**Experiment 10**

**Aim:** Perform Cross-site Scripting attack and analyze its impact on security.

**Theory:**

**Injection Attacks:**

Injection attacks are a type of security vulnerability that occur when an attacker is able to inject malicious code or commands into a computer system or application. Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

The oldest and most harmful attacks against web applications are injections. These may result in data loss, data integrity loss, data theft, service denial, and total system compromise. Insufficient user input validation is typically the main cause of injection vulnerabilities. The huge attack surface of injection vulnerabilities makes them extremely terrifying. Moreover, injection attacks are a form of vulnerability that is well known. This indicates that there are numerous trustworthy tools that are readily available for free that enable even novice attackers to automatically exploit these vulnerabilities.

**Types of Injection Attacks:**

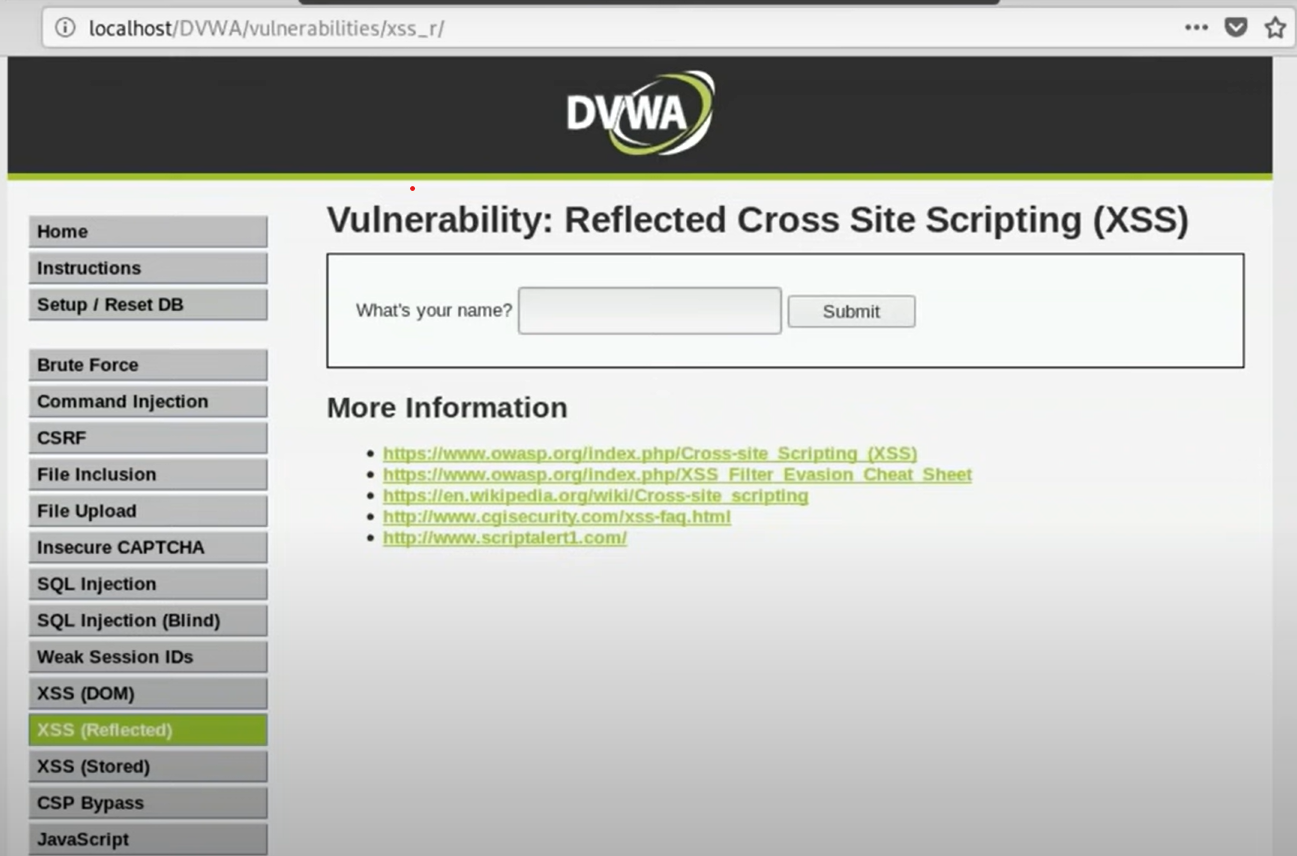
* Code Injection
* CRLF Injection
* Cross-site Scripting (XSS)
* Email Header Injection
* Host Header Injection
* LDAP Injection
* OS Command Injection
* SQL Injection (SQLi)
* Blind XPath Injection

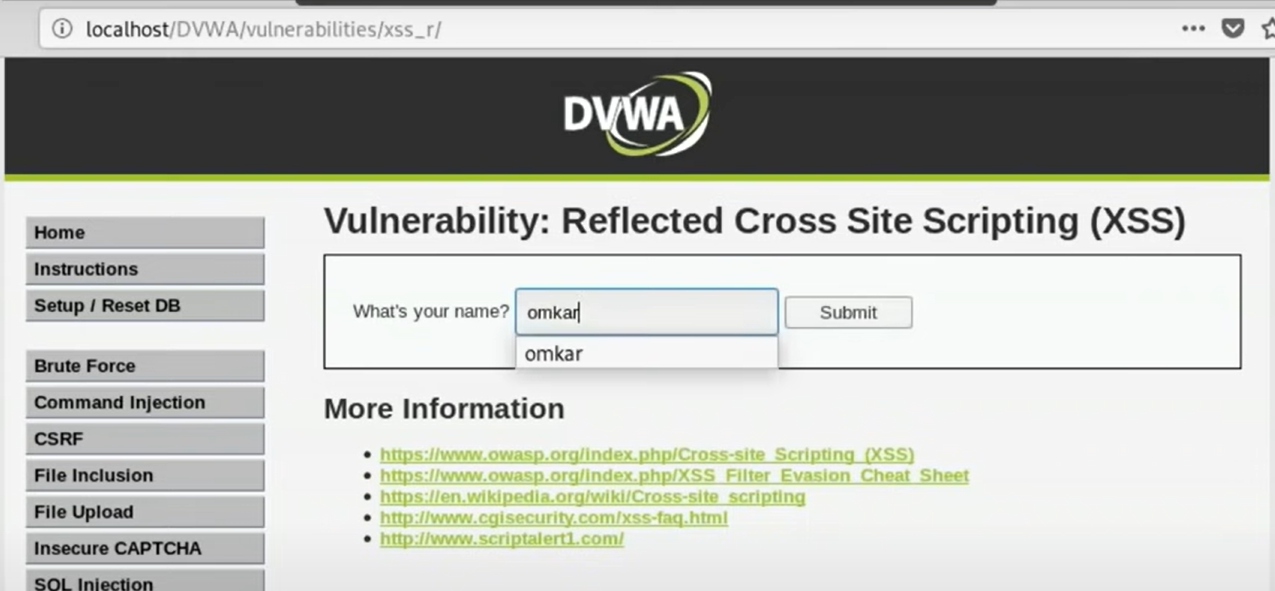
**Cross-site Scripting (XSS) Attack :**

Cross-Site Scripting (XSS) is a type of security vulnerability that can occur in web applications. It involves an attacker injecting malicious code into a web page that is then executed in the user's browser. This can be used to steal sensitive information, such as login credentials or personal data, or to carry out other malicious activities, such as redirecting the user to a phishing site or installing malware on their device.XSS attacks can occur in a number of ways, but one common method is through input fields on a web page, such as search bars or comment boxes. If the application does not properly sanitize user input, an attacker can inject malicious code into the field that is then executed when other users view the page. This can be especially dangerous on sites that require users to log in, as the attacker can potentially steal their login credentials and gain access to sensitive information.

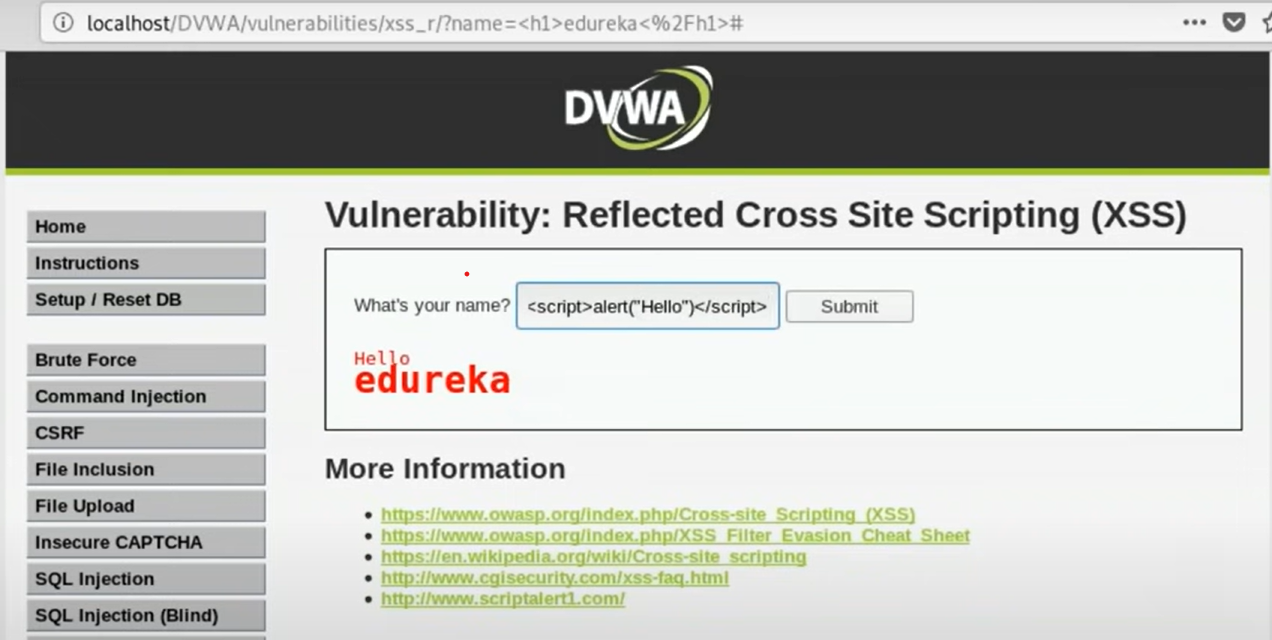
There are two main types of XSS attacks: reflected and stored. Reflected XSS attacks involve the malicious code being injected into a URL that is then sent to the user, such as through a phishing email or social engineering scam. When the user clicks the link, the code is executed in their browser. Stored XSS attacks, on the other hand, involve the malicious code being stored in the application's database, such as in a comment or message on a social media platform. When other users view the stored content, the code is executed in their browser.To prevent XSS attacks, web developers need to ensure that user input is properly sanitized and that any code is properly encoded. This can include using input validation to ensure that only expected characters are allowed in input fields, as well as properly encoding any user-generated content that is displayed on a web page. Additionally, web applications should implement Content Security Policy (CSP) headers, which restricts the sources of content that can be loaded on a page, helping to prevent malicious code from being executed.

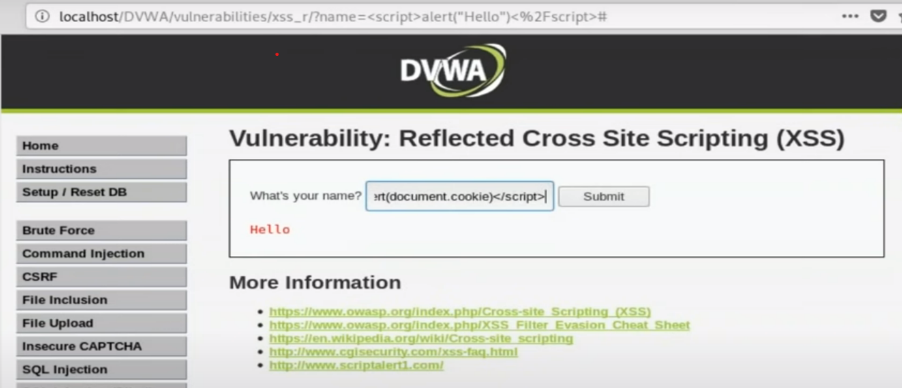
In terms of security, XSS attacks can have serious consequences for both users and website owners. Users can have their personal data stolen, their devices infected with malware, or be redirected to phishing sites. Website owners can suffer damage to their reputation and potentially face legal consequences, as well as lose the trust of their users. It is therefore important for web developers to take steps to prevent XSS attacks and ensure the security of their web applications. Additionally, users can protect themselves by being cautious when clicking on links or entering personal information on unfamiliar websites, as well as keeping their devices up-to-date with the latest security patches and software updates.

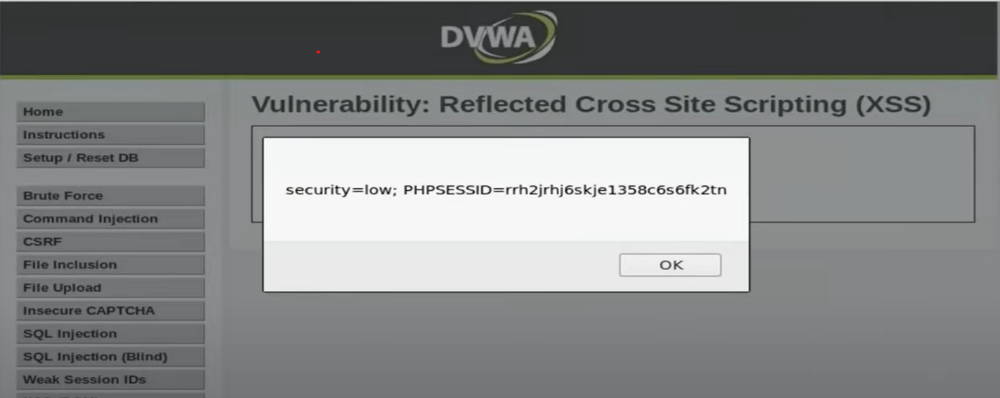


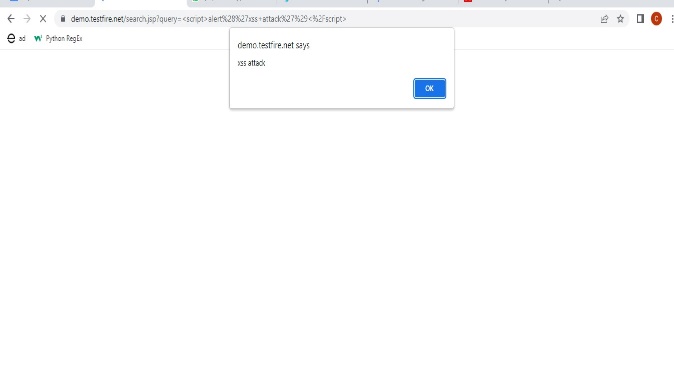












**Conclusion:** We learned about the Injection Attacks and their types and how they can be used by personnel with bad intentions to exploit an organization and get access to important information. We also understood how cross-site scripting (XSS) works and how it has an impact on security.

For Faculty Use

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Correction Parameters** | **Formative Assessment [40%]** | **Timely completion of Practical [ 40%]** | **Attendance / Learning Attitude [20%]** |  |
| **Marks Obtained** |  |  |  |