Engineering and Scientific International Journal (ESIJ)
Volume 1, Issue 1, October - December 2014
ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

An Effective Implementation of HTML Injection

Bharat Bhatia [#1], Charu Sharma [*2]

[1,2] *Department of Electronics and Communication Engineering*
Sarvottam Institute of Technology & Management
[2] *G.B. Nagar, Noida, U.P.-201306, India*
[1] *namewish2661996@gmail.com*
[2] *charusharma.sharma@gmail.com*

Abstract— HTML injection is an attack that is closely related to Cross-site Scripting (XSS). The difference is not in the vulnerability, but in the type of attack that leverages the vulnerability. Hypertext Markup Language (HTML) injection, also sometimes referred to as *virtual defacement*, is an attack on a user made possible by an injection vulnerability in a web application. When an application does not properly handle user supplied data, an attacker can supply valid HTML, typically via a parameter value, and inject their own content into the page. This attack is typically used in conjunction with some form of social engineering, as the attack is exploiting a code-based vulnerability and a user's trust.

Keywords— *HTML, JSP, PHP, E-commerce, social networking*

1. Introduction

HTML stands for Hyper Text Markup Language. It is a standard markup language used to create web pages. HTML is written in the form of HTML elements consisting of tags enclosed in angle brackets (like <html>). HTML tags most commonly come in pairs like <h1> and </h1>, although some tags represent empty elements and so are unpaired, for example <img>. The first tag in a pair is the start tag, and the second tag is the end tag (they are also called opening tags and closing tags)

Basic format of html web pages

```
<!DOCTYPE html>
 <html>
 <head>
<title>This is a title</title>
  </head>
  <body>
   <p>paragraph of body</p>
  </body>
</html>
```

Using this basic format most of the websites are developed. There are 2 types of websites

- Static websites
- Dynamic websites

Difference between static and dynamic websites

1.1 Static websites

Static websites contain fixed number of pages and format of web page is fixed which delivers information to the client. There are 110 changes in contents of web page while page is running on client's browser. This kind of web sites created from HTML and CSS coding on simple text editor like notepad. Example an organization site, institute site etc.

1.2 Dynamic *websites*

Dynamic websites can change the web page contents dynamically while the page is running on client's browser. This kind of websites use server- side programming like PHP, Asp.NET. and JSP etc. to modify page contents on run time. Dynamic websites use client side scripting for prepare dynamic design and server- side code to handle event, manage session and cookies, and storing and retrieving data from database. Example E-commerce sites, online form application, E-governance site, social networking sites etc.

2. Effects of Attack on Website

We had found in the difference the static websites are using only html and css (complementary) and most of the people in world prefers to make static websites instead of dynamic website as if it is affordable, suitable for small scale business and has other different benefits also

2.1 Advantages of static websites

- Generally cheaper to implement on a smaller scale if fewer pages are required.
- Good for smaller companies as there is no need for any management system; it is the responsibility of one person

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

- More flexibility is available, as you are not restricted to any template layout (although this can affect the usability of your website)
- No change is required to your web hosting
- More secured than dynamic one
- More secured than dynamic one

But all these static websites are vernable with one attack that is html- I (HTML Injection). Hypertext Markup Language (HTML) injection, also sometimes referred to as virtual defacement, is an attack on a user made possible by an injection vulnerability in a web application. When an application does not properly handle user supplied data, an attacker can supply valid HTML, typically via a parameter value, and inject their own content into the page.

This attack is typically used in conjunction with some form of social engineering, as the attack is exploiting a code-based vulnerability and a user's trust. Using this injection a user can inject his or her code in a vernable column of a infected website

2.2 Effects of attack on website

- HTMLI leads to delay of the services of the website
- HTMLI can also be used as a phishing attack to threaten the victim
- HTMLI can also be used for big scams for threatening the users on that website
- HTMLI can also be used for the defacement of the website

2.3 Ways to protect the website from the attacker

- For protecting the user or victim to be threatened the web developer should need to apply the word limit in each field
- For protecting the user or victim to be threatened the web developer should need to apply the firewall on every field so that the attacker could not be able to enter the tags which are the basic building blocks of html coding.

3. Implementation

I had taken a vernable website and shown injection in that website. This is the original vernable website on which I will perform out the injection and this is the vernable column of this website.

Fig.1: Image of vemble website

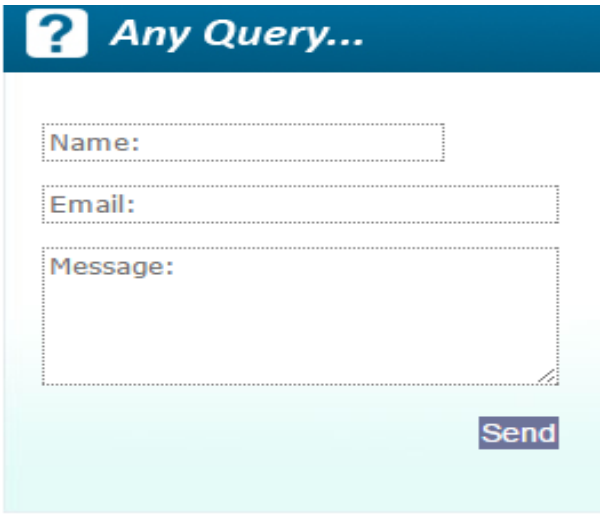

Fig.2: Query page of the website

When I will paste any html code in its name column for an example I am pasting the website source code, then it will inject that code and will develop a fake web page on that similar page Name field containing website source code and on injecting that a fake web page developers on that similar website.

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

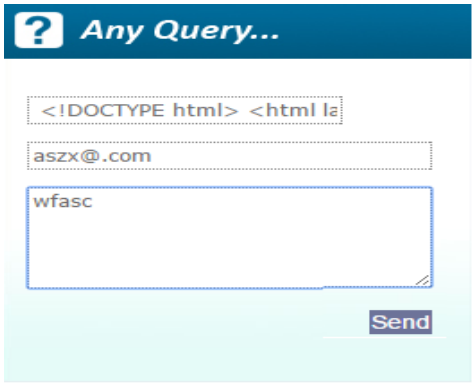

Fig.3:Insertion of HTML code

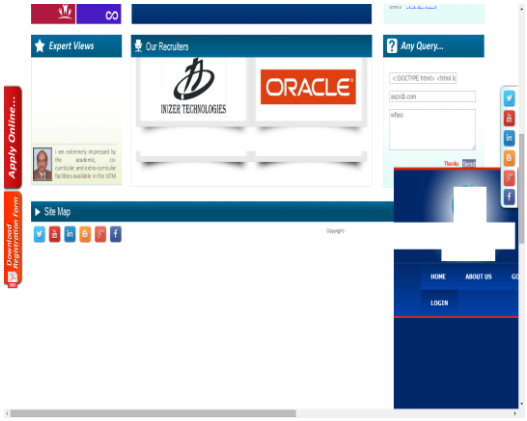

Fig.4: Fake website creation

Here you can see by injecting a code a website start running in another website and using the similar process any other website can also be injected in any vernable website.

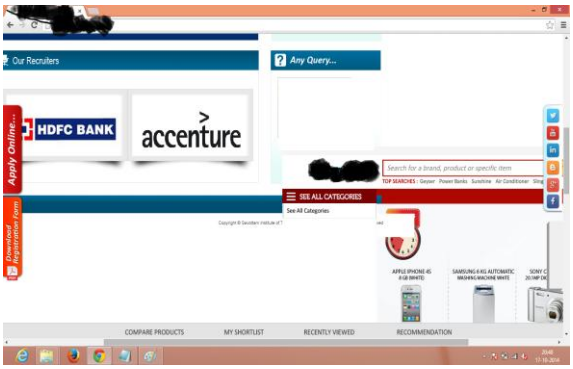

Fig.5: Fake website execution

Hence a lot of exploitation can be performed using HTML Injection. In this way the most secured websites that are static websites can also be found vernable or cold be easily attacked using this injection.

4. Conclusion

HTMLI leads to delay of the services of the website. It can also be used as a phishing attack to threaten the victim and can also be used for big scams for threatening the users on that website. HTMLI can also be used for the defacement of the website.

- for protecting the user or victim to be threatened the web developer should need to apply the word limit in each field
- For protecting the user or victim to be threatened the web developer should need to apply the firewall on every field so that the attacker could not be able to enter the tags which are the basic building blocks of html coding.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. They are also grateful to Sarvottam Institute of Technology & Management for improving my personality.

References

[1] David Kamp, “Deconstructing Dinner”, Review of the Omnivore’s Dilemma: A Natural History of Four Meals, by Michael Pollan, New York Times, April 23, 2006, Sunday Book Review,http://www.nytimes.com/2006/04/23/books/review/23kamp.html.

[2] G. Wassermann and Z. Su., “An Analysis Framework for Security in Web Applications”, Proceedings of the FSE Workshop on Specification and Verification of Component-Based Systems (SAVCBS 2004), pages 70–78, 2004.

[3] G. B. Shelly, T. J. Cashman and M. E. Vermaat, “Discovering Computers 2005: A Gateway to Information,” Course Technology, Boston, 2004.

[4] P. Carey, “Creating Web Pages with HTML and Dynamic HTML”, Course Technology, Boston, 2001.

[5] W. Ke, M. Muthuprasanna and S. Kothari, “Preventing SQL Injection Attacks in Stored Procedures”, Proceedings of the Australian Software Engineering Conference, Brisbane, 31 March-1 April 2005, pp. 191-1978

[6] C. Cerrudo, “Manipulating Microsoft SQL Server Using SQL Injection”, Application Security, Inc., 2005. http://research. journal. com/detail/RES/1124462486_292.html

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

Bharat Bhatia is web and wireless penetration tester who has been trained by several Ethical hacking companies like Sec Vision and recently working with Capswhite information security. Bharat Bhatia is persuing his B.Tech. from Sarvottam Engineering College and is student of ECE branch second year.

.

Charu Sharma is an Assistant Professor in the Department of Electronics and Communication at Sarvottam Engineering College. She has been serving more than 5years of teaching experience .She has published many articles in the National and International Journals of Electronics and Communication and presented papers in many Conferences.