الفصل الثالث عشر
ثغرة ال Rate-Limit

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال Rate-Limit

- ماهو Rate Limit
- هو المسؤول عن التحكم بمقدار الطلبات من الكلاينت او المستخدم (Requests) للسيرفر .
- أنواع Rate Limit
- يوجد ثلاث انواع وهي :-

User rate limiting	نوع يخص endpoint يتعامل معه المستخدم مثل "اضافة منتج" اذا تجاوز العدد المسموح له من الطلبات سوف يرفض السيرفر اي طلب آخر لكن سوف يستطيع بطبيعة الحال التعامل مع endpoints المتبقية مثلا "حذف منتج"
Geographic rate limiting	هو نوع يتبع مكان وزمن يحدده المبرمج يدويا او تلقائيا, مثلا بعد فترة منتصف الليل يقلل من حد rate limit تفاديا لأي هجوم او لأي سبب كان
Server rate limiting	هو نوع يكون على مستوى السيرفر كامل مثلا تجاوزت الحد المعين عن البحث عن صديق لك بنشاط مشبوه, يقوم هذا النوع بحظرك بشكل كامل ويمنعك من زيارة او استخدام اي صفحة او endpoint ان كان مؤقتا او لا .

ثغرة ال Rate-Limit (تكمله...)

- شرح فكرة وأهمية Rate Limit
- في حياتنا العادية عندما نرى تصرفات مسيئة نقول مع أنفسنا "كل شيء له حدود حمراء" , هذه هي فكرة Rate Limiting ف هنا سوف تعرف ان Rate Limit مهم في مشاريعنا او تطبيقاتنا او API الخاص بنا, ف هو يحميك من الهجمات مثل التخمين و هجمات حرمان الخدمة .
- سوف نتحدث بشكل مهم جدا في هذه الفقرة, كما ذكرت سابقا ان فكرة Rate Limiting هي وضع حد للطلبات من المستخدم, لكن سوف نأخذ الجهة قليلا من الضحية الى المخترق , وقبل أتكلم مطولا يجب ان نذكر القصة الشهيرة اللتي حدثت لتويتر سنة 2009

ثغرة ال Rate-Limit (تكمله...)

- وصل المخترق الى صلاحيات مسؤول في تويتر بسبب عدم وجود Rate Limit, وطبعا لن أحكي لكم الخسائر, وأيضا كما نرى دائما في تطبيقات ومواقع البنوك والأتصالات الخ.. حول العالم تستخدم مايسمى OTP للتحقق من المسجل ويكون دائما كود التحقق غالبا مكون من 4-6 خانات !! ماذا لو في هذه الحالة لم يضع المبرمج Rate Limit ماذا يحدث ؟ بكل بساطة لن يحتاج المخترق الا كتابة exploit يقوم بتخمين OTP وصدقني لن يحتاج سوى دقائق معدودة لأختراق بياناتك كاملة ووصول كامل للمستخدم (Full Takeover) فالمبرمج في هذه الحالة لن يستطيع تعويض المستخدم ثمن معلوماته الحساسة, من الأفضل دائما أخذ التدابير الأمنية للبنية التحتية واصغر خطأ سوف يواجهه ضرر بكل تأكيد , وهذه مجرد أمثلة وهناك الكثير من سيناريوهات الهجوم اللي يتبعها المهاجم في عدم وجود rate limit.

ثغرة ال Rate-Limit (تكمله...)

- وضع Rate Limit
- اذا كنت مستخدم اطار العمل Laravel فأستخدم Throttling جدا ممتاز, وتوجد عدة طرق في برمجة Rate limiting بأستخدام طريقتين شهيرتين وهي عن طريق Session والثانية IP, توجد مشاريع جاهزة كثيرة على GitHub اكتب في محرك البحث Rate Limitوسوف ترى الكثير من المشاريع بشتى اللغات البرمجية واطارات العمل اختار ماينا سبك, ولمن لديه Nginx تستطيع استخدام ngx_http_limit_req_module وهي تعتمد على ماذكرت لك في في النوع الأول IP

```
http {
    limit_req_zone $binary_remote_addr zone=one:10m rate=2r/s;
    ...

server {
    ...
    location /YourPathIfYouHave/ {
        limit_req zone=one burst=5;
    }
}
```

ثغرة ال Rate-Limit (تكمله...)

- وأيضا في Apache يوجد mod_ratelimit وهي تعتمد على ماذكرت لك في في النوع الأول IP

```
<Location "/YourPathIFYouHave">
    SetOutputFilter RATE_LIMIT
    SetEnv rate-limit 400
    SetEnv rate-initial-burst 512
</Location>
```

تم بحمد الله انتهاء الفصل الثالث عشر