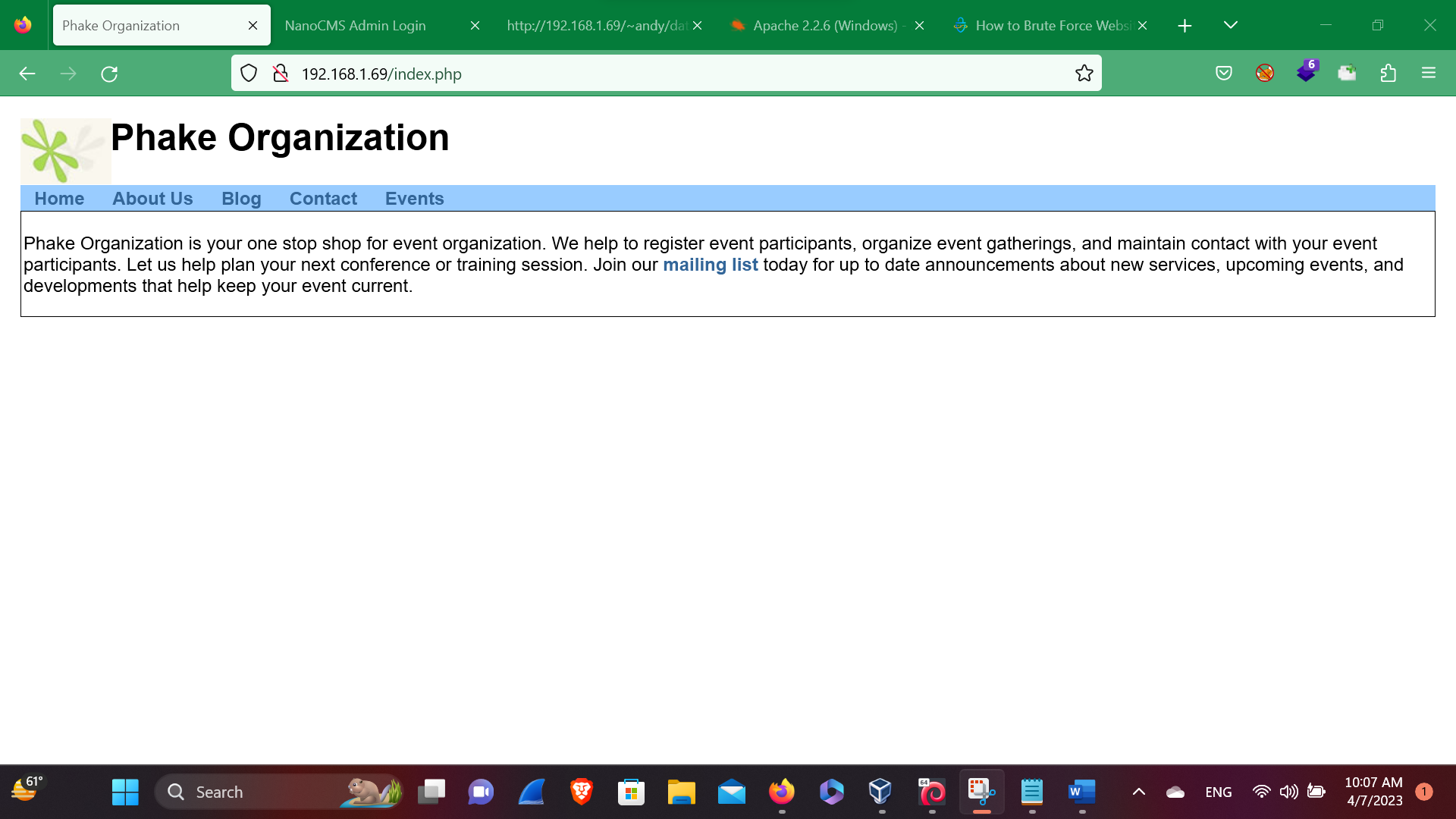
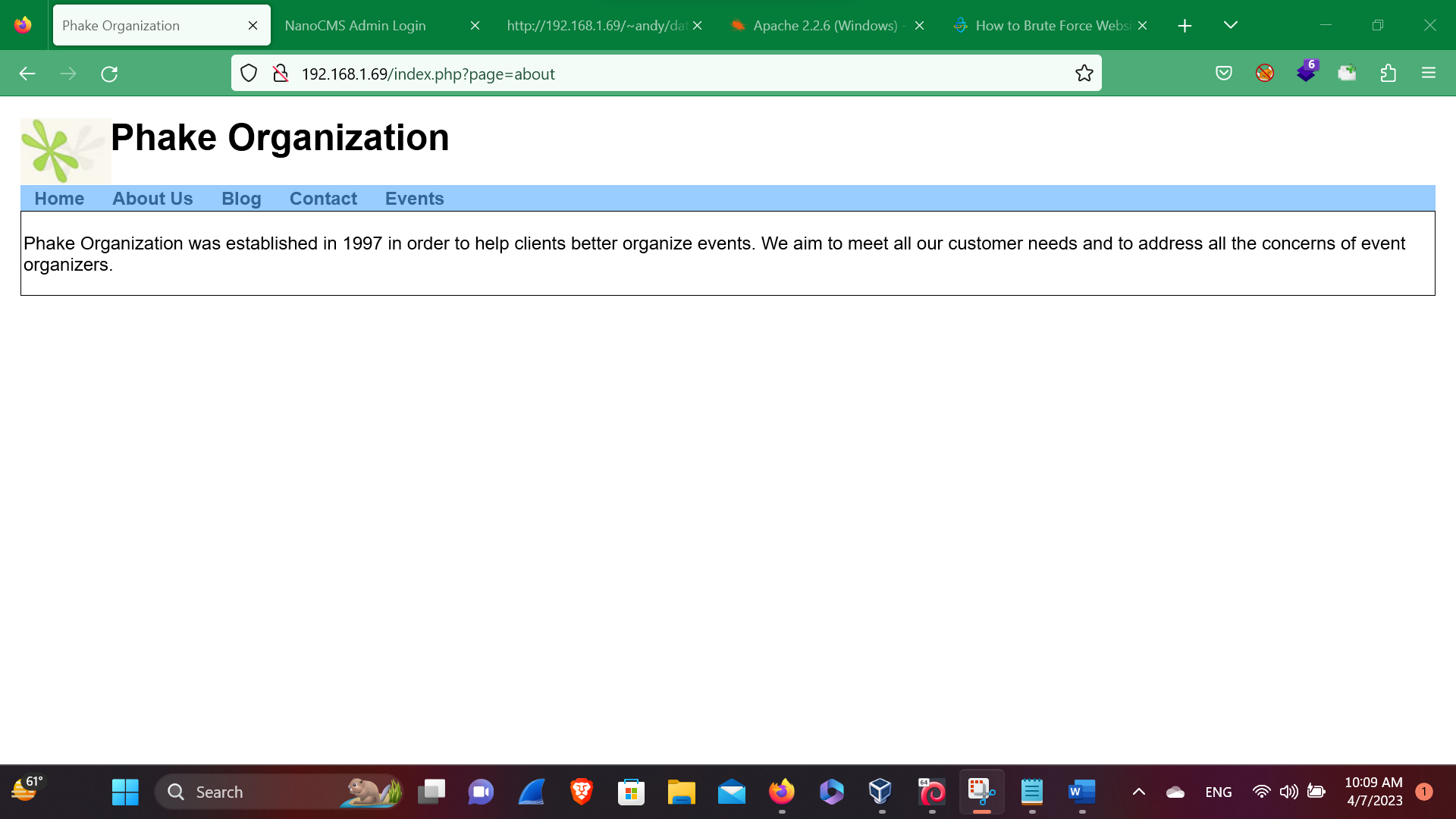
**Name:- Binay Chaudhary**

**Time:- 11:32am**

**Report:- CTF 5**

**Phake organization**

Phake Organization is your one stop shop for event organization. We help to register event participants, organize event gatherings, and maintain contact with your event participants. Let us help plan your next conference or training session. Join our [mailing list](http://192.168.1.69/list/) today for up to date announcements about new services, upcoming events, and developments that help keep your event current.

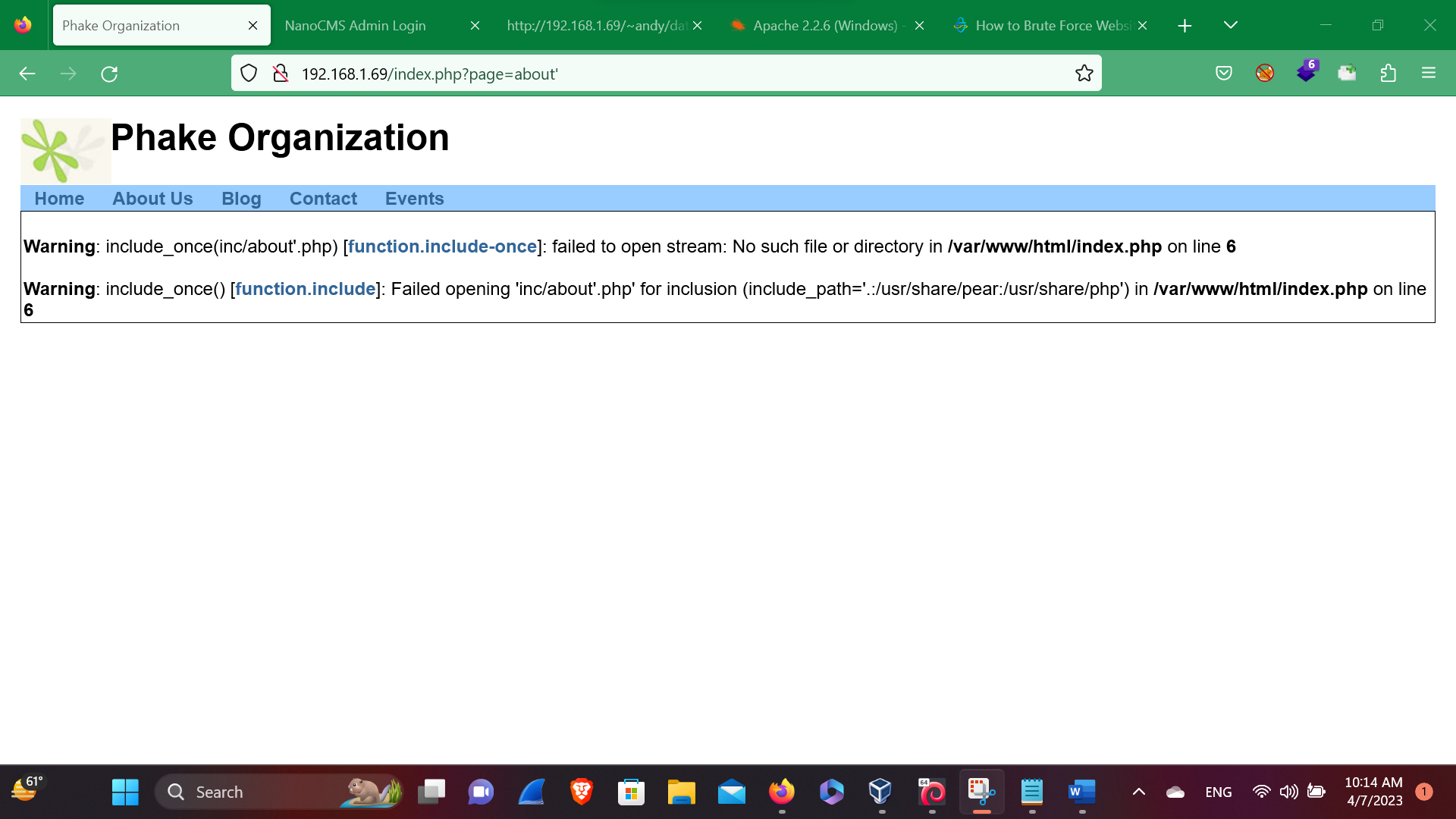
**Control on Url**

<http://192.168.1.69/index.php?page=about>

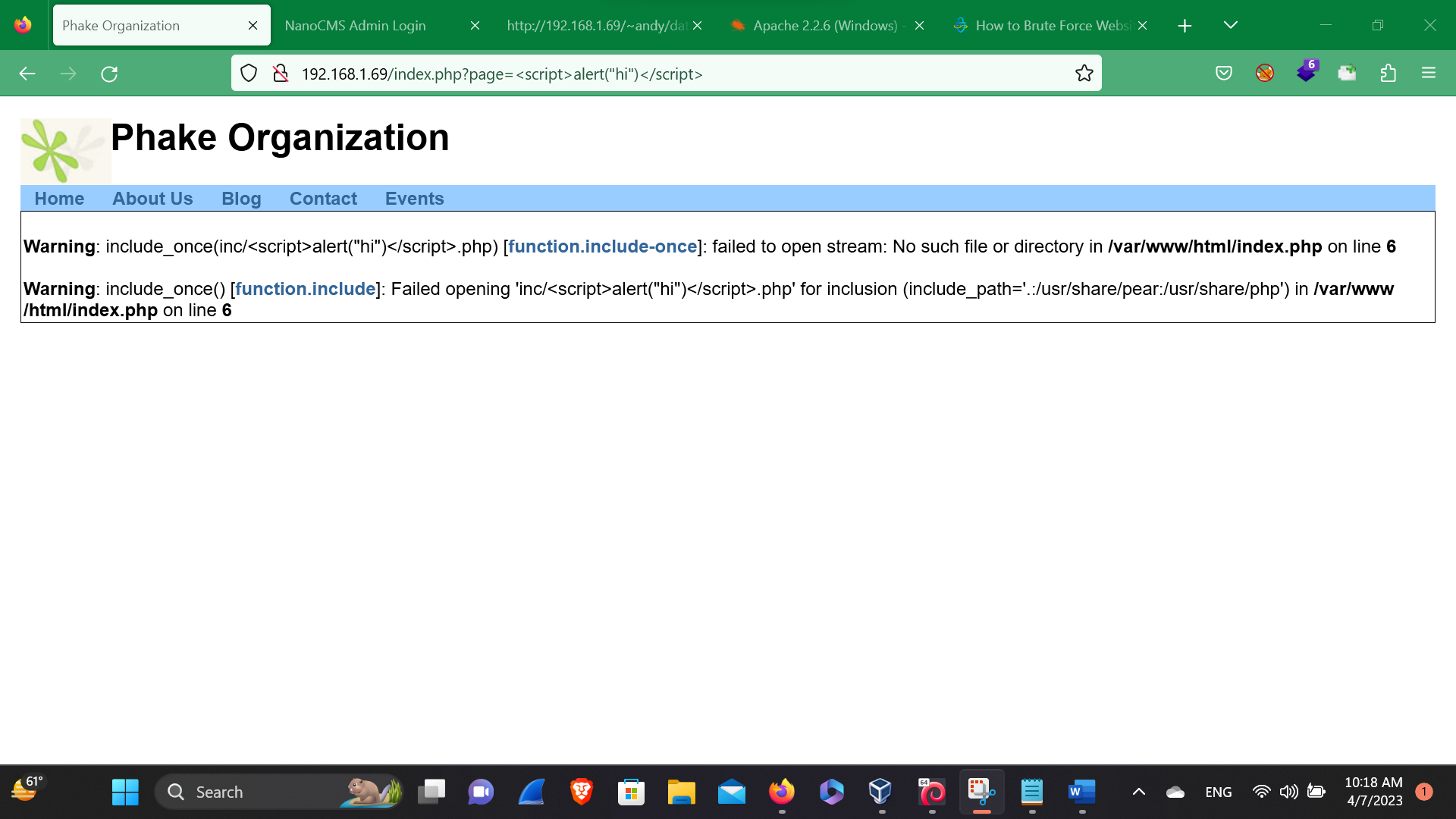
Here, in this above picture we have found the Url that can be controlled by the Attacker and may impact the company website and may breaches the Data of the Company.

So, let’s try for the bug impact in the url bar like

* SQL injection
* Xss
* LFI
* RCE

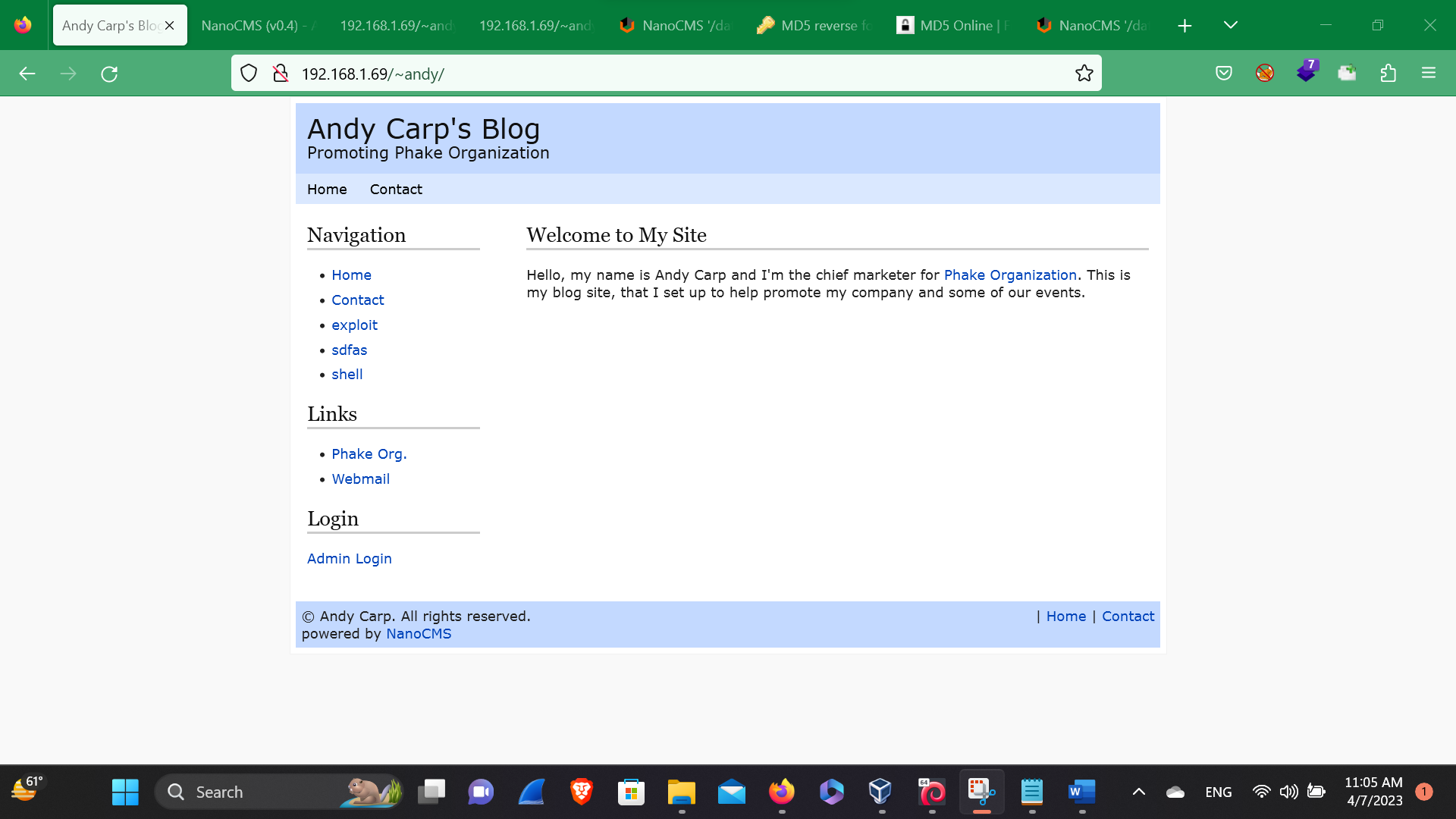
**SQL injection**

Here, in this above picture we’ve found that there is no sql injection that we’ve controlled in the URL bar so, we’ve tried for the sql injection but failed. So let’s move into another impact that can harm the company.

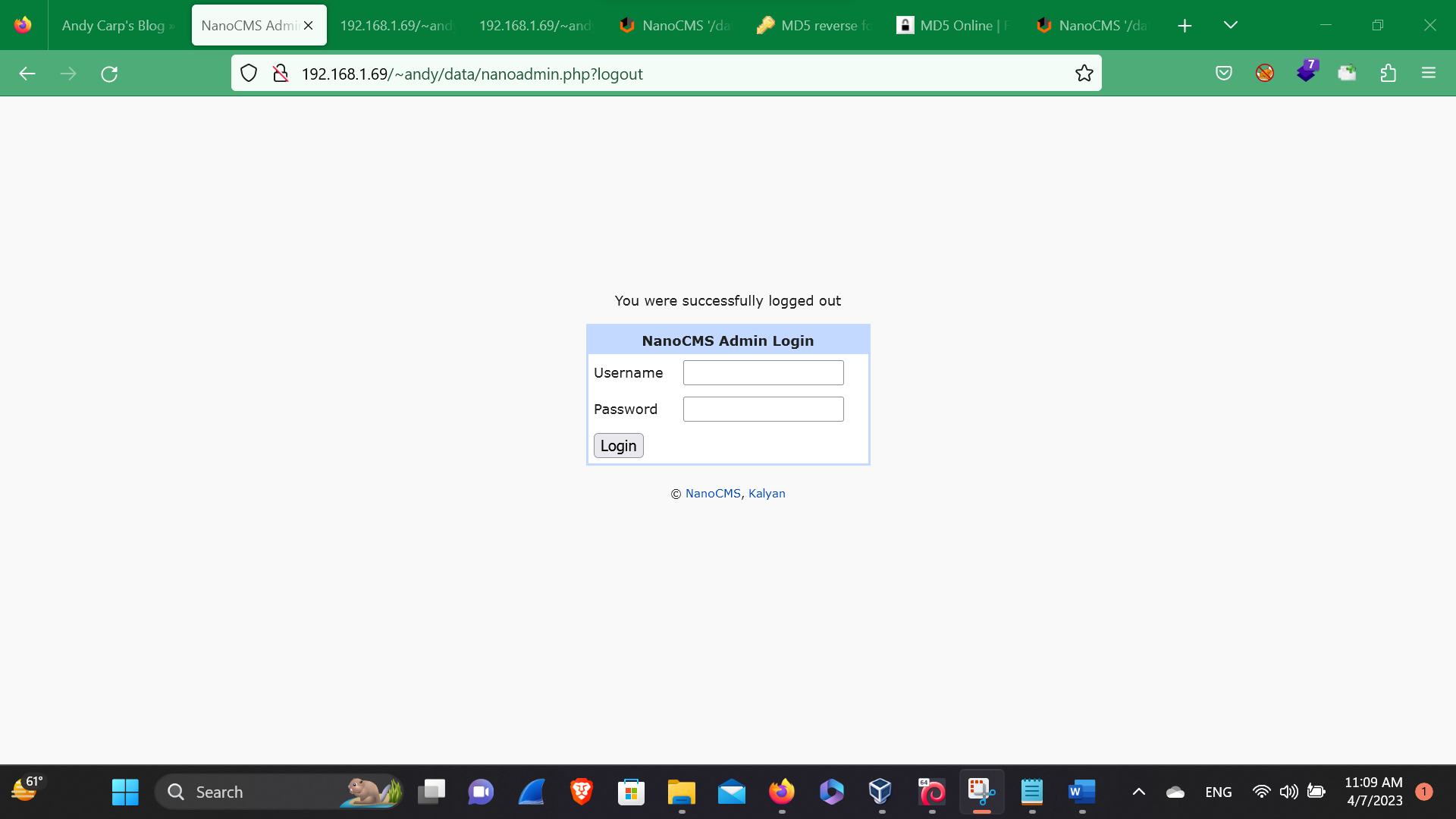
**XSS – Cross Site Scripting**

Here, in this above picture we’ve found that there is no cross site scripting,

So, let’s move into another bug. We’ve injected the following payloads that impact the url bar but it did not worked.

** Blog**

Here, in this above picture we’ve seen the following links and the login page of admin that an admin can login so, let’s go to the login page.

**NanoCMS Admin Login**

Here, by clicking in the Admin Login here, we’ve found the login page so let’s try to exploit and below down here, we have found the CMS i.e. nanoCMS so, let’s try to find out the exploit of the nanoCMS.

# After googling the nanoCMS exploit, we’ve found the informative discloser of i.e. :- NanoCMS '/data/pagesdata.txt' Password Hash Information Disclosure Vulnerability So, let’s try to put the it in the url bar so, that we can get the password and after a while we’ve found the pw. In hashes.

# /data/pagesdata.txt

# Here, in this above picture we,ve found the username and the password, so let’s try to login with the user name but the password has been in md5 so, lets go and decrypt the password with the help of the online tool named MD5 Decrypt. So, after decrypting the hashes we’ve found the password called :- Shannon

# So, let’s try to login with the username and the password.

# Logged in

# Here, in this above picture we,ve logged in the Admin Login page so, we can delete the user and the the content of the website Also, we can edit the pages

# LFI -Local File Inclusion

Here, in this above picture that there is a LFI bug so, At first we’ve done for the payloads like /etc/passwd. After an hour we’ve found some payloads that the website may get impact so, lets try to inject our malicious paylods.

../../../../etc/passwd%00

../../../../../etc/passwd%00

../../../../../../etc/passwd%00

../../../../../../../etc/passwd%00

../../../../../../../../etc/passwd%00

../../../../../../../../../etc/passwd%00