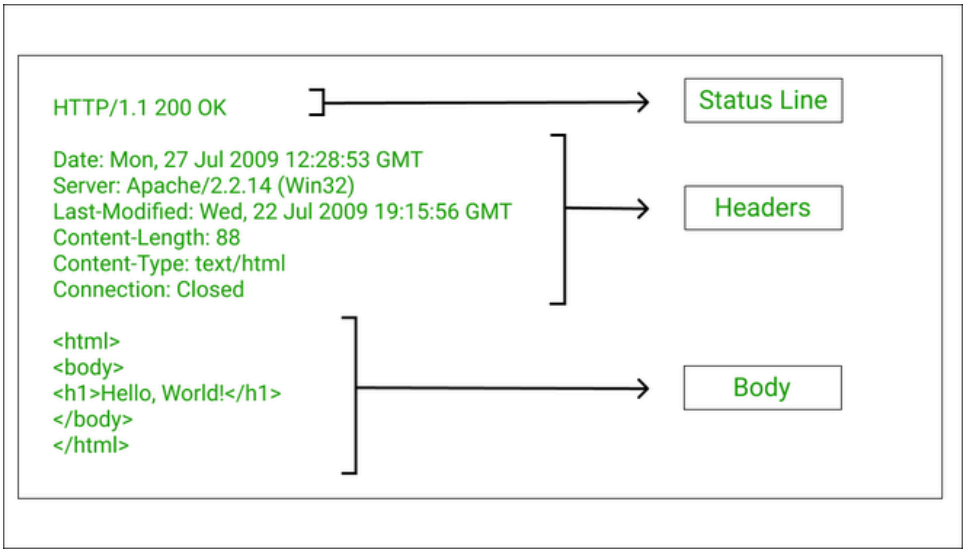
و الهيدر ده اصلا مهمته الاساسياة ان يعرف المتصفح عشان يعرف يفكه .

لانه اكيد المتصفح مش هيفكه من غير ما يعرف نوع الضغط.

4-empty line :

رابع حاجة في ال http response و ديه حاجات اساسيه في اي http message هو ال empty line اللي بيفصل ما بين ال headers و ال body .

5-Body :



و ديه هيا البيانات اللي تبتقا في ال Response .

6-HTTP Cookies and Sessions

—----------

سيرفرات المواقع عندنا بتتشتغل ب طريقتين :

- HTTP stateless :

ال http stateless يعني السيرفر (الموقع) مبيفتكرش حاجة. طب يعني ايه ؟؟؟ يعني ان الموقع مبيفتكرش , يعني اي موقع من غير cookies and sessions مبيفتكركش و و هنشرح يعني ايه cookies and sessions قدام , و بختصار دول حاجة بيخلو الموقع يفتكرك .

مثال :

دلوقتي موقع زي ال facebook , انت اول ما بتدخل بتعمل تسجيل دخول . و لو طلعت و دخلت تاني هتلاقيه افتكرك و دخلك عادي من غير ما تعمل تسحيل دخول تاني و و ده بسب ال cookies and sessions .

- HTTP stateful:

تاني حاجة هيا ال http stateful و هنا بق السيرفر بيفتكرك . بسب ال cookies and sessions . و بسبب هنا الموقع هيتفكرك و لو انت عامل تسجيل دخول قبل كده هيدخلك عادي من غير ما تعمل تاني لانه افتكرك .

—----------

1-cookies :

ال cookies ديه عباره عن ملفات بتحطط في المتصفح بتاعك عشان تفكر الموقع انت مين .

و زي ما قلنا لو انت كنت عامل تسجل دخول في موقع و قفلته و فتحته تاني هتلاقيه دخل علي طول من غير ما تعمل تسجيل دخول تاني . و ده بسبب ال cookies عشان ملفات الكوكيز هي اللي فكرته .

- **Set cookie Header (HTTP Response) :**

لما الموقع يحب يعملك cookie و يبعتهالك , فا بيبعتهالك عن طريق Header اسمه set cookie .

خلينا متفقين ان header ال set cookie بيبقا موجود في ال http Response بس . و مش موجود في ال http Request , يعني بيبقي فيه اختلاف في الاسماء و شوية حاجات هنشرحها قدام .

هيدر ال set cookie بيتكون من جزئين أساسيين :

و هما ال key-value و ال attributes و هنشرح دلوقتي .

1-KEY-VALUE :

ال key and value (بالعربي يعني المفتاح و القيمة)

دول المعلومات الاساسية اللي السيرفر عايز يخزنهم عندك في ال cookie .

مثال :

Set cookie : username=MohamedAdel; password=123;

ال username و ال password هما المفاتيح , دول زي كده العناوين الرئيسية للبيانات اللي السيرفر عايز يخزنها عندك . بس طبعا اسامي ال keys مش ثابتة كده كده السيرفر بيغير اسامي المفاتيح .

MohamedAdel و 123 دول القيم بتاعت المفاتيح . و دول هما البيانات بتاعت المفاتيح .

و دول كلهم هما المحتوي الاساسي لل cookie .

. و كده مش هضطر تسجل دخول كل مره في الموقع لان المتصفح هيبعت للسيرفر ال cookie كل مل تدخل الموقع .

2-Attributes :

الخصائص ديه هيا الخيارات اللي بتتحكم في اعدادات ال cookie و امان ال cookie .

و ال attributes ديه بتيجي بعد المحتوي الاساسي للكوكيز اللي هيا key-value .

و هنقول دلوقتي اهم ال attribute اللي بتتحكم في الكوكيز و أمان الكوكيز .

- Expires :

ال expires هو ال attribute اللي بيحدد الوقت اللي هينتهي فيه ال cookie .

لان كل cookie و بيبقا ليها وقت و بيخلص و لما وقتها يخلص مش هينفع تتبعت تاني .

مثال :

```
Set cookie : user=Mohamed; pass=1234; Expires=Wed, 23 Jul 2025 12:00:00 GMT;
```

- Domain :

ال domain هو attribute بيحدد مين ال domain اللي يتبعتله ال cookie .

لان مش اي موقع بتفتحه يتبعتله ال cookie . لازم يكون نفس ال domain اللي في ال cookie .

فيه تلت طرق بيتحط بيها ال domain في ال cookie :

اول طريقة:

```
Set cookie : Domain=example.com
```

أو

```
Set cookie : Domain=.example.com
```

في الاتنين دول المتصفح هيبعت ال cookie ل دومين example.com و اي دومين فرعي زي مثلا test.example.com .

تاني طريقة :

```
Set cookie : Domain=test.example.com
```

هنا المتصفح هيبعت ل دومين test.example.com و اي دومين فرعي , زي مثلا test2.test.example.com .

ثالث طريقة :

أن attribute ال domain ميبقاش موجود , و في الحالة ديه المتصفح هيبعت ال cookie ل ال domain الرئيسي فقط و مش هيبعت لاي subdomain .

- Path :

ال attribute ده بيتحط فيه المكان اللي هيتبعت فيه ال cookie في الموقع .

يعني ايه ؟؟

يعني ملو كان محطوط في ال path : /login فا وقتيها لو فتحت الموقع علي اي مكان غير ال /login مش هيبعت ال cookie .

```
Set cookie : Domain=example.com ; Path=/login;
```

هنا هو يبعت ل صفحه ال login بس و اي مسار فرعي , زي مثلا

/login/admin

3-Flags :

هتقولي دلوقتي هو احنا مش قولنا ان احنا عندنا جزئيين اساسيين في ال cookies ,
طب امال ايه ال flags ديه ؟؟

ال flags هي عبارة عن attributes بس متخصصه في امان ال cookies ,
لأن زي ما قولتلك في الاول ال attributes هي خيارات للتحكم في ال cookie وكمان أمان ال cookie .

- HttpOnly :

ده attribute بيمنع اي اكواد javascript تتنفذ علي ال cookie .
يعني ايه ؟؟
يعني لو مثلا انت فتحت موقع خبيث , و الموقع ده بينفذ اكواد javascript لسرقة ال cookies من متصفحك , وقيتها لو ال cookies اللي موجوده في متصفحك فيها attribute ال HttpOnly فا ال cookies مش هتتسرق , عشان المتصفح هيمنع ان اكواد ال javascript تتنفذ .

```
Set cookie : Domain=example.com; HttpOnly;
```

- Secure :

ده attribute بيخلي ال cookie متتبعتش لو الموقع http , يعني ال attribute ده بيخليها تتبعت لما الموقع يكون https بس . عشان لما يكون الاتصال http وقتيها الاتصال مش هيكون مشفر , فا بالتالي ممكن ال cookies تتسرق .

مثال :

```
Set cookie : Domain=example.com Secure;
```

لو مثلا موقع example.com اللي ال cookies بتتبعته , حول فجأة و بقى http لاي من الاسباب , فا وقتها ال cookie مش هتتبعته .

و كده انت فهمت ال cookies ديه بتعمل ايه و بتتكون من ايه كمان .

2-Sessions

ال session ديه هيا جلسة بيتحفظ فيها معلومات عنك و الحاجات اللي بتعملها علي الموقع , و الجلسة ديه و البيانات اللي فيها بتتحفظ في السيرفر .

مثال :

لو مثلا عملت تسجيل دخول في موقع , فا بيانات تسجيل الدخول بتتحفظ في الجلسة اللي في السيرفر , عشان لما تفتح الموقع تاني بعد ما تقفله متضطرش انك تعمل تسجيل دخول تاني . فا بالتالي او لما تقفل الموقع و تفتحه هتلاقي الاكونت بتاعك لسا مفتوح .

مثال تاني :

لو مثلا كنت في موقع منشورات و انت مش عامل تسجيل دخول , و عملت حفظ ل منشور ما , و طلعت بره الموقع و دخلت تاني و لقيت المنشور لسا معمولة حفظ مع انك مش عامل تسجيل دخول , فا ده بسبب الجلسة لانها حفظت المنشور في الجلسة بتاعتك .

- **طب ازاي السيرفر بيعرفك و بيدخلك علي الجلسة اللي هو فاتحهالك ؟؟**

كل جلسة انت بتفتحها في السيرفر , بيبقا ليه id يعني رقم معرف للجلسة ديه ,

و السيرفر بيبعتلك ال session id و بيحطها في ال cookie بتاعتك .

عشان لما تبعت ال cookie للموقع يعرف ال id بتاع الجلسة بتاعتك و يدخلك فيها .

```
Set cookie : Domain=example.com; Session_id=1234;
```

كده انت لما تبعت الكوكي ديه للموقع هيدخلك علي طول في الجلشة بتاعتك .

- **طيب هتسالني دلوقتي سؤال و تقولي امال ايه الفرق ما بينها و بين ال cookie ؟؟؟**

الفرق الوحيد بين ال Session و ال cookie , هو ان ال Session بتخزن المعلومات في السيرفر . و ال cookie المعلومات بتتخزن في المتصفح .

طب ده ايه فايدته ؟؟

احب اقولك ان بسبب ال cookie وأن المعلومات بتتخزن في المتصفح , ده ادى ان ممكن اي معلومات تتسرق من ال cookie بسهولة لو ال cookie مش متامنه كويس.

لكن في ال Session , المعلومات بتتخزن في السيرفر و السيرفر في الغالب بيبقا متامن كويس جدا . عكس جهازك اللي ممكن يكون مش متامن و ال cookie تتسرق من متصفحك .

و كده الحمدلله تم شرح ال Web fundamental
