

Magecart Analizi

written by Mert SARICA | 4 April 2020

If you are looking for an English version of this article, please visit [here](#).

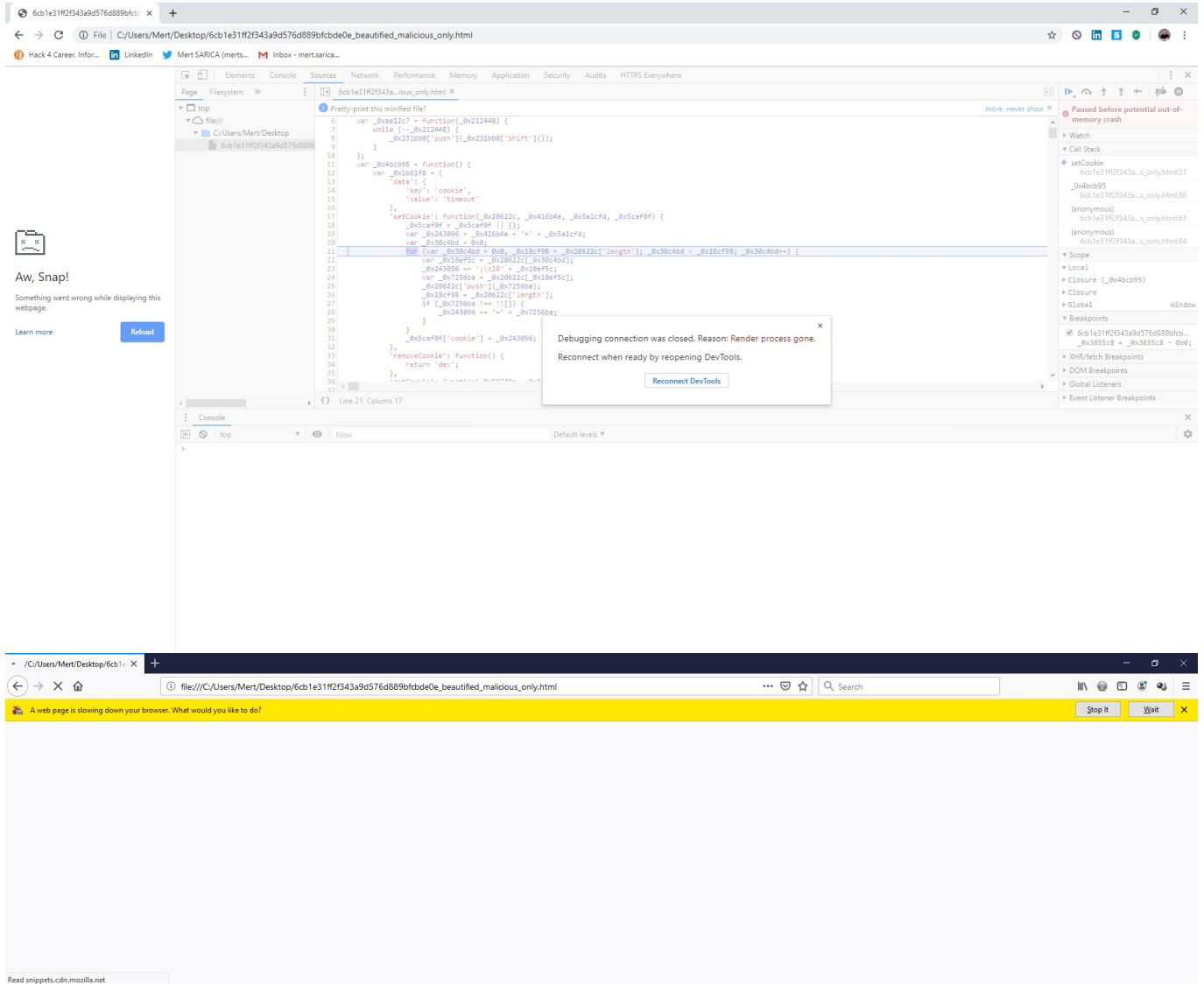
Hatırlarsanız Magecart ile Mücadele başlıklı blog yazımda zararlı JavaScript kodunun analizine başka bir yazımda yer vereceğimi belirtmiştim. Bu zamana dek çok defa zararlı javascript kodu analiz etmiş ve nasıl analiz edilebileceğine dair yaklaşık 3 yıl önce Zararlı JavaScript Analizi başlıklı bir blog yazısı da yazmıştım. Tabii yıllar geçtikçe tehdit aktörlerinin kullandığı yöntemler değişmeye ve siber güvenlik analistlerinin, araştırmacılarının işlerini git gide daha da zorlaştırmaya başladı.

Magecart grubunun geliştirdiği zararlı JavaScript kodu (6cble31ff2f343a9d576d889bfcdbde0e.js) ile ilk karşılaştığımda kodun kolay bir şekilde anlaşılamayacak kadar karmaşıklaştırılmış (obfuscated) olduğu JavaScript Obfuscator veya JavaScript Obfuscator Tool araçlarından biri kullanılmış olabilir.) hemen dikkatimi çekmişti. de4js ve IlluminateJs gibi araçların da varlığına güvenerek karmaşıklaştırılmış kodu kolay bir şekilde alt edeceğimi, en kötü dinamik kod analizi yaparak (debugging) mutlu sona ulaşabileceğimi düşünüyordum fakat evdeki hesap çarşıya uymadı. :)

```
"C:\Users\Mert\Desktop\YeniYazil\Magecart\6cble31ff2f343a9d576d889bfcdbde0e.js - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
6cble31ff2f343a9d576d889bfcdbde0e.js 13
1160 var childImgs=elem.querySelectorAll('img');for(var i=0;i<childImgs.length;i++){(var img=childImgs[i];this.addImage(img);)
1161 if(typeof this.options.background=='string')(var children=elem.querySelectorAll(this.options.background);for(i=0;i<children.length;i++){var child=children[i];this.
addElementBackgroundImages(child);});var elementNodeTypes={1:true,9:true,11:true};ImagesLoaded.prototype.addElementBackgroundImages=function(elem)(var style=getComputedStyle(elem
);if(!style){return;
1162 var reURL=/url\(\s*(.*)?\s*\)/gi;var matches=reURL.exec(style.backgroundImage);while(matches!=null){var url=matches[2];if(url){this.addBackground(url,elem);)
1163 matches=reURL.exec(style.backgroundImage);});ImagesLoaded.prototype.addImage=function(img)(var loadingImage=new LoadingImage(img);this.images.push(loadingImage););ImagesLoaded.
prototype.addBackground=function(url,elem)(var background=new Background(url,elem);this.images.push(background););ImagesLoaded.prototype.check=function(){var _this=this;this.
progressedCount++;this.hasAnyBroken=false;setTimeout(function(){this.complete();return;
1164 function onProgress(image,elem,message){setTimeout(function(){this.complete(image,elem,message);});)
1165 this.images.forEach(function(loadingImage)(loadingImage.once('progress',onProgress);loadingImage.check();));ImagesLoaded.prototype.progress=function(image,elem,message)(this.
progressedCount++;this.hasAnyBroken=this.hasAnyBroken||!image.isLoaded;this.emitEvent('progress',[this,image,elem]);if(this.jqDeferred&&this.jqDeferred.notify)(this.jqDeferred.
notify(this,image));
1166 if(this.progressedCount===this.images.length){this.complete();)
1167 if(this.options.debug&&console){console.log('progress: '+message,image,elem););ImagesLoaded.prototype.complete=function(){var eventName=this.hasAnyBroken?'fail':'done';this.
isComplete=true;this.emitEvent(eventName,[this]);this.emitEvent('always',[this]);if(this.jqDeferred)(var jqMethod=this.hasAnyBroken?'reject':'resolve';this.jqDeferred[jqMethod](
this)););function LoadingImage(img){this.img=img;
1168 LoadingImage.prototype.create(Emitter.prototype.create);LoadingImage.prototype.check=function(){var isComplete=this.getIsImageComplete();if(isComplete){this.confirm(this.img.
naturalWidth===0,'naturalWidth');return;
1169 this.proxyImage=new Image();this.proxyImage.addEventListener('load',this);this.proxyImage.addEventListener('error',this);this.img.addEventListener('load',this);this.img.
addEventListener('error',this);this.proxyImage.src=this.img.src;);LoadingImage.prototype.getIsImageComplete=function(){return this.img.complete&&this.img.naturalWidth;);
LoadingImage.prototype.confirm=function(isLoaded,message)(this.isLoaded=isLoaded;this.emitEvent('progress',[this,this.img,message]););LoadingImage.prototype.handleEvent=function(
event)(var method='on'+event.type;if(this[method]){this[method](event););LoadingImage.prototype.onload=function(){this.confirm(true,'onload');this.unbindEvents(););LoadingImage.
prototype.onerror=function(){this.confirm(false,'onerror');this.unbindEvents(););LoadingImage.prototype.unbindEvents=function(){this.proxyImage.removeEventListener('load',this);
this.proxyImage.removeEventListener('error',this);this.img.removeEventListener('load',this);this.img.removeEventListener('error',this););function Background(url,element)(this.url=
url;this.element=element;this.img=new Image();)
1170 $.fn.imagesLoaded=function(options,callback)(var instance=new ImagesLoaded(this,options,callback);return instance.jqDeferred.promise($(this)););ImagesLoaded.
makeQueryPlugin().return ImagesLoaded.));var _Ox4e75=['wzrDlMOJw7ob','wqfDp2ndtww','wrfciABCQew','WMKypwNIX8OCCQ==','wprCoHPDjQ==','2CAmfA==','w0xw6fDnMKRgwpMm','w7nDlMKRw6Y=','
FUTCjXCCoA==','wvpDmsOI','cV1z6M==','wpjDlIHdnXbdq84=','2M04aMKlJQ==','wzrDwgB1w5w','w5/Cq807wrcnCf0=','wpXDvhrDp2g=','w4rCq8oAwpfCmw=','wzrLn0Usw47Ck2Bw75Pw5YfwUg=','
w0DhncLw4BhwqEKwrDp8kFR8Ew4E=','aMOXw612w5d0','wzrMxw7nDv8RTwpg=','2sOrdeKsMcK8wog2','w0l6wrcCmfcCn8K/QQ==','w5oVwocJw70SVh0=','
fjEzAMRTTMOqWELCtWbCpWdLwUwXDrGUpC02w5NFPcKfMM09FEXDKtZdrsRnoATDgWfDoGAlTsRBT3R9BUjw5zDpsOlwqFdw5HDhsKwAM0owpJcGEEfwQYAMKKIU/Dsg==','w5XCk8R7wgdDnQ==','w68HDMoRtk=','
w4XDtmIiw7Y=','L37dk3k9w==','wzrDrs0rW6A4','w7PCncOPwQT','wonDkjnbokA=','w7EHA80sALCg8KsLMK4','QEDChB402zYN','w73DiYpDtcGw4LDjRV/w6DIw6Qxw8=','w5owQZTbSbCmQ==','
wzgxw6PdnCLmpUuwojDtQjDvs0wqds','wzrHdhjJdUDDlA==','wqjDgcOUw5Sw4HDsxDCo80eChXCVFs=','KlDCKATC0g8=','w77Ct148w8=','wohqwPLCs3Xcm8K/QcKpW4Mdw6fciWc=','SMOpw54=','wpluworCg3w=','
H8Ktw4fdtUit=','w47Dv0bDn8Ka','wovcklTDqA==','QcKBA30v','w43Ck8R6wzA=','wqk2CyCpCnw==','w5HDv0bDhg==','w6fCso06wpg5BB7CvcKw0/DksKRwo5AFECQXwooywQ==','wozHwbpCg20=','
eWw0pTtUQlfa80KwAoNAGjDkxw78T','tCkyypdUo8EArpPG2TCjsoHv7wwoB1KM06JA==','2lYhw7vDuMKlUkM=','MDU5wpgvQ==','woBpQxV6D3vDnyo=','w4RcQ804wHcnlA=','wzvcPgTDjD53NgQ5','
WMN0b15Nqocfsocx','w5/DgTDnMKW4g=','osouw57DlG==','w4cDf8ot','wqgDp3PrcoQgm0M0Q==','w7sXwpgUwzrP','w4xeU8KYw4rDnQ==','wp/ChnnDgMKUvFTBwQ=','cizCgsOI','ecKywo1t','wpzDgcOow60=','
MsOgw4vDbk8NssQJwqC=','wzrxwupDcklJCsK4YsKIw5Izw7Csw==','WDAqesK7BA==','w4bCo18rwr8u','w77DjYpDkg==','w5vdiMKRVw6ZDuso2','BrgLLA==','B3rDiXs=','H8KNw45n','wqjCk2/DJA==','
w0cDl3Xds80W==','WUUP','EsOqw4TDkMRaTA==','EhwRRCrW4zC12c=','w4OXD80uVCM=','w5fDhsKmw6k=','DW7DkHwsQA==','V8K078RX','FcK2w5dkwrPCmQ==','PcoZw7w=','wpDcgRVR','wzXDmsOlB==','
EWZg','XiorfMR7BA==','w4wup85','wqCnXfDjCkQ==','E8K0w52IwPcMq==','wzrDKM0taUFT','w0Fd180w70bW5DbmBacv8ODRCGLClFJc','Ys4w099W80TRhZTHGFCgsOfw4UI','QcOpbMK4','
w4RtKw4XwzdmQ==','wKcGGA==','w6vCncK7wHDncR0w5vclMK8wpjJw7DnMoc','wq7woh','wzrDKM0taUFTB8KlqBdvCv09w6AcwpU','w4DCuV4tw8u','IUTCiQM=','w4zc0Yo','w0LDi80ow60W','
wqzCgPBdIA==','bkDchXoR','w4zc0Ys','w1gUw8=','w4NDM04W==','wqbdJTDpQ==','w6vDu0vDmA==','w0ndQXTDv==','c8RkywoJc','NkDcXkI','w4rDmyTDmw==','w5DC18Rj','CsKvMYtC','
bMKH0wIeq==','w7bDlCRAW6fDu0h','w6HduDTmg==','IMRBw6w=','wz7Dum8=','w4fCso06wQ4BCTCvKQwondQ==','wph/wpAvf10=','w73DjYpDlG==','w5PCmncDmsKSDg==','wpp7wo8zbQ==','w4owupg9BwQ=','
ZeRywoB2w0E','w5XDU14=','dMRWtw==','Ej7Ck80Bw70c','WMow080=','M3cD20s','UcR0SMRTw6X','d8RwMKR2wz0G','w68qwp8=','wqsCpYcnwq4=','
JavaScript file length: 1142,306 lines: 1,171 Ln: 1,129 Col: 1,254 Sel: 8,1 Unix (LF) UTF-8 INS
```

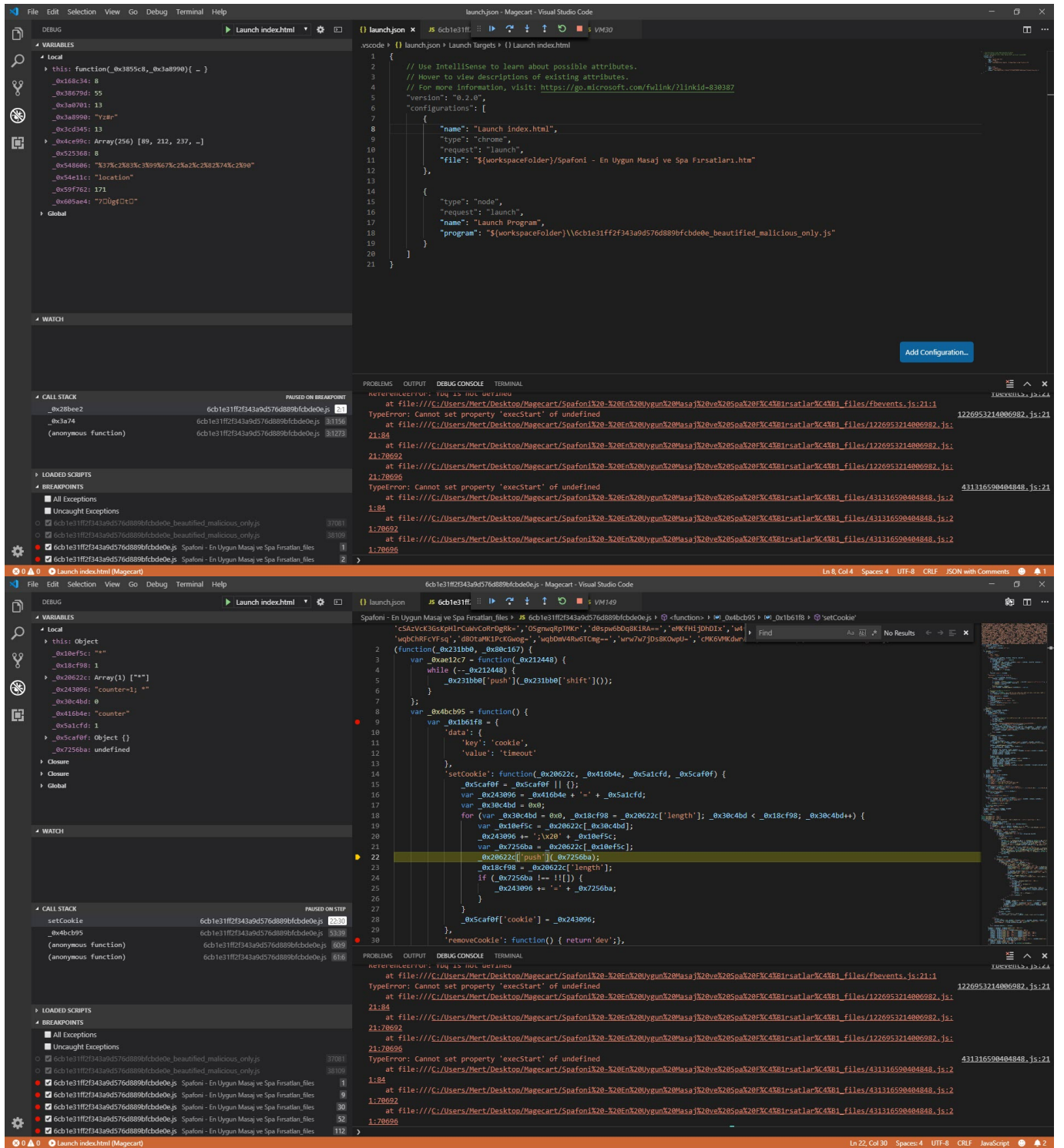
İlk iş olarak JavaScript Beautifier web sitesinden faydalanarak zararlı kod bloğunu okunaklı hale getirdim. Ardından kodu anlaşılır hale getirmek için

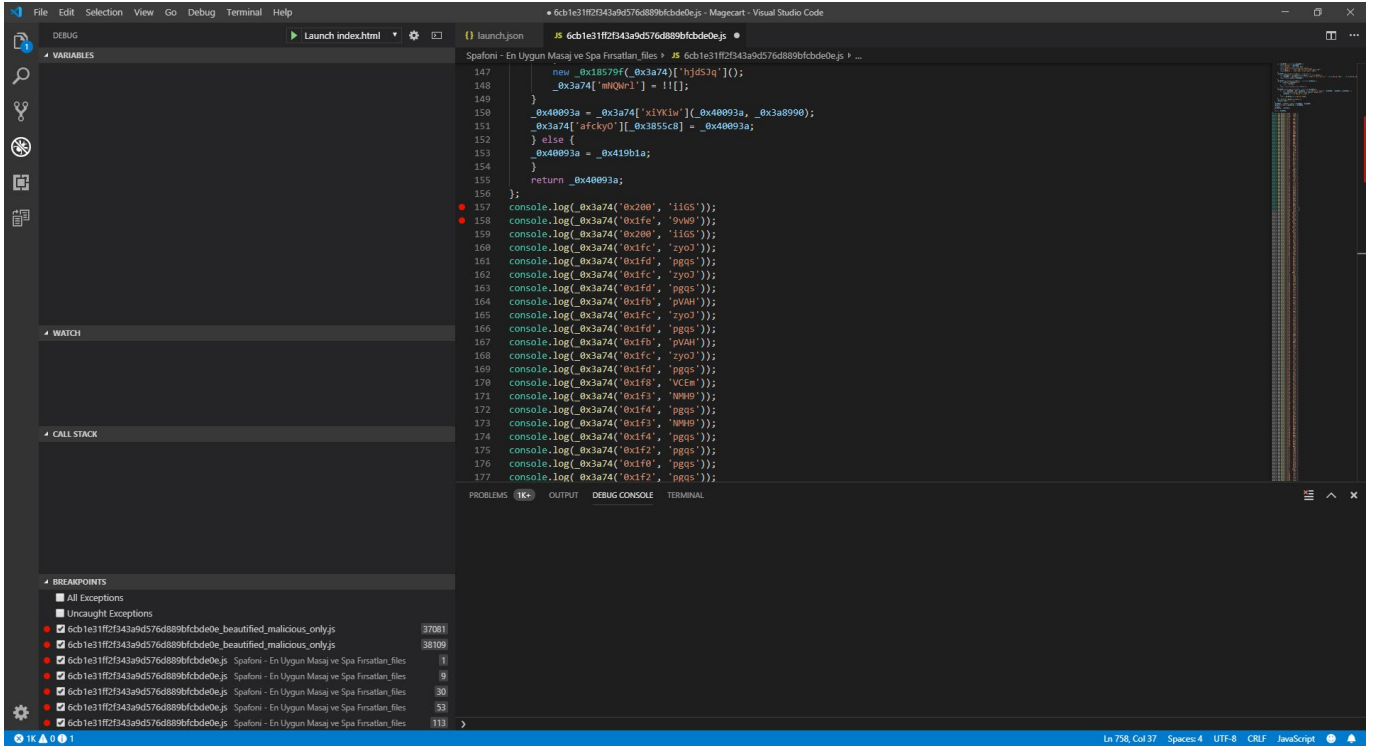
sırasıyla de4js ve IlluminateJs araçlarından faydalanmaya çalıştım ancak başarısız oldum. Chrome DevTools ile zararlı JavaScript kodunu hata ayıklaması (debugging) yaparak analiz etmeye başladım ve çok geçmeden bir zaman sonra işlerin yolunda gitmediğini farkettim. Chrome'dan kaynaklanan bir problem olabileceğini düşünerek şansımı Firefox ile denemeye karar verdim fakat o da birşeylerin yolunda gitmediğine dair uyarı verdi.



Ne yapabileceğime dair hindi gibi düşünüp dururken internet tarayıcısı yerine farklı bir araç ile hata ayıklaması yapabilmek için araştırma yapmaya

başladım ve Visual Studio Code isimli kaynak kodu editörü ile karşılaştım. Chrome hata ayıklama eklentisi sayesinde arka planda HTML, JavaScript kodu analiz etmeye imkan tanıyan ve çok sayıda eklentiye sahip olan bu editör ile hata ayıklaması yapmaya başladığımda, SetCookie ile ilişkili fonksiyonun çok sayıda dizi (Array) oluşturarak bellekteki kullanılabilecek alanları tüketerek hata ayıklamasını etkisiz hale getirdiğini (self defending) gördüm.





Analiz ederken bir yerde Regex ile removeCookie değerinde { işareti ile return kelimesi arasında boşluk kontrolü yapıldığını farkettim. Boşluk karakterinin tespit edilmesi durumunda kodun akışı yukarıda bahsettiğim çok sayıda dizi oluşturup probleme yol açan fonksiyona ilerliyordu. Peki art niyetli geliştirici neden böyle bir kontrol koymuştu ? Bu gibi karmaşılaştırılmış, okunaklı olmayan kodlarla karşılaşan analistlerin ilk yaptığı iş, kodu araçlar (JavaScript Beautifier gibi) yardımıyla okunaklı, formata uygun bir hale getirmek olduğu için bu araçlar otomatik olarak araya boşluk koyuyorlardı ve bu da kodun analiz edildiğine dair art niyetli kişilere güzel bir tespit mekanizması oluşturmaya imkan tanıyordu.

RegExr: Learn, Build, & Test Regi...

https://regex.com

Hack 4 Career, Infor...

LinkedIn

Mert SARICA (merts...

Inbox - merts.sarica...

Untitled Pattern

Save (ctrl+s)

New

Menu

Pattern Settings

My Patterns

Cheatsheet

RegEx Reference

Community Patterns

Help

RegExr is an online tool to **learn, build, & test** Regular Expressions (RegEx / RegExp).

- Supports **JavaScript & PHP/PCRE** RegEx.
- Results update in **real-time** as you type.
- Roll over** a match or expression for details.
- Save** & share expressions with others.
- Use **Tools** to explore your results.
- Full **RegEx Reference** with help & examples.
- Undo** & **Redo** with ctrl+Z / Y in editors.
- Search for & rate **Community Patterns**.

Students and Teachers, save up to 60% on Adobe Creative Cloud.

ADD VIA CARRDS

Expression

JavaScript

Flags

/^\w+.*\(\)\s*(\w+.*["'].*["'];?+)\$/g

Text

No match (0.4ms)

RegExr was created by gskinner.com, and is proudly hosted by Media Temple.

Edit the Expression & Text to see matches. Roll over matches or the expression for details. PCRE & Javascript flavors of RegEx are supported.

The sidebar includes a Cheatsheet, full Reference, and Help. You can also Save & Share with the Community, and view patterns you create or favorite in My Patterns.

Explore results with the Tools below. Replace & List output custom results. Details lists capture groups. Explain describes your expression in plain English.

Tools

Replace

List

Details

Explain

Roll-over elements below to highlight in the Expression above. Click to open in Reference.

"

Character. Matches a "" character (char code 34).

\w

Word. Matches any word character (alphanumeric & underscore).

+

Quantifier. Match 1 or more of the preceding token.

Character. Matches a SPACE character (char code 32).

*

Quantifier. Match 0 or more of the preceding token.

\(

Escaped character. Matches a "(" character (char code 40).

\)

Escaped character. Matches a ")" character (char code 41).

regularexpressions

@regex101

donate

contact

bug reports & feedback

wiki

SAVE & SHARE

Save Regex

ctrl+s

FLAVOR

PCRE (PHP)

ECMAScript (JavaScript)

Python

Golang

TOOLS

Code Generator

Regex Debugger

REGULAR EXPRESSION

no match, 92 steps (~1ms)

/^\w+.*\(\)\s*(\w+.*["'].*["'];?+)\$/gm

TEST STRING

SWITCH TO UNIT TESTS

function(){ return 'dev';}

SUBSTITUTION

EXPLANATION

/

line

^

\w

+

.

*

\(

\)

\s

*

(

\w

+

.

*

"

'

.

*

"

'

;

?

+

\$

/

gm

^

Matches any word character (equal to [a-zA-Z0-9_]).

Quantifier — Matches between one and unlimited times, as many times as possible, giving back as needed (greedy)

.

Matches the character . literally (case sensitive)

Quantifier — Matches between zero and unlimited times, as many times as possible, giving back as needed (greedy)

\(

Matches the character (literally (case sensitive)

\)

Matches the character) literally (case sensitive)

\s

Matches the character \s literally (case sensitive)

Quantifier — Matches between zero and unlimited times, as many times as possible, giving back as needed (greedy)

(

Matches the character (literally (case sensitive)

\w

Matches the character \w literally (case sensitive)

+

Matches the character + literally (case sensitive)

.

Matches the character . literally (case sensitive)

*

Matches the character * literally (case sensitive)

"

Matches the character " literally (case sensitive)

'

Matches the character ' literally (case sensitive)

.

Matches the character . literally (case sensitive)

*

Matches the character * literally (case sensitive)

"

Matches the character " literally (case sensitive)

'

Matches the character ' literally (case sensitive)

;

Matches the character ; literally (case sensitive)

?

Matches the character ? literally (case sensitive)

+

Matches the character + literally (case sensitive)

\$

Matches the character \$ literally (case sensitive)

MATCH INFORMATION

Your regular expression does not match the subject string.

QUICK REFERENCE

Search reference

All Tokens

Common Tokens

General Tokens

anchors

Meta Sequences

Quantifiers

Group Constructs

Character Ranges

A single character of: a, b or c

[abc]

A character except: a, b or c

[^abc]

A character in the range: a-z

[a-z]

A character not in the range: a-z

[^a-z]

A character in the range: a-z or A-Z

[a-zA-Z]

Any single character

.

Any whitespace character

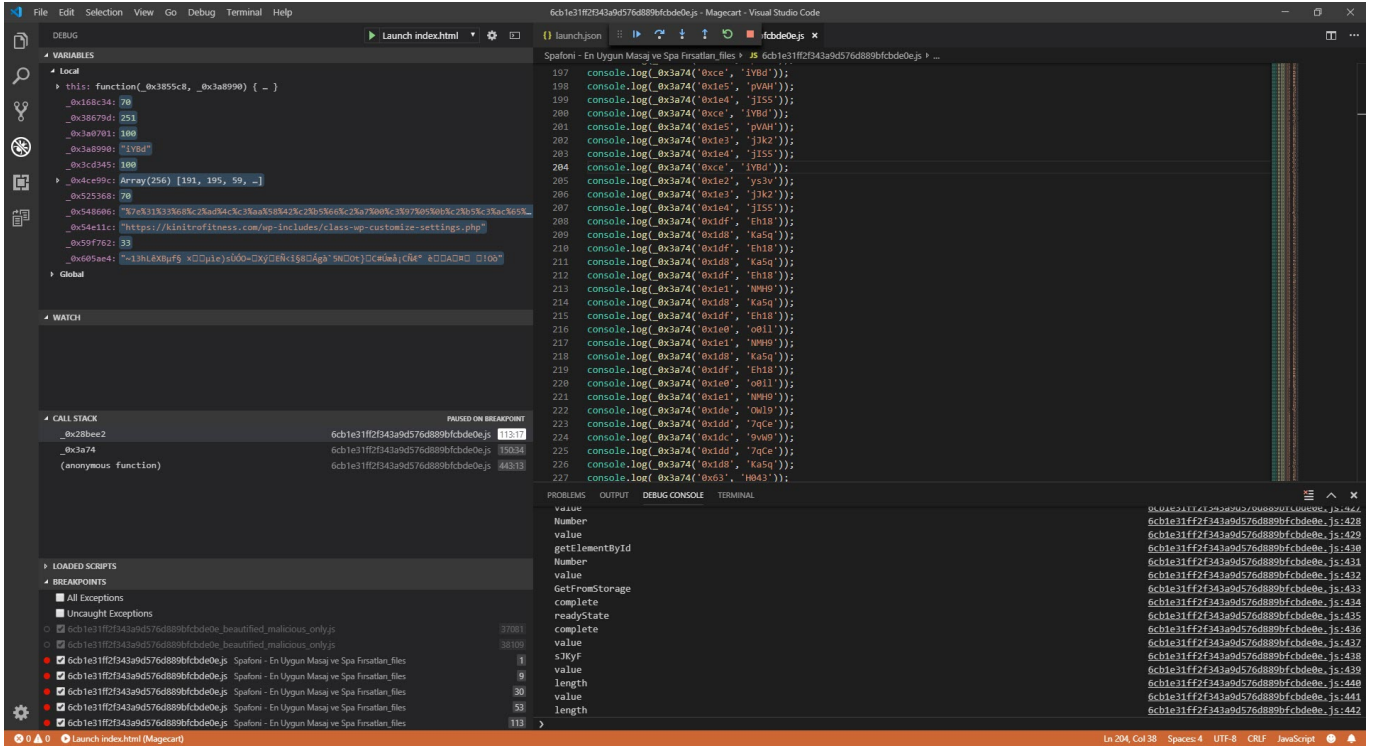
\s

Any non-whitespace character

\S

Any digit

\d



Ülke olarak COVID-19 salgınını geride bırakacağımız sağlıklı günlerde yeni bir yazı ile tekrar görüşmek dileğiyle herkese sağlıklı ve güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediyem Var #17 oyununun çözüm yolunu da içermektedir.