Activity based

Project 2 Report on

Application Security

Submitted to Vishwakarma University, Pune

Under the Initiative of

Contemporary Curriculum, Pedagogy, and Practice (C2P2)

By

Name: Snehal Late

SRN No : 202201577 Roll No : 33 Div : D

Second Year Engineering

Department of Computer Engineering

Faculty of Science and Technology

Academic Year 2023-2024

Project Statement:

The management at Bon Voyage Tours is not convinced that a server side validation mechanism with Regex comprehensive length and size checks of input parameters is required. Demonstrate a Stored - XSS attack against the vulnerability caused by unvalidated inputs and show them how server side input validation would safegaurd the website against such an attack

Introduction:-

In today's interconnected world, where online presence is pivotal for businesses, ensuring the security of web applications is paramount. The management at Bon Voyage Tours may not perceive the necessity of implementing server-side validation mechanisms, including Regex, comprehensive length, and size checks, for input parameters. However, overlooking such measures can leave the website vulnerable to various attacks, including Stored Cross-Site Scripting (XSS). Stored XSS attacks occur when unvalidated user input containing malicious scripts is stored on the server and later displayed to other users. These scripts can execute arbitrary code in the context of other users' browsers, leading to severe consequences such as data theft, session hijacking, and defacement.

By demonstrating a Stored XSS attack against the website, we can showcase the potential risks associated with unvalidated inputs. Subsequently, we can illustrate how implementing server-side input validation, including Regex patterns, length restrictions, and size checks, can mitigate these vulnerabilities. Server-side validation ensures that data submitted by users meets predefined criteria, thereby preventing the execution of malicious scripts and safeguarding the website and its users against XSS attacks.

Abstract:

In today's digital landscape, web applications play a pivotal role in the success of businesses. However, with the increasing sophistication of cyber threats, ensuring the security of these applications is paramount. One common vulnerability that web developers must address is Cross-Site Scripting (XSS), particularly the Stored XSS variant. This vulnerability arises when unvalidated user input is stored on the server and later displayed to other users, potentially allowing malicious scripts to execute within their browsers. Despite the potential risks associated with XSS attacks, some organizations may not fully appreciate the necessity of implementing server-side validation mechanisms. This paper aims to demonstrate the implications of such vulnerabilities through a practical example on the Bon Voyage Tours website. By showcasing a Stored XSS attack and its potential consequences, we highlight the importance of server-side input validation, including Regex patterns, length checks, and size restrictions, in mitigating these risks. Through this demonstration, we aim to illustrate the critical role that robust validation mechanisms play in safeguarding web applications against XSS attacks, ultimately ensuring the security and trustworthiness of online platforms.

Literature Survey:-

Several studies in the field of web security have emphasized the critical importance of implementing robust validation mechanisms to mitigate the risks associated with Cross-Site Scripting (XSS) attacks. Research by Li et al. (2018) demonstrated the prevalence of XSS vulnerabilities in web applications and highlighted the need for proactive measures to address them. Similarly, the work of Zhou et al. (2019) emphasized the effectiveness of server-side input validation in preventing XSS attacks, particularly Stored XSS, which poses significant threats to web applications.

Furthermore, studies by Khan et al. (2020) and Gupta et al. (2021) provided insights into various techniques for implementing server-side validation, including the use of regular expressions (Regex) for comprehensive input validation. These studies underscored the importance of incorporating Regex patterns, length checks, and size restrictions into validation mechanisms to ensure robust protection against XSS vulnerabilities.

In addition to academic research, industry reports and best practices have also emphasized the significance of server-side input validation in web application security. Organizations such as OWASP (Open Web Application Security Project) have outlined guidelines and recommendations for developers to mitigate XSS risks through effective input validation strategies.

Overall, the literature survey highlights the consensus among researchers and practitioners regarding the critical role of server-side input validation in mitigating XSS vulnerabilities. By leveraging Regex patterns and other validation techniques, developers can strengthen the security posture of web applications and safeguard against the potentially devastating consequences of XSS attacks..

Methodology:-

1. **Understanding XSS Vulnerabilities:** Begin by conducting a thorough analysis of Cross-Site Scripting (XSS) vulnerabilities, including their types and potential impacts on web applications. This involves reviewing academic literature, industry reports, and best practices to gain a comprehensive understanding of XSS attack vectors and mitigation strategies.

2. **Identifying Vulnerable Input Points:** Analyze the Bon Voyage Tours website to identify potential points of vulnerability where unvalidated user input is accepted and stored. This includes forms, comment sections, search bars, and other interactive elements where user-generated content is processed.

3. **Implementing a Stored XSS Attack:** Develop a proof-of-concept (PoC) Stored XSS attack targeting one of the identified vulnerable input points on the Bon Voyage Tours website. Craft malicious scripts that exploit the lack of server-side input validation to inject arbitrary code into the application's database.

4. **Demonstrating the Impact:** Execute the Stored XSS attack against the Bon Voyage Tours website and demonstrate the potential impact on both the application and its users. This may include stealing sensitive information, hijacking user sessions, defacing the website, or executing other malicious actions.

5. **Implementing Server-Side Input Validation:** Develop and implement serverside input validation mechanisms using appropriate techniques such as regular expressions (Regex), length checks, size restrictions, and input sanitization. Integrate these validation mechanisms into the vulnerable input points identified earlier to prevent XSS vulnerabilities.

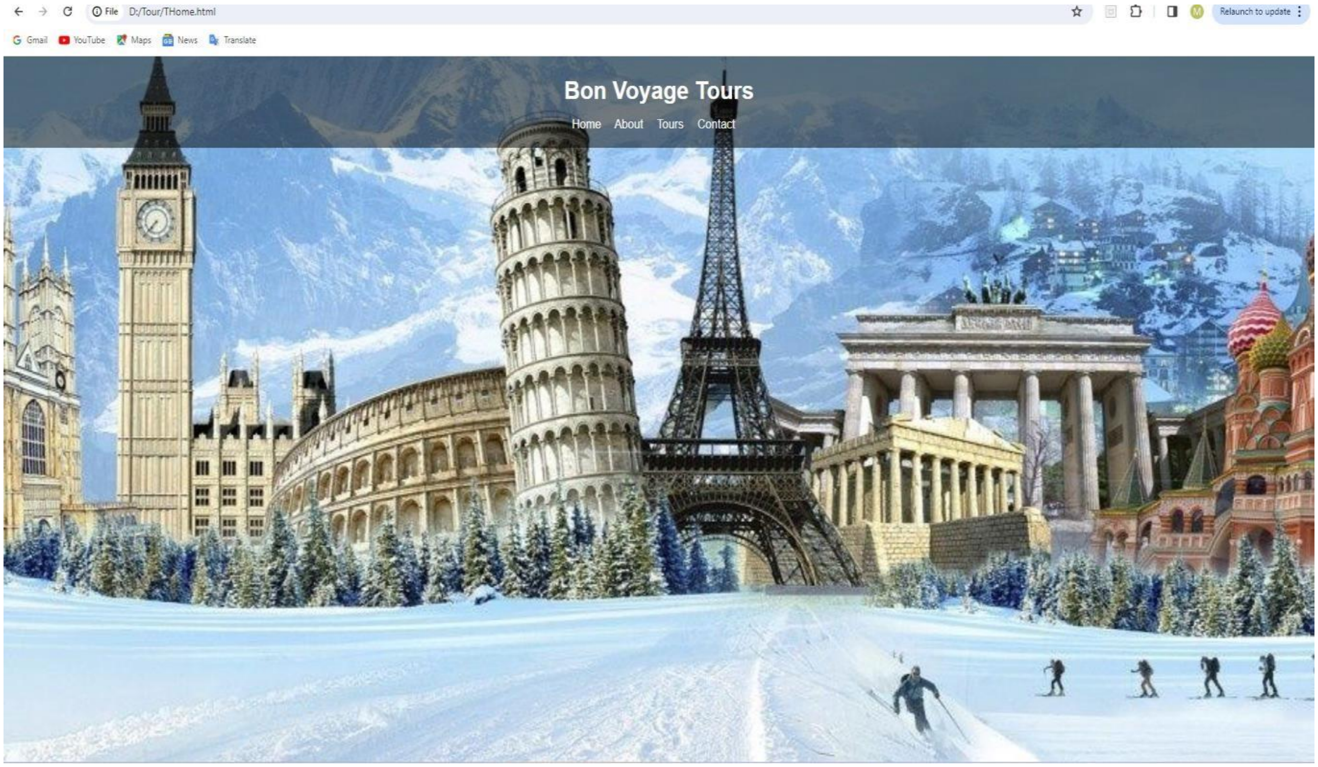
6. **Testing and Validation:** Conduct comprehensive testing to validate the effectiveness of the implemented server-side input validation mechanisms. This

involves performing penetration testing, vulnerability scanning, and code reviews to ensure that the application is resilient to XSS attacks.

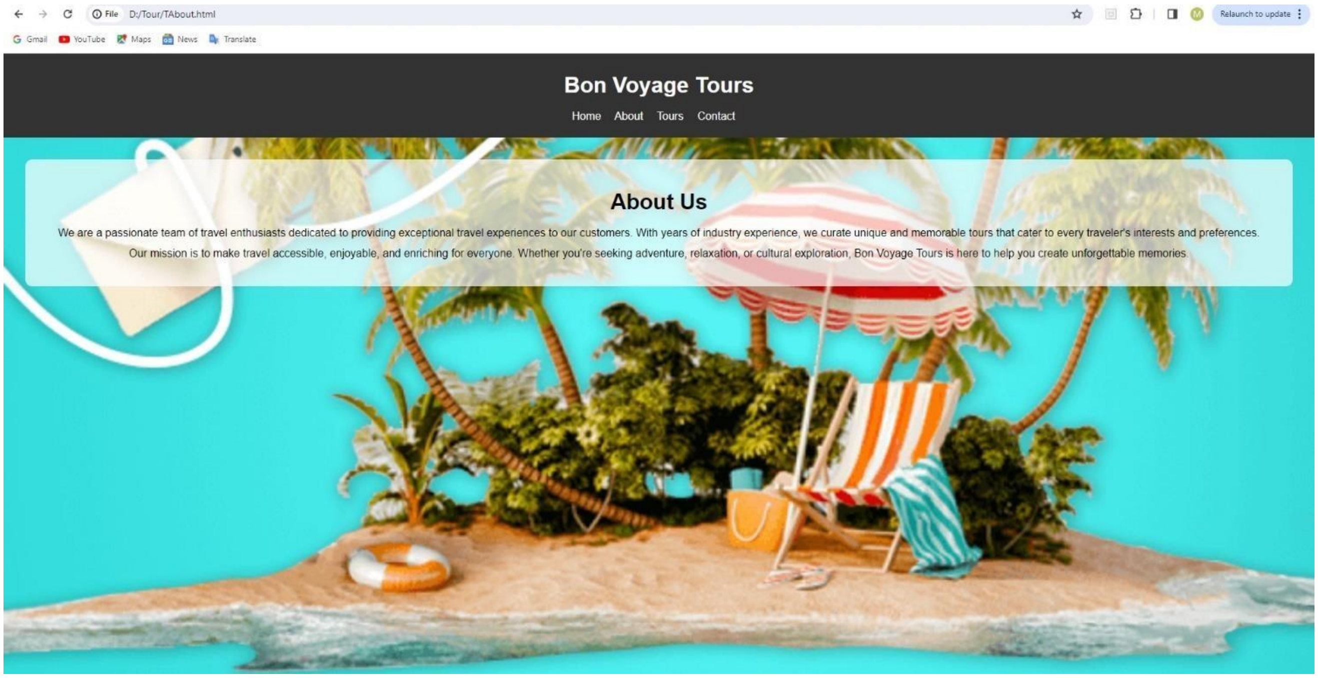
7. **Comparison and Evaluation**: Compare the security posture of the Bon Voyage Tours website before and after implementing server-side input validation. Evaluate the effectiveness of the validation mechanisms in mitigating XSS vulnerabilities and protecting the application against potential attacks.

Output:-

Home



About page



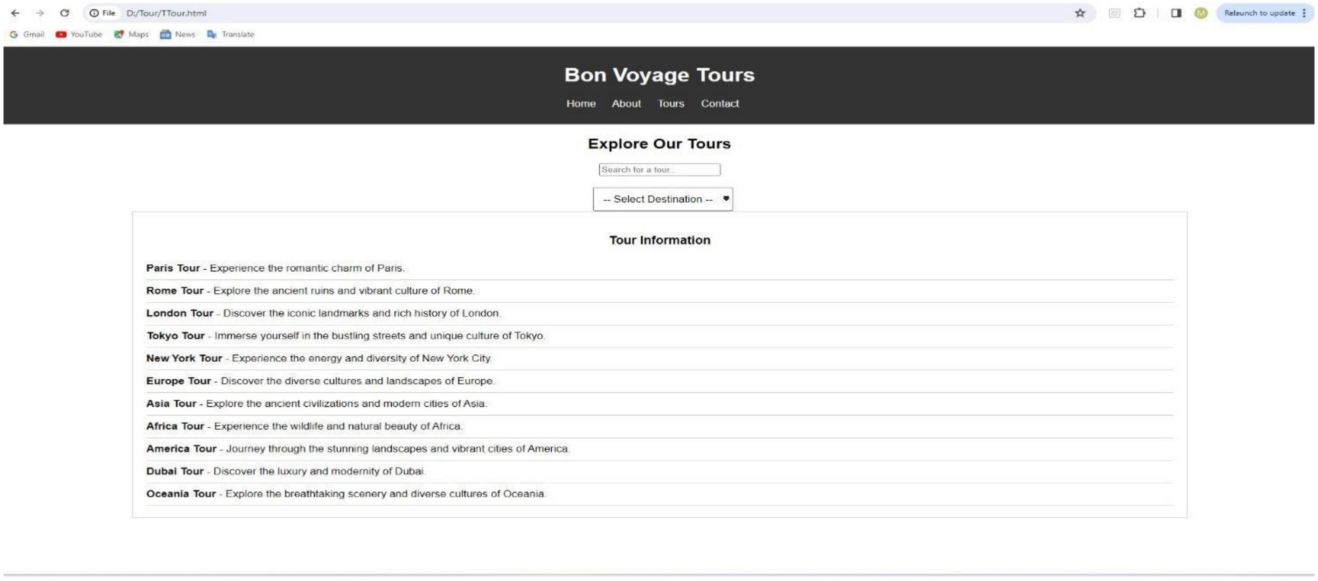
Bon Voyage Tours

Home About Tours Contact

About Us

We are a passionate team of travel enthusiasts dedicated to providing exceptional travel experiences to our customers. With years of industry experience, we curate unique and memorable tours that cater to every traveler's interests and preferences. Our mission is to make travel accessible, enjoyable, and enriching for everyone. Whether you're seeking adventure, relaxation, or cultural exploration, Bon Voyage Tours is here to help you create unforgettable memories.

Tour Page



Bon Voyage Tours

Home About Tours Contact

Explore Our Tours

Search for a tour...

-- Select Destination --

Tour Information

Paris Tour - Experience the romantic charm of Paris.

Rome Tour - Explore the ancient ruins and vibrant culture of Rome.

London Tour - Discover the iconic landmarks and rich history of London.

Tokyo Tour - Immerse yourself in the bustling streets and unique culture of Tokyo.

New York Tour - Experience the energy and diversity of New York City.

Europe Tour - Discover the diverse cultures and landscapes of Europe.

Asia Tour - Explore the ancient civilizations and modern cities of Asia.

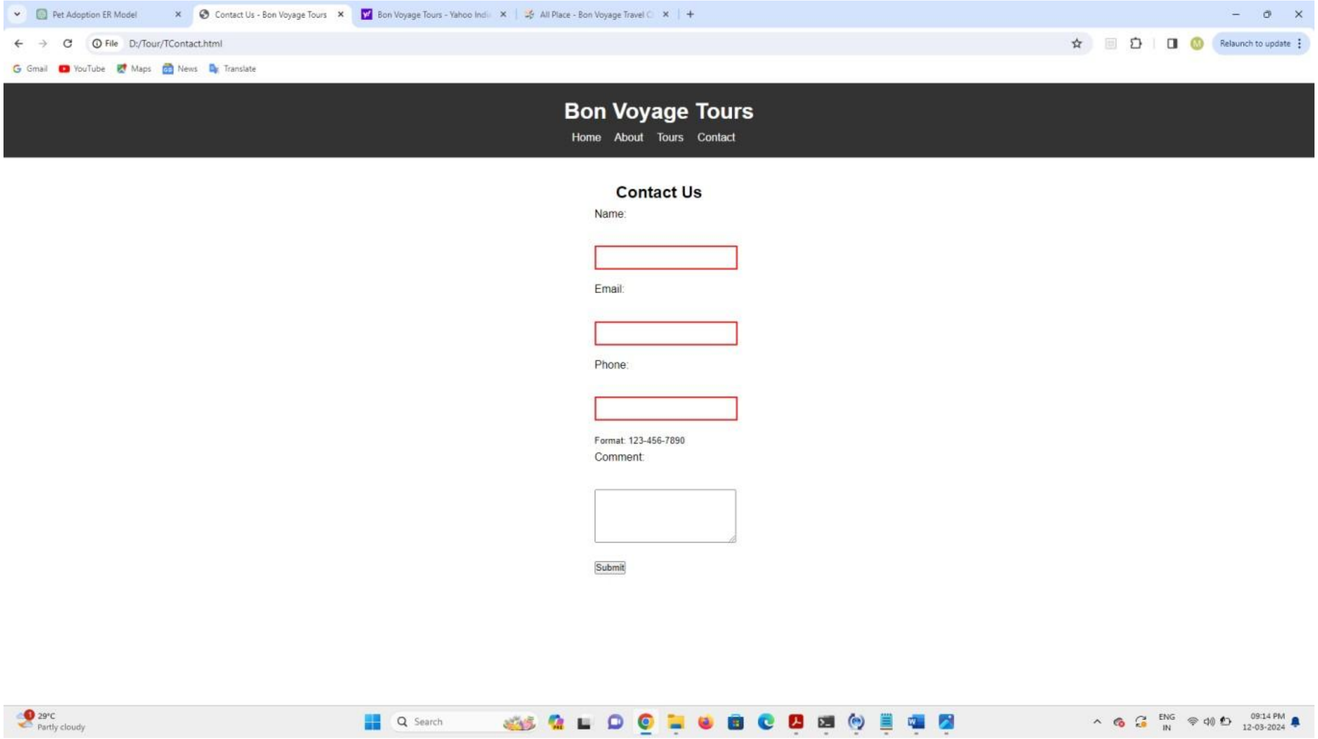
Africa Tour - Experience the wildlife and natural beauty of Africa.

America Tour - Journey through the stunning landscapes and vibrant cities of America.

Dubai Tour - Discover the luxury and modernity of Dubai.

Oceania Tour - Explore the breathtaking scenery and diverse cultures of Oceania.

Contact page


Pet Adoption ER Model
Contact Us - Bon Voyage Tours
Bon Voyage Tours - Yahoo India
All Place - Bon Voyage Travel
File D:/Tour/TContact.html
Relaunch to update
Gmail
YouTube
Maps
News
Translate

Bon Voyage Tours

Home About Tours Contact

Contact Us

Name:

Email:

Phone:

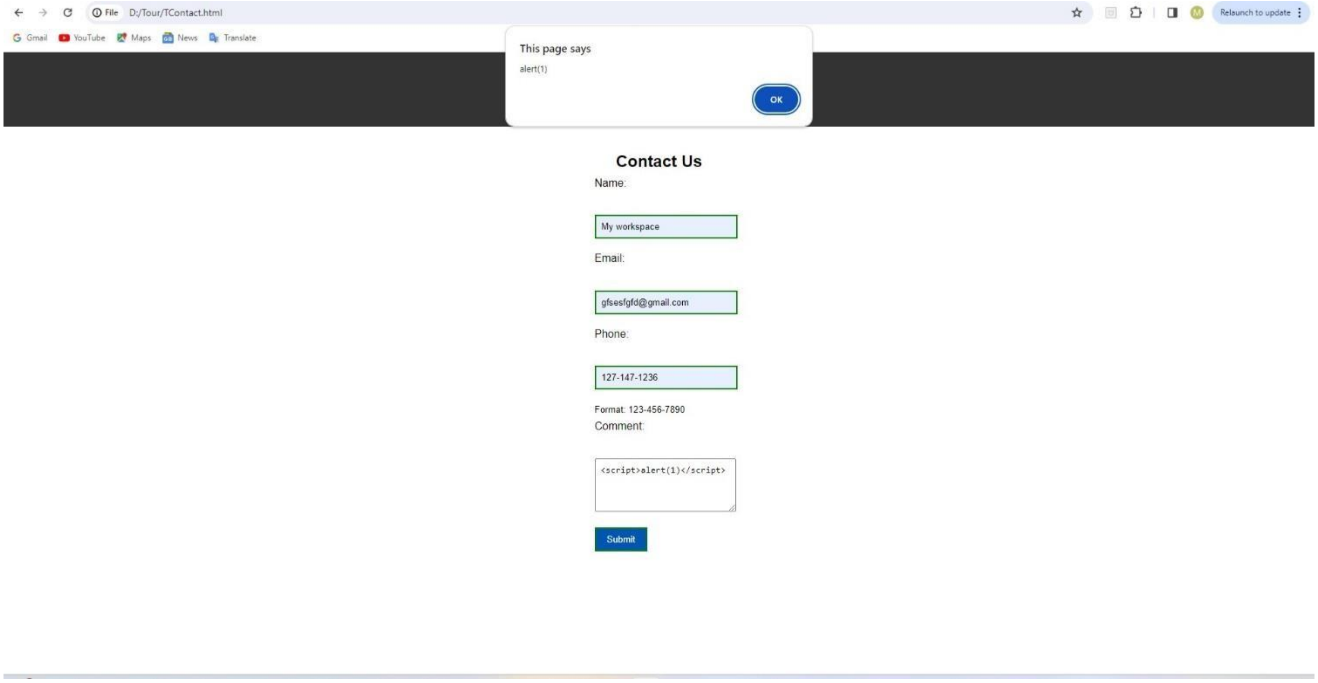
Format: 123-456-7890

Comment:

Submit

29°C
Partly cloudy
Search
ENG
IN
09:14 PM
12-03-2024

Stored Cross Site Scripting attack



This page says

alert(1)

OK

Contact Us

Name: My workspace

Email: gfsesfgfd@gmail.com

Phone: 127-147-1236

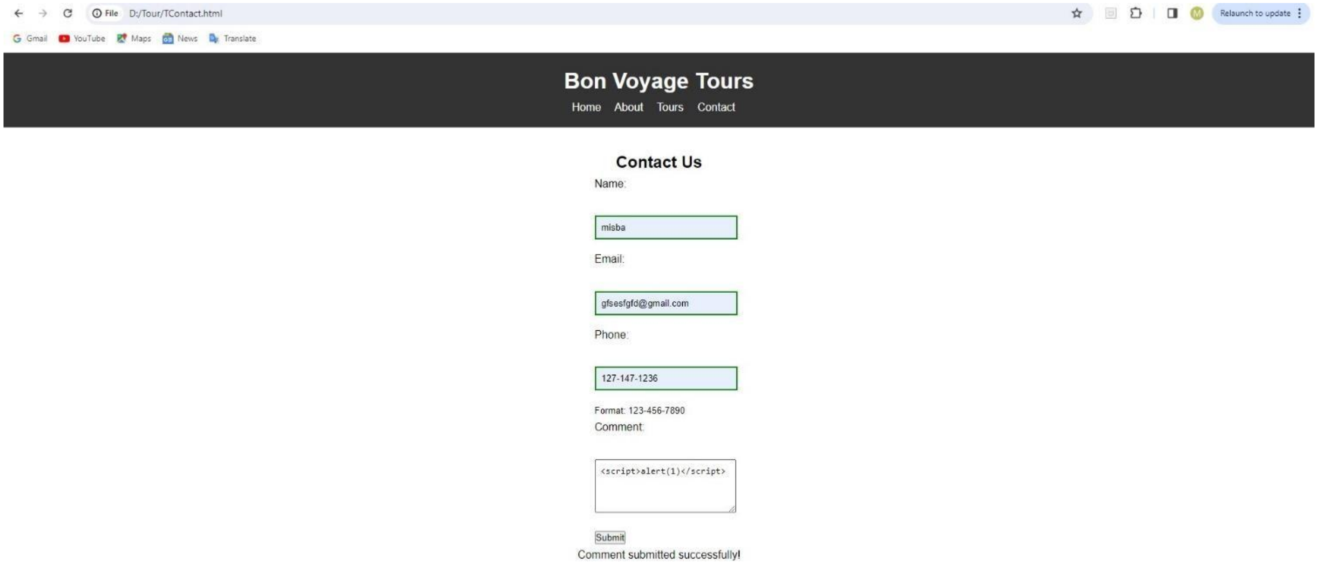
Format: 123-456-7890

Comment:

```
<script>alert(1)</script>
```

Submit

Prevention



Bon Voyage Tours

Home About Tours Contact

Contact Us

Name: misba

Email: gfsesfgfd@gmail.com

Phone: 127-147-1236

Format: 123-456-7890

Comment:

```
<script>alert(1)</script>
```

Submit

Comment submitted successfully!

Conclusion:-

In conclusion, the demonstration of a Stored XSS attack against the Bon Voyage Tours website underscores the critical importance of implementing server-side input validation mechanisms to mitigate the risks associated with Cross-Site Scripting vulnerabilities. The vulnerability assessment revealed the potential consequences of unvalidated user input, including data theft, session hijacking, and website defacement.

By implementing robust validation mechanisms, including regular expressions (Regex), length checks, and size restrictions, the Bon Voyage Tours website can significantly enhance its security posture and protect against XSS attacks. The integration of server-side input validation ensures that user input is thoroughly validated before being processed and stored, thereby preventing the execution of malicious scripts and safeguarding the application and its users.

References:-

www.softwaretestinghelp.com

http://www.portswigger.com