

Forum:[Hack Forums](#)

Thread: [\[Help\] Cookie Decoding](#)

Avocado - July 2, 2014, 2:55 am

Hey,

Anyone got any articles/info/tutorials on cookie decoding or encoding.

Thanks.

The Sly - July 2, 2014, 5:59 am

Hey,

Read some of this I suppose:

<https://hackforums.net/search.php?action=results&sid=f3c9ac0002437ff141af2226f71d3008&sortby=lastpost&order=desc>

Next time, use the search option. ^^ Saves alot of time and effort.

Avocado - July 2, 2014, 7:31 am

(Jul 2, 2014 05:59 AM)?WYc?ED Wrote: [\[CITE\]](#) Hey,

Read some of this I suppose:

<https://hackforums.net/search.php?action=results&sid=f3c9ac0002437ff141af2226f71d3008&sortby=lastpost&order=desc>

Next time, use the search option. ^^ Saves alot of time and effort.

The search option is always a good bet, when it returns what I am looking for. However in this case it doesn't.

Forezza - July 2, 2014, 7:37 pm

Cookies are an interesting subject in my eyes. It's always quite interesting to see how different companies form them. Some generate random alpha numeric values and store it in their database to identify you at a later date, some actually generate the hash of a specific value that they don't want you directly seeing (this can be cracked in some cases), some encode values as it doesn't really matter if you see them, some simply just generate random hashes as an identifier in their database, or some issue an encrypted value that you don't have the key to.

In most cases, most sites are not dumb enough to store critical information in cookies, they're just used as identifiers for who the user is and this same identifier is stored inside the companies database. It's also quite common to see companies storing encrypted information in cookies but decrypting them is out of the question in most cases as you don't know the key or algorithm.

The mistakes come when

- > They store hashed values of passwords, important information, or other info you shouldn't know by just hashing it. There is always the possibility of cracking it.
- > People encoding important information in things like base64 and storing them in cookies.
- > Basic values being hashed and used as identifiers (e.g. MD5 a numerical value to be used as a session identifier). If you managed to crack this, then you could easily just generate another MD5

hash with a different numerical value similar and steal others sessions (I have seen this before).
-> And so many more.

Just learn a bit about cryptography and you should understand it a bit better

Avocado - July 2, 2014, 9:13 pm

(Jul 2, 2014 07:37 PM)Forezza Wrote: [\[CITE\]](#) Cookies are an interesting subject in my eyes. It's always quite interesting to see how different companies form them. Some generate random alpha numeric values and store it in their database to identify you at a later date, some actually generate the hash of a specific value that they don't want you directly seeing (this can be cracked in some cases), some encode values as it doesn't really matter if you see them, some simply just generate random hashes as an identifier in their database, or some issue an encrypted value that you don't have the key to.

In most cases, most sites are not dumb enough to store critical information in cookies, they're just used as identifiers for who the user is and this same identifier is stored inside the companies database. It's also quite common to see companies storing encrypted information in cookies but decrypting them is out of the question in most cases as you don't know the key or algorithm.

The mistakes come when

-> They store hashed values of passwords, important information, or other info you shouldn't know by just hashing it. There is always the possibility of cracking it.
-> People encoding important information in things like base64 and storing them in cookies.
-> Basic values being hashed and used as identifiers (e.g. MD5 a numerical value to be used as a session identifier). If you managed to crack this, then you could easily just generate another MD5 hash with a different numerical value similar and steal others sessions (I have seen this before).
-> And so many more.

Just learn a bit about cryptography and you should understand it a bit better

That was a brilliant read, It was good to hear about a few of the common encoding methods that applications apply. I think I just need to read a bit more into Cryptography so I can identify the encryptions used, I can usually identify b64, md5 but in the cases that I decode such cookies, I realize that they must be double encoded due to the decoding being mumbo jumbo.

Thanks for the help though.