Tharani Maaneeivaannan
2575198

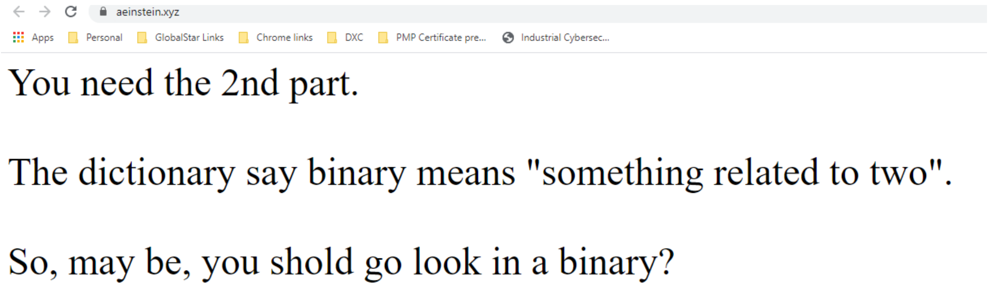
Question-1

Flag Captured: **4621_ctf{not_a11_sh4rks_mak3_y0u_cry_s0me_l3t_y0u_spy}**

Opened the dump.pcapng file in wireshark. Used Find a packet option in Wireshark and searched for the text 'ctf' because we know that the flag format is 4621_ctf. Using this option I found the packet 9745 in which the first part of the flag is found 1 of 2: 4621_ctf{not_a11_sh4rks_mak3_y0u_

To find the second part of the flag. I further investigated the packet 9745. This packet seems to be a response sent by the url http://aeinstein.xyz

The website showed this message,

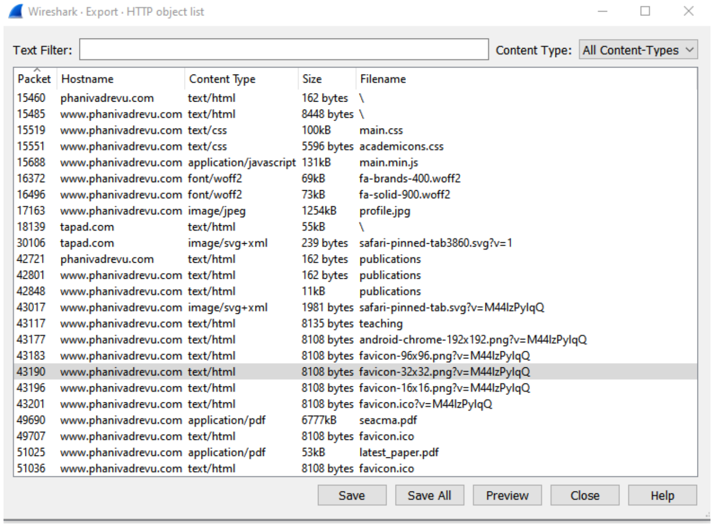


You need the 2nd part.

The dictionary say binary means "something related to two".

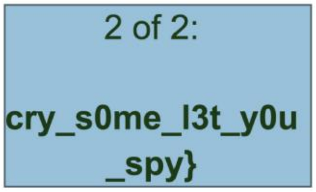
So, may be, you shold go look in a binary?

Which gives a hint to look in the binary. To export all the files transferred in the network traffic Wireshark has an option File → Export Objects → http. This option gave the HTTP Object list.



Packet	Hostname	Content Type	Size	Filename
15460	phanivadrevu.com	text/html	162 bytes	\
15485	www.phanivadrevu.com	text/html	8448 bytes	\
15519	www.phanivadrevu.com	text/css	100kB	main.css
15551	www.phanivadrevu.com	text/css	5596 bytes	academicons.css
15688	www.phanivadrevu.com	application/javascript	131kB	main.min.js
16372	www.phanivadrevu.com	font/woff2	69kB	fa-brands-400.woff2
16496	www.phanivadrevu.com	font/woff2	73kB	fa-solid-900.woff2
17163	www.phanivadrevu.com	image/jpeg	1254kB	profile.jpg
18139	tapad.com	text/html	55kB	\
30106	tapad.com	image/svg+xml	239 bytes	safari-pinned-tab3860.svg?v=1
42721	phanivadrevu.com	text/html	162 bytes	publications
42801	www.phanivadrevu.com	text/html	162 bytes	publications
42848	www.phanivadrevu.com	text/html	11kB	publications
43017	www.phanivadrevu.com	image/svg+xml	1981 bytes	safari-pinned-tab.svg?v=M44lzPylqQ
43117	www.phanivadrevu.com	text/html	8135 bytes	teaching
43177	www.phanivadrevu.com	text/html	8108 bytes	android-chrome-192x192.png?v=M44lzPylqQ
43183	www.phanivadrevu.com	text/html	8108 bytes	favicon-96x96.png?v=M44lzPylqQ
43190	www.phanivadrevu.com	text/html	8108 bytes	favicon-32x32.png?v=M44lzPylqQ
43196	www.phanivadrevu.com	text/html	8108 bytes	favicon-16x16.png?v=M44lzPylqQ
43201	www.phanivadrevu.com	text/html	8108 bytes	favicon.ico?v=M44lzPylqQ
49690	www.phanivadrevu.com	application/pdf	6777kB	seacma.pdf
49707	www.phanivadrevu.com	text/html	8108 bytes	favicon.ico
51025	www.phanivadrevu.com	application/pdf	53kB	latest_paper.pdf
51036	www.phanivadrevu.com	text/html	8108 bytes	favicon.ico

I saved all the Files and was able to find the second part of the flag in the pdf file latest_paper.pdf



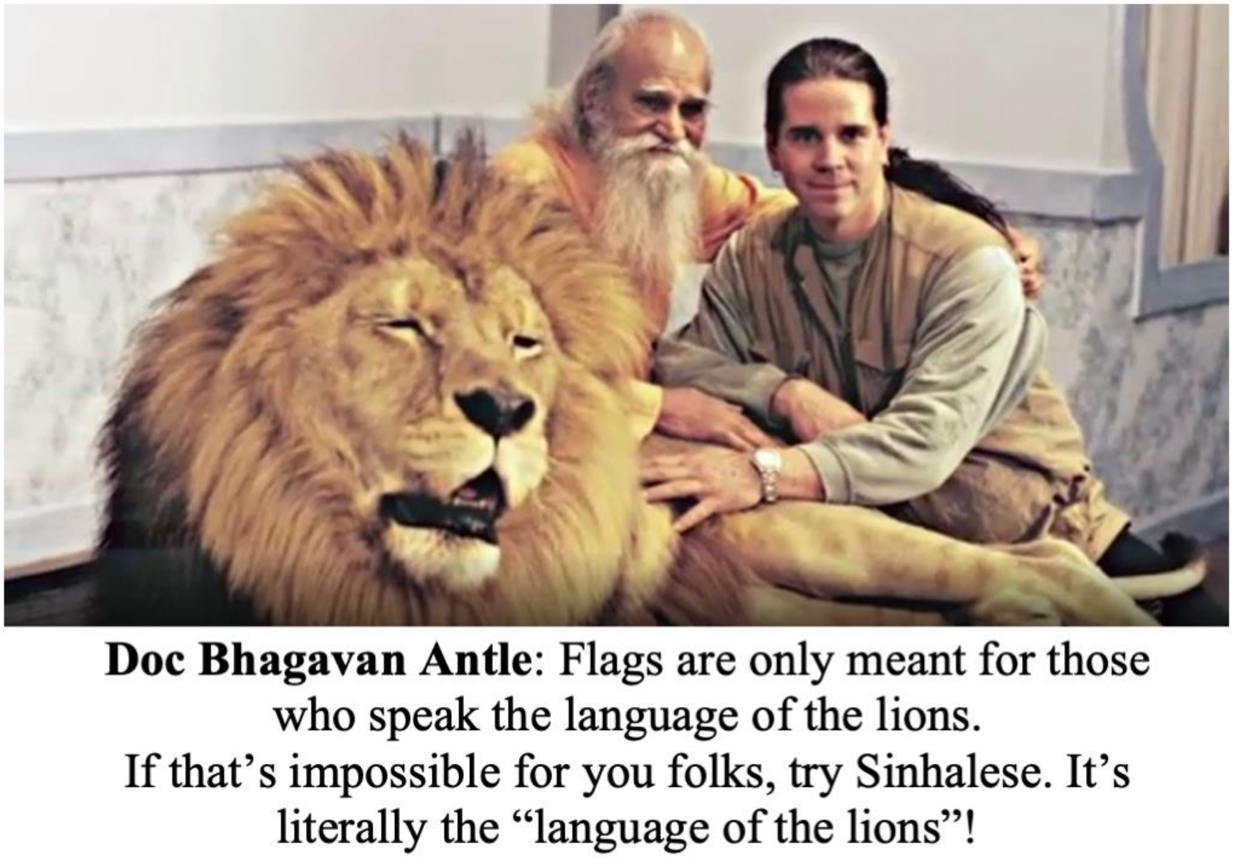
2 of 2:

cry_s0me_l3t_y0u
_spy}

Question-2

Flag Captured: **4621_ctf{tiger_king_is_the_new_thing}**

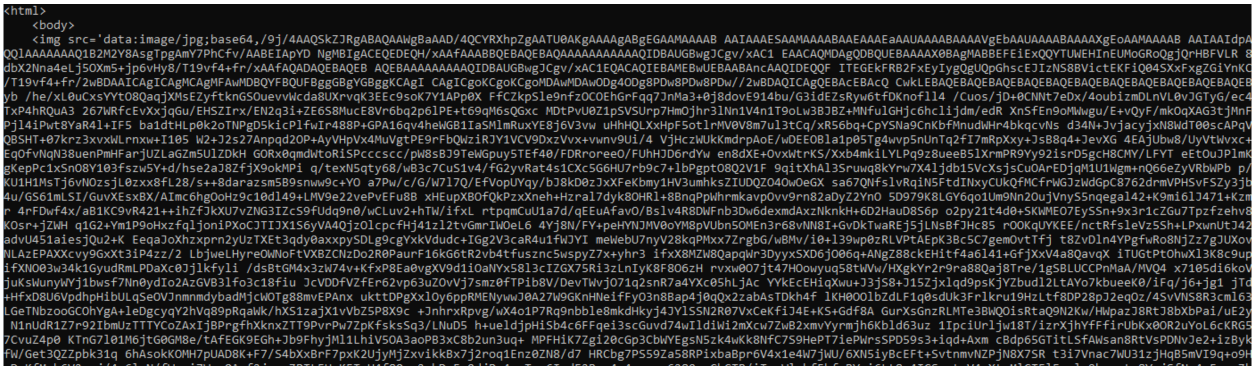
This is a website header changing CTF challenge. The website given http://a3-q2.unoprivateers.xyz/ showed the below picture



Doc Bhagavan Antle: Flags are only meant for those who speak the language of the lions.
If that's impossible for you folks, try Sinhalese. It's literally the "language of the lions"!

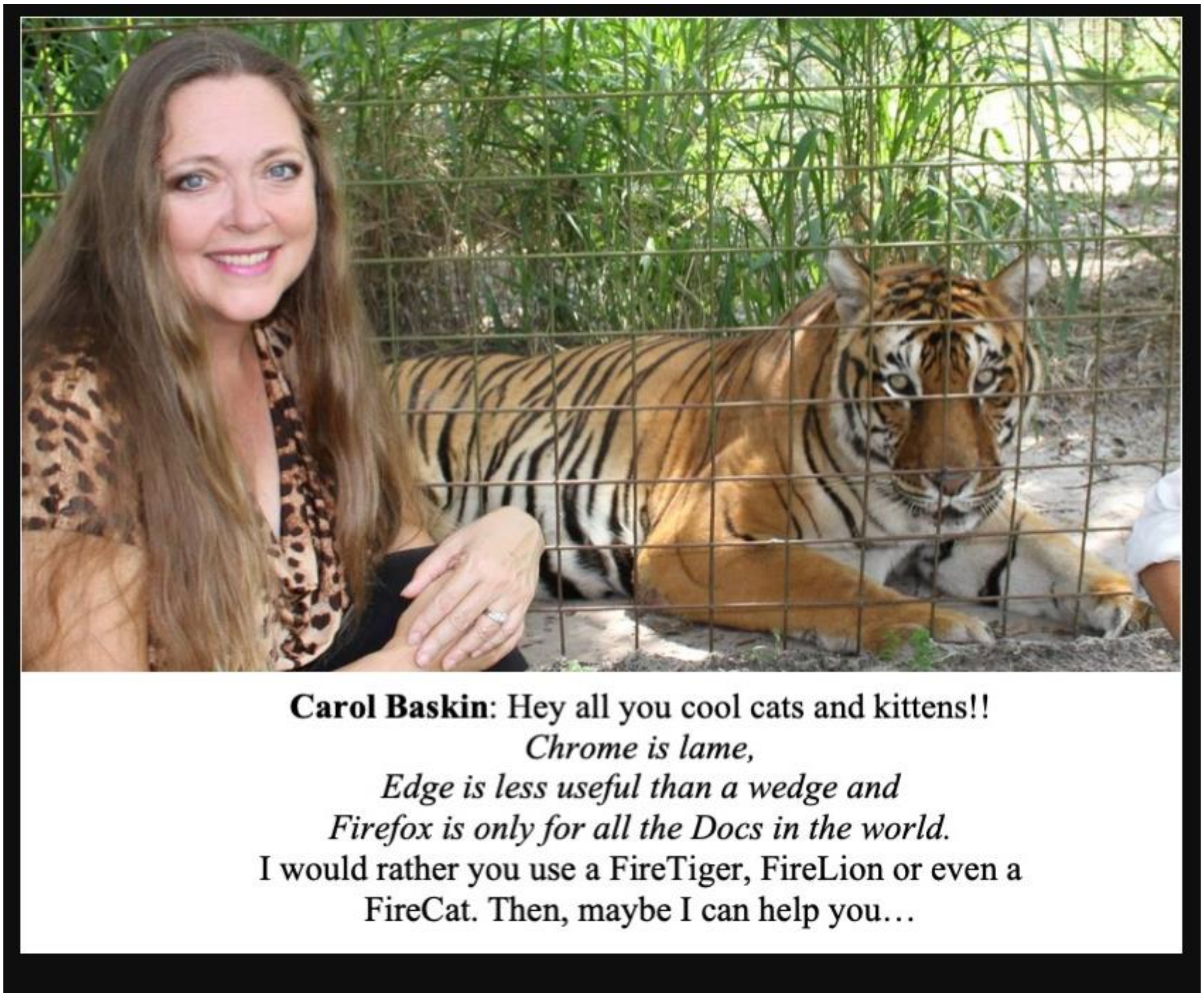
This website just had a picture saying speak language of lions which is the language of Sinhalese. So I tried sending a curl request by changing the header Accept-Language: si.

Curl -H "Accept-Language: si" http://a3-q2.unoprivateers.xyz/



```
<html>
    <body>
    <img src='data:image/jpg;base64,/9j/4AAQSkZJRgABAQAAWgBaAAD/4QCYRXhpZgAATU0AKgAAAAgABgEGAAMAAAAB AAIAAAESAAMAAAABAAEAAAEaAAUAAAABAAAAVgEbAAUAAAABAAAAXgEoAAMAAAAB AAIAAIdpA
QQlAAAAAAAQ1B2M2Y8AsgTpgAmY7PhCfv/AABEIApYD NgMBIgACEQEDEQH/xAAfAAABBQEBAQEBAQAAAAAAAAAAAQIDBAUGBwgJCgv/xAC1 EAACAQMDAgQDBQUEBAAAAX0BAgMABBEFEiExQQYTUWEHInEUMoGRoQgjQrHBFVLR 8
dbX2Nna4eLj5OXm5+jp6vHy8/T19vf4+fr/xAAfAQADAQEBAQEB AQEBAAAAAAAAAQIDBAUGBwgJCgv/xAC1EQACAQIEBAMEBwUEBAABAncAAQIDEQQF ITEGEkFRB2FxEyIygQgUQpGhscEJIzNS8BVictEKFiQ04SXxFxgZGiYnKC
/T19vf4+fr/2wBDAAICAgICAgMCAgMFAwMDBQYFBQUFBggGBgYGBggKCAgI CAgICgoKCgoKCgoMDAwMDAwODg4ODg8PDw8PDw8PDw//2wBDAQICAgQEBAcEBAcQ CwkLEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEB
yb /he/xL0uCxsYYtO8QaqjXMsEZyftknGSOuevvWcda8UXrvqK3EEc9soK7Y1APp0X FfCZkpSle9nfzOCOEhGrFqq7JnMa3+0j8dovE914bu/G3idEZsRyw6tfDKnofll4 /Cuos/jD+0CNNt7eDx/4oubizmDLnVL0vJGTyG/ec4
TxP4hRQuA3 267WRfcEvXxjqGu/EHSZIrx/EN2q3i+ZE6S8MucE8Vr6bq2p6lPE+t69qM6sQGxc MDtPvU0Z1pSVSUrp7HmOjhr3lNn1V4n1T9oLw3BJBZ+MNfulGHjc6hclijdm/edR XnSfEn9oMWwgu/E+vQyF/mkOqXAG3tjMnF
Pjl4iPwt8YaR4l+IF5 ba1dtHLp0k2oTNPgD5kicPlfwIr488P+GPA16qv4heWGB1IaSMlmRuxYE8j6V3vw uHhHQLXxHpF5otlrMV0V8m7ul3tCq/xR56bq+CpYSNa9CnKbfMnudWHr4bkqcvNs d34N+JvjacyjxN8WdT00scAPqV
QBSHT+07krz3xvxWLrnxw+I105 W2+J2s27Anpqd2OP+AyVHpVx4MuVgtPE9rFbQWziRJY1VCV9DxzVvx+vwnv9Ui/4 VjHczWUkKmdrpAoE/wDEEOBla1p05Tg4wvp5nUnTq2fI7mRpXxy+JsB8q4+JevXG 4EAjUbw8/UyVtWvxc+
EqOfvNqN38uenPmHFarjUZLaGZm5UlZDkH GORx0qmdWtoRiSPcccscc/pW8sBJ9TeWGpuy5TEf40/FDRroreeO/FUhHJD6rdYw en8dXE+OvxWtrKS/Xxb4mkiLYLPq9z8ueeB5lXrmPR9Yy92isrD5gcH8CMY/LFYT eEtOuJPlmK
gKepPc1xSnO8Y103fszw5Y+d/hse2aJ8ZfjX9okMPi q/texN5qty68/wB3c7CuS1v4/fG2yvRat4s1CXc5G6HU7rb9c7+lbPgptO8Q2V1F 9qitXhAl3Sruwq8kYrw7X4ljdb15VcXsjsCuOArEDjqM1U1Wgm+nQ66eZyVRbWPb p/
KU1H1MsTj6vNOzsjL0zxx8fL28/s++8darazsm5B9snww9c+YO a7Pw/c/G/W7l7Q/EfVopUYqy/bJ8kD0zJxXFeKbmy1HV3umhksZIUDQZO4OwOeGX sa67QNfslvRqiN5FtdINxyCUkQfMCfrWGJzWdGpC8762drmVPHSvFSZy3jb
4u/GS61mLSI/GuvXEsxBX/AImc6hgOoHz9c10dl49+LMV9e22vePvEFu8B xHEupXBOfQkPzxXneh+Hzral7dyk8OHRl+8BnqPpWhrmkavpOvv9rn82aDyZ2YnO 5D979K8LGY6qo1Um9Nn2OujVnyS5nqegal42+K9mi6lJ471+Kzm
r 4rFDwf4x/aB1KC9vR421++ihZfJkXU7vZNG3IZcS9fUdq9n0/wCLuv2+hTW/ifxL rtpqmCuU1a7d/qEEuAfavO/Bslv4R8DWFnb3Dw6dexmdAxzNknkH+6D2HauD8S6p o2py21t4d0+SKWMEO7EySSn+9x3r1cZGu7Tpzfzehv8
KOsr+jZWH q1G2+Ym1P9oHxzfqljoniPXoCJTIJX1S6yVA4QjzOlcpcfHj41zl2tvGmrIWOeL6 4Yj8N/FY+peHYNJMV0oYM8pVUbn5OMEn3r68vNN8I+GvDkTwaREj5jLNsBfJHc85 rOOKqUYKEE/nctRfsleVz5Sh+LPxwnUtJ42
advU451aiesjQu2+K EeqaJoXhzxprn2yUzTXEt3qdy0axxpySDLg9cgYxkVdudc+IGg2V3caR4u1fWJYI meWebU7nyV28kqPMxx7ZrgbG/wBMv/i0+l39wp0zRLVPtAEpK3Bc5C7gemOvtTfj t8ZvDln4YPgfwRo8NjZz7gJUXov
NLAzEPAXXcvy9GxXt3iP4zz/2 LbjweLHyreOWNoFtVXBZCNzDo2R0PaurF16kG6tR2vb4tfusznc5wspyZ7x+yhr3 ifxX8MZW8QapqWr3DyyxSXD6jO06q+ANgZ88ckEHitf4a6l41+GfjXxV4a8QavqX iTUGtPtOhwXl3K8c9up
ifXNO03w34k1GyudRmLPDaXc0Jjlkfyli /dsBtGM4x3zW74v+KfxP8Ea0vgXV9d1iOaNYx58l3cIZGX75Ri3zLnIyK8F8O6zH rvxw0O7jt47HOowyuq58tWVw/HXgkYr2r9ra88Qaj8Tre/1gSBLUCCPnMaA/MVQ4 x7105di6koV
juKsWunyWYj1bwsf7Nn0ydIo2AzGVB3lfo3c18fiu JcVDDfVZfEr62vp63uZOvVj7smz0fTPib8V/DevTWvjO71q2snR7a4YXc05hLjAc YYkEcEHiqXwu+J3jS8+J15Zjxlqd9psKjYZbudl2LtAYo7kbueeK0/iFq/j6+jg1 jTd
+HfxD8U6VpdhpHibULqSeOVJnmnmdybadMjcWOTg88mvEPAnx ukttDPgXxlOy6ppRMENywwJ0A27W9GKnHNeifFyO3n8Bap4j0qQx2zabAsTDkh4f lKH0OOlbZdLF1q0sdUk3Frlkru19HzLtf8DP28pJ2eqOz/4SvVNS8R3cml63
LGeTNbzooGCOhYgA+leDgcyqY2hVq89pRqaWk/hXS1zajX1vVbZ5P8X9c +JnhrxRpvg/wX4o1P7Rq9nbble8mkdHkyj4JYlSSN2R07VxCeKfiJ4E+KS+Gdf8A GurXsGnzRLMTe3BWQOisRtaQ9N2Kw/HWpazJ8RtJ8bXbPai/uE2y
 N1nUdR1Z7r92IbmUzTTTYCoZAxIjBPrgfhXknxZTT9PvrPw7ZpKfsksSq3/LNuD5 h+ueldjpHiSb4c6FFqei3scGuvd74wIldiWi2mXcw7ZwB2xmvYyrmjh6Kbld63uz 1IpciUrljw18T/izrXjhYfFfirUbKx0OR2uYoL6cKRG5
7CvuZ4p0 KTnG7l01M6jtG0GM8e/tAfEGK9EGh+Jb9FhyjMl1LhiV5OA3aoPB3xC8b2un3uq+ MPFHiK7Zgi20cGp3CbWYEgsN5zk4wKk8NfC7S9HePT7iePWrsSPD59s3+iqd+Axm cBdp65GTitLSfAWsan8RtVsPDNvJe2+izByk
fW/Get3QZZpbk31q 6hAsokKOMH7pUAD8K+F7/S4bXxBrF7pxK2UjyMjZxvikkBx7j2roq1Enz0ZN8/d7 HRCbg7PS59Za58RPixbaBpr6V4x1e4W7jWU/6XN5iyBcEFt+SvtnmvNZPjN8X7SR t3i7Vnac7WU31zjHqB5mVI9q+o9H
```

I got an image with Carol Baskin

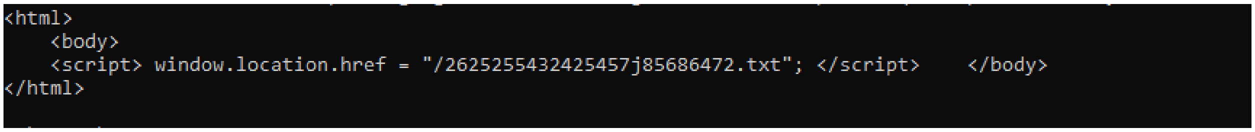


Carol Baskin: Hey all you cool cats and kittens!!
Chrome is lame,
Edge is less useful than a wedge and
Firefox is only for all the Docs in the world.
I would rather you use a FireTiger, FireLion or even a
FireCat. Then, maybe I can help you…

This hint says do not use any normal browser. Which means I need to change the User-Agent header. I tried sending a curl request with Header option FireTiger, FireLion and FireCat.

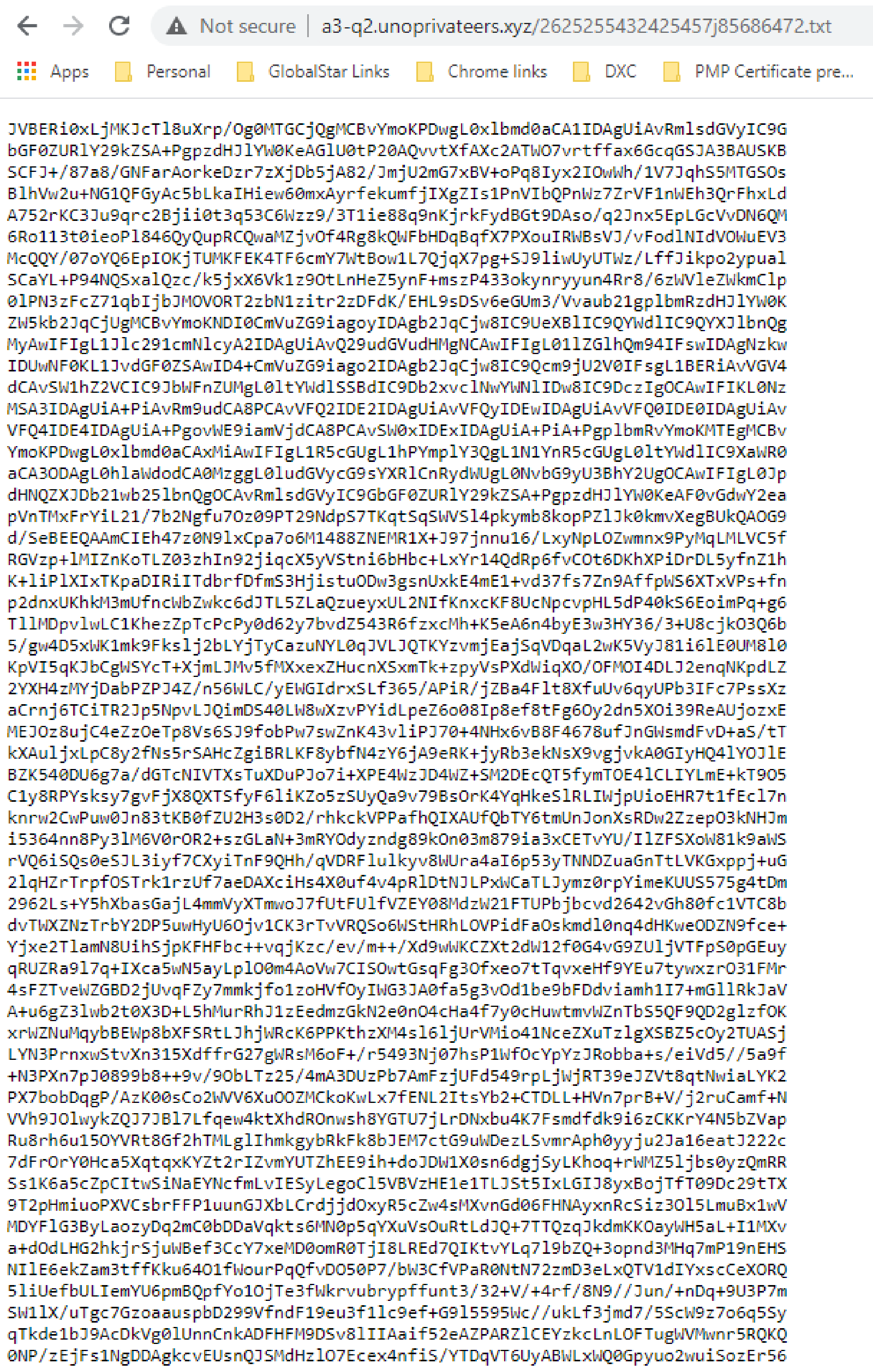
curl -H "Accept-Language: si" -A User-Agent:FireCat [*http://a3-q2.unoprivateers.xyz/*](http://a3-q2.unoprivateers.xyz/)

When I used the User-Agent FireCat I got a different response as shown below



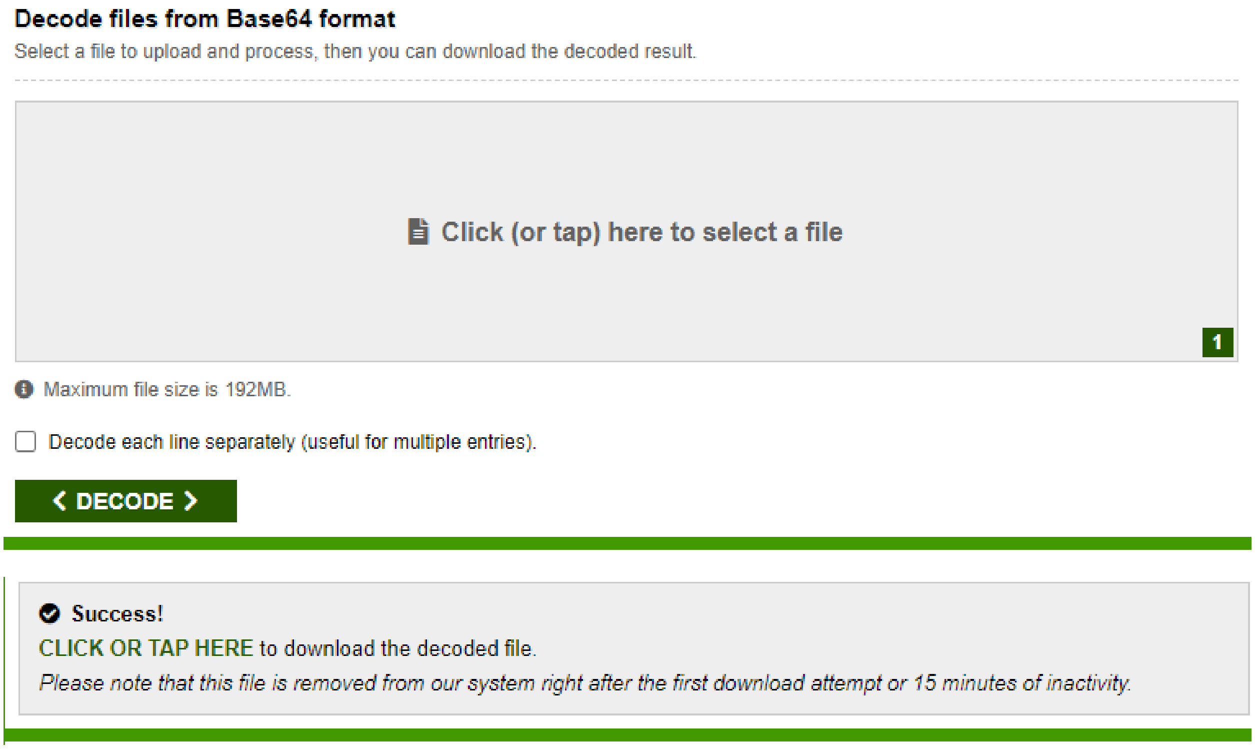
```
<html>
    <body>
    <script> window.location.href = "/2625255432425457j85686472.txt"; </script>    </body>
</html>
```

I got a reference to a txt file with some random base64 characters



```
JVBERi0xLjMKJcTl8uXrp/Og0MTGCjQgMCBvYmoKPDwgL0xlbmd0aCA1IDAgUiAvRmlsdGVyIC9G
bGF0ZURlY29kZSA+PgpzdHJlYW0KeAGlU0tP20AQvvtXfAXc2ATWO7vrtffax6GcqGSJA3BAUSKB
SCFJ+/87a8/GNFarAorkeDzr7zXjDb5jA82/JmjU2mG7xBV+oPq8Iyx2IOwWh/1V7JqhS5MTGSOs
BlhVw2u+NG1QFGyAc5bLkaIHiew60mxAyrfekumfjIXgZIs1PnVIbQPnWz7ZrVF1nWEh3QrFhxLd
A752rKC3Ju9qrc2Bjii0t3q53C6Wzz9/3T1ie88q9nKjrkFydBGt9DAso/q2Jnx5EpLGcVvDN6QM
6Ro113t0ieoPl846QyQupRCQwaMZjvOf4Rg8kQWFbHDqBqfX7PXouIRWBsVJ/vFodlNIdVOWuEV3
McQQY/07oYQ6EpIOKjTUMKFEK4TF6cmY7WtBow1L7QjqX7pg+SJ9liwUyUTWz/LffJikpo2ypual
SCaYL+P94NQSxalQzc/k5jxX6Vk1z9OtLnHeZ5ynF+mszP433okynryyun4Rr8/6zWVleZWkmClp
0lPN3zFcZ71qbIjbJMOVORT2zbN1zitr2zDFdK/EHL9sDSv6eGUm3/Vvaub21gplbmRzdHJlYW0K
ZW5kb2JqCjUgMCBvYmoKNDI0CmVuZG9iagoyIDAgb2JqCjw8IC9UeXBlIC9QYWdlIC9QYXJlbnQg
MyAwIFIgL1Jlc291cmNlcyA2IDAgUiAvQ29udGVudHMgNCAwIFIgL01lZGlhQm94IFswIDAgNzkw
IDUwNF0KL1JvdGF0ZSAwID4+CmVuZG9iago2IDAgb2JqCjw8IC9Qcm9jU2V0IFsgL1BERiAvVGV4
dCAvSW1hZ2VCIC9JbWFnZUMgL0ltYWdlSSBdIC9Db2xvclNwYWNlIDw8IC9DczIgOCAwIFIKL0Nz
MSA3IDAgUiA+PiAvRm9udCA8PCAvVFQ2IDE2IDAgUiAvVFQyIDEwIDAgUiAvVFQ0IDE0IDAgUiAv
VFQ4IDE4IDAgUiA+PgovWE9iamVjdCA8PCAvSW0xIDExIDAgUiA+PiA+PgplbmRvYmoKMTEgMCBv
YmoKPDwgL0xlbmd0aCAxMiAwIFIgL1R5cGUgL1hPYmplY3QgL1N1YnR5cGUgL0ltYWdlIC9XaWR0
aCA3ODAgL0hlaWdodCA0MzggL0ludGVycG9sYXRlCnRydWUgL0NvbG9yU3BhY2UgOCAwIFIgL0Jp
dHNQZXJDb21wb25lbnQgOCAvRmlsdGVyIC9GbGF0ZURlY29kZSA+PgpzdHJlYW0KeAF0vGdwY2ea
pVnTMxFrYiL21/7b2Ngfu7Oz09PT29NdpS7TKqtSqSWVSl4pkymb8kopPZlJk0kmvXegBUkQAOG9
d/SeBEEQAAmCIEh47z0N9lxCpa7o6M1488ZNEMR1X+J97jnnu16/LxyNpLOZwmnx9PyMqLMLVC5f
RGVzp+lMIZnKoTLZ03zhIn92jiqcX5yVStni6bHbc+LxYr14QdRp6fvCOt6DKhXPiDrDL5yfnZ1h
K+liPlXIxTKpaDIRiITdbrfDfmS3HjistuODw3gsnUxkE4mE1+vd37fs7Zn9AffpWS6XTxVPs+fn
p2dnxUKhkM3mUfncWbZwkc6dJTL5ZLaQzueyxUL2NIfKnxcKF8UcNpcvpHL5dP40kS6EoimPq+g6
TllMDpvlwLC1KhezZpTcPcPy0d62y7bvdZ543R6fzxcMh+K5eA6n4byE3w3HY36/3+U8cjkO3Q6b
5/gw4D5xWK1mk9FksljZ2bLYjTyCazuNYL0qJVLJQTKYzvmjEajSqVDqaL2wK5VyJ81i6lE0UM8l0
KpVI5qKJbCgWSYcT+XjmLJMv5fMXxexZHucnXSxmTk+zpyVsPXdWiqXO/OFMOI4DLJ2enqNKpdLZ
2YXH4zMYjDabPZP/n56WLC/yEWGIdrxSLf365/APiR/jZBa4Flt8XfuUv6qyUPb3IFc7Pssxz
aCrnj6TCiTR2Jp5NpvLJQimDS40LW8wXzvPYidLpeZ6o08Ip8ef8tFg6Oy2dn5XOi39ReAUjozxE
MEJOz8ujC4eZzOeTp8Vs6SJ9fobPw7swZnK43vliPJ70+4NHx6vB8F4678ufJnGWsmdFvD+aS/tT
kXAuljxLpC8y2fNs5rSAHcZgiBRLKF8ybfN4zY6jA9eRK+jyRb3ekNsX9vgjvkA0GIyHQ4lYOJlE
BZK540DU6g7a/dGTcNIVTXsTuXDuPJo7i+XPE4WZ+SM2DEcQT5fymTOE41lCLIYLmE+kT9O5
C1y8RPYsksy7gvFjX8QXTSfyF6liKZo5zSUyQa9v79BsOrK4YqHkeS1RLIWjpUioEHR7t1fEcl7n
knrw2CwPuw0Jn83tKB0fZU2H3s0D2/rhkckVPPafhQIXAUfQbTY6tmUnJonXsRDw2ZzepO3kNHJm
i5364nn8Py3lM6V0rOR2+szGLaN+3mRYOdyzndg89kOn03mRYOdyzndg89kOn03m879ia3xCETvYU/IlZFSXoW81k9aWS
rVQ6iSQs0eSJL3iyf7CXyiTnF9QHh/qVDRFlulkyv8WUra4aI6p53yTNNDZuaGnTtLVKGxppj+uG
2lqHZrTrpfOSTrk1rzUf7aeDAXciHs4X0uf4v4pRlDtNJLPxWCaTLJymz0rpYimeKUUS575g4tDm
2962Ls+Y5hXbasGajL4mmVyXTmwoJ7fUtFUlfVZEY08MdzW21FTUPbjbcvd2642vGh80fc1VTC8b
dvTWXZNzTrbY2DP5uwHyU6Ojv1CK3rTvVRQSo6WStHRhLOVPidFaOskmdl0nq4dHKweODZN9fce+
Yjxe2TlamN8UihSjpKFHFbc++vqjKzc/ev/m++/Xd9wWKCZXt2dW12f0G4vG9ZUljVTFpS0pGEuy
qRUZRa9l7q+IXca5wN5ayLpl00m4AoVw7CISOwtGsqFg3Ofxeo7tTqvxeHf9YEu7tywzrO31FMr
4sFZTveWZGBD2jUvqFZy7mmkjfo1zoHVfOyIWG3JA0fa5g3vOd1be9bFDdviamh1I7+mGllRkJaV
A+u6gZ3lwb2t0X3D+L5hMurRhJ1zEedmzGkN2e0nO4cHa4f7y0cHuwtmvWZnTbS5QF9QD2glzfOK
xrWZNuMqybBEWp8bXFSRtLJhjWRcK6PPKthzXM4sl6ljUrVMio41NceZXuTzlgXSBZ5cOy2TUASj
LYN3PrnxwStvXn315XdffrG27gWRsM6oF+/r5493Nj07hsP1WfOcYpYzJRobba+s/eiVd5//5a9f
+N3PXn7pJ0899b/b/UwPb87AmFzjUFd549rpLjWjRT39eJZVt8qtNwiaLYK2
PX7bobDqgP/AzK00sCo2WVV6XuOOZMCkoKwLx7fENL2ItsYb2+CTDLL+HVn7prB+V/j2ruCamf+N
VVh9JOlwykZQJ7JBl7Lfqew4ktXhdROnwsh8YGTU7jLrDNxbu4K7Fsmdfdk9i6zCKKrY4N5bZVap
Ru8rh6u15OYVRt8Gf2hTMLglIhmkgybRkFk8bJEM7ctG9uWDezLSvmrAph0yyju2Ja16eatJ222c
7dFrOrY0Hca5XqtqxKYZt2rIZvmYUTZhEE9ih+doJDW1X0sn6dgjSyLKhoq+rWMZ5ljbs0yzQmRR
Ss1K6a5cZpCItwSiNaEYNcfmLvIESyLegoCl5VBVzHE1e1TLJSt5IxLGIJ8yxBojTfT09Dc29tTX
9T2pHmiuoPXVCsbrFFP1uunGJXbLCrdjjdOxyR5cZw4sMXvnGd06FHNAyxnRcSiz3Ol5LmuBx1wV
MDYFlG3ByLaozyDq2mC0bDDaVqkts6MN0p5qYXuVsOuRtLdJQ+7TTQzqJkdmKKOayWH5aL+I1MXv
a+dOdLHG2hkjrSjuWBef3CcY7xeMD0omR0TjI8LREd7QIKtvYLq7l9bZQ+3opnd3MHq7mP19nEHS
NIlE6ekZam3tffKku64O1fWourPqQfvDO50P7/bW3CfVPaR0NtN72zmD3eLxQTV1dIYxscCeXORQ
5liUefbULIemYU6pmBQpfYo1OjTe3fWkrvubypbrpff/+N9//8N9//Jun/+nDq+9U3P7m/5sc
SW1lX/uTgc7GzoaausDGzoaauspbD299VfndF19+eu3+G9l5595Wc//ukLf3jmd7/5ScW9z7o6q5Sy
qTkde1bJ9AcDkVg0lUnnCnkADFHFM9DSv8lIIAaif52eAZPARZlCEYzkcLnLOFTugWVMwnr5RQKQ
0NP/zEjFs1NgDDAgkcvEUsnQJSMdHzl07OAyp/YTDqVT6UyABWLxWQ0GpyuoSozEr56
```

I saved this text file and used a online base64 decoder https://www.base64decode.org/ uploaded the file into this website



Decode files from Base64 format

Select a file to upload and process, then you can download the decoded result.

Click (or tap) here to select a file

Maximum file size is 192MB.

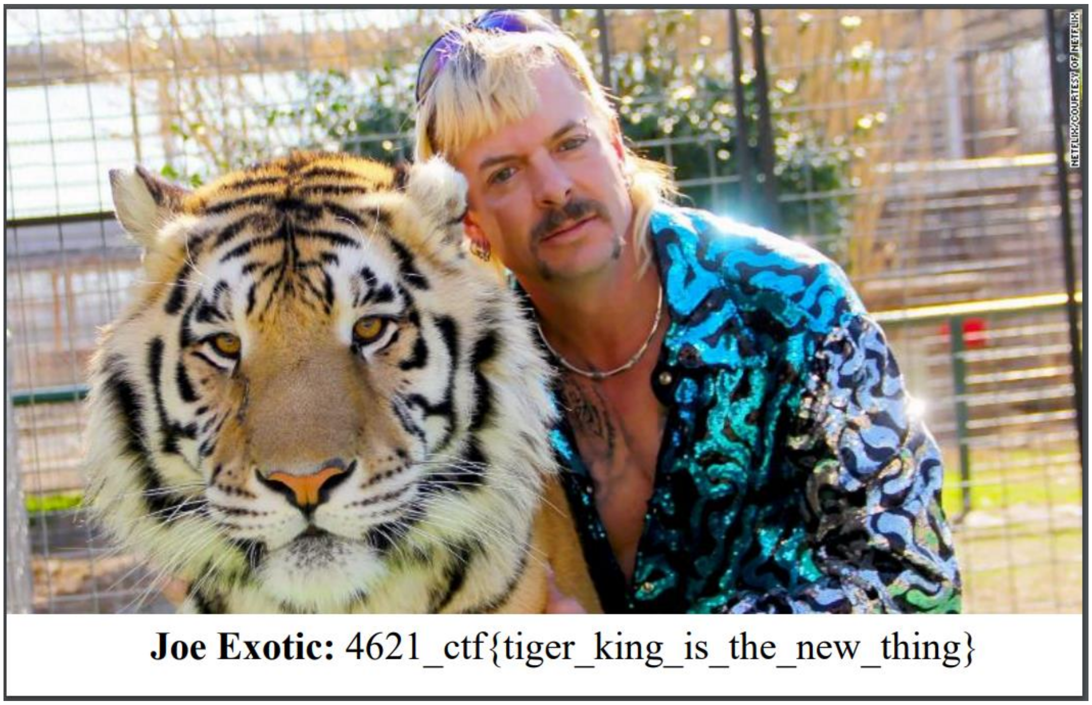
□ Decode each line separately (useful for multiple entries).

Success!

CLICK OR TAP HERE to download the decoded file.

Please note that this file is removed from our system right after the first download attempt or 15 minutes of inactivity.

and I got a decoded pdf file which when opened showed me the flag for this challenge

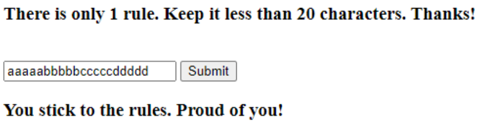


Joe Exotic: 4621_ctf{tiger_king_is_the_new_thing}

Question-3

Flag captured: **4621_ctf{rul3_breakers_r_fl4g_t4ker5}**

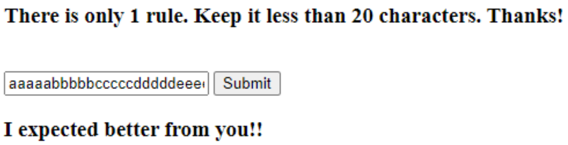
This is a JavaScript task. Using Chrome developer options source tab I was able to see the JavaScript used to render the response text on the page.



There is only 1 rule. Keep it less than 20 characters. Thanks!

aaaaabbbbbccccddddd Submit

You stick to the rules. Proud of you!



There is only 1 rule. Keep it less than 20 characters. Thanks!

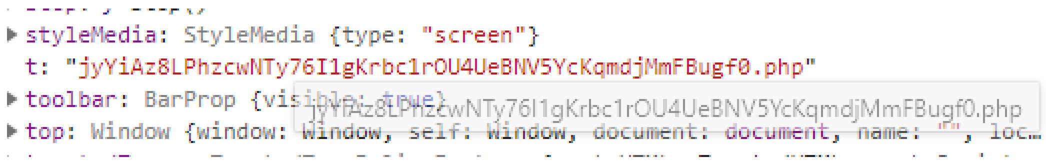
aaaaabbbbbcccccddddeee Submit

I expected better from you!!

The website renders a h3 element based on the input text's length. If the input length is less than 20 it displays "*You stick to the rules*" else "*I expect better from you*"

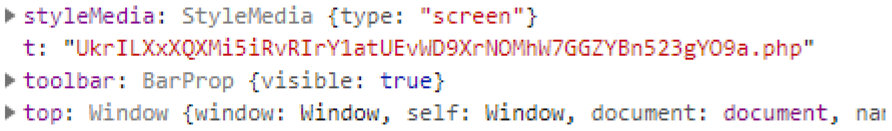
To understand how it is rendering these outputs I started adding breakpoints in the script and started debugging the code. The function se(u,x) seems to be the main function in the script. This function based on the length of the input text it calls a different .php file.

If length less than 20 `jyYiAz8LPhzcwNTy76I1gKrbc1rOU4UeBNV5YcKqmdjMmFBugf0.php` is called else `UkrILXxXQXMi5iRvRIrY1atUEvWD9XrNOMhW7GGZYBn523gYO9a.php` is called



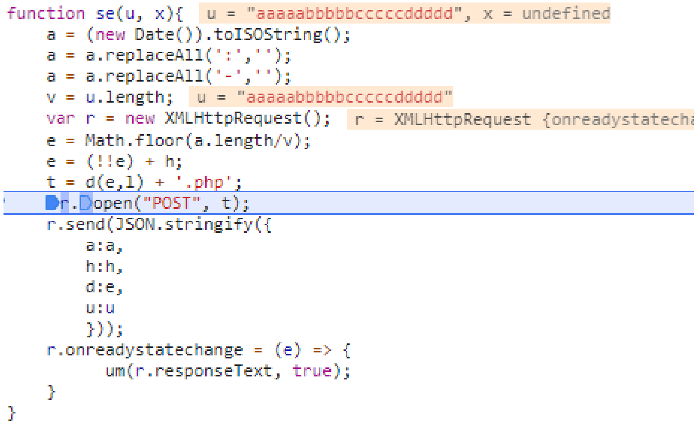
```
▶ styleMedia: StyleMedia {type: "screen"}
  t: "jyYiAz8LPhzcwNTy76I1gKrbc1rOU4UeBNV5YcKqmdjMmFBugf0.php"
▶ toolbar: BarProp {visible: true}
▶ top: Window {window: Window, self: Window, document: document, name: "", loc…
```

jyYiAz8LPhzcwNTy76I1gKrbc1rOU4UeBNV5YcKqmdjMmFBugf0.php



```
▶ styleMedia: StyleMedia {type: "screen"}
  t: "UkrILXxXQXMi5iRvRIrY1atUEvWD9XrNOMhW7GGZYBn523gYO9a.php"
▶ toolbar: BarProp {visible: true}
▶ top: Window {window: Window, self: Window, document: document, na
```

I assumed to get the Flag; I should call the `jyYiAz8LPhzcwNTy76I1gKrbc1rOU4UeBNV5YcKqmdjMmFBugf0.php` service with a proper input parameter.

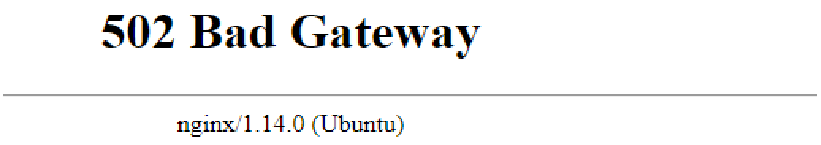


```
function se(u, x){  u = "aaaaabbbbbccccddddd", x = undefined
    a = (new Date()).toISOString();
    a = a.replaceAll(':','');
    a = a.replaceAll('-','');
    v = u.length;  u = "aaaaabbbbbccccddddd"
    var r = new XMLHttpRequest();  r = XMLHttpRequest {onreadystatecha
    e = Math.floor(a.length/v);
    e = (!!e) + h;
    t = d(e,l) + '.php';
    r.open("POST", t);
    r.send(JSON.stringify({
        a:a,
        h:h,
        d:e,
        u:u
        }));
    r.onreadystatechange = (e) => {
         um(r.responseText, true);
    }
}
```

But if I use the input box in the website I will not be calling the php script that I want always. So to bypass this behavior, I wrote my own function ac_lt_func(text) similar to se(u,x) and tried to call the `jyYiAz8LPhzcwNTy76I1gKrbc1rOU4UeBNV5YcKqmdjMmFBugf0.php` This function which I wrote always calls the php script which runs when input length is less than 20 with the POST parameters a,h,d,u

```
function ac_lt_func(inp)
{
    a = (new Date()).toISOString();
    a = a.replaceAll(':',");
    a = a.replaceAll('-',");
    //Skipping the part of verifying length
    h = 'rules.unoprivateers.xyz';
    // setting e to true
    e = 'true' + h;
    u = inp;
    t = 'jyYiAz8LPhzcwNTy76I1gKrbc1rOU4UeBNV5YcKqmdjMmFBugf0.php';
    var r = new XMLHttpRequest();
    r.open("POST", t);
    r.send(JSON.stringify({
        a:a,
        h:h,
        d:e,
        u:u
        }));
    r.onreadystatechange = (e) => {
          um(r.responseText, true);
    }
}
```

The server is currently returning 502 Gateway error. So, I could not take a screenshot of the working of this JavaScript that I wrote. Luckily, I noted down the Flag earlier



502 Bad Gateway

nginx/1.14.0 (Ubuntu)