|  |  |
| --- | --- |
| NAME: VAISHNAVI PARULEKAR | ROLL ID: 22203A0048 |
| COURSE:CO (COMPUTER ENGINNERING) | Subject: Task Assignment: XSS Vulnerability Testing for adidas.cvicte.sk |
| COMPANY: SECURER CYBER FUTURE | COLLEGE: VIDYALANKAR POLYTECHNIC |

REPORT

XSS Vulnerability Testing for adidas.cvicte.sk (<https://adidas.cvicte.sk/>)

**Detailed descriptions of each identified vulnerability:**

Reflected XSS

The malicious script is reflected off a web server, usually in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request.

It is delivered to the victim via another route, such as an email or a link on a different website.

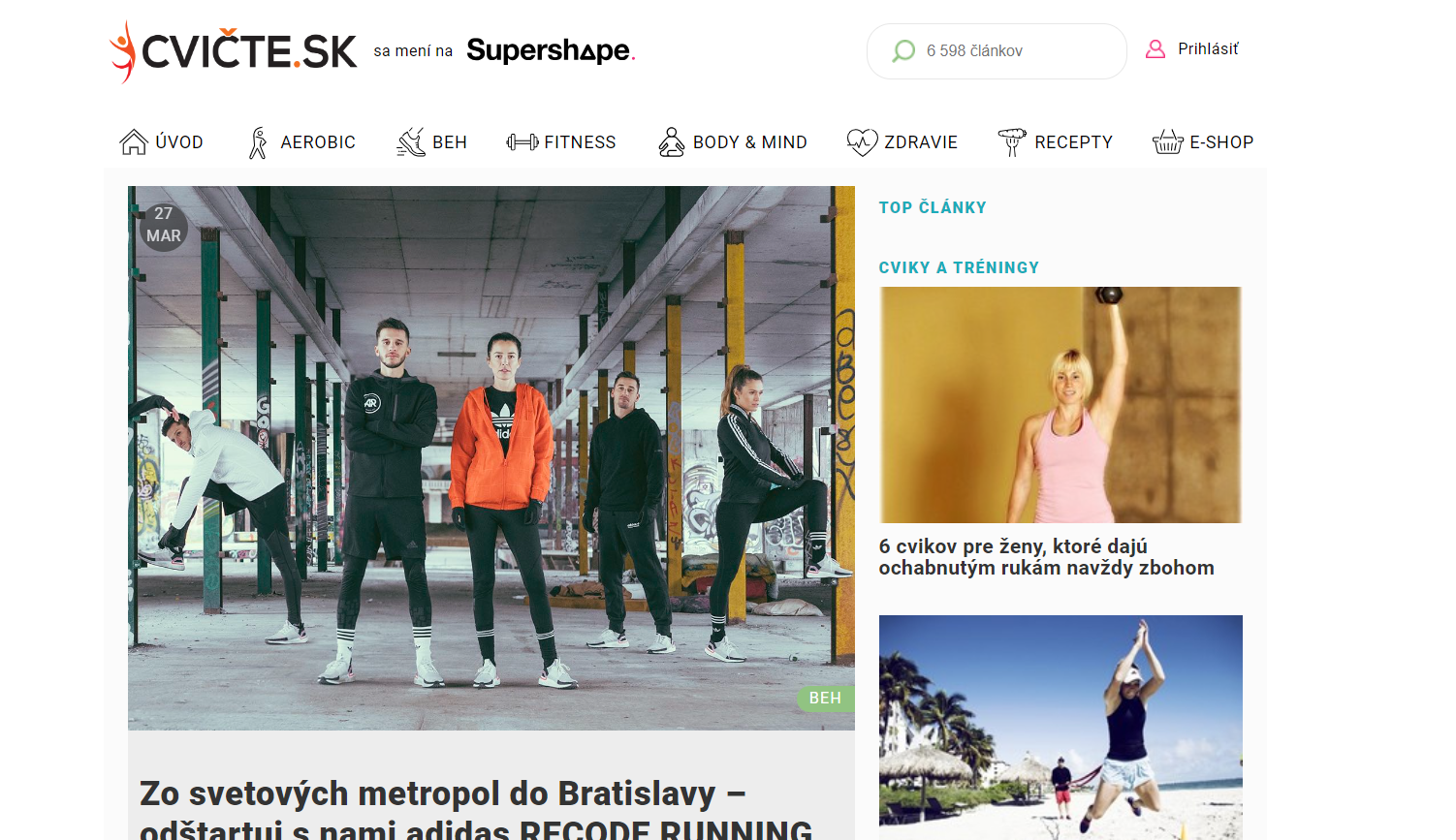
Stored XSS

The malicious script is permanently stored on the target server, such as in a database, comment field, or forum post.

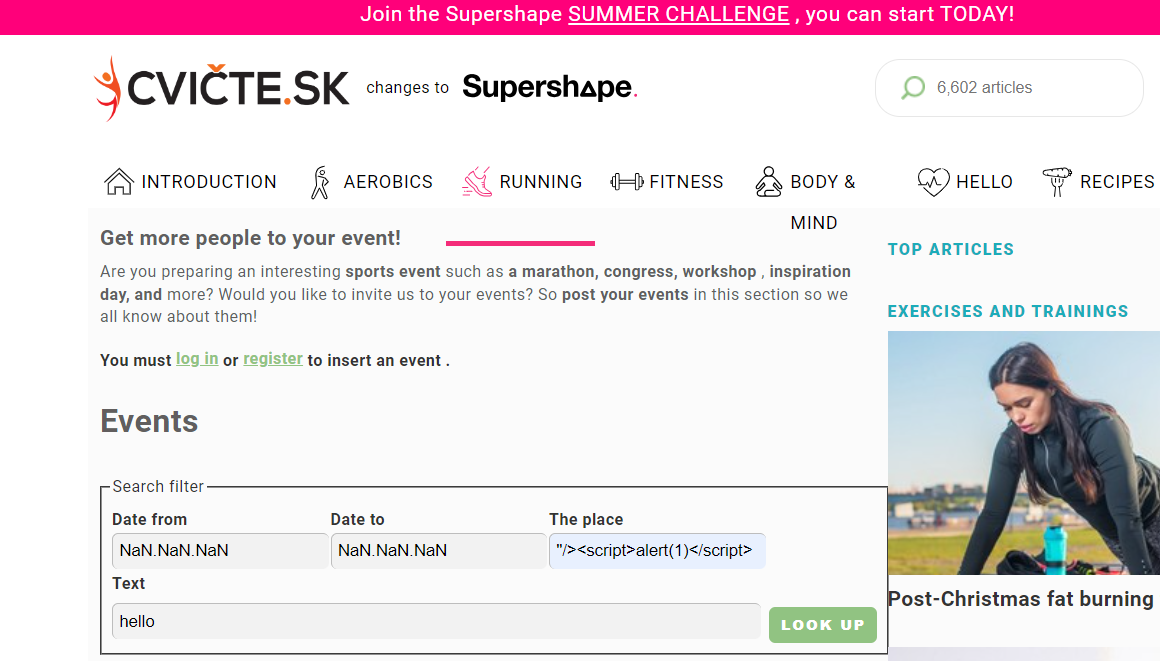
When a victim visits the infected page, the script is delivered as part of the webpage and executed in their browser.

**The steps taken to discover and reproduce the vulnerabilities:**

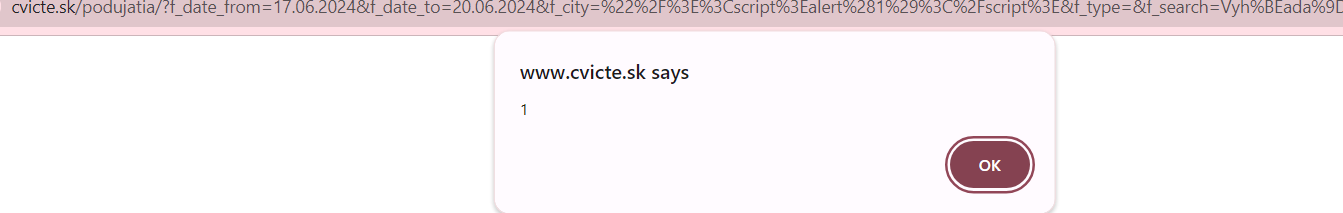
1) I watched the videos which were been provided to us which gave me detailed knowledge about XSS (Cross Site Scripting) its types and its impact in real world.

2) 

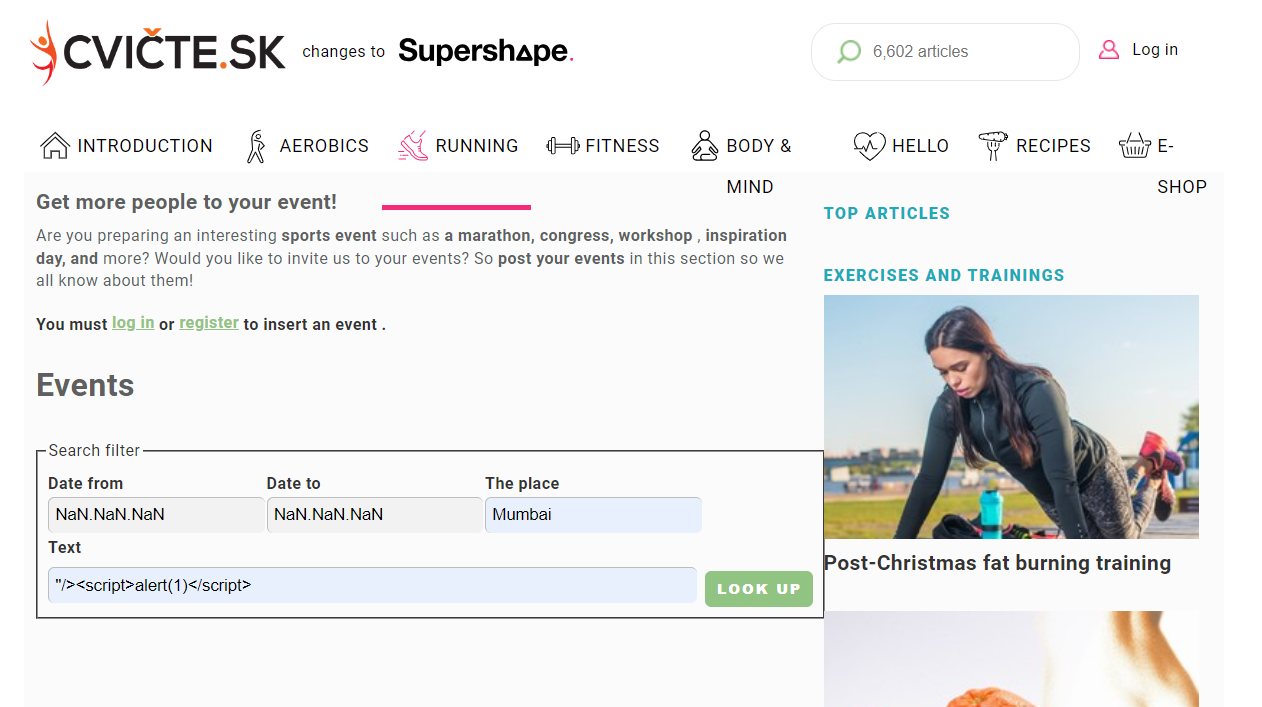
This was the website provided to us having XSS vulnerability

3) 

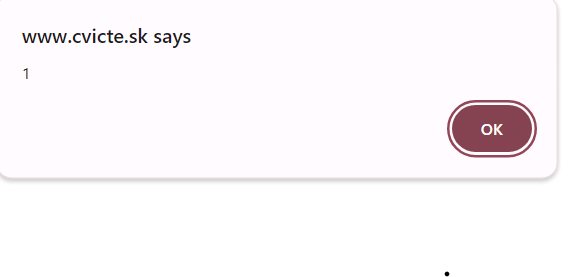
Here the place(Miesto) field is vulnerable so the java script code is injected their



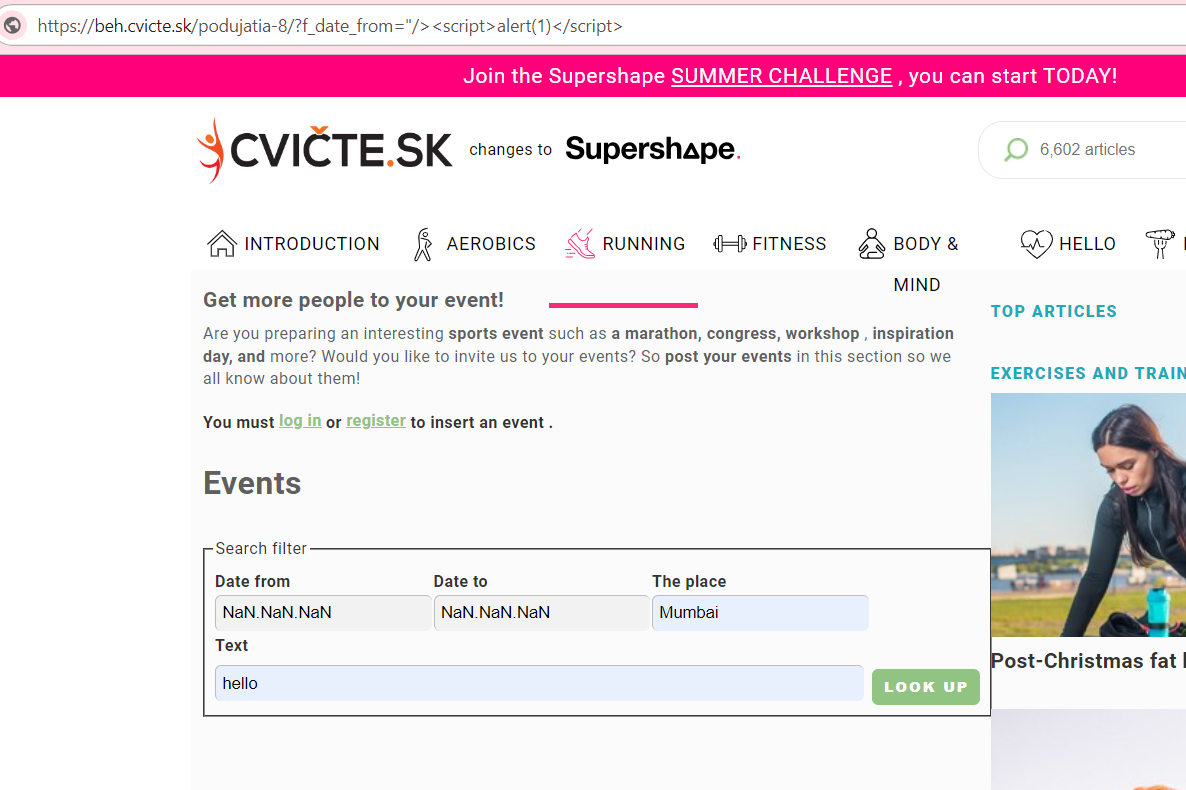
The result is as above

4) 

Here the text bar is vulnerable so java script code is injected their



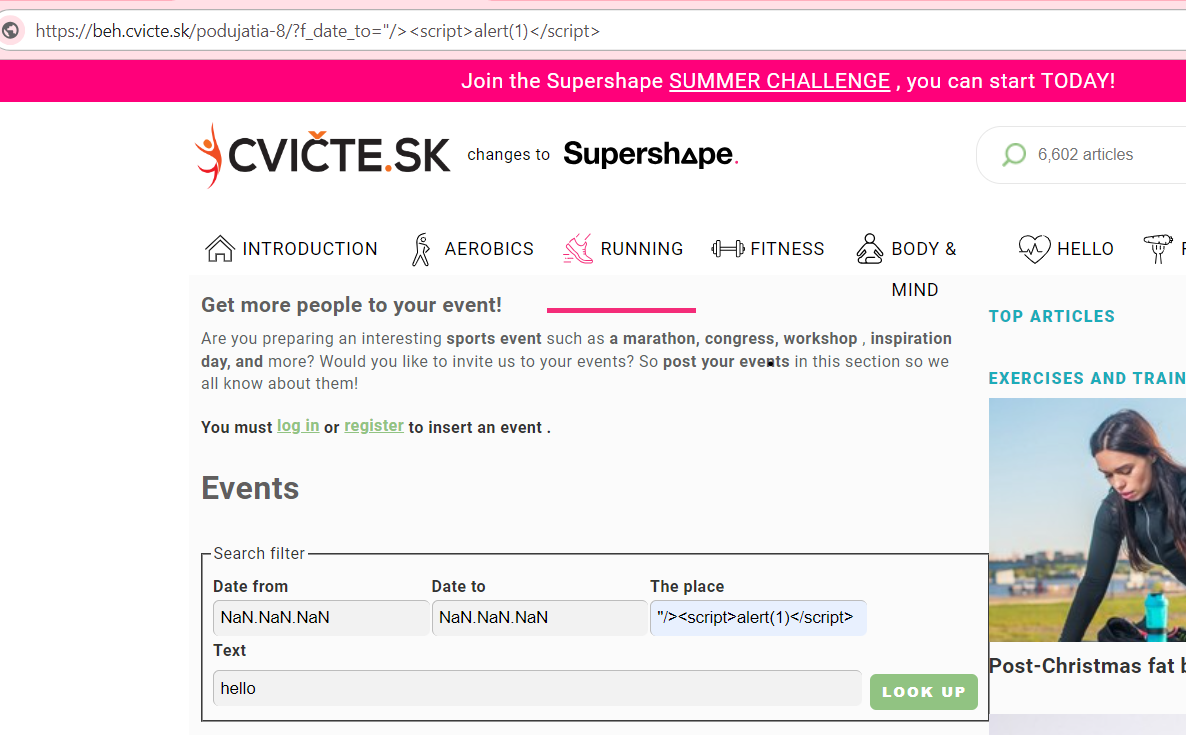
The result is as above

5) 

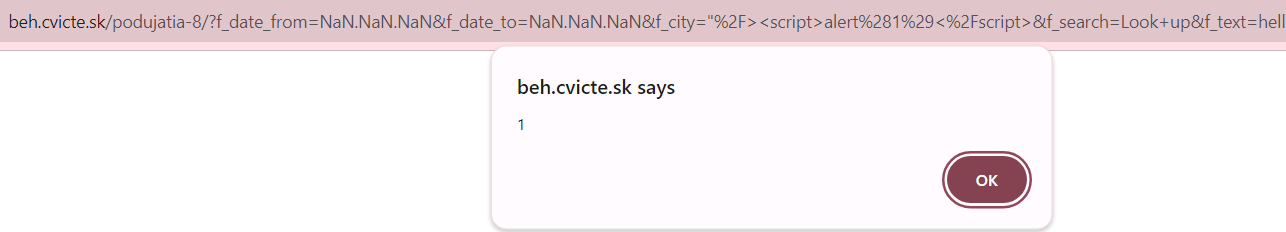
The Date from is vulnerable as we cant inject java script code their we injected it the URL of the website



The result as above

6) 

The Date to is vulnerable as we cant inject java script code their we injected it the URL of the website



The result as above

7) Manual testing method is been used

**Potential impacts of the vulnerabilities:**

Cross-site scripting (XSS) is a type of attack that involves injecting malicious code into a trusted website here it is of adidas. Attackers can use a variety of methods to trigger an XSS attack, including execution, injection which can cause various impact to the website.

The Impact can be:

Cookie Theft: Attackers can steal session cookies and impersonate users.

Defacement: The attacker can modify the content of the webpage.

Phishing: Displaying fake login forms to steal user credentials.

Keylogging: Capturing keystrokes to gather sensitive information.

Redirects: Redirecting users to malicious sites.

**Recommendations for mitigation:**

1) Secure development practice for a website:

Ensure proper coding to avoid XSS vulnerability

2)Incident response plan:

Have an incident response plan in place to quickly address any XSS vulnerabilities that are discovered.

3)Regular testing

Use Automated scanners, Code review and Manual Testing.

4) Encryption:

 Reduces data vulnerability by making it harder for malicious actors to access data.

5) Input Validation and Sanitization:

**Validate Inputs**: Ensure that inputs conform to expected formats and reject any that don't.

**Sanitize Inputs**: Remove any potentially dangerous characters or scripts from inputs.