

Generic Web Application Testing With URL Argumenting

Triosec , SecNiche Security

Reliability Factor : 70%

This brief article simply layout the generic way to check the coding flaw of websites. This is entirely based on the penetration testing analysis .Number of websites have been tested to get to this conclusion. The technique is called as URL argumenting. This technique is quiet driven in its aspect. In this URL structured as:

http://<website name /login.php | http://<website name /login.asp
http://<website name> /members/login.php | http://<website name> /members/login.aspx
http://<website name>/smr/login/form.php | http://<website name>/smr/login/form.asp

A very general form which we encounter usually. Now a days coders are getting more security prone but there is still a problem. In this technique arguments are induced as

https:// <website name /login.php?x == x
https:// <website name /login.php?x == x&y == y& z==z

This works very craftily for non argumentative pages as this are parameters that are induced on the run. It is considered to be as dynamic infection. Due to this web pages get deflated with string of ///// which is the clear indication of coding flaw.

Metacharacters can also be induced as:

- 1 Metacharacters : ~!@#\$%^&*()
- 2 Buffer Crafting is also possible.
- 3 Weird Scripting is also possible.

These specific characters can be used that are infused with parameters. The combination of tick character ` and 0 in `0'0'0'0==`0'0'0'0 is also a good injection for testing of web applications. The Argumenting is showing its effect.



This test has been run after number of site those which are sustain to poor coding throw results like that. The attack is specific not so proliferate at every website testing. But still going great.