

Forum:[Hack Forums](#)

Thread: [PHPSESSID decoding\encoding](#)

z3nd3r - November 3, 2018, 4:49 pm

Hi guys. I have one task to log in to the website knowing only victim's username

But I have other credentials.

And I think I can log in to the webpage changing PHPSESSID.

Just look at my PHPSESSID

If I use username: test-user1 and pass:test-user1

I receive

PHPSESSID=MTIudGVzdC11c2VyMS5YRFBSS1ZIUKVILiwhlyZmIzs3N3ksISMmZiM7Nzd5

which decodes to 12.test-user1.XDPRKVHREH.,!#&f#;77y,!#&f#;77y

I know that "12" is ID of my user.

And What should I do if I know the victim's ID = '11" and his username "richy"?

If I encode "11.richy." I get "MTEucmljaHku" What should I add to this encoded string for logging to the webpage in the name of "richy"???

Thanks in advance!

VoIPv2 - November 3, 2018, 6:42 pm

It would depend how the application renders a different session. If the session isn't being checked then you can just do plug and play. Correct me if I am incorrect.

M L T - November 4, 2018, 1:51 pm

(Nov 3, 2018 04:49 PM)z3nd3r Wrote: [\[CITE\]](#) Hi guys. I have one task to log in to the website knowing only victim's username

But I have other credentials.

And I think I can log in to the webpage changing PHPSESSID.

Just look at my PHPSESSID

If I use username: test-user1 and pass:test-user1

I receive

PHPSESSID=MTIudGVzdC11c2VyMS5YRFBSS1ZIUKVILiwhlyZmIzs3N3ksISMmZiM7Nzd5

which decodes to 12.test-user1.XDPRKVHREH.,!#&f#;77y,!#&f#;77y

I know that "12" is ID of my user.

And What should I do if I know the victim's ID = '11' and his username "richy"?

If I encode "11.richy." I get "MTEucmljaHku" What should I add to this encoded string for logging to the webpage in the name of "richy"???

Thanks in advance!

have you tried reversing the base64'd string? or double-encoding it? or maybe try a ceaser shift on the remaining chars

e..g. the remainder of the string that isnt regular base64 encoded