Ethics in IT

Class 10

Lab 4

UNITED TRUST

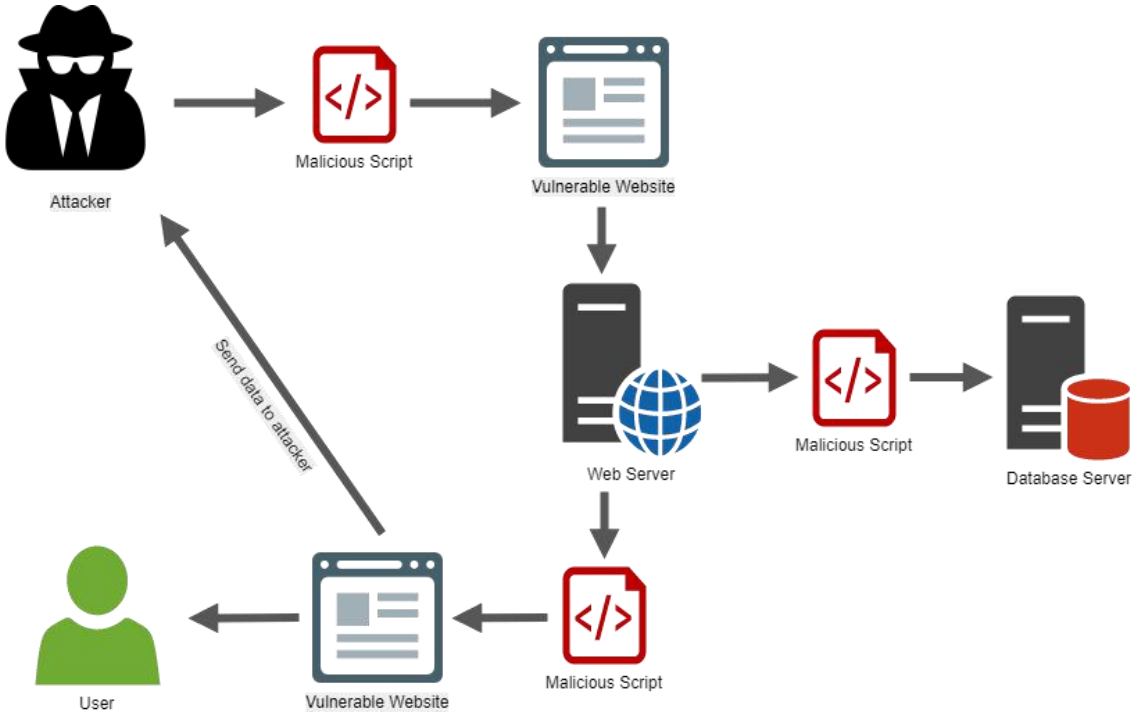
bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

Lab Objectives:

- XSS
- SQLi

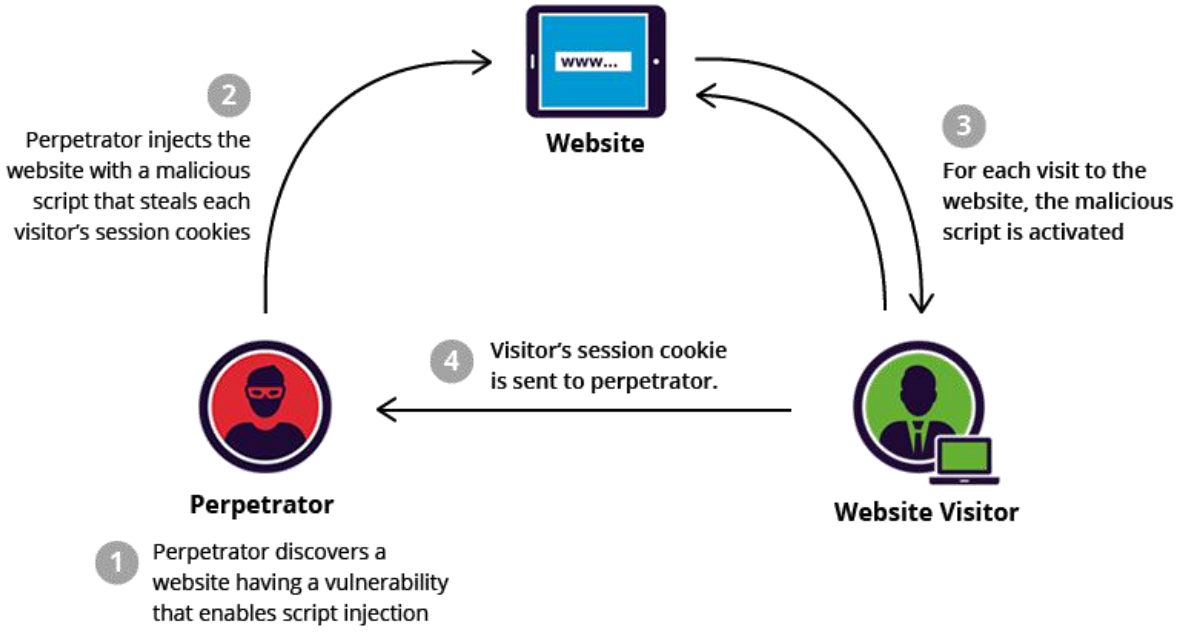
Cross-Site Scripting

Cross-site scripting (XSS) is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.



The attacker does not directly target his victim. Instead, he exploits a vulnerability in a website that the victim visits, in order to get the website to deliver the malicious JavaScript for him.

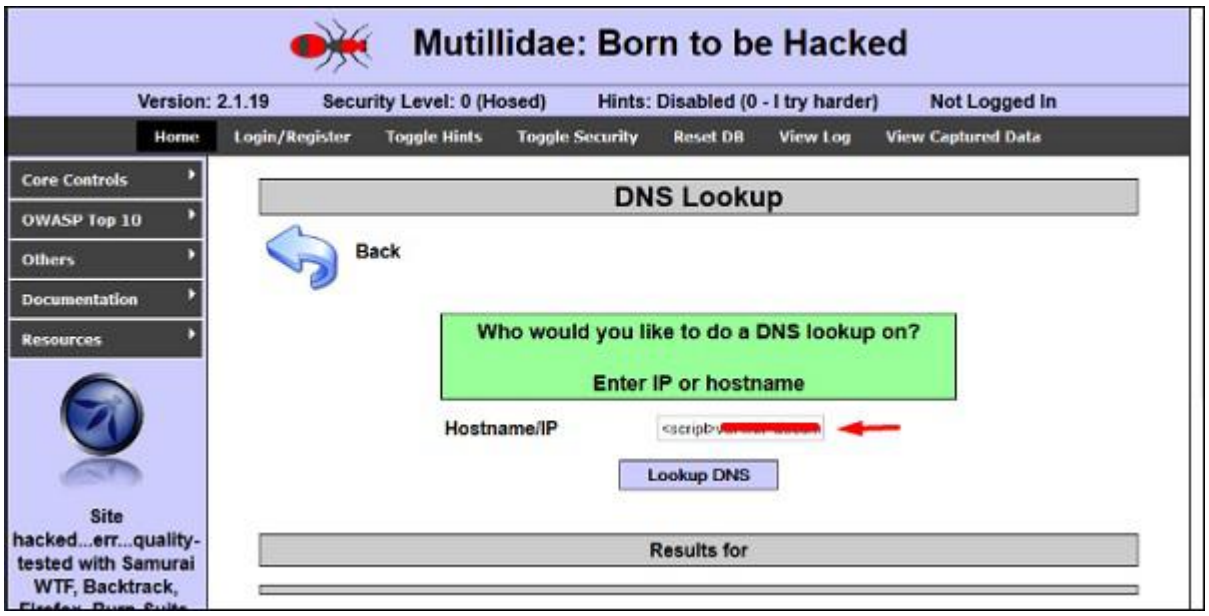
To the victim's browser, the malicious JavaScript appears to be a legitimate part of the website, and the website has thus acted as an unintentional accomplice to the attacker. These attacks can be carried out using HTML, JavaScript, VBScript, ActiveX, Flash, but the most used XSS is malicious JavaScript.



These attacks also can gather data from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising and create DoS attacks.

Example

Let’s take an example to understand how it works. We have a vulnerable webpage that we got by the metasploitable machine. Now we will test the field that is highlighted in red arrow for XSS.



First of all, we make a simple alert script

```
<script>
    alert(‘I am Vulnerable’)
</script>
```

It will produce the following output −

Types of XSS Attacks

XSS attacks are often divided into three types −

1. Persistent XSS, where the malicious string originates from the website's database.
2. Reflected XSS, where the malicious string originates from the victim's request.
3. DOM-based XSS, where the vulnerability is in the client-side code rather than the server-side code.

Generally, cross-site scripting is found by vulnerability scanners so that you don’t have to do all the manual job by putting a JavaScript on it like


```
<script>
    alert('XSS')
</script>
```

Burp Suite and acunetix are considered as the best vulnerability scanners.

SQL Injection

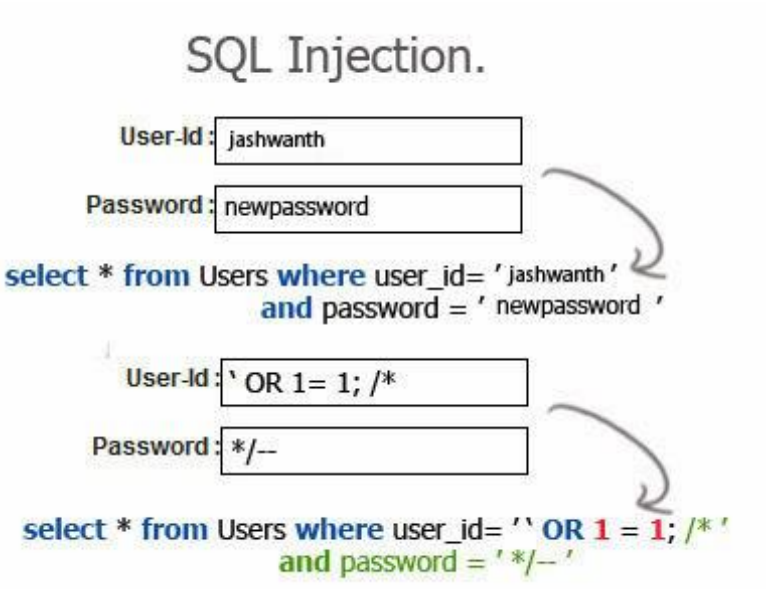
SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. This type of attacks generally takes place on webpages developed using PHP or ASP.NET.

An SQL injection attack can be done with the following intentions −

- To dump the whole database of a system,
- To modify the content of the databases, or
- To perform different queries that are not allowed by the application.

This type of attack works when the applications don’t validate the inputs properly, before passing them to an SQL statement. Injections are normally placed put in address bars, search fields, or data fields.

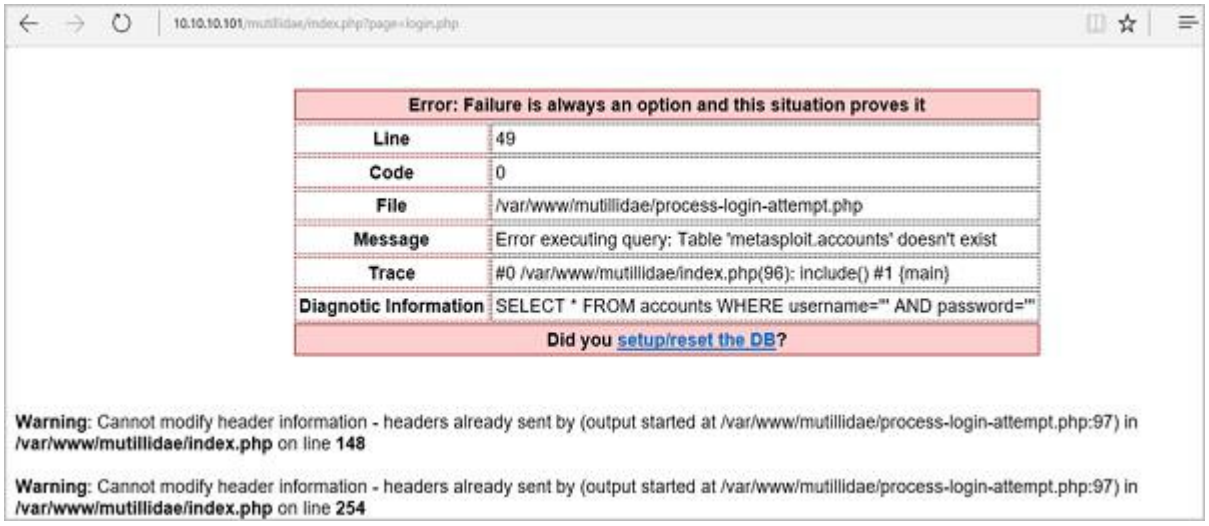
The easiest way to detect if a web application is vulnerable to an SQL injection attack is to use the " ‘ " character in a string and see if you get any error.



Example 1

Let’s try to understand this concept using a few examples. As shown in the following screenshot, we have used a " ‘ " character in the Name field.

Now, click the Login button. It should produce the following response −



It means that the “Name” field is vulnerable to SQL injection.

Example 2

We have this URL – http://10.10.10.101/mutillidae/index.php?page=site-footer-xssdiscussion.php

And we want to test the variable “page” but observe how we have injected a " ‘ " character in the string URL.

When we press Enter, it will produce the following result which is with errors.

SQLMAP

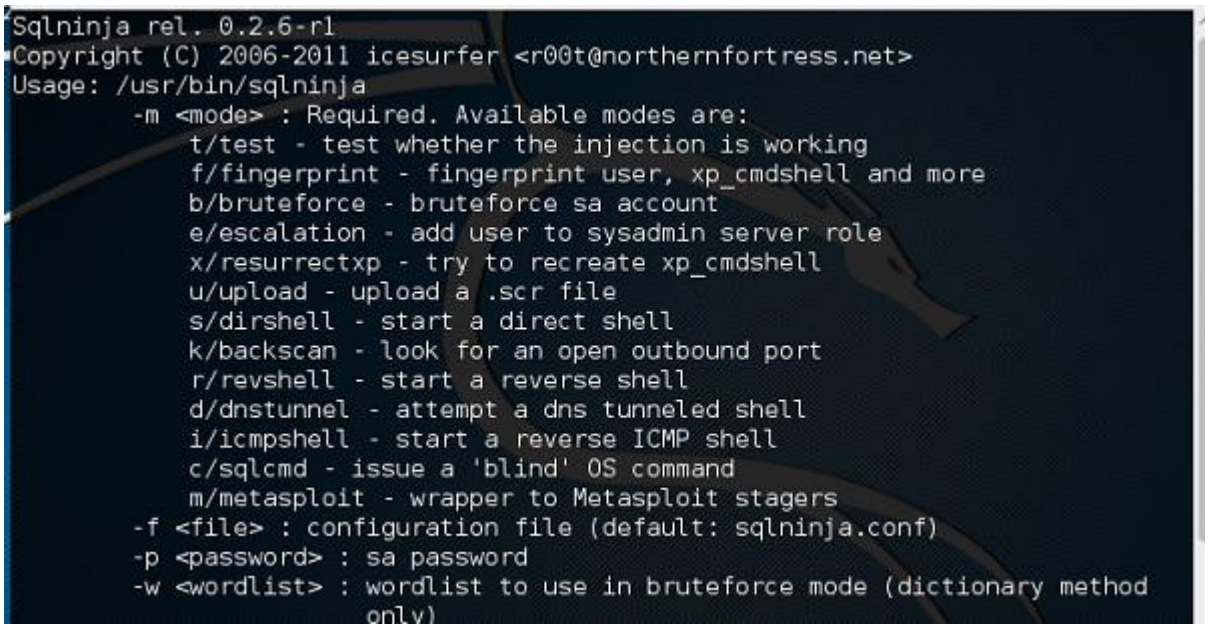
SQLMAP is one of the best tools available to detect SQL injections. It can be downloaded from http://sqlmap.org/

It comes pre-compiled in the Kali distribution. You can locate it at – Applications → Database Assessment → Sqlmap.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.0.5.63#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

SQLNinja

SQLNinja is another SQL injection tool that is available in Kali distribution.



JSQL Injection

JSQL Injection is in Java and it makes automated SQL injections.

So you need all of these hacking technique and methodologies to prevent hacker from the cyber space.