

Broken Access Control

Admin Cookie

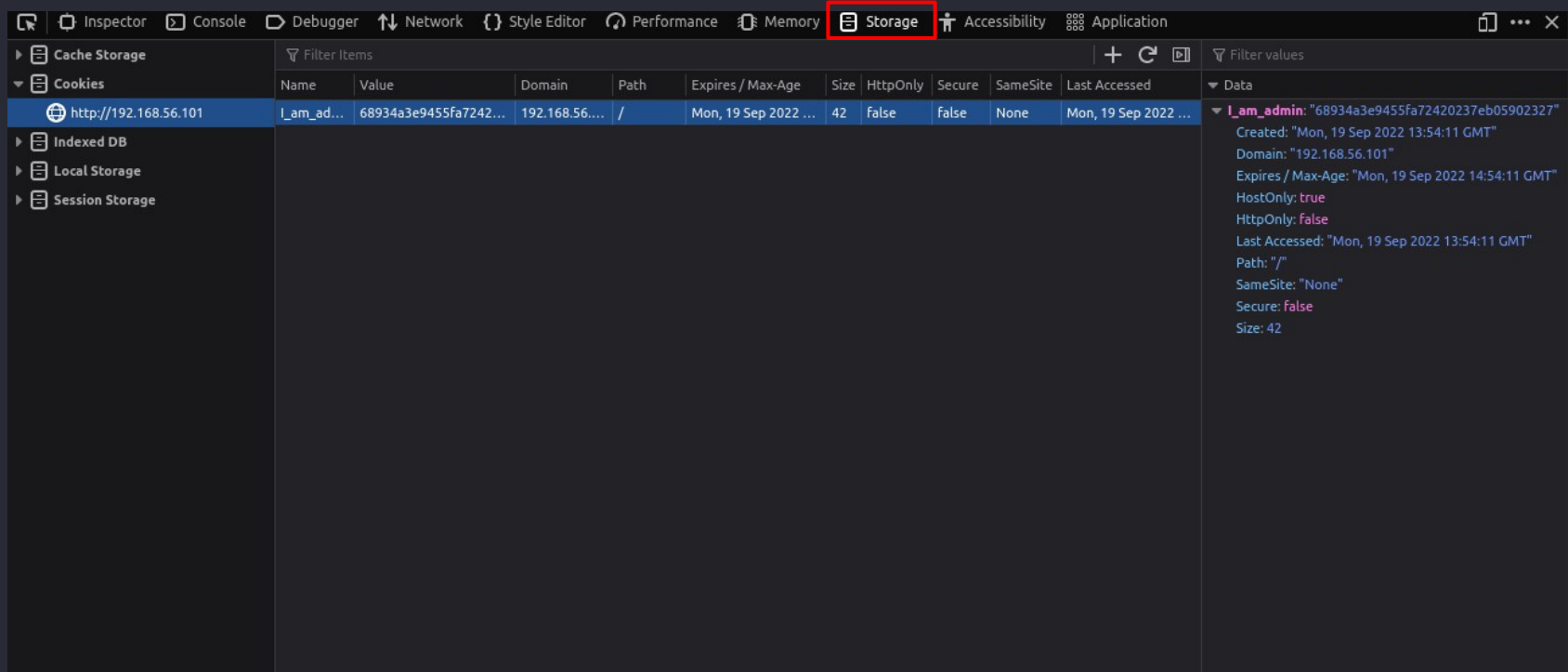
Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k. Notable Common Weakness Enumerations (CWEs) included are *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor*, *CWE-201: Insertion of Sensitive Information Into Sent Data*, and *CWE-352: Cross-Site Request Forgery*.

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

In this context we talk about a insecure admin cookie.

Walk Through

Step 1 : Open the web developer console on your browser and go to the Storage tab:



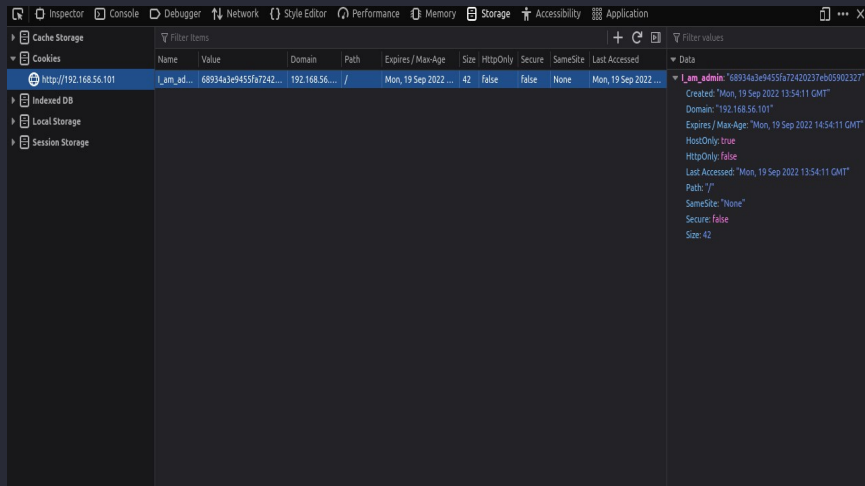
The screenshot shows the Chrome DevTools interface with the 'Storage' tab selected. The left sidebar lists storage types: Cache Storage, Cookies, Indexed DB, Local Storage, and Session Storage. The main pane displays a table of cookies. The right sidebar shows the details for the selected cookie, 'I_am_admin'.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
I_am_ad...	68934a3e9455fa7242...	192.168.56....	/	Mon, 19 Sep 2022 ...	42	false	false	None	Mon, 19 Sep 2022 ...

Cookie Details:

- Name:** I_am_admin
- Value:** "68934a3e9455fa72420237eb05902327"
- Created:** "Mon, 19 Sep 2022 13:54:11 GMT"
- Domain:** "192.168.56.101"
- Expires / Max-Age:** "Mon, 19 Sep 2022 14:54:11 GMT"
- HostOnly:** true
- HttpOnly:** false
- Last Accessed:** "Mon, 19 Sep 2022 13:54:11 GMT"
- Path:** "/"
- SameSite:** "None"
- Secure:** false
- Size:** 42

Step 2 : Copy the value of the cookie and try to decrypt it with <https://md5decrypt.net/> for example

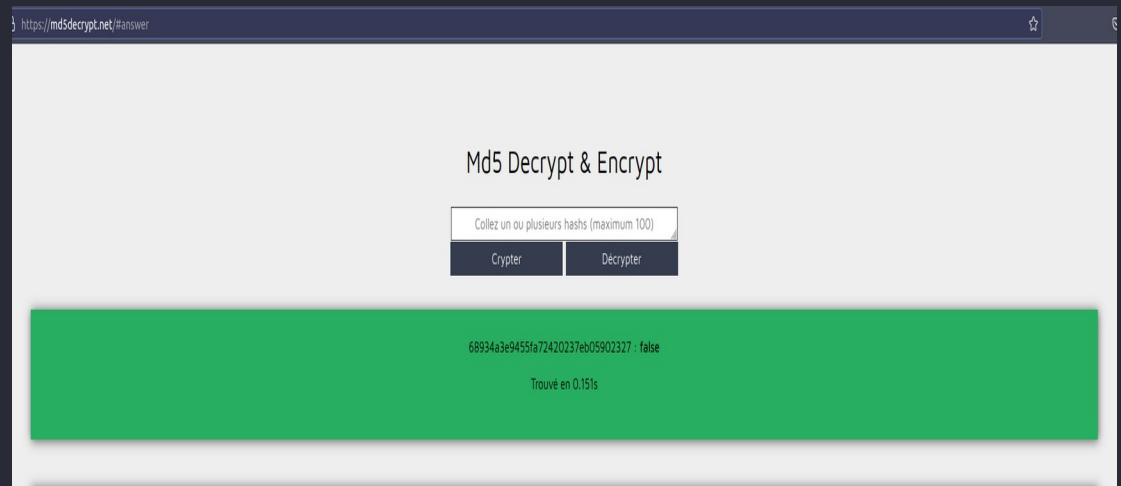


The screenshot shows the Chrome DevTools Application tab with the 'Cookies' section expanded. A table lists cookies for the URL 'http://192.168.56.101'. The selected cookie has the name 'l_am_admin' and a value '68934a3e9455fa72420237eb05902327'. The 'Data' pane on the right shows details for this cookie, including its creation time, domain, expiration, and security flags.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
l_am_admin	68934a3e9455fa7242...	192.168.56...	/	Mon, 19 Sep 2022 ...	42	false	false	None	Mon, 19 Sep 2022 ...

Data

- l_am_admin: "68934a3e9455fa72420237eb05902327"
- Created: "Mon, 19 Sep 2022 13:54:11 GMT"
- Domain: "192.168.56.101"
- Expires / Max-Age: "Mon, 19 Sep 2022 14:54:11 GMT"
- HttpOnly: true
- HttpOnly: false
- Last Accessed: "Mon, 19 Sep 2022 13:54:11 GMT"
- Path: "/"
- SameSite: "None"
- Secure: false
- Size: 42



The screenshot shows the 'Md5 Decrypt & Encrypt' website. The input field contains the hash '68934a3e9455fa72420237eb05902327'. The 'Décrypter' button is active. The output area, highlighted in green, displays the result: '68934a3e9455fa72420237eb05902327 : false' and 'Trouvé en 0.151s'.

Md5 Decrypt & Encrypt

Collez un ou plusieurs hashes (maximum 100)

Crypter Décrypter

68934a3e9455fa72420237eb05902327 : false

Trouvé en 0.151s

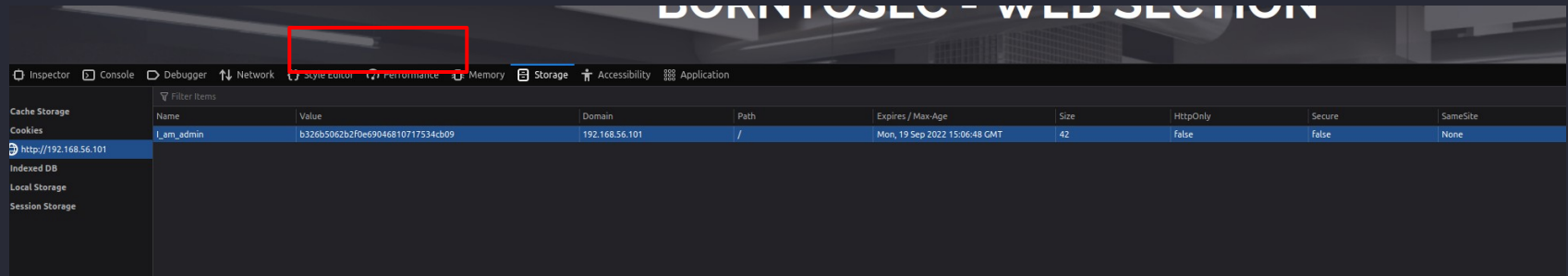
Step 3 : We see the decrypted hash value is : false so try encrypt true in md5 and replace the value of the cookie by the new hash

Md5 Decrypt & Encrypt

Crypter

Décrypter

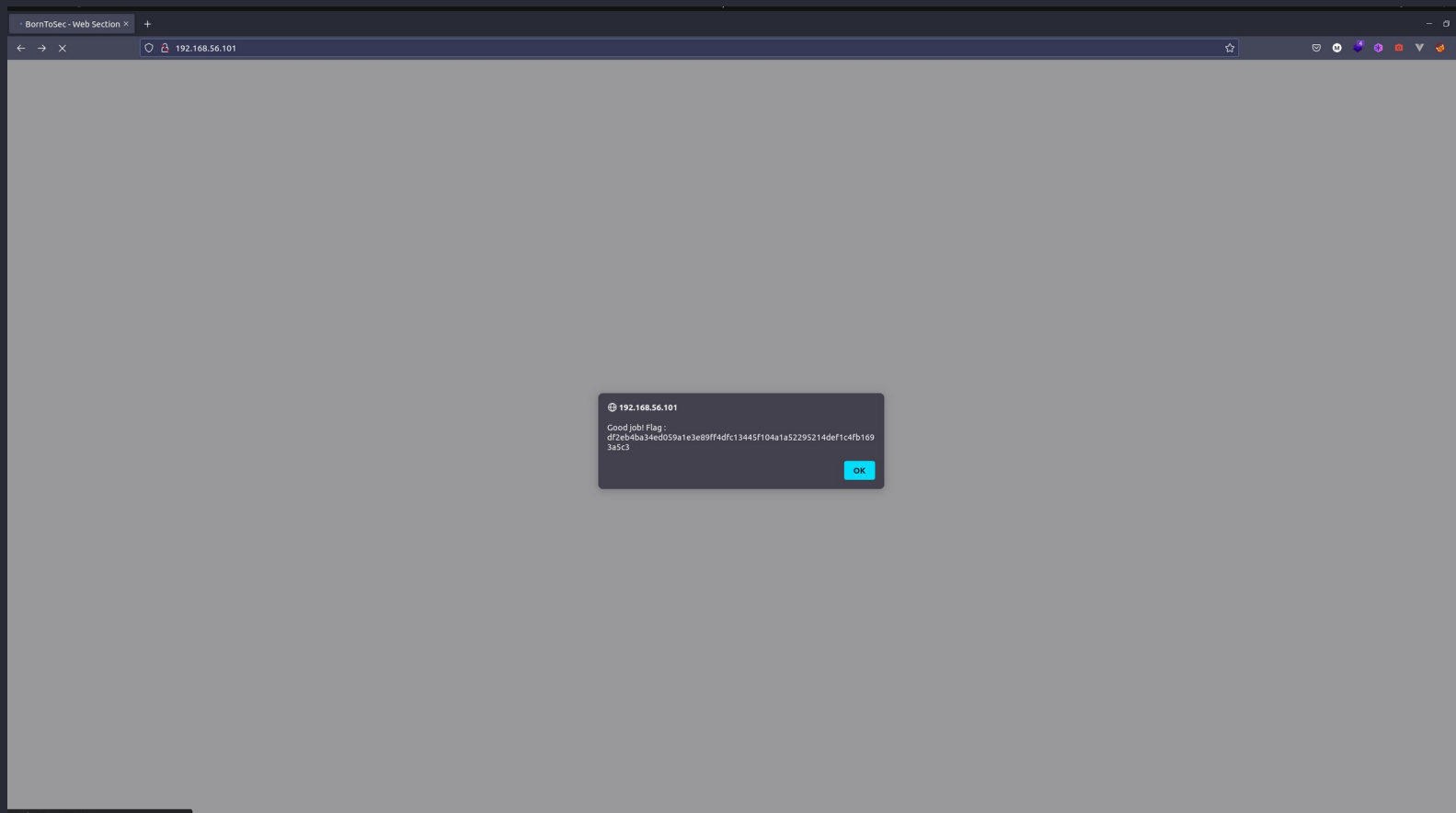
Md5(true) = b326b5062b2f0e69046810717534cb09



The screenshot shows the 'Cookies' tab in a web browser's developer tools. The table lists cookies for the domain 192.168.56.101. The 'Name' column header is highlighted with a red box.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
l_am_admin	b326b5062b2f0e69046810717534cb09	192.168.56.101	/	Mon, 19 Sep 2022 15:06:48 GMT	42	false	false	None

Step 4 : Reload the page and we are admin, we got the flag !!



Tools :

- <https://md5decrypt.net/>

How to fix :

- Use a more secure Algorithm than md5 like sha-512 or RSA
- Use an uid rather than a boolean to set the admin cookie
- Make check in the back when a cookie is changed.