Challenges

HDC

Network Setup

- Connected to HTB OpenVPN Server via OVPN file

Found Vulnerabilities

- Credentials found in jsquery-3.2.1.js file under ‘name1’(username) and ‘name2’(password) parameters
- Email Lists under an image logo path location directory

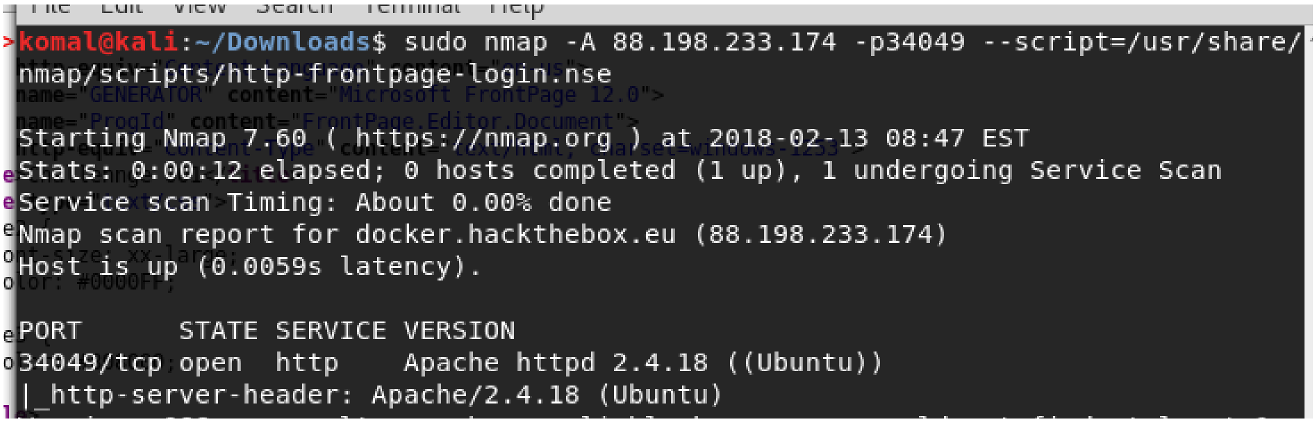
Exploits/Payloads Used

- None

Key Findings

- **Web Server:** Apache httpd 2.4.18
- **OS:** Ubunutu
- **Language:** .php, .js

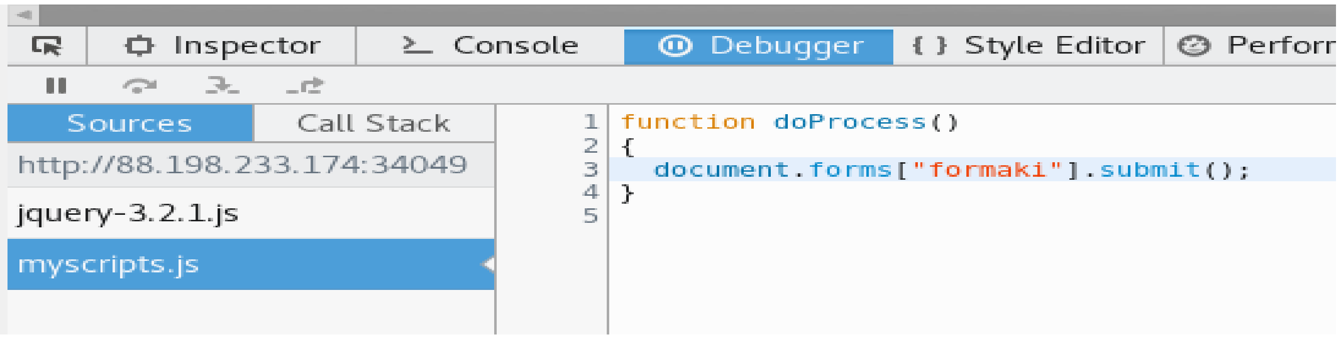
Write-Ups & Screenshots



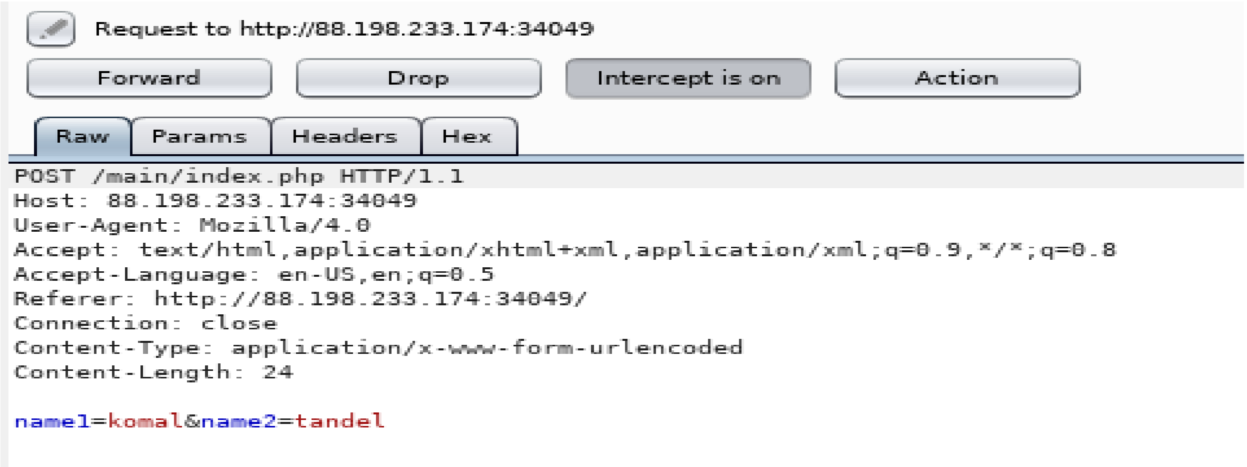
```
komal@kali:~/Downloads$ sudo nmap -A 88.198.233.174 -p34049 --script=/usr/share/
nmap/scripts/http-frontpage-login.nse

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-13 08:47 EST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for docker.hackthebox.eu (88.198.233.174)
Host is up (0.0059s latency).

PORT      STATE SERVICE VERSION
34049/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
```



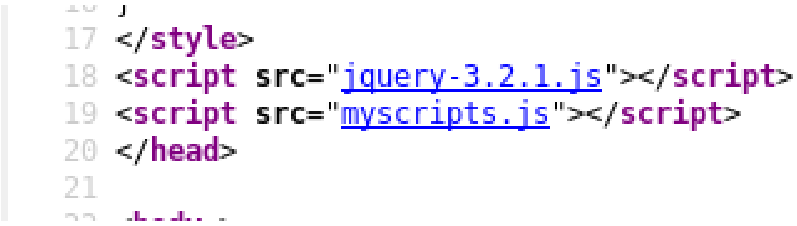
```
function doProcess()
{
  document.forms["formaki"].submit();
}
```



```
POST /main/index.php HTTP/1.1
Host: 88.198.233.174:34049
User-Agent: Mozilla/4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://88.198.233.174:34049/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

name1=komal&name2=tandel
```

>> Under the source code you will find two script files.



```
</style>
<script src="jquery-3.2.1.js"></script>
<script src="myscripts.js"></script>
</head>
```

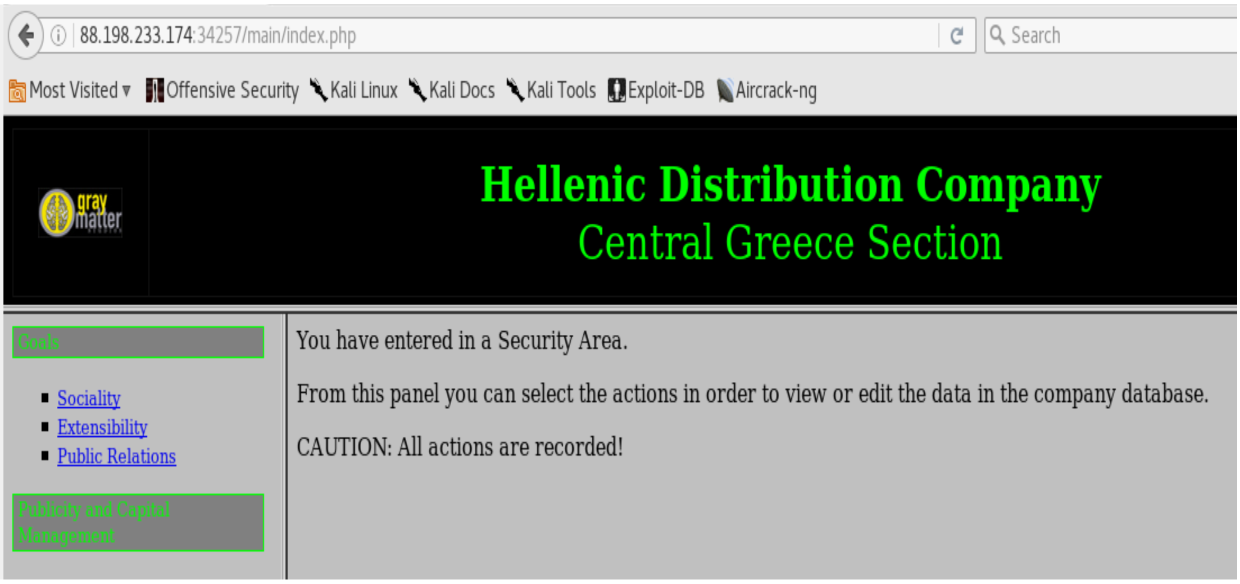
```
hiddenField.setAttribute("name","name1");
hiddenField.setAttribute("value","TXlMaXR0bGU");

var hiddenField2=document.createElement("input");

hiddenField2.setAttribute("type","hidden");

hiddenField2.setAttribute("name","name2");

hiddenField2.setAttribute("value","cDB3bmll");
```



Hellenic Distribution Company
Central Greece Section

You have entered in a Security Area.

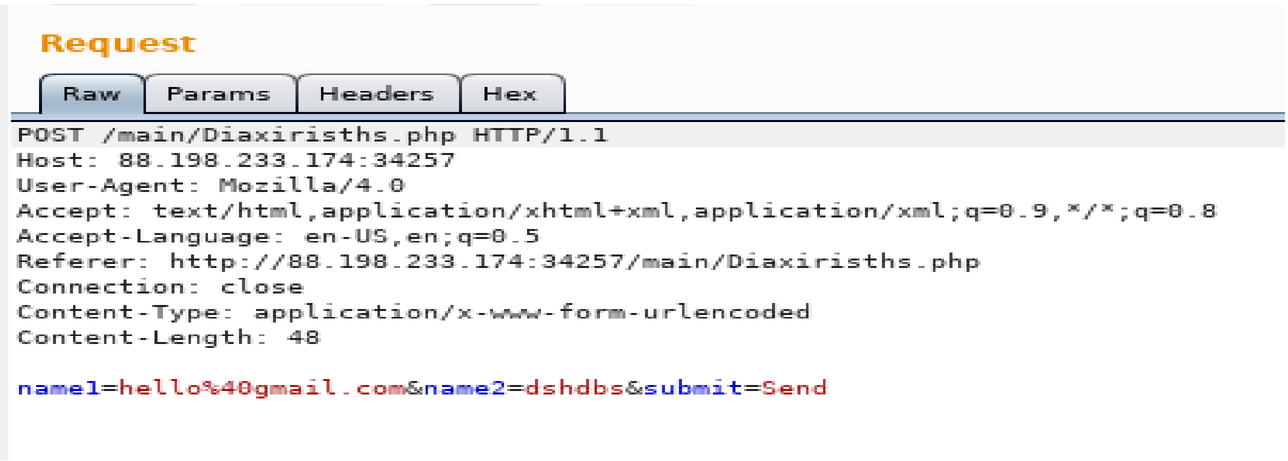
From this panel you can select the actions in order to view or edit the data in the company database.

CAUTION: All actions are recorded!

After logging, the page redirects to:

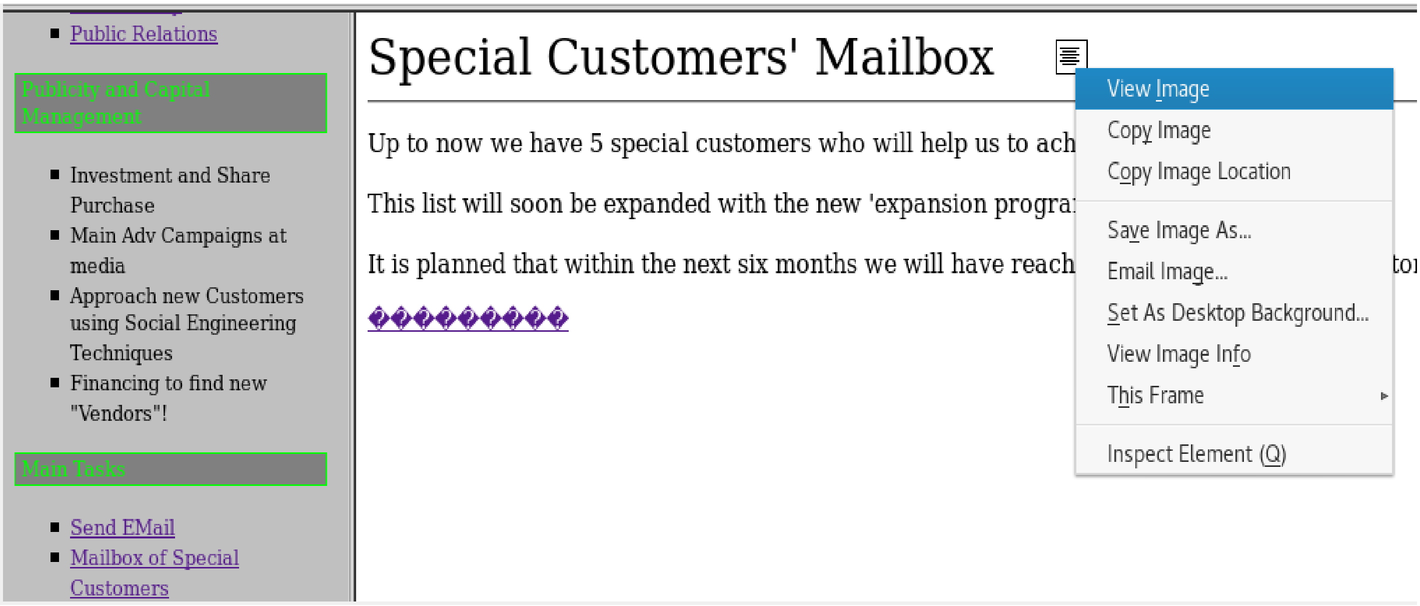
main/Vbanner.php and then… main/index.php

However, Nothing interesting Found



```
POST /main/Diaxirisths.php HTTP/1.1
Host: 88.198.233.174:34257
User-Agent: Mozilla/4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://88.198.233.174:34257/main/Diaxirisths.php
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

name1=hello%40gmail.com&name2=dshdbs&submit=Send
```



- Public Relations

Publicity and Capital Management

- Investment and Share Purchase
- Main Adv Campaigns at media
- Approach new Customers using Social Engineering Techniques
- Financing to find new "Vendors"!

Main Tasks

- Send EMail
- Mailbox of Special Customers

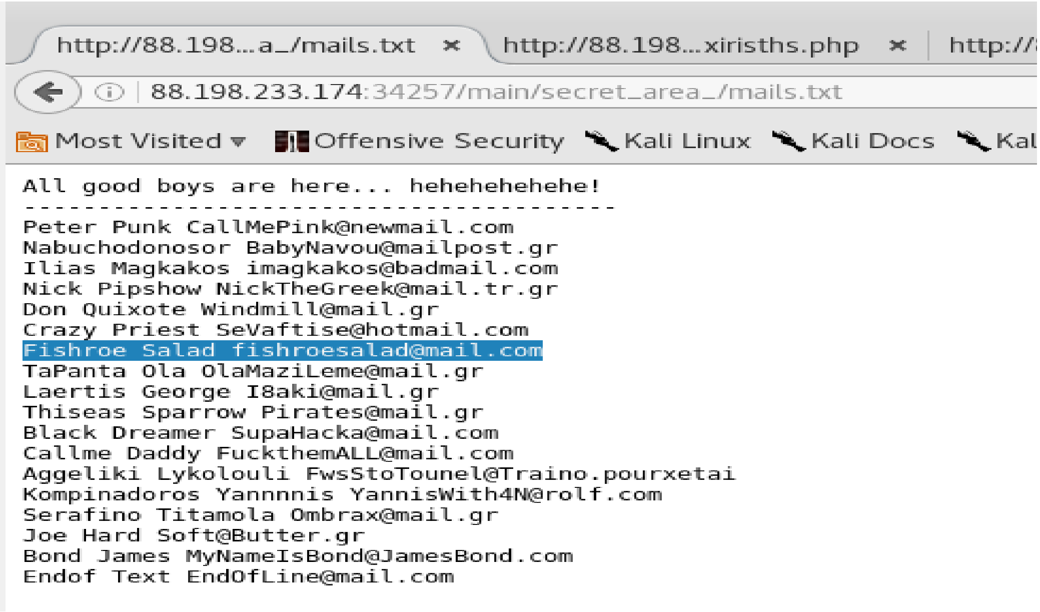
Special Customers' Mailbox

Up to now we have 5 special customers who will help us to ach

This list will soon be expanded with the new 'expansion progra

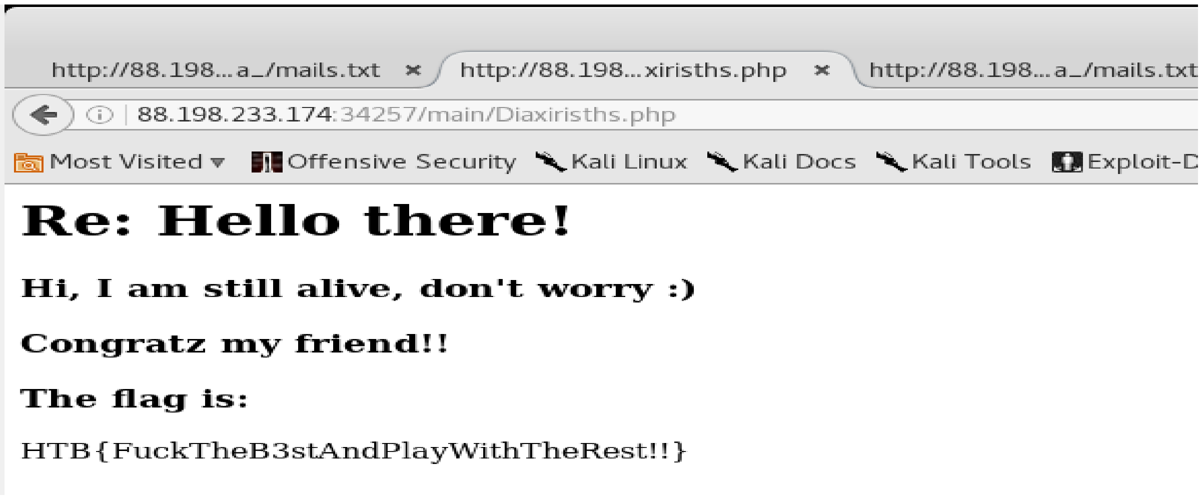
It is planned that within the next six months we will have reach   to

���������



http://88.198....a_/mails.txt
http://88.198....xirisths.php
http://
88.198.233.174:34257/main/secret_area_/mails.txt
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kal

```
All good boys are here... hehehehehehe!
----------------------------------------
Peter Punk CallMePink@newmail.com
Nabuchodonosor BabyNavou@mailpost.gr
Ilias Magkakos imagkakos@badmail.com
Nick Pipshow NickTheGreek@mail.tr.gr
Don Quixote Windmill@mail.gr
Crazy Priest SeVaftise@hotmail.com
Fishroe Salad fishroesalad@mail.com
TaPanta Ola OlaMaziLeme@mail.gr
Laertis George I8aki@mail.gr
Thiseas Sparrow Pirates@mail.gr
Black Dreamer SupaHacka@mail.com
Callme Daddy FuckthemALL@mail.com
Aggeliki Lykolouli FwsStoTounel@Traino.pourxetai
Kompinadoros Yannnnis YannisWith4N@rolf.com
Serafino Titamola Ombrax@mail.gr
Joe Hard Soft@Butter.gr
Bond James MyNameIsBond@JamesBond.com
Endof Text EndOfLine@mail.com
```



http://88.198....a_/mails.txt
http://88.198....xirisths.php
http://88.198....a_/mails.txt
88.198.233.174:34257/main/Diaxirisths.php
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-D

Re: Hello there!

Hi, I am still alive, don't worry :)

Congratz my friend!!

The flag is:

HTB{FuckTheB3stAndPlayWithTheRest!!}