

JBU CTF

picoCTF writeup

발 표 자 허 송 이



CONTENTS

01

Insp3ct0r

02

dont-use
-client-side

03

logon

04

Open-to
-admins

05

Client-side-again



Insp3ct0r - Points: 50 - (Solves: 31702)

Web Exploitation - Solved

Solve

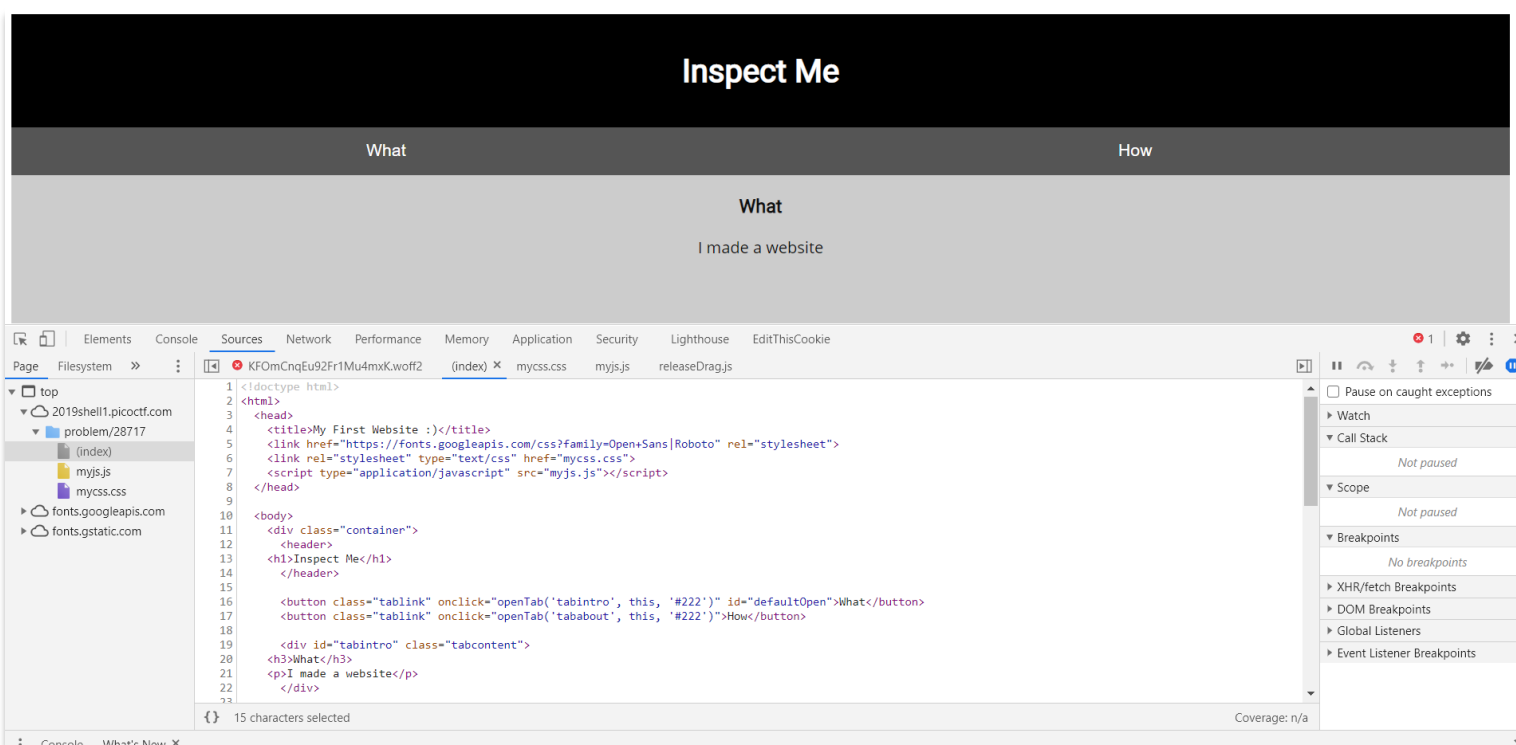
Hints

Kishor Balan tipped us off that the following code may need inspection: <https://2019shell1.picoctf.com/problem/28717/>
(link) or <http://2019shell1.picoctf.com:28717>

Submit!

picoCTF{FLAG}





개발자 도구 여는 법: F12

```
(index) x mycss.css myjs.js
18
19     <div id="tabintro" class="tabcontent">
20     <h3>What</h3>
21     <p>I made a website</p>
22     </div>
23
24     <div id="tababout" class="tabcontent">
25     <h3>How</h3>
26     <p>I used these to make this site: <br/>
27         HTML <br/>
28         CSS <br/>
29         JS (JavaScript)
30     </p>
31     <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
32     </div>
33
34     </div>
35
36 </body>
37 </html>
38
```

01

```
(index)  mycss.css  myjs.js x
1  function openTab(tabName,elmnt,color) {
2      var i, tabcontent, tablinks;
3      tabcontent = document.getElementsByClassName("tabcontent");
4      for (i = 0; i < tabcontent.length; i++) {
5          tabcontent[i].style.display = "none";
6      }
7      tablinks = document.getElementsByClassName("tablink");
8      for (i = 0; i < tablinks.length; i++) {
9          tablinks[i].style.backgroundColor = "";
10     }
11     document.getElementById(tabName).style.display = "block";
12     if(elmnt.style != null) {
13         elmnt.style.backgroundColor = color;
14     }
15 }
16
17 window.onload = function() {
18     openTab('tabintro', this, '#222');
19 }
20
21 /* Javascript sure is neat. Anyways part 3/3 of the flag: Lucky?2717d7be */
22
```



```
(index) mycss.css x myjs.js
33 font-size: 17px,
34 width: 50%;
35 }
36
37 .tablink:hover {
38   background-color: #777;
39 }
40
41 .tabcontent {
42   color: #111;
43   display: none;
44   padding: 50px;
45   text-align: center;
46 }
47
48 #tabintro { background-color: #ccc; }
49 #tababout { background-color: #ccc; }
50
51 /* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```

picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?2717d7be}

dont-use-client-side - Points: 100 - (Solves: 25278)

Web Exploitation - Solved

Solve

Hints

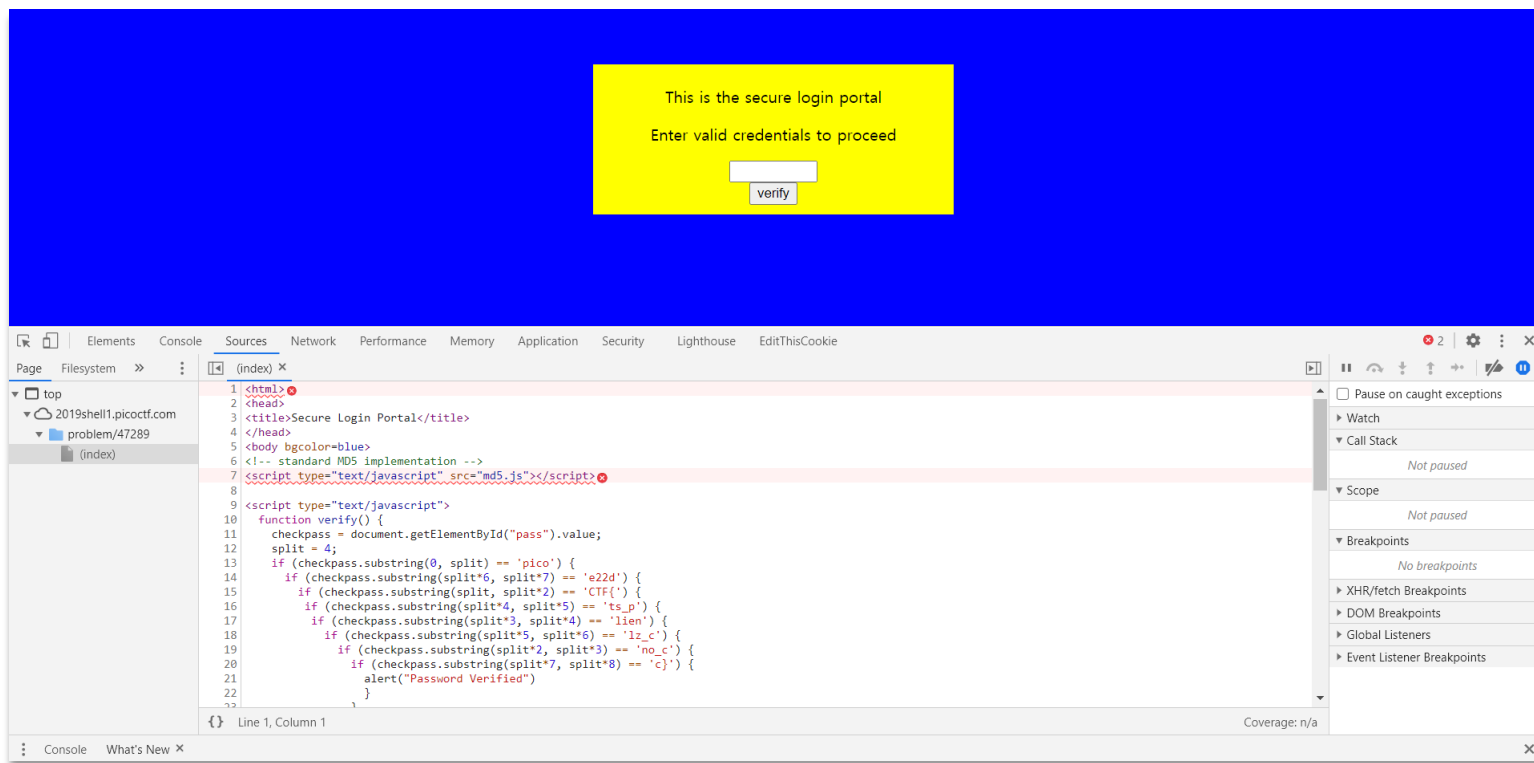
Can you break into this super secure portal? <https://2019shell1.picoctf.com/problem/47289/> (link) or
<http://2019shell1.picoctf.com:47289>

Submit!

picoCTF{FLAG}



02



02

```
(index) x
1 <html>✖
2 <head>
3 <title>Secure Login Portal</title>
4 </head>
5 <body bgcolor=blue>
6 <!-- standard MD5 implementation -->
7 <script type="text/javascript" src="md5.js"></script>
8
9 <script type="text/javascript">
10     function verify() {
11         checkpass = document.getElementById("pass").value;
12         split = 4;
13         if (checkpass.substring(0, split) == 'pico') {
14             if (checkpass.substring(split*6, split*7) == 'e22d') {
15                 if (checkpass.substring(split, split*2) == 'CTF{') {
16                     if (checkpass.substring(split*4, split*5) == 'ts_p') {
17                         if (checkpass.substring(split*3, split*4) == 'lien') {
18                             if (checkpass.substring(split*5, split*6) == 'lz_c') {
19                                 if (checkpass.substring(split*2, split*3) == 'no_c') {
20                                     if (checkpass.substring(split*7, split*8) == 'c}') {
21                                         alert("Password Verified")
22                                     }
23                                 }
24                             }
25                         }
26                     }
27                 }
28             }
29         }
30     }
31     else {
32         alert("Incorrect password");
33     }
34 }
```

The diagram illustrates the client-side security concept. It shows a web browser window displaying a login portal. The HTML code for the page is shown, including a JavaScript function named `verify()` that checks the password. The JavaScript code is then shown in a separate window, highlighting the `onclick="verify()"` attribute on the submit button. The diagram shows how the JavaScript code is embedded in the HTML and how the HTML is rendered in the browser.

Web Page (index.html):

```
1 <html>
2 <head>
3 <title>Secure Login Portal</title>
4 </head>
5 <body bgcolor=blue>
6 <!-- standard MD5 implementation -->
7 <script type="text/javascript" src="md5.js"></script>
8
9 <script type="text/javascript">
10 function verify() {
11   checkpass = document.getElementById("pass").value;
12   split = 4;
13   if (checkpass.length < split) {
14     if (checkpass.length < 4) {
15       if (checkpass.length < 2) {
16         if (checkpass.length < 1) {
17           alert("Incorrect password");
18         }
19       }
20     }
21   }
22 }
23
24 </script>
25
26 <div>
27   <p>Enter valid credentials to proceed</p>
28   <form action="index.html" method="post">
29     <input type="password" id="pass" size="8" />
30     <br/>
31     <input type="submit" value="verify" onclick="verify()" />
32   </form>
33 </div>
34 </body>
35 </html>
```

JavaScript Code (md5.js):

```
1 function md5(str) {
2   var i, len, h0, h1, h2, h3, h4, h5, h6, h7, h8, h9,
3       A, B, C, D, E, F, G, H, T1, T2, T3, T4, T5, T6, T7, T8,
4       T9, TA, TB, TC, TD, TE, TF, TG, TH, TI, TJ, TK, TL, TM,
5       TN, TO, TP, TP, TT, TV, TW, TX, TY, TZ, UA, UB, UC,
6       UD, UE, UF, UG, UH, UI, UJ, UK, UL, UM, UN, UO, UP,
7       UQ, UR, US, UT, UV, UW, UX, UY, UZ, V0, V1, V2, V3,
8       V4, V5, V6, V7, V8, V9, VA, VB, VC, VD, VE, VF, VG,
9       VH, VI, VJ, VK, VL, VM, VN, VO, VP, VQ, VR, VS, VT,
10      VW, VX, VY, VZ, W0, W1, W2, W3, W4, W5, W6, W7, W8,
11      W9, WA, WB, WC, WD, WE, WF, WG, WH, WI, WJ, WK, WL,
12      WM, WN, WO, WP, WQ, WR, WS, WT, WV, WW, WX, WY, WZ,
13      X0, X1, X2, X3, X4, X5, X6, X7, X8, X9, XA, XB, XC,
14      XD, XE, XF, XG, XH, XI, XJ, XK, XL, XM, XN, XO, XP,
15      XQ, XR, XS, XT, XV, XW, XX, XY, XZ, Y0, Y1, Y2, Y3,
16      Y4, Y5, Y6, Y7, Y8, Y9, YA, YB, YC, YD, YE, YF, YG,
17      YH, YI, YJ, YK, YL, YM, YN, YO, YP, YQ, YR, YS, YT,
18      YV, YW, YX, YY, YZ, Z0, Z1, Z2, Z3, Z4, Z5, Z6, Z7,
19      Z8, Z9, ZA, ZB, ZC, ZD, ZE, ZF, ZG, ZH, ZI, ZJ, ZK,
20      ZL, ZM, ZN, ZO, ZP, ZQ, ZR, ZS, ZT, ZV, ZW, ZX, ZY,
21      ZZ, AA, AB, AC, AD, AE, AF, AG, AH, AI, AJ, AK, AL,
22      AM, AN, AO, AP, AQ, AR, AS, AT, AV, AW, AX, AY, AZ,
23      BA, BB, BC, BD, BE, BF, BG, BH, BI, BJ, BK, BL, BM,
24      BN, BO, BP, BQ, BR, BS, BT, BV, BW, BX, BY, BZ, CA,
25      CB, CC, CD, CE, CF, CG, CH, CI, CJ, CK, CL, CM, CN,
26      CO, CP, CQ, CR, CS, CT, CV, CW, CX, CY, CZ, DA, DB,
27      DC, DD, DE, DF, DG, DH, DI, DJ, DK, DL, DM, DN, DO,
28      DP, DQ, DR, DS, DT, DV, DW, DX, DY, DZ, EA, EB, EC,
29      ED, EE, EF, EG, EH, EI, EJ, EK, EL, EM, EN, EO, EP,
30      EQ, ER, ES, ET, EV, EW, EX, EY, EZ, FA, FB, FC, FD,
31      FE, FF, FG, FH, FI, FJ, FK, FL, FM, FN, FO, FP, FQ,
32      FR, FS, FT, FV, FW, FX, FY, FZ, GA, GB, GC, GD, GE,
33      GF, GG, GH, GI, GJ, GK, GL, GM, GN, GO, GP, GQ, GR,
34      GS, GT, GV, GW, GX, GY, GZ, HA, HB, HC, HD, HE, HF,
35      HG, HH, HI, HJ, HK, HL, HM, HN, HO, HP, HQ, HR, HS,
36      HT, HV, HW, HX, HY, HZ, IA, IB, IC, ID, IE, IF, IG,
37      IH, II, IJ, IK, IL, IM, IN, IO, IP, IQ, IR, IS, IT,
38      IV, IW, IX, IY, IZ, JA, JB, JC, JD, JE, JF, JG, JH,
39      JI, JJ, JK, JL, JM, JN, JO, JP, JQ, JR, JS, JT, JV,
40      JW, JX, JY, JZ, KA, KB, KC, KD, KE, KF, KG, KH, KI,
41      KJ, KK, KL, KM, KN, KO, KP, KQ, KR, KS, KT, KV, KW,
42      KX, KY, KZ, LA, LB, LC, LD, LE, LF, LG, LH, LI, LJ,
43      LK, LL, LM, LN, LO, LP, LQ, LR, LS, LT, LV, LW, LX,
44      LY, LZ, MA, MB, MC, MD, ME, MF, MG, MH, MI, MJ, MK,
45      ML, MN, MO, MP, MQ, MR, MS, MT, MV, MW, MX, MY, MZ,
46      NA, NB, NC, ND, NE, NF, NG, NH, NI, NJ, NK, NL, NM,
47      NO, NP, NQ, NR, NS, NT, NV, NW, NX, NY, NZ, OA, OB,
48      OC, OD, OE, OF, OG, OH, OI, OJ, OK, OL, OM, ON, OO,
49      OP, OQ, OR, OS, OT, OV, OW, OX, OY, OZ, PA, PB, PC,
50      PD, PE, PF, PG, PH, PI, PJ, PK, PL, PM, PN, PO, PP,
51      PQ, PR, PS, PT, PV, PW, PX, PY, PZ, QA, QB, QC, QD,
52      QE, QF, QG, QH, QI, QJ, QK, QL, QM, QN, QO, QP, QQ,
53      QR, QS, QT, QV, QW, QX, QY, QZ, RA, RB, RC, RD, RE,
54      RF, RG, RH, RI, RJ, RK, RL, RM, RN, RO, RP, RQ, RR,
55      RS, RT, RV, RW, RX, RY, RZ, SA, SB, SC, SD, SE, SF,
56      SG, SH, SI, SJ, SK, SL, SM, SN, SO, SP, SQ, SR, SS,
57      ST, SV, SW, SX, SY, SZ, TA, TB, TC, TD, TE, TF, TG,
58      TH, TI, TJ, TK, TL, TM, TN, TO, TP, TQ, TR, TS, TV,
59      TW, TX, TY, TZ, UA, UB, UC, UD, UE, UF, UG, UH, UI,
60      UJ, UK, UL, UM, UN, UO, UP, UQ, UR, US, UT, UV, UW,
61      UX, UY, UZ, V0, V1, V2, V3, V4, V5, V6, V7, V8, V9,
62      VA, VB, VC, VD, VE, VF, VG, VH, VI, VJ, VK, VL, VM,
63      VN, VO, VP, VQ, VR, VS, VT, VW, VX, VY, VZ, W0, W1,
64      W2, W3, W4, W5, W6, W7, W8, W9, WA, WB, WC, WD, WE,
65      WF, WG, WH, WI, WJ, WK, WL, WM, WN, WO, WP, WQ, WR,
66      WS, WT, WV, WW, WX, WY, WZ, X0, X1, X2, X3, X4, X5,
67      X6, X7, X8, X9, XA, XB, XC, XD, XE, XF, XG, XH, XI,
68      XJ, XK, XL, XM, XN, XO, XP, XQ, XR, XS, XT, XV, XW,
69      XX, XY, XZ, Y0, Y1, Y2, Y3, Y4, Y5, Y6, Y7, Y8, Y9,
70      YA, YB, YC, YD, YE, YF, YG, YH, YI, YJ, YK, YL, YM,
71      YN, YO, YP, YQ, YR, YS, YT, YV, YW, YX, YY, YZ, Z0,
72      Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, ZA, ZB, ZC, ZD,
73      ZE, ZF, ZG, ZH, ZI, ZJ, ZK, ZL, ZM, ZN, ZO, ZP, ZQ,
74      ZR, ZS, ZT, ZV, ZW, ZX, ZY, ZZ, AA, AB, AC, AD, AE,
75      AF, AG, AH, AI, AJ, AK, AL, AM, AN, AO, AP, AQ, AR, AS,
76      AT, AV, AW, AX, AY, AZ, BA, BB, BC, BD, BE, BF, BG, BH,
77      BI, BJ, BK, BL, BM, BN, BO, BP, BQ, BR, BS, BT, BV, BW,
78      BX, BY, BZ, CA, CB, CC, CD, CE, CF, CG, CH, CI, CJ, CK,
79      CL, CM, CN, CO, CP, CQ, CR, CS, CT, CV, CW, CX, CY, CZ,
80      DA, DB, DC, DD, DE, DF, DG, DH, DI, DJ, DK, DL, DM, DN,
81      DO, DP, DQ, DR, DS, DT, DV, DW, DX, DY, DZ, EA, EB, EC,
82      ED, EE, EF, EG, EH, EI, EJ, EK, EL, EM, EN, EO, EP, EQ,
83      ER, ES, ET, EV, EW, EX, EY, EZ, FA, FB, FC, FD, FE, FF,
84      FG, FH, FI, FJ, FK, FL, FM, FN, FO, FP, FQ, FR, FS, FT,
85      FV, FW, FX, FY, FZ, GA, GB, GC, GD, GE, GF, GG, GH, GI,
86      GJ, GK, GL, GM, GN, GO, GP, GQ, GR, GS, GT, GV, GW, GX,
87      GY, GZ, HA, HB, HC, HD, HE, HF, HG, HH, HI, HJ, HK, HL,
88      HM, HN, HO, HP, HQ, HR, HS, HT, HV, HW, HX, HY, HZ, IA,
89      IB, IC, ID, IE, IF, IG, IH, II, IJ, IK, IL, IM, IN, IO, IP,
90      IQ, IR, IS, IT, IV, IW, IX, IY, IZ, JA, JB, JC, JD, JE, JF,
91      JG, JH, JI, JJ, JK, JL, JM, JN, JO, JP, JQ, JR, JS, JT, JV,
92      JW, JX, JY, JZ, KA, KB, KC, KD, KE, KF, KG, KH, KI, KJ,
93      KK, KL, KM, KN, KO, KP, KQ, KR, KS, KT, KV, KW, KX, KY,
94      KZ, LA, LB, LC, LD, LE, LF, LG, LH, LI, LJ, LK, LL, LM,
95      LN, LO, LP, LQ, LR, LS, LT, LV, LW, LX, LY, LZ, MA, MB,
96      MC, MD, ME, MF, MG, MH, MI, MJ, MK, ML, MN, MO, MP, MQ,
97      MR, MS, MT, MV, MW, MX, MY, MZ, NA, NB, NC, ND, NE, NF,
98      NG, NH, NI, NJ, NK, NL, NM, NO, NP, NQ, NR, NS, NT, NV,
99      NW, NX, NY, NZ, OA, OB, OC, OD, OE, OF, OG, OH, OI, OJ,
100     OK, OL, OM, ON, OO, OP, OQ, OR, OS, OT, OV, OW, OX, OY,
101     OZ, PA, PB, PC, PD, PE, PF, PG, PH, PI, PJ, PK, PL, PM,
102     PN, PO, PP, PQ, PR, PS, PT, PV, PW, PX, PY, PZ, QA, QB,
103     QC, QD, QE, QF, QG, QH, QI, QJ, QK, QL, QM, QN, QO, QP,
104     QQ, QR, QS, QT, QV, QW, QX, QY, QZ, RA, RB, RC, RD, RE,
105     RF, RG, RH, RI, RJ, RK, RL, RM, RN, RO, RP, RQ, RR, RS,
106     RT, RV, RW, RX, RY, RZ, SA, SB, SC, SD, SE, SF, SG, SH,
107     SI, SJ, SK, SL, SM, SN, SO, SP, SQ, SR, SS, ST, SV, SW,
108     SX, SY, SZ, TA, TB, TC, TD, TE, TF, TG, TH, TI, TJ, TK,
109     TL, TM, TN, TO, TP, TQ, TR, TS, TV, TW, TX, TY, TZ, UA,
110     UB, UC, UD, UE, UF, UG, UH, UI, UJ, UK, UL, UM, UN, UO,
111     UP, UQ, UR, US, UT, UV, UW, UX, UY, UZ, V0, V1, V2, V3,
112     V4, V5, V6, V7, V8, V9, VA, VB, VC, VD, VE, VF, VG, VH,
113     VI, VJ, VK, VL, VM, VN, VO, VP, VQ, VR, VS, VT, VW, VX,
114     VY, VZ, W0, W1, W2, W3, W4, W5, W6, W7, W8, W9, WA, WB,
115     WC, WD, WE, WF, WG, WH, WI, WJ, WK, WL, WM, WN, WO, WP,
116     WQ, WR, WS, WT, WV, WW, WX, WY, WZ, X0, X1, X2, X3, X4,
117     X5, X6, X7, X8, X9, XA, XB, XC, XD, XE, XF, XG, XH, XI,
118     XJ, XK, XL, XM, XN, XO, XP, XQ, XR, XS, XT, XV, XW, XX,
119     XY, XZ, Y0, Y1, Y2, Y3, Y4, Y5, Y6, Y7, Y8, Y9, YA, YB,
120     YC, YD, YE, YF, YG, YH, YI, YJ, YK, YL, YM, YN, YO, YP,
121     YQ, YR, YS, YT, YV, YW, YX, YY, YZ, Z0, Z1, Z2, Z3, Z4,
122     Z5, Z6, Z7, Z8, Z9, ZA, ZB, ZC, ZD, ZE, ZF, ZG, ZH, ZI,
123     ZJ, ZK, ZL, ZM, ZN, ZO, ZP, ZQ, ZR, ZS, ZT, ZV, ZW, ZX,
124     ZY, ZZ, AA, AB, AC, AD, AE, AF, AG, AH, AI, AJ, AK, AL, AM,
125     AN, AO, AP, AQ, AR, AS, AT, AV, AW, AX, AY, AZ, BA, BB, BC,
126     BD, BE, BF, BG, BH, BI, BJ, BK, BL, BM, BN, BO, BP, BQ, BR,
127     BS, BT, BV, BW, BX, BY, BZ, CA, CB, CC, CD, CE, CF, CG, CH,
128     CI, CJ, CK, CL, CM, CN, CO, CP, CQ, CR, CS, CT, CV, CW, CX,
129     CY, CZ, DA, DB, DC, DD, DE, DF, DG, DH, DI, DJ, DK, DL, DM,
130     DN, DO, DP, DQ, DR, DS, DT, DV, DW, DX, DY, DZ, EA, EB, EC,
131     ED, EE, EF, EG, EH, EI, EJ, EK, EL, EM, EN, EO, EP, EQ, ER,
132     ES, ET, EV, EW, EX, EY, EZ, FA, FB, FC, FD, FE, FF, FG, FH,
133     FI, FJ, FK, FL, FM, FN, FO, FP, FQ, FR, FS, FT, FV, FW, FX,
134     FY, FZ, GA, GB, GC, GD, GE, GF, GG, GH, GI, GJ, GK, GL, GM,
135     GN, GO, GP, GQ, GR, GS, GT, GV, GW, GX, GY, GZ, HA, HB, HC,
136     HD, HE, HF, HG, HH, HI, HJ, HK, HL, HM, HN, HO, HP, HQ, HR,
137     HS, HT, HV, HW, HX, HY, HZ, IA, IB, IC, ID, IE, IF, IG, IH,
138     II, IJ, IK, IL, IM, IN, IO, IP, IQ, IR, IS, IT, IV, IW, IX,
139     IY, IZ, JA, JB, JC, JD, JE, JF, JG, JH, JI, JJ, JK, JL, JM,
140     JN, JO, JP, JQ, JR, JS, JT, JV, JW, JX, JY, JZ, KA, KB, KC,
141     KD, KE, KF, KG, KH, KI, KJ, KK, KL, KM, KN, KO, KP, KQ, KR,
142     KS, KT, KV, KW, KX, KY, KZ, LA, LB, LC, LD, LE, LF, LG, LH,
143     LI, LJ, LK, LL, LM, LN, LO, LP, LQ, LR, LS, LT, LV, LW, LX,
144     LY, LZ, MA, MB, MC, MD, ME, MF, MG, MH, MI, MJ, MK, ML, MN,
145     MO, MP, MQ, MR, MS, MT, MV, MW, MX, MY, MZ, NA, NB, NC, ND,
146     NE, NF, NG, NH, NI, NJ, NK, NL, NM, NO, NP, NQ, NR, NS, NT,
147     NV, NW, NX, NY, NZ, OA, OB, OC, OD, OE, OF, OG, OH, OI, OJ,
148     OK, OL, OM, ON, OO, OP, OQ, OR, OS, OT, OV, OW, OX, OY, OZ,
149     PA, PB, PC, PD, PE, PF, PG, PH, PI, PJ, PK, PL, PM, PN, PO,
150     PP, PQ, PR, PS, PT, PV, PW, PX, PY, PZ, QA, QB, QC, QD, QE,
151     QF, QG, QH, QI, QJ, QK, QL, QM, QN, QO, QP, QQ, QR, QS, QT,
152     QV, QW, QX, QY, QZ, RA, RB, RC, RD, RE, RF, RG, RH, RI, RJ,
153     RK, RL, RM, RN, RO, RP, RQ, RR, RS, RT, RV, RW, RX, RY, RZ,
154     SA, SB, SC, SD, SE, SF, SG, SH, SI, SJ, SK, SL, SM, SN, SO,
155     SP, SQ, SR, SS, ST, SV, SW, SX, SY, SZ, TA, TB, TC, TD, TE,
156     TF, TG, TH, TI, TJ, TK, TL, TM, TN, TO, TP, TQ, TR, TS, TV,
157     TW, TX, TY, TZ, UA, UB, UC, UD, UE, UF, UG, UH, UI, UJ, UK,
158     UL, UM, UN, UO, UP, UQ, UR, US, UT, UV, UW, UX, UY, UZ, V0,
159     V1, V2, V3, V4, V5, V6, V7, V8, V9, VA, VB, VC, VD, VE, VF,
160     VG, VH, VI, VJ, VK, VL, VM, VN, VO, VP, VQ, VR, VS, VT, VW,
161     VX, VY, VZ, W0, W1, W2, W3, W4, W5, W6, W7, W8, W9, WA,
162     WB, WC, WD, WE, WF, WG, WH, WI, WJ, WK, WL, WM, WN, WO, WP,
163     WQ, WR, WS, WT, WV, WW, WX, WY, WZ, X0, X1, X2, X3, X4, X5,
164     X6, X7, X8, X9, XA, XB, XC, XD, XE, XF, XG, XH, XI, XJ, XK,
165     XL, XM, XN, XO, XP, XQ, XR, XS, XT, XV, XW, XX, XY, XZ, Y0,
166     Y1, Y2, Y3, Y4, Y5, Y6, Y7, Y8, Y9, YA, YB, YC, YD, YE, YF,
167     YG, YH, YI, YJ, YK, YL, YM, YN, YO, YP, YQ, YR, YS, YT, YV,
168     YW, YX, YY, YZ, Z0, Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, ZA,
169     ZB, ZC, ZD, ZE, ZF, ZG, ZH, ZI, ZJ, ZK, ZL, ZM, ZN, ZO, ZP,
170     ZQ, ZR, ZS, ZT, ZV, ZW, ZX, ZY, ZZ, AA, AB, AC, AD, AE, AF,
171     AG, AH, AI, AJ, AK, AL, AM, AN, AO, AP, AQ, AR, AS, AT, AV,
172     AW, AX, AY, AZ, BA, BB, BC, BD, BE, BF, BG, BH, BI, BJ, BK,
173     BL, BM, BN, BO, BP, BQ, BR, BS, BT, BV, BW, BX, BY, BZ, CA,
174     CB, CC, CD, CE, CF, CG, CH, CI, CJ, CK, CL, CM, CN, CO, CP,
175     CQ, CR, CS, CT, CV, CW, CX, CY, CZ, DA, DB, DC, DD, DE, DF,
176     DG, DH, DI, DJ, DK, DL, DM, DN, DO, DP, DQ, DR, DS, DT, DV,
177     DW, DX, DY, DZ, EA, EB, EC, ED, EE, EF, EG, EH, EI, EJ, EK,
178     EL, EM, EN, EO, EP, EQ, ER, ES, ET, EV, EW, EX, EY, EZ, FA,
179     FB, FC, FD, FE, FF, FG, FH, FI, FJ, FK, FL, FM, FN, FO, FP,
180     FQ, FR, FS, FT, FV, FW, FX, FY, FZ, GA, GB, GC, GD, GE, GF,
181     GG, GH, GI, GJ, GK, GL, GM, GN, GO, GP, GQ, GR, GS, GT, GV,
182     GW, GX, GY, GZ, HA, HB, HC, HD, HE, HF, HG, HH, HI, HJ, HK,
183     HL, HM, HN, HO, HP, HQ, HR, HS, HT, HV, HW, HX, HY, HZ, IA,
184     IB, IC, ID, IE, IF, IG, IH, II, IJ, IK, IL, IM, IN, IO, IP, IQ,
185     IR, IS, IT, IV, IW, IX, IY, IZ, JA, JB, JC, JD, JE, JF, JG,
186     JH, JI, JJ, JK, JL, JM, JN, JO, JP, JQ, JR, JS, JT, JV, JW,
187     JX, JY, JZ, KA, KB, KC, KD, KE, KF, KG, KH, KI, KJ, KK, KL,
188     KM, KN, KO, KP, KQ, KR, KS, KT, KV, KW, KX, KY, KZ, LA, LB,
189     LC, LD, LE, LF, LG, LH, LI, LJ, LK, LL, LM, LN, LO, LP, LQ,
190     LR, LS, LT, LV, LW, LX, LY, LZ, MA, MB, MC, MD, ME, MF, MG,
191     MH, MI, MJ, MK, ML, MN, MO, MP, MQ, MR, MS, MT, MV, MW, MX,
192     MY, MZ, NA, NB, NC, ND, NE, NF, NG, NH, NI, NJ, NK, NL, NM,
193     NO, NP, NQ, NR, NS, NT, NV, NW, NX, NY, NZ, OA, OB, OC, OD,
194     OE, OF, OG, OH, OI, OJ, OK, OL, OM, ON, OO, OP, OQ, OR, OS,
195     OT, OV, OW, OX, OY, OZ, PA, PB, PC, PD, PE, PF, PG, PH, PI,
196     PJ, PK, PL, PM, PN, PO, PP, PQ, PR, PS, PT, PV, PW, PX, PY,
197     PZ, QA, QB, QC, QD, QE, QF, QG, QH, QI, QJ, QK, QL, QM, QN,
198     QO, QP, QQ, QR, QS, QT, QV, QW, QX, QY, QZ, RA, RB, RC, RD,
199     RE, RF, RG, RH, RI, RJ, RK, RL, RM, RN, RO, RP, RQ, RR, RS,
200     RT, RV, RW, RX, RY, RZ, SA, SB, SC, SD, SE, SF, SG, SH, SI,
201     SJ, SK, SL, SM, SN, SO, SP, SQ, SR, SS, ST, SV, SW, SX, SY,
202     SZ, TA, TB, TC, TD, TE, TF, TG, TH, TI, TJ, TK, TL, TM, TN,
203     TO, TP, TQ, TR, TS, TV, TW, TX, TY, TZ, UA, UB, UC, UD, UE,
204     UF, UG, UH, UI, UJ, UK, UL, UM, UN, UO, UP, UQ, UR, US, UT,
205     UV, UW, UX, UY, UZ, V0, V1, V2, V3, V4, V5, V6, V7, V8, V9,
206     VA, VB, VC, VD, VE, VF, VG, VH, VI, VJ, VK, VL, VM, VN, VO,
207     VP, VQ, VR, VS, VT, VW, VX, VY, VZ, W0, W1, W2, W3, W4, W5,
208     W6, W7, W8, W9, WA, WB, WC, WD, WE, WF, WG, WH, WI, WJ, WK,
209     WL, WM, WN, WO, WP, WQ, WR, WS, WT, WV, WW, WX, WY, WZ, X0,
210     X1, X2, X3, X4, X5, X6, X7, X8, X9, XA, XB, XC, XD, XE, XF,
211     XG, XH, XI, XJ, XK, XL, XM, XN, XO, XP, XQ, XR, XS, XT, XV,
212     XW, XX, XY, XZ, Y0, Y1, Y2, Y3, Y4, Y5, Y6, Y7, Y8, Y9, YA,
213     YB, YC, YD, YE, YF, YG, YH, YI, YJ, YK, YL, YM, YN, YO, YP,
214     YQ, YR, YS, YT, YV, YW, YX, YY, YZ, Z0, Z1, Z2, Z3, Z4, Z5,
215     Z6, Z7, Z8, Z9, ZA, ZB, ZC, ZD, ZE, ZF, ZG, ZH, ZI, ZJ, ZK,
216     ZL, ZM, ZN, ZO, ZP, ZQ, ZR, ZS, ZT, ZV, ZW, ZX, ZY, ZZ, AA,
217     AB, AC, AD, AE, AF, AG, AH, AI, AJ, AK, AL, AM, AN, AO, AP,
218     AQ, AR, AS, AT, AV, AW, AX, AY, AZ, BA, BB, BC, BD, BE, BF,
219     BG, BH, BI, BJ, BK, BL, BM, BN, BO, BP, BQ, BR, BS, BT, BV,
220     BW, BX, BY, BZ, CA, CB, CC, CD, CE, CF, CG, CH, CI, CJ, CK,
221     CL, CM, CN, CO, CP, CQ, CR, CS, CT, CV, CW, CX, CY, CZ, DA,
222     DB, DC, DD, DE, DF, DG, DH, DI, DJ, DK, DL, DM, DN, DO, DP,
223     DQ, DR, DS, DT, DV, DW, DX, DY, DZ, EA, EB, EC, ED, EE, EF,
224     EG, EH, EI, EJ, EK, EL, EM, EN, EO, EP, EQ, ER, ES, ET, EV,
225     EW, EX, EY, EZ, FA, FB, FC, FD, FE, FF, FG, FH, FI, FJ, FK,
226     FL, FM, FN, FO, FP, FQ, FR, FS, FT, FV, FW, FX, FY, FZ, GA,
227     GB, GC, GD, GE, GF, GG, GH, GI, GJ, GK, GL, GM, GN, GO, GP,
228     GQ, GR, GS, GT, GV, GW, GX, GY, GZ, HA, HB, HC, HD, HE, HF,
229     HG, HH, HI, HJ, HK, HL, HM, HN, HO, HP, HQ, HR, HS, HT, HV,
230     HW, HX, HY, HZ, IA, IB, IC, ID, IE, IF, IG, IH, II, IJ, IK,
231     IL, IM, IN, IO, IP, IQ, IR, IS, IT, IV, IW, IX, IY, IZ, JA,
232     JB, JC, JD, JE, JF, JG, JH, JI, JJ, JK, JL, JM, JN, JO, JP,
233     JQ, JR, JS, JT, JV, JW, JX, JY, JZ, KA, KB, KC, KD, KE, KF,
234     KG, KH, KI, KJ, KK, KL, KM, KN, KO, KP, KQ, KR, KS, KT, KV,
235     KW, KX, KY, KZ, LA, LB, LC, LD, LE, LF, LG, LH, LI, LJ, LK,
236     LL, LM, LN, LO, LP, LQ, LR, LS, LT, LV, LW, LX, LY, LZ, MA,
237     MB, MC, MD, ME, MF, MG, MH, MI, MJ, MK, ML, MN, MO, MP, MQ,
238     MR, MS, MT, MV, MW, MX, MY, MZ, NA, NB, NC, ND, NE, NF, NG,
239     NH, NI, NJ, NK, NL, NM, NO, NP, NQ, NR, NS, NT, NV, NW, NX,
240     NY, NZ, OA, OB, OC, OD, OE, OF, OG, OH, OI, OJ, OK, OL, OM,
241     ON, OO, OP, OQ, OR, OS, OT, OV, OW, OX, OY, OZ, PA, PB, PC,
242     PD, PE, PF, PG, PH, PI, PJ, PK, PL, PM, PN, PO, PP, PQ, PR,
243     PS, PT, PV, PW, PX, PY, PZ, QA, QB, QC, QD, QE, QF, QG, QH,
244     QI, QJ, QK, QL, QM, QN, QO, QP, QQ, QR, QS, QT, QV, QW, QX,
245     QY, QZ, RA, RB, RC, RD, RE, RF, RG, RH, RI, RJ, RK, RL, RM,
246     RN, RO, RP, RQ, RR, RS, RT, RV, RW, RX, RY, RZ, SA, SB, SC,
247     SD, SE, SF, SG, SH, SI, SJ, SK, SL, SM, SN, SO, SP, SQ, SR,
248     SS, ST, SV, SW, SX, SY, SZ, TA, TB, TC, TD, TE, TF, TG, TH,
249     TI, TJ, TK, TL, TM, TN, TO, TP, TQ, TR, TS, TV, TW, TX, TY,
250     TZ, UA, UB, UC, UD, UE, UF, UG, UH, UI, UJ, UK, UL, UM, UN,
251     UO, UP, UQ, UR, US, UT, UV, UW, UX, UY, UZ, V0, V1, V2, V3,
252     V4, V5, V6, V7, V8, V9, VA, VB, VC, VD, VE, VF, VG, VH, VI,
253     VJ, VK, VL, VM, VN, VO, VP, VQ, VR, VS, VT, VW, VX, VY, VZ,
254     W0, W1, W2, W3, W4, W5, W6, W7, W8, W9, WA, WB, WC, WD, WE,
255     WF, WG, WH, WI, WJ, WK, WL, WM, WN, WO, WP, WQ, WR, WS, WT,
256     WV, WW, WX, WY, WZ, X0, X1, X2, X3, X4, X5, X6, X7, X8, X9,
257     XA, XB, XC, XD, XE, XF, XG, XH, XI, XJ, XK, XL, XM, XN, XO,
258     XP, XQ, XR, XS, XT, XV, XW, XX, XY, XZ, Y0, Y1, Y2, Y3, Y4,
259     Y5, Y6, Y7, Y8, Y9, YA, YB, YC, YD, YE, YF, YG, YH, YI, YJ,
260     YK, YL, YM, YN, YO, YP, YQ, YR, YS, YT, YV, YW, YX, YY, YZ,
261     Z0, Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, ZA, ZB, ZC, ZD, ZE,
262     ZF, ZG, ZH, ZI, ZJ, ZK, ZL, ZM, ZN, ZO, ZP, ZQ, ZR, ZS, ZT,
263     ZV, ZW, ZX, ZY, ZZ, AA, AB, AC, AD, AE, AF, AG, AH, AI, AJ,
264     AK, AL, AM, AN, AO, AP, AQ, AR, AS, AT, AV, AW, AX, AY, AZ, BA,
265     BB, BC, BD, BE, BF, BG, BH, BI, BJ, BK, BL, BM, BN, BO, BP, BQ,
266     BR, BS, BT, BV, BW, BX, BY, BZ, CA, CB, CC, CD, CE, CF, CG, CH,
267     CI, CJ, CK, CL, CM, CN, CO, CP, CQ, CR, CS, CT, CV, CW, CX, CY,
268     CZ, DA, DB, DC, DD, DE, DF, DG, DH, DI, DJ, DK, DL, DM, DN, DO,
269     DP, DQ, DR, DS, DT, DV, DW, DX, DY, DZ, EA, EB, EC, ED, EE, EF,
270     EG, EH, EI, EJ, EK, EL, EM, EN, EO, EP, EQ, ER, ES, ET, EV, EW,
271     EX, EY, EZ, FA, FB, FC, FD, FE, FF, FG, FH, FI, FJ, FK, FL, FM,
272     FN, FO, FP, FQ, FR, FS, FT, FV, FW, FX, FY, FZ, GA, GB, GC, GD,
273     GE, GF, GG, GH, GI, GJ, GK, GL, GM, GN, GO, GP, GQ, GR, GS, GT,
274     GV, GW, GX, GY, GZ, HA, HB, HC, HD, HE, HF, HG, HH, HI, HJ, HK,
275     HL, HM, HN, HO, HP, HQ, HR, HS, HT, HV, HW, HX, HY, HZ, IA, IB,
276     IC, ID, IE, IF, IG, IH, II, IJ, IK, IL, IM, IN, IO, IP, IQ, IR,
277     IS, IT, IV, IW, IX, IY, IZ, JA, JB, JC, JD, JE, JF, JG, JH, JI,
278     JJ, JK, JL, JM, JN, JO, JP, JQ, JR, JS, JT, JV, JW, JX, JY, JZ,
279     KA, KB, KC, KD, KE, KF, KG, KH, KI, KJ, KK, KL, KM, KN, KO, KP,
280     KQ, KR, KS, KT, KV, KW, KX, KY, KZ, LA, LB, LC, LD, LE, LF, LG,
281     LH, LI, LJ, LK, LL, LM, LN, LO, LP, LQ, LR, LS, LT, LV, LW, LX,
282     LY, LZ, MA, MB, MC, MD, ME, MF, MG, MH, MI, MJ, MK, ML, MN, MO,
283     MP, MQ, MR, MS, MT, MV, MW, MX, MY, MZ, NA, NB, NC, ND, NE, NF,
284     NG, NH, NI, NJ, NK, NL, NM, NO, NP, NQ, NR, NS, NT, NV, NW, NX,
285     NY, NZ, OA, OB, OC, OD, OE, OF, OG, OH, OI, OJ, OK, OL, OM, ON,
286     OO, OP, OQ, OR, OS, OT, OV, OW, OX, OY, OZ, PA, PB, PC, PD, PE,
287     PF, PG, PH, PI, PJ, PK, PL, PM, PN, PO, PP, PQ, PR, PS, PT, PV,
288     PW, PX, PY, PZ, QA, QB, QC, QD, QE, QF, QG, QH, QI, QJ, QK, QL,
289     QM, QN, QO, QP, QQ, QR, QS, QT, QV, QW, QX, QY, QZ, RA, RB, RC,
290     RD, RE, RF, RG, RH, RI, RJ, RK, RL, RM, RN, RO, RP, RQ, RR, RS,
291     RT, RV, RW, RX, RY, RZ, SA, SB, SC, SD, SE, SF, SG, SH, SI, SJ,
292     SK, SL, SM, SN, SO, SP, SQ, SR, SS, ST, SV, SW, SX, SY, SZ, TA,
293     TB, TC, TD, TE, TF, TG, TH, TI, TJ, TK, TL, TM, TN, TO, TP, TQ,
294     TR, TS, TV, TW, TX, TY, TZ, UA, UB, UC, UD, UE, UF, UG, UH, UI,
295     UJ, UK, UL, UM, UN, UO, UP, UQ, UR, US, UT, UV, UW, UX, UY, UZ,
296     V0, V1, V2, V3, V4, V5, V6, V7, V8, V9, VA, VB, VC, VD, VE, VF,
297     VG, VH, VI, VJ, VK, VL, VM, VN, VO, VP, VQ, VR, VS, VT, VW, VX,
298     VY, VZ, W0, W1, W2, W3, W4, W5, W6, W7, W8, W9, WA, WB, WC,
299     WD, WE, WF, WG, WH, WI, WJ, WK, WL, WM, WN, WO, WP, WQ, WR,
300     WS, WT, WV, WW, WX, WY, WZ, X0, X1, X2, X3, X4, X5, X6, X7,
301     X8, X9, XA, XB, XC, XD, XE, XF, XG, XH, XI, XJ, XK, XL, XM, XN,
302     XO, XP, XQ, XR, XS, XT, XV, XW, XX, XY, XZ, Y0, Y1, Y2, Y3, Y4,
303     Y5, Y6, Y7, Y8, Y9, YA, YB, YC, YD, YE, YF, YG, YH, YI, YJ,
304     YK, YL, YM, YN, YO, YP, YQ, YR, YS, YT, YV, YW, YX, YY, YZ, Z0,
305     Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, ZA, ZB, ZC, ZD, ZE, ZF, ZG,
306     ZH, ZI, ZJ, ZK, ZL, ZM, ZN, ZO, ZP, ZQ, ZR, ZS, ZT, ZV, ZW, ZX,
307     ZY, ZZ, AA, AB, AC, AD, AE, AF, AG, AH, AI, AJ, AK, AL, AM, AN,
308     AO, AP, AQ, AR, AS, AT, AV, AW, AX, AY, AZ, BA, BB, BC, BD, BE,
309     BF, BG, BH, BI, BJ, BK, BL, BM, BN, BO, BP, BQ, BR, BS, BT, BV,
310     BW, BX, BY, BZ, CA, CB, CC, CD, CE, CF, CG, CH, CI, CJ, CK, CL,
311     CM, CN, CO, CP, CQ, CR, CS, CT, CV, CW, CX, CY, CZ, DA, DB, DC,
312     DD, DE,
```



(index) X

```
1 <html>
```

(index) X

```
40 <p>Enter valid credentials to proceed</p>
41 <form action="index.html" method="post">
42 <input type="password" id="pass" size="8" />
43 <br/>

8
9 <script type="text/javascript">
10   function verify() {
11     checkpass = document.getElementById("pass").value;
12     split = 4;
13     if (checkpass.substring(0, split) == 'pico') {
14       if (checkpass.substring(split*6, split*7) == 'e22d') {
15         if (checkpass.substring(split, split*2) == 'CTF{') {
16           if (checkpass.substring(split*4, split*5) == 'ts_p') {
17             if (checkpass.substring(split*3, split*4) == 'lien') {
18               if (checkpass.substring(split*5, split*6) == 'lz_c') {
19                 if (checkpass.substring(split*2, split*3) == 'no_c') {
20                   if (checkpass.substring(split*7, split*8) == 'c') {
21                     alert("Password Verified")
22                   }
23                 }
24             }
25           }
26         }
27       }
28     }
29   }
30 }
```

입력값

Substring(시작 인덱스, 종료 인덱스)

: 시작 인덱스부터 종료 인덱스 전까지 문자열을 자른다.

02

Substring(시작 인덱스, 종료 인덱스)
: 시작 인덱스부터 종료 인덱스 전까지 문자열을 자른다.

This is the secure login portal
Enter valid credentials to proceed

verify

```
9 <script type="text/javascript">
10   function verify() {
11       checkpass = document.getElementById("pass").value;
12       split = 4;
13       if (checkpass.substring(0, split) == 'pico') {
14           if (checkpass.substring(split*6, split*7) == 'e22d') {
15               if (checkpass.substring(split, split*2) == 'CTF{') {
16                   if (checkpass.substring(split*4, split*5) == 'ts p') {
17                       if (checkpass.substring(split*3, split*4) == 'lien') {
18                           if (checkpass.substring(split*5, split*6) == 'lz c') {
19                               if (checkpass.substring(split*2, split*3) == 'no_c') {
20                                   if (checkpass.substring(split*7, split*8) == 'c}') {
21                                       alert("Password Verified")
22                                   }
23                               }
24                           }
25                       }
26                   }
27               }
28           }
29       }
```

→ 입력값

pico
CTF{
no_c
lien
ts_p
lz_c
e22d
c}

logon - Points: 100 - (Solves: 17486)

Web Exploitation - Solved

Solve

Hints

The factory is hiding things from all of its users. Can you login as logon and find what they've been looking at?

<https://2019shell1.picoctf.com/problem/45163/> (link) or <http://2019shell1.picoctf.com:45163>

Submit!

picoCTF{FLAG}



Factory Login

Home Sign Out

Username 1234

Password 1234

Sign In

The screenshot shows a web browser window with a login form titled "Factory Login". The form has two input fields: "Username" and "Password", both containing the text "1234". Below the inputs is a green "Sign In" button. In the top right corner, there are two links: "Home" and "Sign Out". The browser's developer tools are open, showing the "Sources" tab. The file "jquery.min.js" is selected, and the source code is visible. The code defines a "jumbotron" class and a "lead" class, and contains a "login-form" form with a "login" action. The form has two input fields: "user" (email) and "password". The "password" field is highlighted in the code. The browser's console and other developer tool panels are also visible.

```
36
37 <div class="jumbotron">
38   <p class="lead"></p>
39   <div class="login-form">
40     <form role="form" action="/login" method="post">
41       <div class="form-group">
42         <input type="text" name="user" id="email" class="form-control input-lg" placeholder="Username">
43       </div>
44       <div class="form-group">
45         <input type="password" name="password" id="password" class="form-control input-lg" placeholder="Password">
46       </div>
47     </form>
48     <div class="row">
49       <div class="col-xs-12 col-sm-12 col-md-12">
50         <input type="submit" class="btn btn-lg btn-success btn-block" value="Sign In">
51       </div>
52     </div>
53   </div>
54 </div>
```


Factory Login

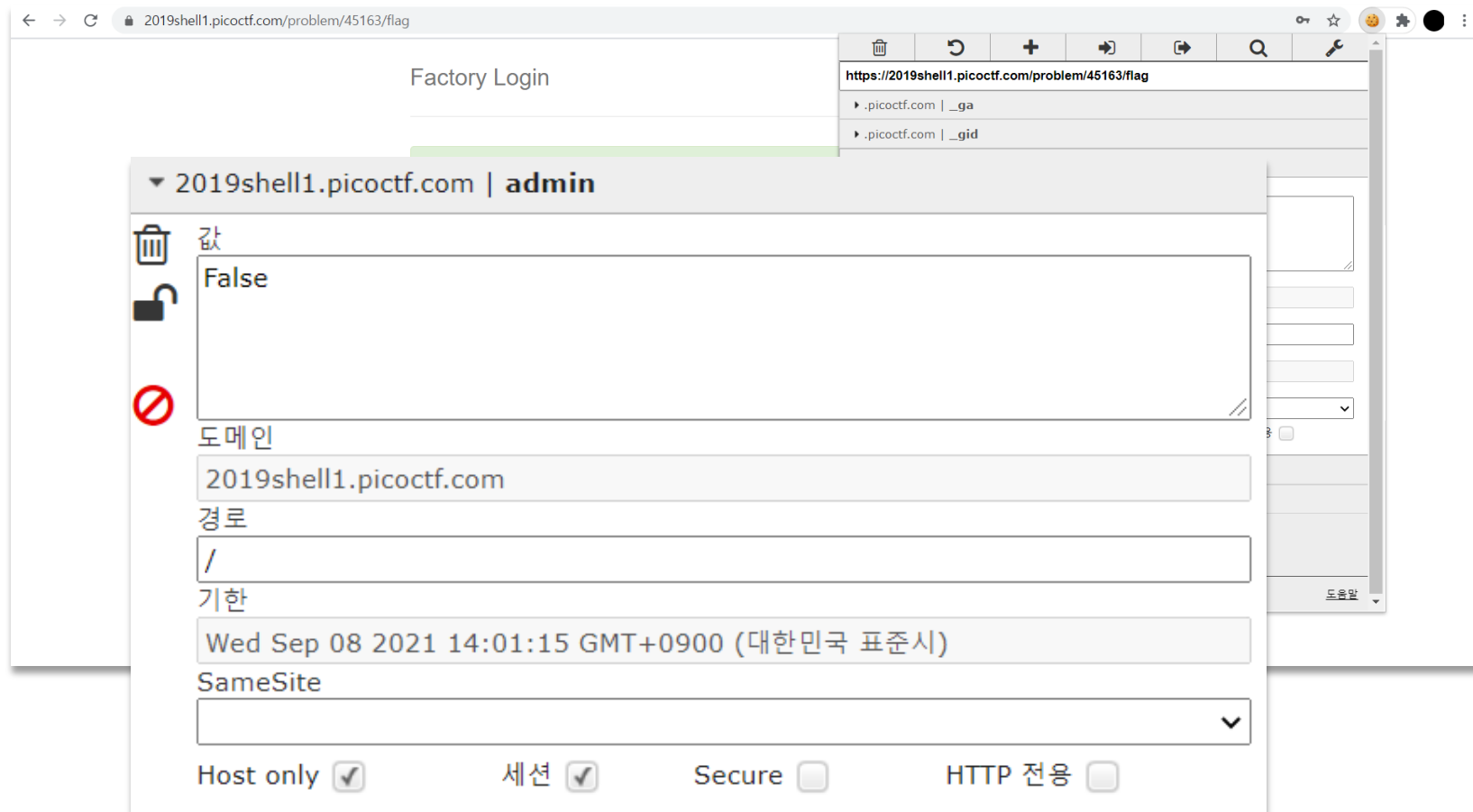
[Home](#)[Sign Out](#)

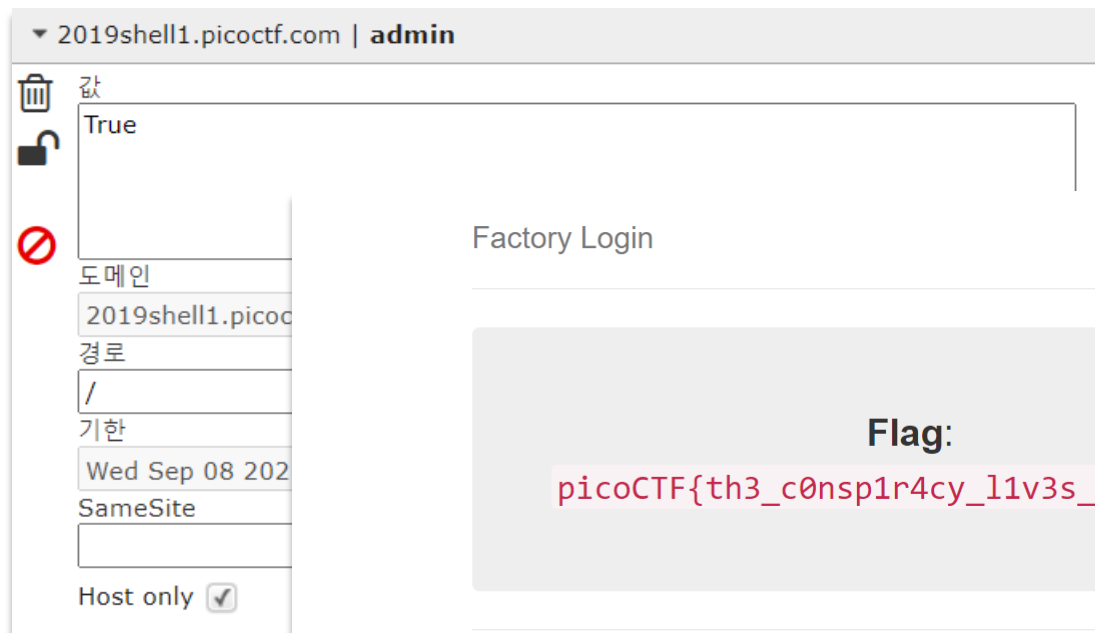
Success: You logged in! Not sure you'll be able to see the flag though.



No flag for you

© PicoCTF 2019





Open-to-admins - Points: 200 - (Solves: 10238)

Web Exploitation - Solved

Solve

Hints

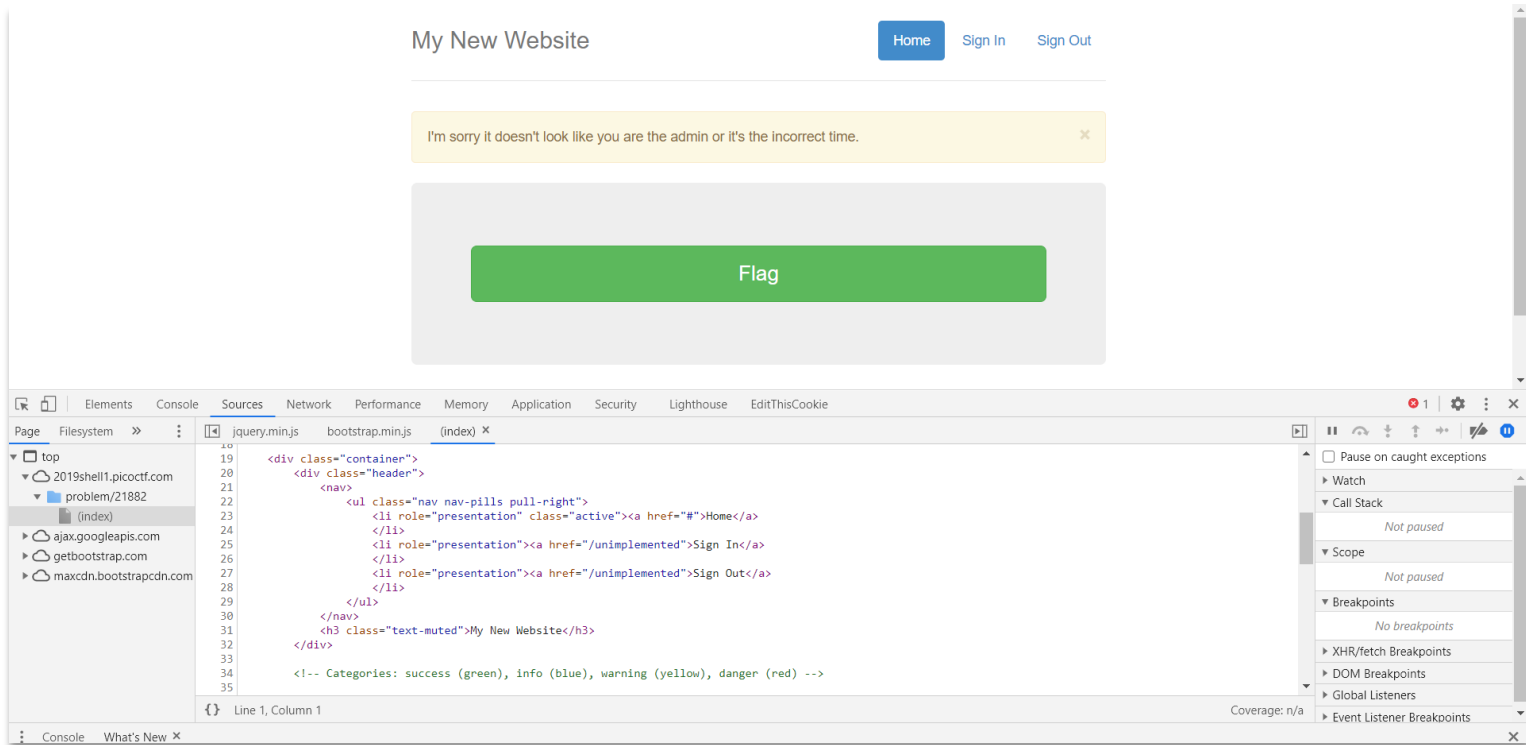
This secure website allows users to access the flag only if they are **admin** and if the **time** is exactly 1400.

<https://2019shell1.picoctf.com/problem/21882/> (link) or <http://2019shell1.picoctf.com:21882>

Submit!

picoCTF{FLAG}





04

| Name | Value |
|----------|----------------------------|
| _ga | GA1.2.632616608.1599509902 |
| _gid | GA1.2.514000781.1599509902 |
| admin | False |
| password | 1234 |
| username | 1234 |



| Name | Value |
|----------|----------------------------|
| _ga | GA1.2.632616608.1599509902 |
| _gid | GA1.2.514000781.1599509902 |
| admin | True |
| time | 1400 |
| username | 1234 |

My New Website

[Home](#)[Sign In](#)[Sign Out](#)

Flag: `picoCTF{0p3n_t0_adm1n5_b6ea8359}`

© PicoCTF 2019

Client-side-again - Points: 200 - (Solves: 13213)

Web Exploitation - Solved

Solve

Hints

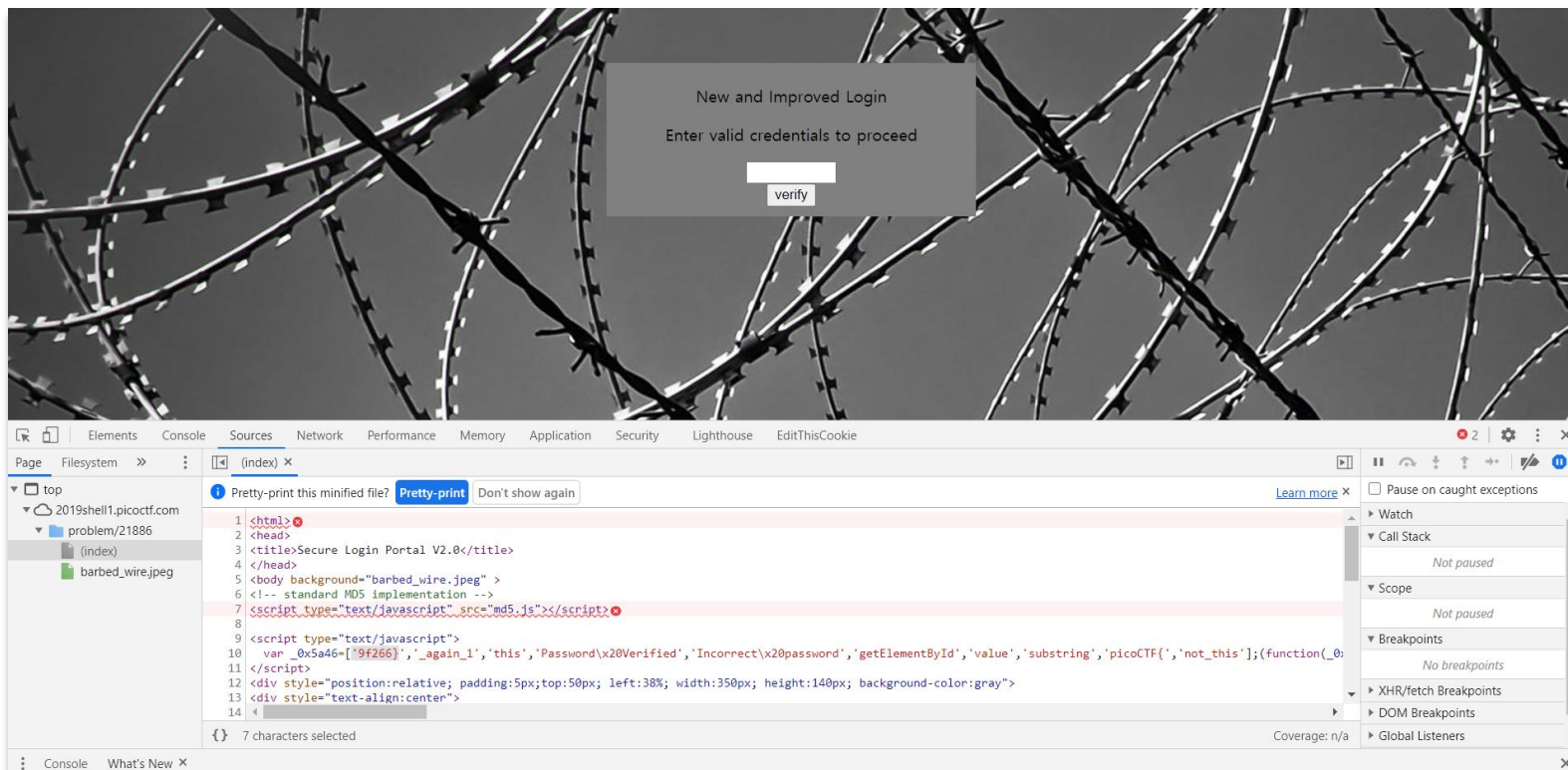
Can you break into this super secure portal? <https://2019shell1.picoctf.com/problem/21886/> (link) or
<http://2019shell1.picoctf.com:21886>

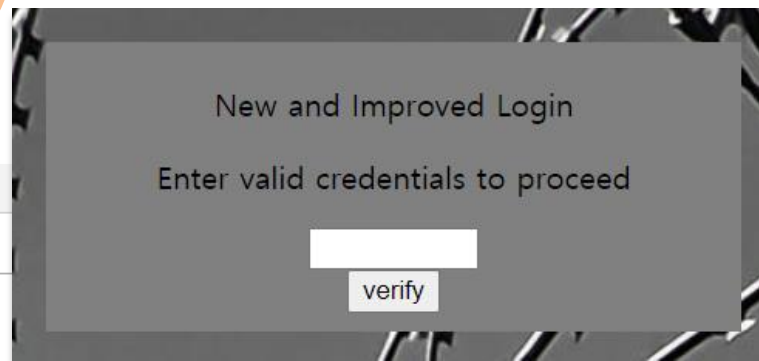
Submit!

picoCTF{FLAG}



05





```
(index) x
i Pretty-print this minified file? Pretty-print Don't show again
15
16 <p>Enter valid credentials to proceed</p>
17 <form action="index.html" method="post">
18 <input type="password" id="pass" size="8" />
19 <br/>
20 <input type="submit" value="verify" onclick="verify(); return false;" />
21 </form>
22 </div>
23 </div>
```

```
(index) x
i Pretty-print this minified file? Pretty-print Don't show again
1 <html>ⓧ
2 <head>
3 <title>Secure Login Portal V2.0</title>
4 </head>
5 <body background="barbed_wire.jpeg" >
6 <!-- standard MD5 implementation -->
7 <script type="text/javascript" src="md5.js"></script>ⓧ
8
9 <script type="text/javascript">
10   var _0x5a46=["9f266"],'_again_1','this','Password\x20Verified','Incorrect\x20password','getElementById','value','substring','picoCTF{','not_this'};(
11 </script>
12 <div style="position:relative; padding:5px;top:50px; left:38%; width:350px; height:140px; background-color:gray">
13 <div style="text-align:center">
14 <p>New and Improved Login</p>
15
16 <p>Enter valid credentials to proceed</p>
17 <form action="index.html" method="post">
18
```

7 characters selected

```
(index) :formatted x
8 <script type="text/javascript">
9   var _0x5a46 = ['9f266}', '_again_1', 'this', 'Password\x20Verified', 'Incorrect\x20password', 'getElementById', 'value', 'substring', 'picoCTF{', 'not_this'];
10   (function(_0x4bd822, _0x2bd6f7) {
11     var _0xb4bdb3 = function(_0x1d68f6) {
12       while (--_0x1d68f6) {
13         _0x4bd822['push'](_0x4bd822['shift']());
14       }
15     };
16     _0xb4bdb3(++_0x2bd6f7);
17   })(_0x5a46, 0x1b3));
18   var _0x4b5b = function(_0x2d8f05, _0x4b81bb) {
19     _0x2d8f05 = _0x2d8f05 - 0x0;
20     var _0x4d74cb = _0x5a46[_0x2d8f05];
21     return _0x4d74cb;
22   };
23   function verify() {
24     checkpass = document[_0x4b5b('0x0')]( 'pass' )[_0x4b5b('0x1')];
25     split = 0x4;
26     if (checkpass[_0x4b5b('0x2')](0x0, split * 0x2) == _0x4b5b('0x3')) {
27       if (checkpass[_0x4b5b('0x2')](0x7, 0x9) == '{n'} {
28         if (checkpass[_0x4b5b('0x2')](split * 0x2, split * 0x2 * 0x2) == _0x4b5b('0x4')) {
29           if (checkpass[_0x4b5b('0x2')](0x3, 0x6) == 'oCT') {
30             if (checkpass[_0x4b5b('0x2')](split * 0x3 * 0x2, split * 0x4 * 0x2) == _0x4b5b('0x5')) {
31               if (checkpass['substring'](0x6, 0xb) == 'F{not') {
32                 if (checkpass[_0x4b5b('0x2')](split * 0x2 * 0x2, split * 0x3 * 0x2) == _0x4b5b('0x6')) {
33                   if (checkpass[_0x4b5b('0x2')](0xc, 0x10) == _0x4b5b('0x7')) {
34                     alert(_0x4b5b('0x8'));
35                   }
36                 }
37               }
38             }
39           }
40         }
41       }
42     }
43   }
44 }
```

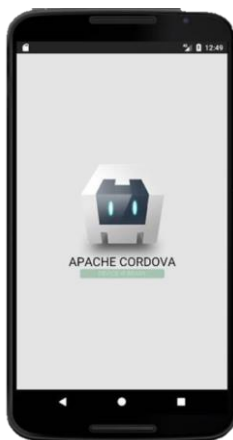
Line 9, Column 28

Coverage: n/a

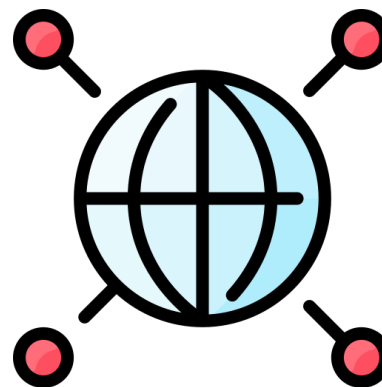
개발자 도구란?



Debugging



Emulator



**Network
analysis**

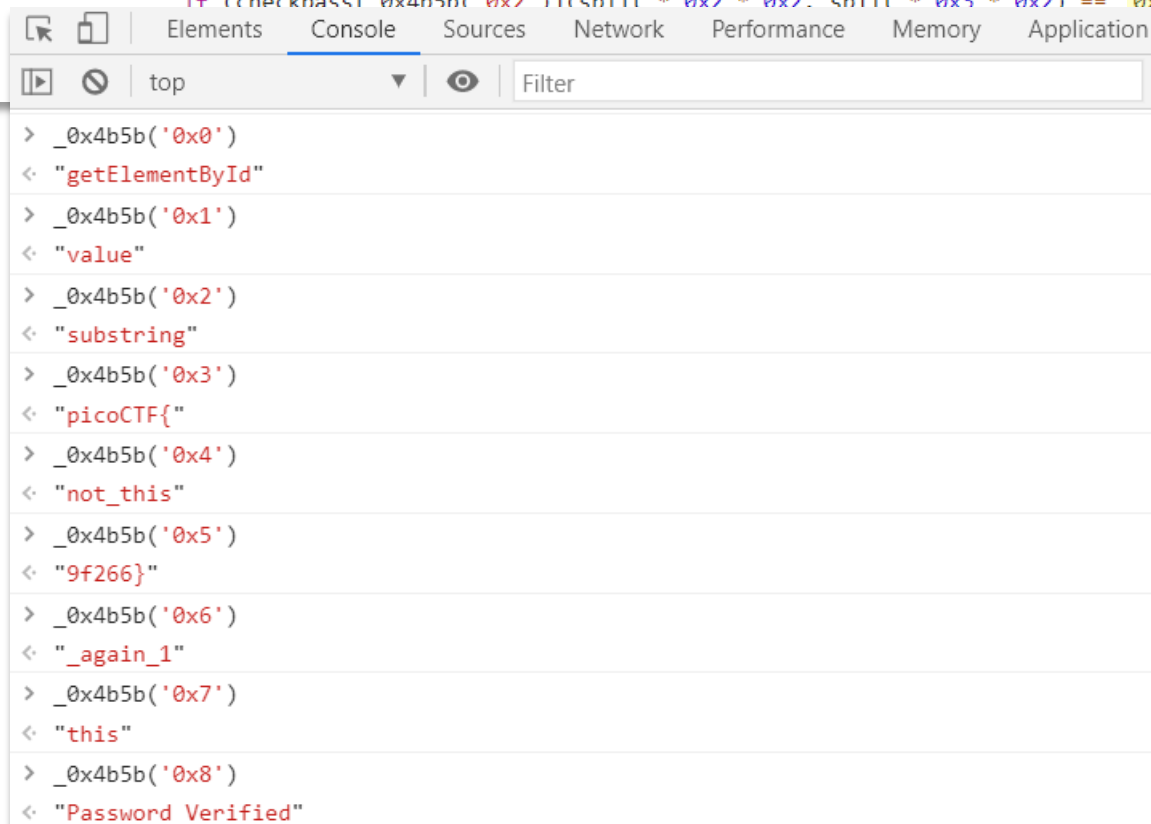
...

Console

스크립트 명령어를 입력하는 패널로,
break를 건 시점의 변수를 확인할 수 있고
값을 평가하거나 수정할 수 있다.

05

```
function verify() {  
  checkpass = document[_0x4b5b('0x0')]( 'pass' )[_0x4b5b('0x1')];  
  split = 0x4;  
  if (checkpass[_0x4b5b('0x2')](0x0, split * 0x2) == _0x4b5b('0x3')) {  
    if (checkpass[_0x4b5b('0x2')](0x7, 0x9) == '{n'} {  
      if (checkpass[_0x4b5b('0x2')](split * 0x2, split * 0x2 * 0x2) == _0x4b5b('0x4')) {  
        if (checkpass[_0x4b5b('0x2')](0x3, 0x6) == 'oCT') {  
          if (checkpass[_0x4b5b('0x2')](split * 0x3 * 0x2, split * 0x4 * 0x2) == _0x4b5b('0x5')) {  
            if (checkpass['substring'](0x6, 0xb) == 'F{not}') {  
              if (checkpass[_0x4b5b('0x2')](split * 0x2 * 0x2, split * 0x3 * 0x2) == _0x4b5b('0x6')) {
```



```
function verify(){
  checkpass=document['getElementById']('pass')['value'];
  split=0x4;
  if(checkpass['substring'](0x0,split*0x2)=='picoCTF'){
    if(checkpass['substring'](0x7,0x9)=='{n'){
      if(checkpass['substring'](split*0x2,split*0x2*0x2)=='not_this'){
        if(checkpass['substring'](0x3,0x6)=='oCT'){
          if(checkpass['substring'](split*0x3*0x2,split*0x4*0x2)=='9f266'){
            if(checkpass['substring'](0x6,0xb)=='F{not'){
              if(checkpass['substring'](split*0x2*0x2,split*0x3*0x2)=='_again_1'){
                if(checkpass['substring'](0xc,0x10)=='this'){
                  alert('Password Verified');
                }
              }
            }
          }
        }
      }
    }
  }
  else{
    alert('Incorrect password');
  }
}
```

```
function verify(){
  checkpass=document['getElementById']('pass')['value'];
  split=0x4;
  if(checkpass['substring'](0x0,split*0x2)=='picoCTF{'){
    if(checkpass['substring'](0x7,0x9)=='{n'){
      if(checkpass['substring'](split*0x2,split*0x2*0x2)=='not_this'){
        if(checkpass['substring'](0x3,0x6)=='oCT'){
          if(checkpass['substring'](split*0x3*0x2,split*0x4*0x2)=='9f266'){
            if(checkpass['substring'](0x6,0xb)=='F{not'){
              if(checkpass['substring'](split*0x2*0x2,split*0x3*0x2)=='_again_1'){
                if(checkpass['substring'](0xc,0x10)=='this'){
                  alert('Password Verified');
                }
              }
            }
          }
        }
      }
    }
  }
  else{
    alert('Incorrect password');
  }
}
```

picoCTF{ not_this _again_1 9f266}

<https://subicura.com/2018/02/14/javascript-debugging.html#%ED%81%AC%EB%A1%AC-%EA%B0%9C%EB%B0%9C%EC%9E%90-%EB%8F%84%EA%B5%AC-devtools>

1. 소스코드만 보면 풀 수 있는 문제

2. 소스코드 이해와 감이 필요한 문제

THANK
YOU

발 표 자 허 송 이