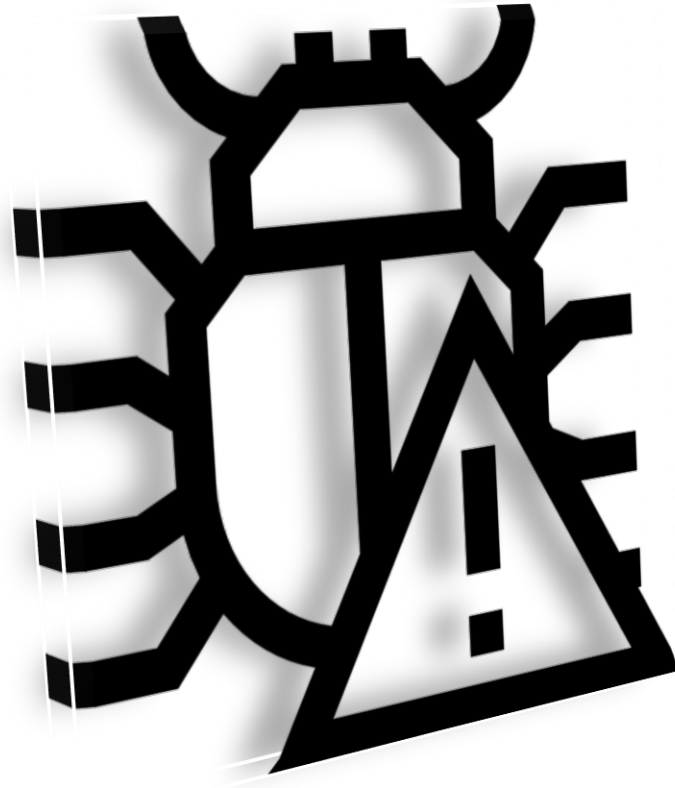


BUG REPORT



Generated by : Charchit Subedi

Date : 2022/may/8

Time : 1:06 pm

Website : <https://www.hamrobazar.com/>

CONTENT

PG.NO

Introduction -----

2

Introduction to Subdomain Scanner.....

2

Use of Subdomain Scanner 3

Introduction to Nmap 4

Use of Nmap in scanning 4

Introduction to Sql Map 5

Use of Sql Map 5

Introduction to cross site Scripting (XSS)

6

Use of Cross Site Scripting (XSS) 6-

7

Conclusion 8

INTRODUCTION TO HAMROBAZAR COMPANY

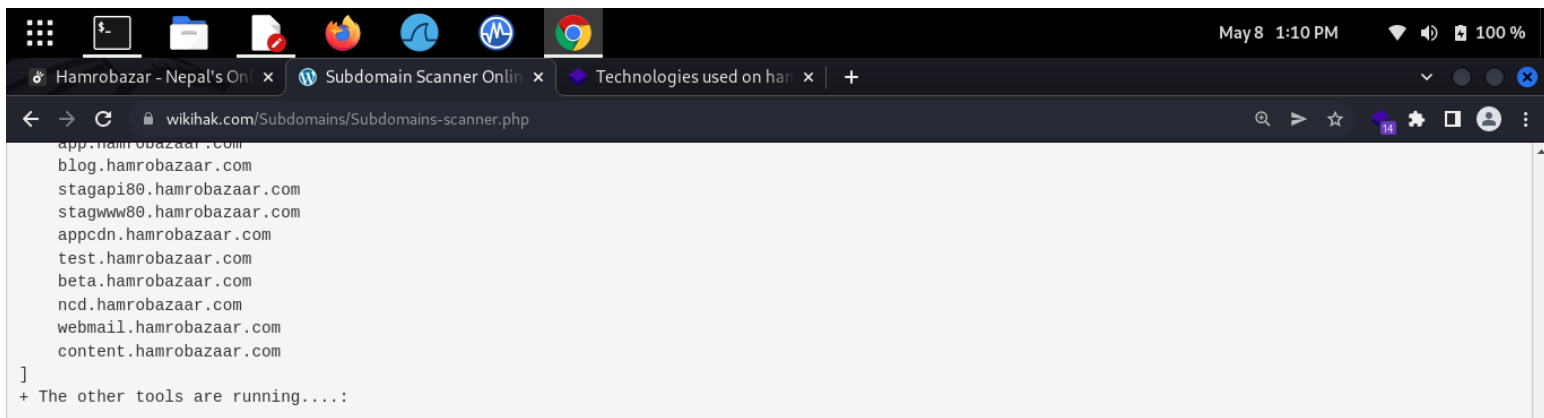
Hamrobazar.com is FREE online classified which enables individuals as well as companies to list wide variety of new or used product online. We at hamrobazar.com believe that Internet is a great promotional vehicle as well as communication channel for connecting buyers and sellers. Hamrobazar.com is perfect solution that helps to list your products for FREE.

As per NTA April 2019 report, the internet users in Nepal has reached 18.24 million (including 14.24 million mobile data users) which itself indicates that the market for internet advertising is highly lucrative. Hamrobazar is visited by around 800,000 unique visitors monthly who use the site for buying and selling purpose. Compared to newspaper classifieds, in hamrobazar.com your product will have more comprehensive detail and pictures thus enabling consumer to choose better. Hamrobazar.com has created such platform where both seller and buyers can interact with each other.

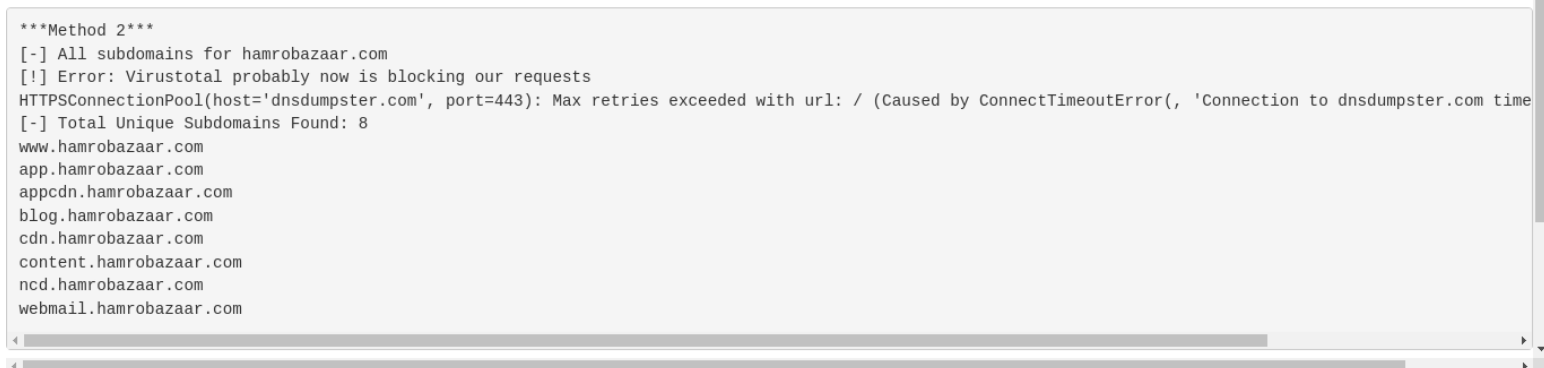
INTRODUCTION TO SUBDOMAIN SCANNER

The subdomains scanner tool will help penetration testers and ethical hackers to find and gather subdomains of any domain online.

Use of Subdomain Scanner



Method 2:



In the above picture I have scanned the <http://hamrobazar.com/> using subdomain scanner tool. And I have found the 8 Unique subdomain . They are listed below :-

www.hamrobazaar.com

app.hamrobazaar.com

appcdn.hamrobazaar.com

blog.hamrobazaar.com

cdn.hamrobazaar.com

content.hamrobazaar.com

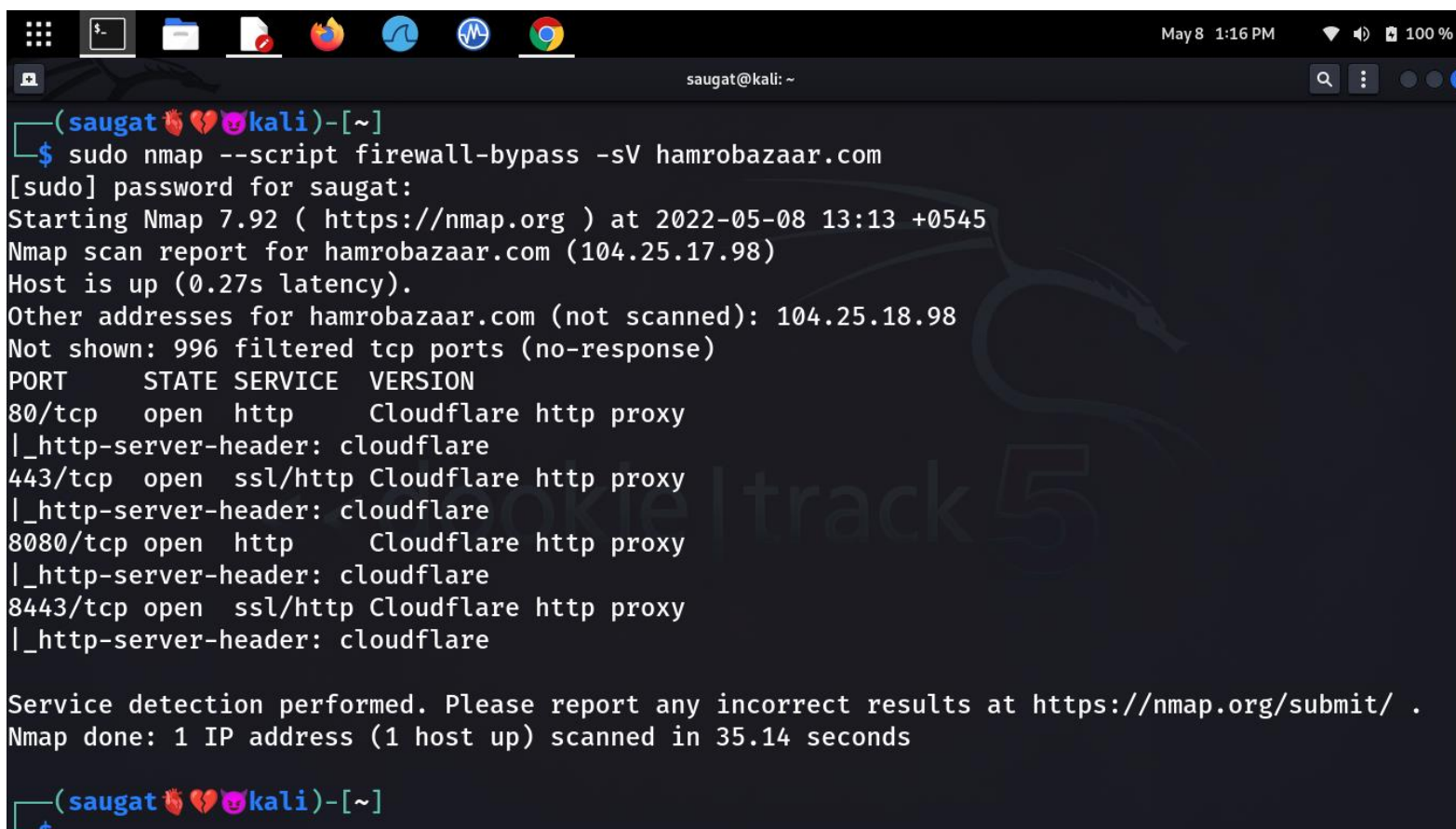
ncd.hamrobazaar.com

webmail.hamrobazaar.com

INTRODUCTION TO NMAP

Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).

USE OF NMAP IN SCANNING



```
(saugat💖💔💖kali)-[~]
$ sudo nmap --script firewall-bypass -sV hamrobazaar.com
[sudo] password for saugat:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-08 13:13 +0545
Nmap scan report for hamrobazaar.com (104.25.17.98)
Host is up (0.27s latency).
Other addresses for hamrobazaar.com (not scanned): 104.25.18.98
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Cloudflare http proxy
|_http-server-header: cloudflare
443/tcp    open  ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
8080/tcp   open  http     Cloudflare http proxy
|_http-server-header: cloudflare
8443/tcp   open  ssl/http Cloudflare http proxy
|_http-server-header: cloudflare

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.14 seconds

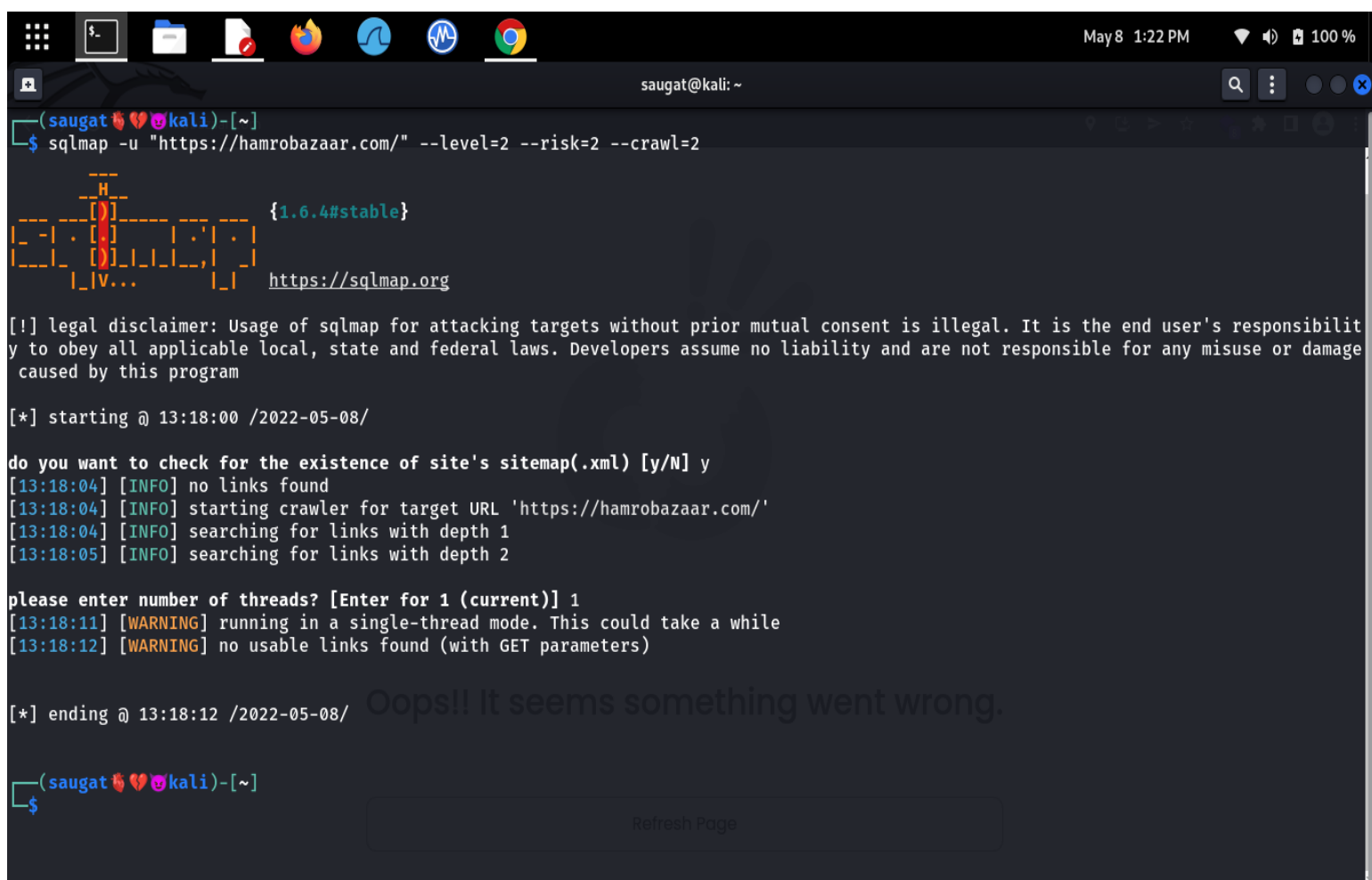
(saugat💖💔💖kali)-[~]
```

In the above picture I have used the nmap tool . From the above picture we can see that only 4 ports are open which is secured by firewall. In the above picture I have used the command “**nmap -script firewall-bypass -sV hamrobazar.com**”

INTRODUCTION TO SQL MAP

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

USE OF SQL MAP IN SCANNING



```
(saugat@kali)-[~]
$ sqlmap -u "https://hamrobazaar.com/" --level=2 --risk=2 --crawl=2

--H--
-- . -- {1.6.4#stable}
-- V -- https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:18:00 /2022-05-08/

do you want to check for the existence of site's sitemap(.xml) [y/N] y
[13:18:04] [INFO] no links found
[13:18:04] [INFO] starting crawler for target URL 'https://hamrobazaar.com/'
[13:18:04] [INFO] searching for links with depth 1
[13:18:05] [INFO] searching for links with depth 2

please enter number of threads? [Enter for 1 (current)] 1
[13:18:11] [WARNING] running in a single-thread mode. This could take a while
[13:18:12] [WARNING] no usable links found (with GET parameters)

[*] ending @ 13:18:12 /2022-05-08/

Oops!! It seems something went wrong.

(saugat@kali)-[~]
$
```

In the above picture I have done sql injection from the sql map. From the above picture we can see that nothing is happening from sql injection, but no usable link is found so, we can say that the sql injection is not possible in the website.

Introduction to Cross-site scripting(XSS)

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

Use Of Cross-site scripting(XSS)

May 8 1:15 PM100 %

GitHub - payloadbox/xss- xHamrobazar - Nepal's Onl x+

hamrobazaar.com

Network Error

hamrobazar

Entire Nepal

<embed code=javascript:javascript:alert(1) x

2रुनै

Wi-Fi MOBILITY

Over 14,000+ Hotspots

Free Value Added Services

eSewa

MONEY TRANSFER

आन्तरिक र बाह्य रेमिट्यान्स

केहि मिनेटमै बैंक खातामा पैसा डिपोजिट हुने

e

ईसेवा वालेटमा सिधै लोड गर्न सकिने

All Categories

Apparels & Accessories (5712)

Automobiles (10363)

Beauty & Health (4361)

Books & Learning (1152)

Business & Industrial (400)

Top Viewed

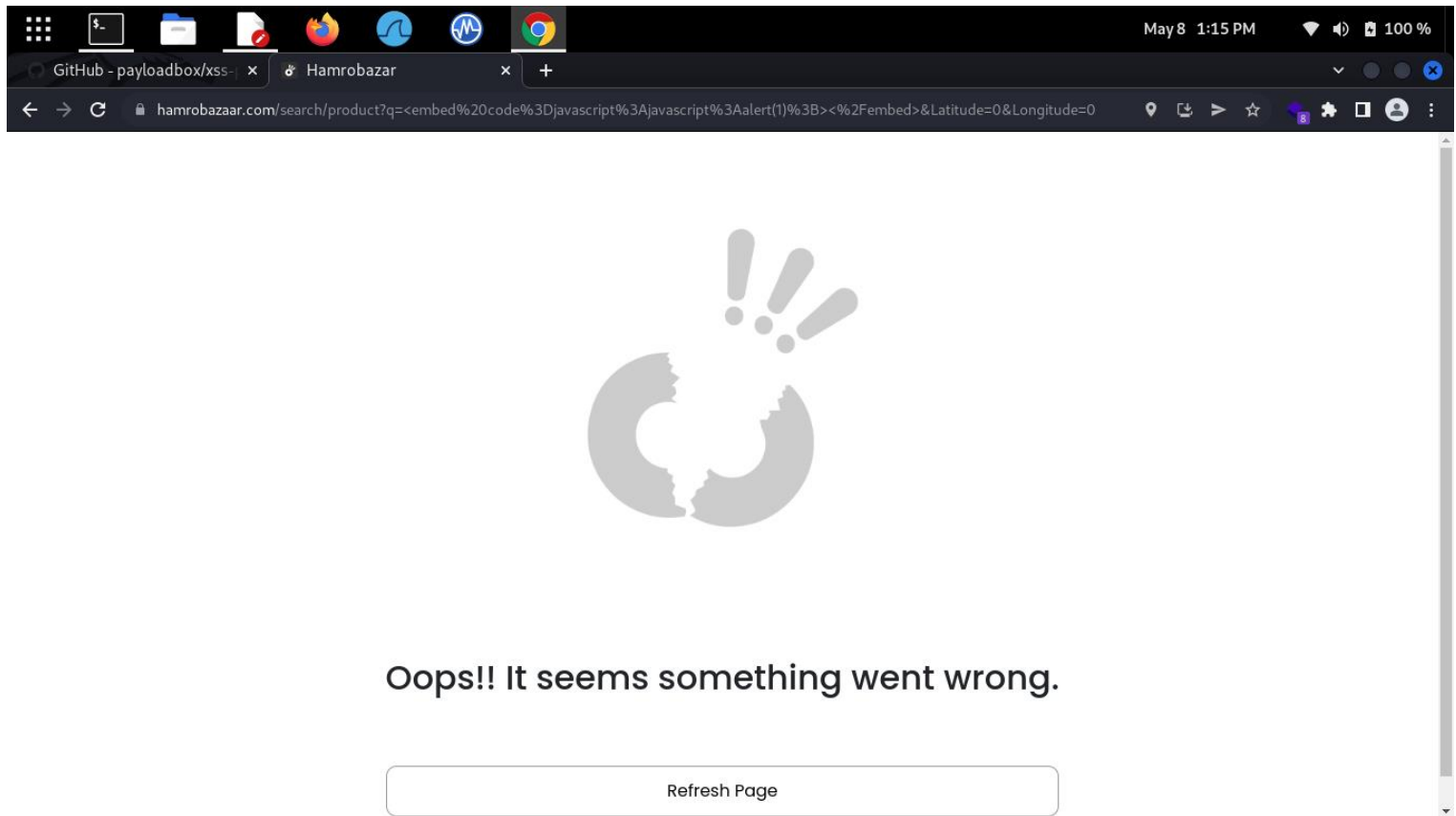
2 Acre Land Sale in

iPhone 7 Blue

Ford Figo Trend 2016

Canon 800d with

https://worldlink.com.np/home/refer-offer



In the first picture I have put the simple java script code of XSS but due to the firewall it is showing us that my internet connection is not active.

In the second picture when I hit the enter using XSS code the website is said that something went Wrong and popup the blank page. So we can say that the XSS vulnerability is not possible in the website.

CONCLUSION

Hence, We can Say that the Website is Secure and Protected by Cloudfare Firewall and Nginix Firewall. The Developer Have patched the all Loophole and Fix the vulnerability in the Website and make the layer of firewall around the Website.