

SMIT

INTRODUCTION

INTRODUCTION

1.1 OVERVIEW OF THE PROJECT

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. If it's a name they recognize, they're more likely to trust it. So they'll click malicious links, open malware attachments, send sensitive data and even wire corporate funds.

Email spoofing is possible due to the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.

Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, not every email service has security protocols in place. Still, users can review email headers packaged with every message to determine whether the sender address is forged.

1.2 SCOPE OF THE PROJECT

A successful spoofing attack can have serious consequences – including stealing personal or company information, harvesting credentials for use in further attacks, spreading malware, gaining unauthorized network access, or bypassing access controls. There is no bigger scope for attack on your organisation than e-mail.

We all use it. We all have stacks of it. And we have all fallen for some gimmick or promise. Or not even that, spoofing, where you thought Stuart in Product Development was genuinely asking you out for dinner and so needing you to send back your phone number! Only to then get inundated with phone calls as you've given your number out to the bad guys.

1.3 GOALS AND OBJECTIVES

The goal of email spoofing is to trick users into believing the email is from someone they know or can trust in most cases, a colleague, vendor or brand. Exploiting that trust, the attacker asks the recipient to divulge information or take some other action.

Primary motive behind phishing attack:

The motive of the attacker can be anything, but the most reasonable reason is earning money. Mostly Phishing is used to get sensitive information. This information may be used by the attacker or may be sold for cash to a third party. Other motives are possible, but money is the primary concern in most cases.

Purpose of phishing attack:

- **Provide Sensitive Information:** This aims to gain sensitive information such as login credentials, ATM PINs, credit card details, social security numbers from victims and use that information for financial gain.
- **Download Malware:** This includes affecting the victim's system by providing some link to click and trying to gain access once the victim downloads the malicious code. By doing this, the Attacker will be able to control the victim's computer or device and can do anything harmful.

SMIT

SYSTEM ANALYSIS

SYSTEM ANALYSIS

2.1.1 EXISTING SYSTEM

- Normally we steal the data from the users each and every time when the user installing and login to our web page.
- So there is no existing system for data hold-up by email spoofing and web scraping present in all the applications which we are downloading.

2.1.2 DISADVANTAGES OF EXISTING SYSTEM

- Sadly, most online users do not know how to find whether the Webpage where they are entering the data is safe or unsafe for all their accounts.
- These types of website are extremely dangerous to crack and once an Account is compromised, there's nothing the user can do about it.

2.2.1 PROPOSED SYSTEM

- Our proposed system is data hold-up by email spoofing and web scraping and phishing.
- User will input his/her email id and password for login purpose in our fake web page and after signing into the web page, it hold-up the data which was given by the user and his /her Account will be taken over by us.
- It enables us to know the information about the user and misuse it

2.2.2 ADVANTAGES OF PROPOSED SYSTEM

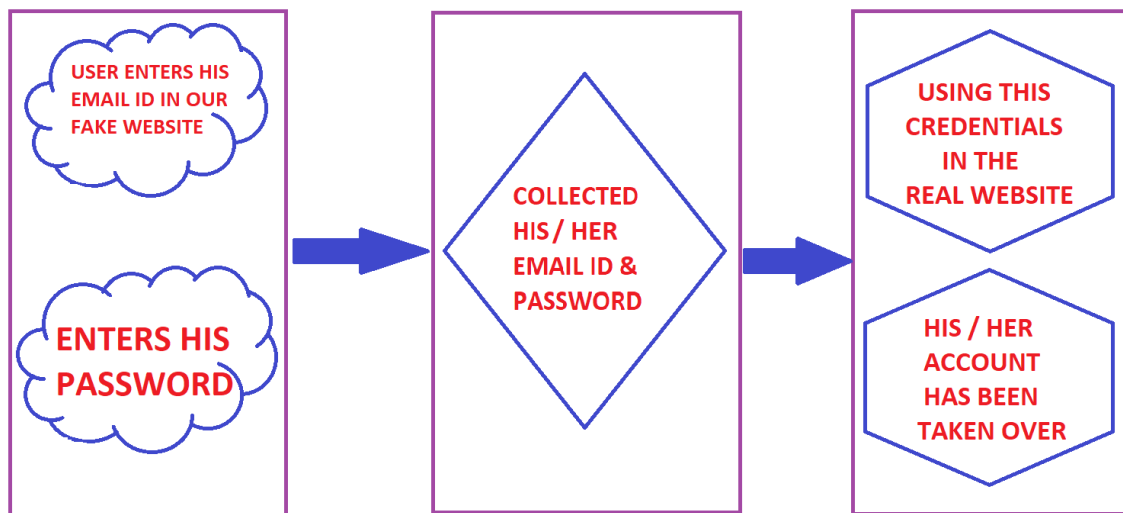
- **Hide the fake sender's real identity.** Bypass spam filters and block lists. Users can minimize this threat by block listing internet service providers (ISPs) and Internet Protocol (IP) addresses.
- **Pretend to be a trusted individual** - a colleague or a friend -- to elicit confidential information.

SMIT

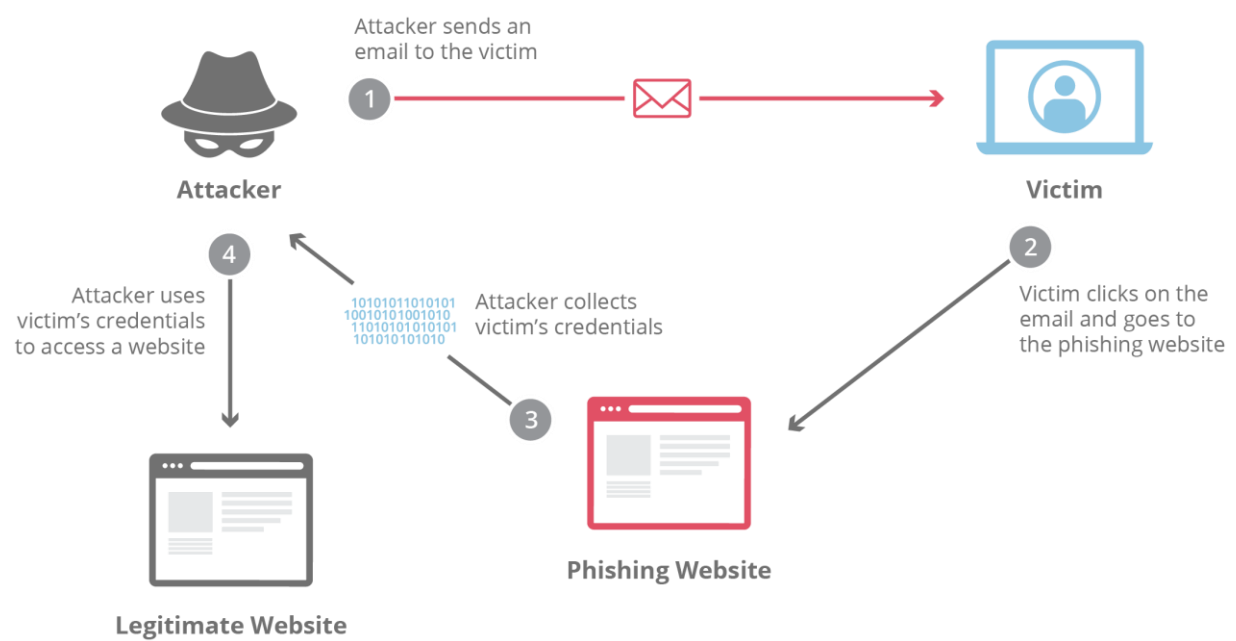
SYSTEM DESIGN

SYSTEM DESIGN

2.3 ARCHITECTURE DESIGN



2.3.1 USECASE DIAGRAM



SMIT

MODULES

2.4 SYSTEM MODULES

MODULE 1: WEBSCRAPING

For every application, the Structure and Function of the Website varies. Some needs Verification for Login. Some needs just the basic Credentials. So different types of Function are fixed in this module based On Website.

This includes HTML, PHP for the Structure & Function. The Code used for Web scraping is also mentioned in this module.

The Cloned Website is hosted in Internet & the URL has been shortened in order to avoid Suspicious Doubts by the User Before using the Credentials

MODULE 2: EMAIL SPOOFING & PHISHING

Now the Shortened URL will be sent to the Victim by email which holds the sender's address as the Legitimate Company with the Cloned Website's Link

To send the Spoofed Email with the Shortened URL, we use the Anonymous Mailer. Where the Attacker's Credentials will be protected.

When the Victim receives this Spoofed Email with the Shortened URL from the Legitimate Company name. He / She will click this Link and to go the cloned website which we are using for Phishing and the Credentials of the User will be compromised

MODULE 3: ACCOUNT TAKE OVER

Based on the Credentials collected from the Victim in our cloned Website. We will go to the Real Website & Enter the Login Credentials of the Victim and Enter into his Account.

Once the Account has been Compromised, the Consequences will be unpredictable for Example we can use this Account and get the Saved Card Numbers, Order Details, Payment Details and we can also order things which will cause a great damage

Once logged in to a customer account, the fraudster will take it over by changing the password and other details. Then, posing as the real customer, they have free rein to make fraudulent purchases and steal loyalty points and rewards.

SMIT

SYSTEM REQUIREMENTS

3.1 HARDWARE REQUIREMENTS

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as hardware. A hardware requirements list is often accompanied by a hardware compatibility list (HCL), especially in case of operating systems. An HCL lists tested, compatible, and sometimes incompatible hardware devices for a particular operating system or application. The following sub-sections discuss the various aspects of hardware requirements.

- Operating system: Windows Vista, 7, 8, 10 or higher.
- 400 MHz Intel Pentium II processor or higher.
- At least 4 GB of RAM or more.
- At least 50 MB of free space on the hard disk.

3.2 SOFTWARE REQUIREMENTS

The software requirements are description of features and functionalities of the target system. Requirements convey the expectations of users from the software product. The requirements can be obvious or hidden, known or unknown, expected or unexpected from client's point of view.

A condition or capability needed by a user to solve a problem or achieve an objective

A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification or other formally imposed documents

A software requirement can be of 3 types:

1. Functional requirements
2. Non-functional requirements
3. Domain requirements

List of Software Requirements are

- HTML
- PHP

3.2.1 HTML

HTML stands for Hyper Text Markup Language

HTML is the standard markup language for creating Web pages

HTML describes the structure of a Web page

HTML consists of a series of elements

HTML elements tell the browser how to display the content

HTML elements label pieces of content such as "this is a heading", "this is a paragraph", "this is a link", etc.

Web Browsers

The purpose of a web browser (Chrome, Edge, Firefox, Safari) is to read HTML documents and display them correctly.

A browser does not display the HTML tags, but uses them to determine how to display the document

View HTML Source Code:

Right-click in an HTML page and select "View Page Source" (in Chrome) or "View Source" (in Edge), or similar in other browsers. This will open a window containing the HTML source code of the page.

Inspect an HTML Element:

Right-click on an element (or a blank area), and choose "Inspect" or "Inspect Element" to see what elements are made up of (you will see both the HTML and the CSS). You can also edit the HTML or CSS on-the-fly in the Elements or Styles panel that opens.

3.2.2 PHP

PHP is a server scripting language, and a powerful tool for making dynamic and interactive Web pages. PHP is a widely-used, free, and efficient alternative to competitors such as Microsoft's ASP. PHP is an acronym for "PHP: Hypertext Pre-processor". PHP is a widely-used, open source scripting language. PHP scripts are executed on the server. PHP is free to download and use. It is powerful enough to be at the core of the biggest blogging system on the web (WordPress). It is deep enough to run large social networks. It is also easy enough to be a beginner's first server side language!

PHP files can contain text, HTML, CSS, JavaScript, and PHP code. PHP code is executed on the server, and the result is returned to the browser as plain HTML. PHP files have extension ".php"

PHP runs on various platforms (Windows, Linux, Unix, Mac OS X, etc.). PHP is compatible with almost all servers used today (Apache, IIS, etc.). PHP supports a wide range of databases. PHP is free. Download it from the official PHP resource: www.php.net. PHP is easy to learn and runs efficiently on the server side

SMIT

TESTING STRATEGIES

3.3 TESTING STRATEGIES

3.3.1 SECURITY TESTING

It is a type of Software Testing that uncovers vulnerabilities of the system and determines that the data and resources of the system are protected from possible intruders.

It ensures that the software system and application are free from any threats or risks that can cause a loss. Security testing of any system is focuses on finding all possible loopholes and weaknesses of the system which might result into the loss of information or reputе of the organization.

Principle of Security Testing:

Below are the six basic principles of security testing:

1. Confidentiality
2. Integrity
3. Authentication
4. Authorization
5. Availability
6. Non-repudiation

3.3.2 FUNCTIONAL TESTING

It is a type of testing that seeks to establish whether each application feature works as per the software requirements.

Each function is compared to the corresponding requirement to ascertain whether its output is consistent with the end user's expectations.

The testing is done by providing sample inputs, capturing resulting outputs, and verifying that actual outputs are the same as expected outputs.

Functional testing is a quality assurance process and a type of black-box testing that bases its test cases on the specifications of the software component under test.

Functions are tested by feeding them input and examining the output, and internal program structure is rarely considered.

3.3.3 INTEGRATION TESTING

It also known as integration and testing (I&T) -- is a type of software testing in which the different units, modules or components of a software application are tested as a combined entity. However, these modules may be coded by different programmers.

The aim of integration testing is to test the interfaces between the modules and expose any defects that may arise when these components are integrated and need to interact with each other.

To perform integration testing, testers use test drivers and stubs, which are dummy programs that act as substitutes for any missing modules and simulate data communications between modules for testing purposes.

3.3.4 BLACKBOX TESTING

It is a type of software testing in which the functionality of the software is not known. The testing is done without the internal knowledge of the products.

Black Box Testing is a testing technique where no knowledge of the internal functionality and structure of the system is available. This testing technique treats the system as a black box or closed box.

The tester only knows the formal inputs and expected outputs, but does not know how the program actually arrives at those outputs.

As a result, all testing must be based on functional specifications. For this reason black box testing is also considered to be functional testing and is also a form of behavioural testing or opaque box testing or simply closed box testing.

Although black box testing is behavioural testing, behavioural test design is slightly different from black box test design because internal knowledge may be available in behavioural testing.

SMIT

CONCLUSION

CONCLUSION

Spoofed emails are also used to carry infections like Trojans to do harm to victim systems. Administrators need to take a variety of measures to prevent, detect and provide remedial measures to email spoofing attacks. The causes of email spoofing have been described in the preceding sections. Gmail administrators should set up email authentication to protect their organization's email. Authentication helps prevent messages from your organization from being marked as spam. It also prevents spammers from impersonating your domain or organization in spoofing and phishing emails.

SMIT

APPENDIX 1

APPENDIX 1

5.1 Source code

Saved as “index.html”

```
<html>
<body>
<form action="next.php" method="post">
<img src = "1.PNG" width = "100%">
<center>
<div>
<input type = "text" placeholder = "Email" name = "eml">
<br><br>
<input type = "password" placeholder = "password" name = "pss">
<br>
<br><br>
<input type = "submit" value = "Sign in">
</div>
</center>
<img src = "2.PNG" width = "100%">
</form>
</body>
<html>
```

Saved as “next.php”

```
<html>
```

```
<body>
```

```
Your email address is: <?php echo $_POST["eml"]; ?><br>
```

```
Your password is: <?php echo $_POST["pss"]; ?>
```

```
<br>
```

```
Hey...!!!!
```

```
You have been Hacked
```

```
<h1> Prank by Sangeetha V & Sindhu S</h1>
```

```
<br><br>
```

```
<img src ="hacked.jpg" width = "800" height = "600">
```

```
</body>
```

```
</html>
```

SMIT

APPENDIX 2

APPENDIX 2

6.1 SCREENSHOTS

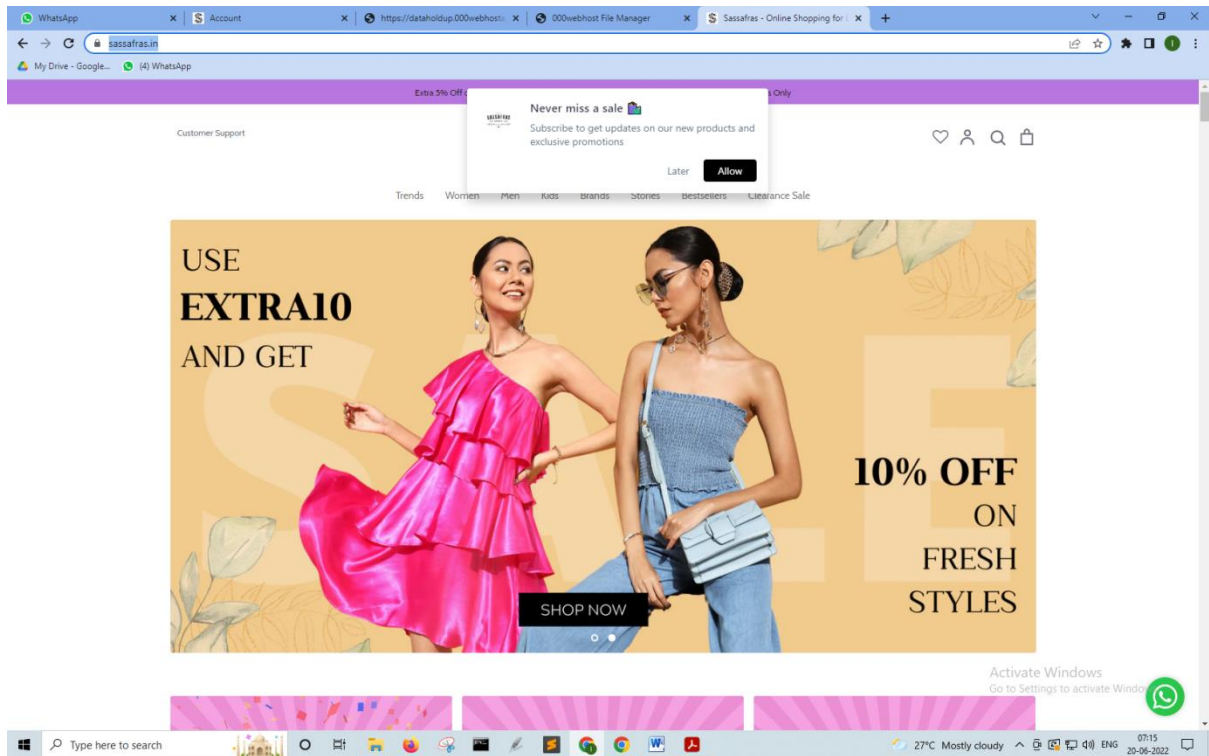


Fig A2.6.1.1

SPF Record Testing Tools

[Home](#)
[About](#)
[Site](#)

Overview

These tools are meant to help you deploy SPF records for your domain. They use an actual RFC 7208 compliant library (pyspf) for tests and will dynamically test for processing limit errors (no other testers I'm aware of do this). This site uses a caching DNS resolver, so for tests that use live DNS, results will be cached for the Time To Live of the DNS record. For most basic uses, these tests should be reasonably self explanatory. Advanced users may need, and probably want, some additional information on how these tools work. It can be found [here](#).

Does my domain already have an SPF record? What is it? Is it valid?

Retrieves SPF records for the specified domain name and determines if the record is valid.

Domain name:

NOTE: The domain is everything to the right of the '@' in the e-mail address.

Is this SPF record valid - syntactically correct?

Tests the supplied SPF record to see if it is valid. This test does NOT look up the record for the supplied domain. It only tests the validity of the supplied record. This test is for checking the syntax of records before you publish them. The domain is used only for mechanisms such as a bare 'a' mechanism that have an implied domain. It will also be used for the '%d' macro if present.

Domain:

SPF Record:

Contact :
E-mail

Links :
[Sender Policy Framework](#)
DNS provides the support
TXT (SPF)

Content Copyright 2005 - 2018
Kitterman Technical Services, Inc.
Design by Minimalistic Design

Fig A2.6.1.2

Domain name:

NOTE: The domain is everything to the right of the '@' in the e-mail address.

Fig A2.6.1.3

SPF record lookup and validation for: sassafra.in

SPF records are published in DNS as TXT records.

The TXT records found for your domain are:

v=spf1 +a +mx include:secureserver.net -all

v=spf1 a mx ptr include:secureserver.net all

google-site-verification=rQ5HV1fHjUe6xrdgkh9Gxxc-7Z5wd01EnaLU2pIHtQ4

v=spf1 include:shops.shopify.com include:secureserver.net.com ~all

Checking to see if there is a valid SPF record.

Results - Permanent Error Two or more type TXT spf records found.

No valid SPF record found of either type TXT or type SPF.

[Return to SPF checking tool \(clears form\)](#)

Use the back button on your browser to return to the SPF checking tool without clearing the form.

Fig A2.6.1.4

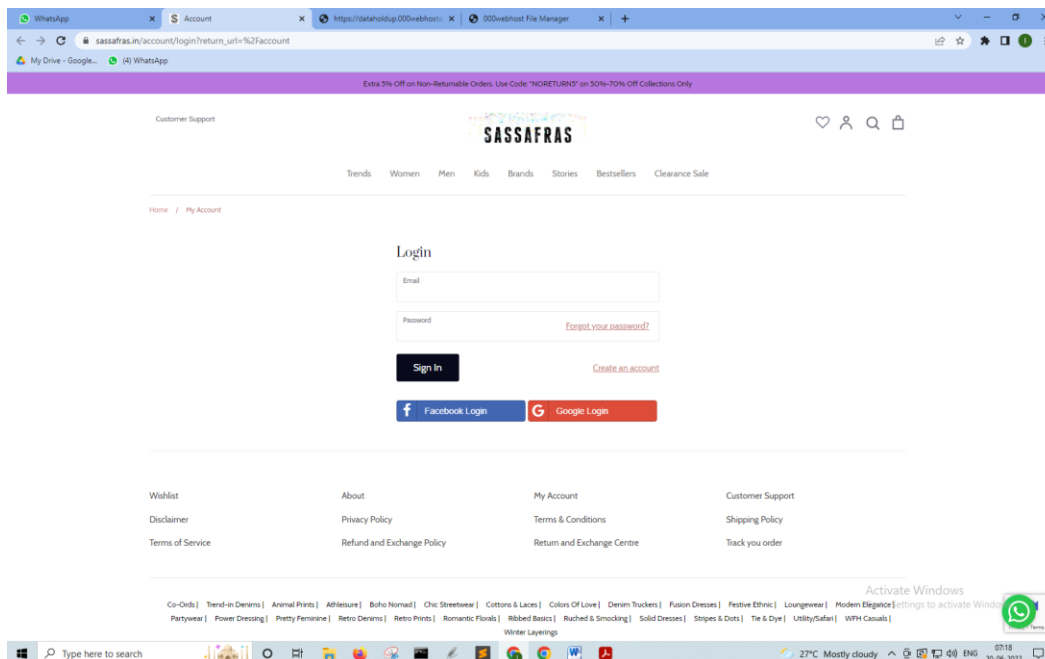
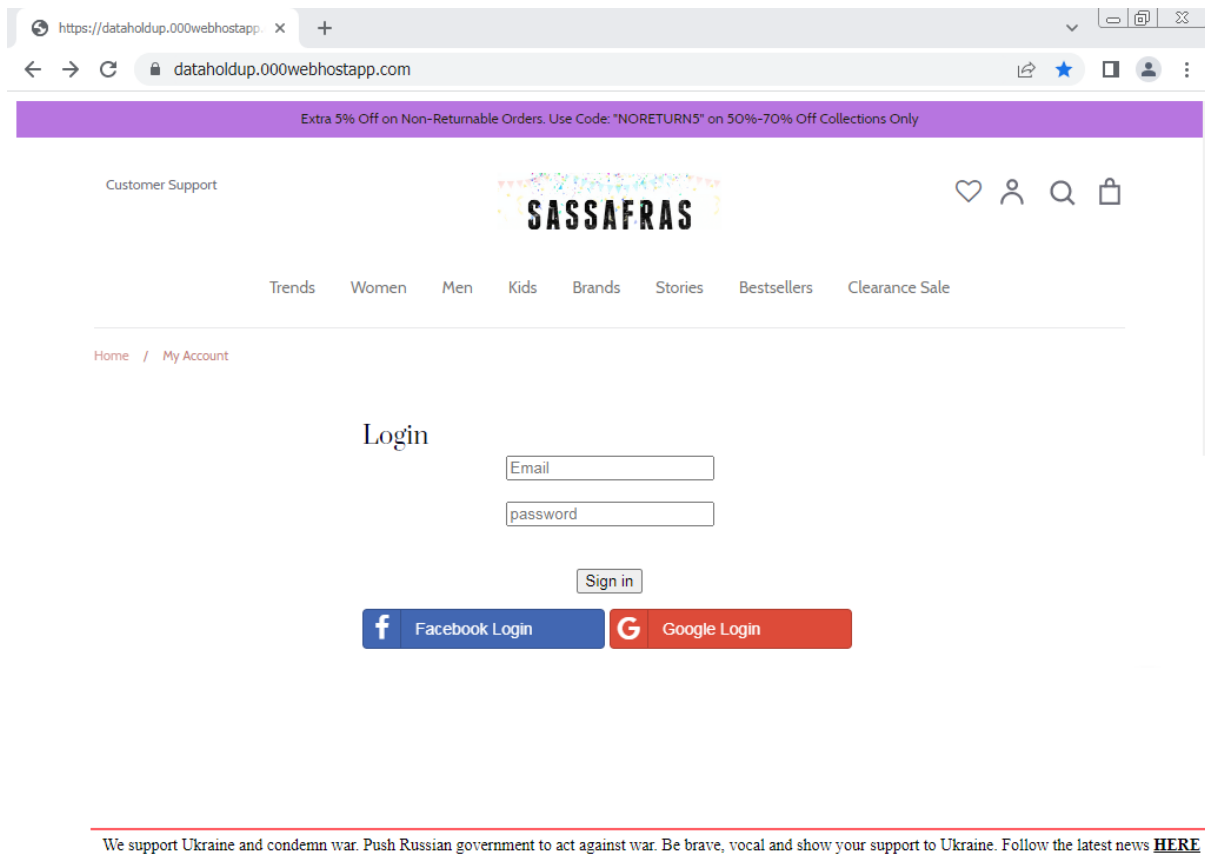



Fig A2.6.1.5



The screenshot shows a web browser window with the URL `https://dataholdup.000webhostapp.com`. The page features a purple banner at the top with the text "Extra 5% Off on Non-Returnable Orders. Use Code: 'NORETURNS' on 50%-70% Off Collections Only". Below the banner, the "SASSAFRAS" logo is centered, flanked by "Customer Support" on the left and navigation icons (heart, person, magnifying glass, shopping bag) on the right. A horizontal menu lists categories: Trends, Women, Men, Kids, Brands, Stories, Bestsellers, and Clearance Sale. Below this, a breadcrumb trail shows "Home / My Account". The "Login" section contains two input fields labeled "Email" and "password", a "Sign in" button, and two social login buttons: "Facebook Login" and "Google Login". At the bottom, a red banner contains the text: "We support Ukraine and condemn war. Push Russian government to act against war. Be brave, vocal and show your support to Ukraine. Follow the latest news [HERE](#)".

Fig A2.6.1.6



The screenshot shows a URL shortener interface. It features a text input field containing the URL `https://dataholdup.000webhostapp.com/`. To the right of the input field is a blue button labeled "Shorten".

Fig A2.6.1.7

Copy

By using our service you accept the [Terms of service](#) and [Privacy](#).

dataholdup.000webhostapp.com
https://dataholdup.000webhostapp.com/

2022-06-20

<https://cutt.ly/pKfEPgB>
register to use other features

0 clicks

Fig A2.6.1.8



EMKEE'S MAILER

5K

Share

Tweet

Share

Free online anonymous mailer with attachments, encryption, HTML editor and advanced settings...

From Name:
From E-mail:
To:
Subject:
Attachment: No file chosen

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text:

Fig A2.6.1.9



Free online anonymous mailer with attachments, encryption,
HTML editor and advanced settings...

From Name: Administrator

From E-mail: admin@sassafras.in

To: rep123hel@gmail.com

Subject: Testing

Attachment: No file chosen
[Attach another file](#)

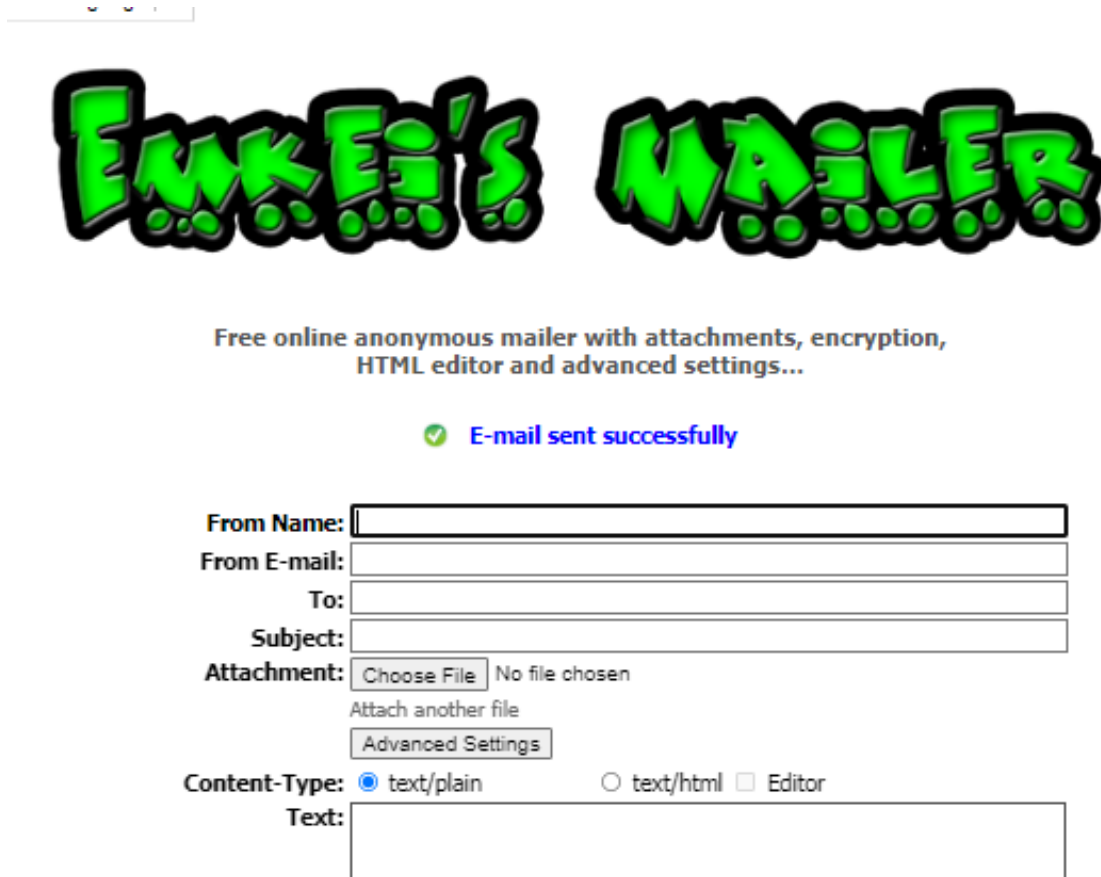
Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text:

© 2009–2022 Emkei • info@emkei.cz

This service does not violate any EU law. We are not obliged to keep any logs.

Fig A2.6.1.10



Ewke's MAILER

Free online anonymous mailer with attachments, encryption, HTML editor and advanced settings...

✔ E-mail sent successfully

From Name:

From E-mail:

To:

Subject:

Attachment: No file chosen
Attach another file

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text:

Fig A2.6.1.11

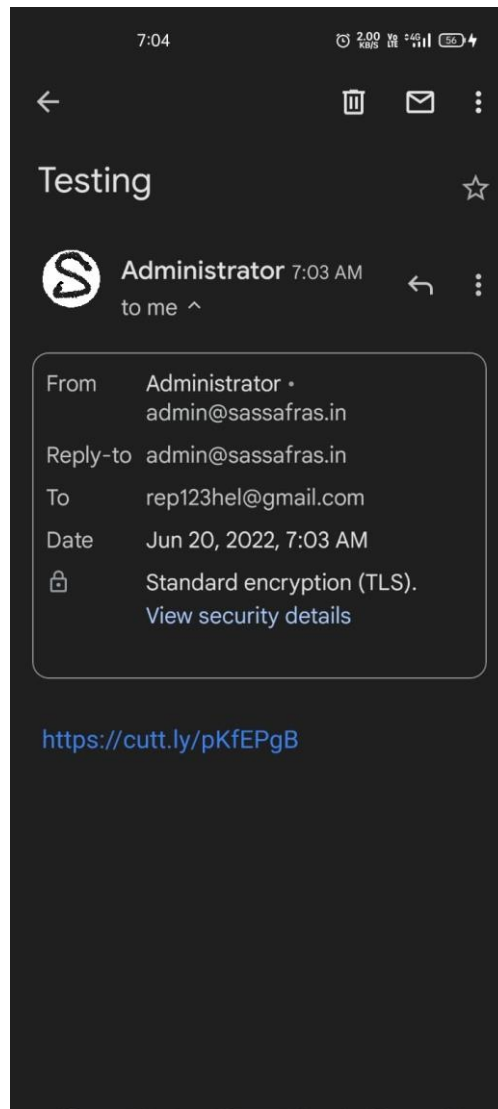


Fig A2.6.1.12

https://dataholdup.000webhostapp.com

dataholdup.000webhostapp.com

Extra 5% Off on Non-Returnable Orders. Use Code: "NORETURN5" on 50%-70% Off Collections Only

Customer Support

SASSAFRAS

Trends Women Men Kids Brands Stories Bestsellers Clearance Sale

Home / My Account

Login

Admin123@gmail.com

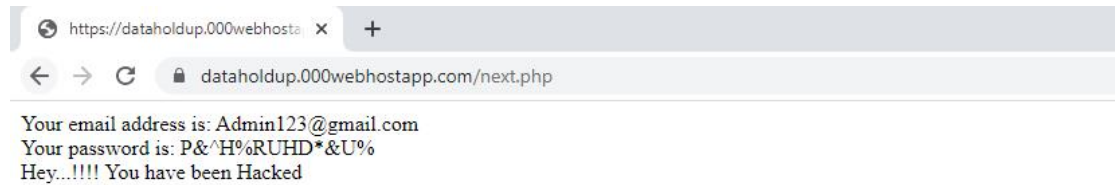
.....

Sign in

f Facebook Login G Google Login

We support Ukraine and condemn war. Push Russian government to act against war. Be brave, vocal and show your support to Ukraine. Follow the latest news [HERE](#)

Fig A2.6.1.13



Prank by Sangeetha V & Sindhu S



Fig A2.6.1.14

SMIT

REFERENCES

REFERENCES

- [1] Varshney, Gaurav; Misra, Manoj; Atrey, Pradeep K. (2016-10-26). [*"A survey and classification of web phishing detection schemes: Phishing is a fraudulent act that is used to deceive users"*](#). Security and Communication Networks.
- [2] Siebenmann, Chris. [*"A quick overview of SMTP"*](#). University of Toronto. [Archived](#) from the original on 2019-04-03.
- [3] Barnes, Bill (2002-03-12). [*"E-Mail Impersonators"*](#). [Archived](#) from the original on 2019-04-13. Retrieved 2019-04-08.
- [4] [*"Prevent spoofed messages with spoofed senders detection"*](#). [Archived](#) from the original on 2019-03-23. Retrieved 2019-04-08.
- [5] [*"Anti-spoofing protection in Office 365"*](#). [Archived](#) from the original on 2019-04-09. Retrieved 2019-04-08.
- [6] Christopher Hadnagy is the founder and CEO of Social-Engineer, LLC. In his sixteen years in the industry, he has written the world's first social engineering-framework, created the first social engineering-based podcast and newsletter, and written four books on the topic.
- [7] Les Hatton M.A, M.Sc., LL.M., Ph.D. is Professor of Forensic Software Engineering at Kingston University in the UK. After studying mathematics at King's College Cambridge and Manchester Universities, he was a recipient of the Conrad Schlumberger Award as a geophysicist before his research interests led him to a career studying failures and vulnerabilities in software controlled systems.