Forum:Hack Forums

Thread: [TIPS] Very Short Bug Hunting Tips [/TIPS]

Aakash_Choudhary - *August 9, 2016, 6:33 am*

Hello friends. I am CodeNinja a.k.a. Aakash Choudhary

Today i am giving a very small tip on Bug Hunting.

==========

Browse Testing Site which you want to test the site and then try to find
all APPLICATION ENTRY POINTS

Like :->

GET

POST

COOKIE

SEARCH BOX

Comment Section

Contact Us Section

Hidden POST in FORMS

LOGIN

After finding User Input Field or can say Application Entry Fields try to testing those fields.

Try to understand the Mechanism of those fields like what those fileds do actions.

Check JAVASCRIPT Validation and try to understand them.

Next thing to remember during TESTING is always try to test both CLIENT SIDE Request & SERVER SIDE Request

Try to intercept Request/Response through Burpsuite to understand them.

Example :->

A PASSWORD Change Field i am going to test.

Three Fields i see :->

Current Password

New Password

Confirm New Password

So in this MECHANISM we have to use current password.
As for testing Intercept this reuqest and using burpsuite remove the parameter :-> Current Passwod and then Forward Request and if we see
200 OK Response then its mean We Bypass Server Side Request Validation
Note that first input any text on current password and input our new password in next two fields and then intercept it.

About to understand MECHANISM see another MECHANISM example :-

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.
The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.
Once the attacker have successfully stolen the Session Token of the user, the attacker is able to log into the victim’s session by using the cookies which he have stolen.

Conclusion :->

Check both Client Side Request & Server Side Request. Find Application Entry Points and then testing on them

I will give more tips on this in future

CREDIT :-> My brother [Shawar Khan]

Thanks

Kashmiri Hunter - *August 9, 2016, 10:22 am*
Nice Effort CodeNinja.Keep It Up.Wish You Good Luck !

surelyenough - *August 11, 2016, 10:11 am*
(Aug 9, 2016 10:22 AM)Kashmiri Hunter Wrote: *[CITE]* Nice Effort CodeNinja.Keep It Up.Wish You Good Luck !Why are you writing like a crippled Indian?