

## Sensitive Response

```
HTTP/1.1 200 OK
Content-Length: Number
Content-Type: application/json

{
    "phone" : "01********",
    "token" : "**********"
}
```

Mahmoud M. Awali
©@0xAwali



Try To Inject Origin Header e.g. Origin: http://me.com And If Response Contains Access-Control-Allow-Origin: http://me.com AND Access-Control-Allow-Credentials: True, There is CORS

- 1 Writeup
- 1 Writeup
- M Writeup

GET /getInfo HTTP/1.1

Host: www.company.com User-Agent: Mozilla/5.0

Referer: https://previous.com/path

Origin: http://me.com



Try To Inject Origin Header With Your Domain e.g. http://company.com.me.com, http://company.com, http://company.com http://comp

- Video
- Video
- Tweet

**GET /getInfo HTTP/1.1** 

Host: www.company.com User-Agent: Mozilla/5.0

Referer: https://previous.com/path

Origin: http://company.com.me.com

Try To Inject Origin Header With Special Chars e.g., & ' "; !  $^*$  \* () + = ` ~ - \_ = | { } % OR Non Printable Chars e.g.  $^*$ 01-08,  $^*$ 0b,  $^*$ 0c,  $^*$ 0e,  $^*$ 0f,  $^*$ 10- $^*$ 1f AND  $^*$ 7f



Blog



Writeup

**GET /getInfo HTTP/1.1** 

Host: www.company.com User-Agent: Mozilla/5.0

Referer: https://previous.com/path

Origin: http://me.com`.company.com

Try To Inject Origin Header e.g. Origin: http://me.com And If Response Contains Access-Control -Allow-Origin: \* AND There Is Cache-Control: no-cache Header Try Use This POC

- Writeup

Blog

Tweet

```
method: 'GET',
  cache: 'force-cache'
</script>
```



Try To Use Web Cache Deception Attack, Add Static File e.g. nonexistent.css OR logo.png To Your Endpoint To Cache Sensitive Response



Slides



Writeup

• [1]

Writeup

• **M** 

Writeup

• **M** 

Writeup

GET /getInfo/nonexistent.css HTTP/1.1

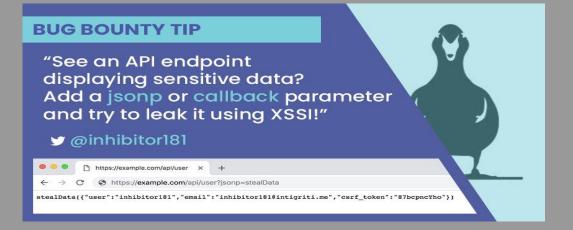
Host: www.company.com User-Agent: Mozilla/5.0

Referer: https://previous.com/path Origin: https://www.company.com



Try To Add jsonp OR callback To Any Sensitive Endpoints e.g. http://company.com/getInfo?jsonp=function To You Can Read The Response

- Tweet
- 1 Writeup



Try To Figure Out, There Is Cache-Control: no-cache Header In HTTP/1.1 Response OR Pragma: no-cache Header In HTTP/1.0 Response, If Yes There Is Issue Here

• 😏

**Tweet** 

### Try To Figure Out, There Is X-Frame-Option Header OR Not In The Response



Blog



Writeup



Writeup



There Are JSONP Endpoints OR JavaScript URL e.g. http://company.com/getInfo.js Contains Sensitive Data Based Only On Cookie, Try To Include It To Achieve XSSI



Slides



Blog



Writeup

#### Steps to produce :-

- 1 Filter Burp Suite History To MIME type Script
- 2 Lookout For JS Endpoints Without X-Content-Type-Options: nosniff
- 3 Search About

**Sensitive Data** 

4 - Make Sure There Isn't Authorization Headers



Try To Figure Out, There Is postMessage API e.g. Window.postMessage("text", "\*"); OR addEventListener("message", function(message){message.origin});

- 🚇 Blog
- 🚇 Blog
- 🚇 Blog
- 👸 Blog
- Blog

#### Steps to produce :-

- 1 Browse To http://company.com/getInfo
- 2 Right Clicking, Click On View Page Source
- 3 Search About

postMessage With \* addEventListener With Argument-Function.origin

# Thank You

Mahmoud M. Awali
©@0xAwali