Ashit Rai
160166

Securing VIHS

CSE 628A
April 9, 2019

Authentication Bypass Vulnerability

- VIHS has a very simple and easy to exploit authentication bypass vulnerability in the field for password. Let us assume that the entry in password is ”input”, then the correspoding SQL query that would be formed is:

  $ **Select** uname **From** student **Where** password = $_GET[”*input*”]

- It was really easy to exploit this vulnerabitlity by just providing this as input to password field. $ *pass = 2’ or email = ’ashitr@iitk.ac.in* One can also exploit this by using someone else’s email and modifying the password accordingly.

- **Seps to Prevent Authentication bypass Vulnerability** One can use function such as MySQL’s mysql_real_escape_string() to enforce input validation. This simply makes sure that all the dangerous characters such as ’ which result in this Vulnerability are not passed as a SQL query back to the server.

File Inclusion Vulnerability

LocalFile Inclusion LFI

- To avoid LFI attacks one either needs to prevent user made inputs from being passed to any framework API in VIHS or sanitize all such inputs before passing them.

Remote File Inclusion RFI

- To avoid RFI attacks one needs to disallow any and all remote file includes that are specified via local file paths. One can do this by simply putting the allow_url_include flag to be set to 0.

SQL Injection Vulnerability

This was the main Vulnerability leading to many exploitations from the SEARCH field.

- There was a simple step that removes any keywords like AND,WHERE,SELECT,Union and so on, but this can be very easily bypassed by dividing the word into 2 groups of letters and adding them to left and right of the original word so that even if the original word is removed we still get the word back by combining the letters back.

  Example: ’oorr’ becomes ’or’ after the check removes one or.

- **Seps to Prevent SQL Injection Vulnerability** Instead of using data sensitization techniques one should wither use stored procedures or prepared statements so that simple hacks like ’oorr’ will not work anymore.