

Angstrom CTF 2021


Revex

- Chúng ta nhận được một dãy các **regex** pattern từ tác giả như sau:

```
^(?=.*re)(?=.*{21}[^_]{4}\}$)(?=.*{14}b[^_]{2})(?=.*{8}[C-L])(?=.*{8}[B-F])(?=.*{
```

- Để có thể solve tách từng pattern → mỗi pattern sẽ chứa một điều kiện. **FLAG** là chuỗi thỏa mãn tất cả các regex pattern này:

```
1  ^(?=.*re)
2  (?=.{21}[^_]{4}\}$)
3  (?=.{14}b[^_]{2})
4  (?=.{8}[C-L])
5  (?=.{8}[B-F])
6  (?=.{8}[^B-DF])
7  (?=.{7}G(?<pepega>...){7}t\k<pepega>)
8  (?=.*u[^z].$)
9  (?=.{11}(?<pepeega>[13])s.{2}(?! \k<pepeega>)[13]s)
10 (?=.*_{2}_)
11 (?=actf\{)
12 (?=.{21}[p-t])
13 (?=.*1.*3)
14 (?=.{20}(?=.*u)(?=.*y)(?=.*z)(?=.*q)(?=.*_))
15 (?=.*Ex)
```

 Để đơn giản, gọi tên các pattern bằng STT dòng như hiển thị ở trên, ngoài ra format mặc định của flag là **actf{some-strings}**

- Xét 3 pattern p(4), p(5) và p(6):
 - p(4) ký tự thứ 9 của chuỗi nằm trong đoạn C-L
 - p(5) ký tự thứ 9 của chuỗi nằm trong đoạn từ B-F
 - Suy ra: Ký tự nằm trong đoạn C-F (có 4 khả năng C, D, E, F), lại có p(6): ký tự thứ 9 khác {B, D, F}
 - Vậy ký tự thứ 9 là E**

- Theo như (7) thì ký tự thứ 8 là **G**, p(1) và p(15) nói rằng trong flag phải chứa "re" và "Ex"
 - Từ các dữ kiện trên, ta dự đoán từ đầu tiên sau chuỗi "**actf{**" là "**reGEx**"
- Cũng từ p(7):
 - 2 ký tự thuộc group được đặt tên *pepega* là "**Ex**", sau lần xuất hiện đầu tiên thì sau 7 ký tự tùy chọn và ký tự **t** thì Ex lại xuất hiện lần nữa, ta có:
 - **actf{reGEx * * * * * tEx...**
- Xét p(2): **21** ký tự đầu tiên + **4 ký tự cuối** (khác "_" + "}"), suy ra len(flag) là 26:

actf{reGEx * * * * * tEx***}**
 - pattern (14): **(?={20})(?=.u)(?=.y)(?=.z)(?=.q)(?=_)** - sau 20 ký tự thì 5 ký tự cuối(không tính "}") sẽ thuộc { u, y, z, q, _} nhưng vì 4 ký tự khác "_", **vì vậy nên ký tự 21 phải là "_"**
 - p(12): **(?={21}[p-t])** - suy ra **ký tự 22 phải là q**
 - p(8): **(?=.u[^z].\$)**: thì 3 ký tự cuối là "**u***", nhưng * khác z, suy ra * phải là y
 - suy ra: **actf{reGEx * * * * * tEx_qzuy}**
- Theo p(9), ký tự thứ 12 sẽ thuộc {1,3}sau đó là **s**, lại có p(13): **(?=.1.*3)** - ta sẽ có thứ tự xuất 1 đến 3, nên **ta suy đoán ký tự thứ 12 là "1", "1s"**, quá hợp lý luôn
 - Lại có p(10): **(?=_.{2}_)** → 2 ký tự nằm giữa 2 "_", có vẻ "**_1s_**" là hợp lí.
 - Và theo p(3): **(?={14}b[^_]{2})** ==> ký tự thứ 15 là "b". Lúc này ta có:
 - **actf{reGEx_1s_b * * tEx_qzuy}**
 - Theo p(9): thì ký tự 16 thuộc group **pepega={1, 3}**, nhưng khác lần xuất hiện đầu tiên => "**3**", sau đó là **s**

Flag: **actf{reGEx_1s_b3stEx_qzuy}**