**🧠 1. Havij Nedir?**

**Havij**, özellikle SQL Injection (SQLi) zafiyetlerini **otomatize etmek** için geliştirilmiş bir **Windows tabanlı GUI araçtır**.

📌 Geliştirici: ITSecTeam  
📌 İlk sürüm: 2010’ların başı  
📌 GUI ile çalışır – kod yazmadan SQLi gerçekleştirme imkanı sunar

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 SQL Injection bulma | Verilen URL’de SQLi olup olmadığını test eder |
| 📥 Veritabanı dump işlemi | Tabloları, kolonları ve verileri indirir |
| 🧾 Database bilgisi çıkarımı | Database version, DBMS türü, kullanıcı vs. |
| 🧪 Login bypass ve shell yükleme | Bazı durumlarda komut çalıştırma veya admin panel bypass |
| ⚙️ Desteklenen veritabanları | MySQL, MSSQL, PostgreSQL, Oracle, MSAccess, DB2 |

**🖥️ 3. Arayüz ve Kullanım Adımları**

**✅ 1. Havij’i başlat (Windows)**

* Program çalıştırıldığında sade bir GUI açılır

**✅ 2. Hedef URL’yi gir**

http://target.com/page.php?id=1

🔸 Dinamik sayfalar, GET parametreleri içeren yapılar önerilir

**✅ 3. "Analyze" butonuna tıkla**

* Havij hedefi analiz eder
* SQLi varsa tipini tespit eder (error-based, union-based, vs.)

**✅ 4. Veritabanı bilgilerini çek**

* Database name, sürüm, kullanıcı vs.

**✅ 5. "Tables" → tablo adlarını getir**

**✅ 6. "Columns" → tablo içinde kolonlar**

**✅ 7. "Dump" → verileri indir (örneğin kullanıcı adı/parola)**

**🧪 4. Örnek Senaryo**

Hedef site:

http://vulnerable-site.com/news.php?id=5

Havij çıktısı:

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧷 5. Shell & Command Özellikleri**

Bazı sistemlerde Havij şu ekstra fonksiyonları da sunar:

* **Shell yükleme (CMD / PHP)**
* **File upload**
* **Login bypass**
* **Current path** öğrenme

⚠️ Bu işlemler genellikle sadece zayıf yapılandırmalarda mümkündür!

**🔒 6. Havij Kullanımına Dikkat!**

| **Durum** | **Risk** |
| --- | --- |
| ❌ GUI kullanım kolaylığı | Bilgi seviyesi düşük kişilerce kötüye kullanılabilir |
| ❌ Güncel AV yazılımları | Havij’ı zararlı olarak tanıyabilir |
| ❌ Web tarayıcı logları | IP adresiniz kayıt altına alınabilir |

**🎯 7. Öğrenim Kazanımları**

* SQL Injection sürecini grafiksel arayüz üzerinden tanıma
* Veritabanı yapılarını anlama ve keşfetme
* Hangi SQLi türlerinin hangi veri erişimlerine neden olduğunu görme
* Pentest otomasyonunun avantajlarını fark etme