

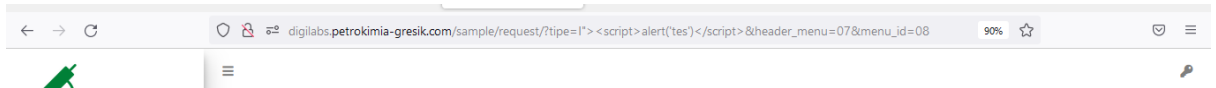
LAPORAN PERBAIKAN PENTEST APLIKASI

Digilabs.petrokimia-gresik.com

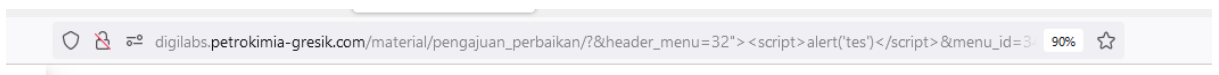
8. Reflected Cross Site Scripting pada menu “Sample Request”

Sudah diperbaiki untuk Reflected Cross Site Scripting Ketika URL diberi input javascript sudah tidak mengeksekusi javascript

8.1.1 Reflected Cross Site Scripting pada menu “Sample Request”



8.2.1 Reflected Cross Site Scripting pada menu “Pengajuan Perbaikan”



9. Stored Cross Site Scripting pada Menu “Pengajuan Perbaikan/Kalibrasi”

Sudah diperbaiki untuk Stored Cross Site Scripting ketika form diberi input javascript sudah tidak mengeksekusi javascript

9.1.1 Stored Cross Site Scripting pada menu “Sample Request” (sebelum disimpan / submit)

Sample Request

Peminta Jasa* Peminta Jasa Test Tgl Pengajuan 08-02-2022 13:13:44

Jenis Sample* Kalibrasi Wet Test Tgl Memo* 08-02-2022 00:00:00

Jenis Pekerjaan* Pekerjaan Test Nomor Memo* 1

PIC Pengirim Sample <script>alert('test pentest')</script> Identitas* Kalibrasi Wet Test

Ext Pengirim Sample 1 * jika identitas tidak ada silahkan pilih sesuai jenis sample & tuliskan identitas sample anda di NOTE

Jumlah Sample* 1 Parameter* 1

Note 123

Foto Sample* Browse... Screenshot_3.png

Close Simpan

Copyright © 2021 Petrokimia Gresik. Version 1.0.1

9.1.2 Stored Cross Site Scripting pada menu “Sample Request” (setelah disimpan / submit)

Sample Request

Peminta Jasa* Peminta Jasa Test

Jenis Sample* Kalibrasi Wet Test

Jenis Pekerjaan* Pekerjaan Test

PIC Pengirim Sample [removed]alert('test pentest')[remc]

Ext Pengirim Sample* 1

Jumlah Sample* 1

Tgl Pengajuan 08-02-2022

Tgl Memo* 08-02-2022

Nomor Memo* 1

Identitas* Kalibrasi Wet Test

* jika identitas tidak ada silahkan pilih sesuai jenis sample & tuliskan identitas sample anda di NOTE

Parameter* 1

Note 123

Foto Sample* Browse... No file selected.

Foto Sebelumnya

Close Edit

9.2.1 Stored Cross Site Scripting pada menu “pengajuan perbaikan” (sebelum disimpan / submit)

Pengajuan Perbaikan

Tgl Penyerahan* 8-2-2022

Nomor Aset* 123

Nama Aset* Aset Test

Serial Number* 123456789

Jenis Pekerjaan* Perbaikan

Pengelola Aset* Peminta Jasa Test

Vendor* <script>alert('tes')</script>

Note* <script>alert('tes')</script>

File* Browse... Screenshot_4.png

Close Simpan

9.2.2 Stored Cross Site Scripting pada menu “pengajuan perbaikan” (setelah disimpan / submit)

The screenshot shows a web application interface for 'Pengajuan Perbaikan / Kalibrasi'. It includes a filter section with a date input set to '2022-02' and a 'cari' button. Below is a table with columns: No, Tgl Penyerahan, Tgl Selesai, Nomor Aset, Serial Number, Nama Aset, Pengelola Aset, Note, Status, File, and A. The first row contains the following data: No 1, Tgl Penyerahan 08-02-2022, Tgl Selesai (empty), Nomor Aset 123, Serial Number 123456789, Nama Aset Aset Test, Pengelola Aset Peminta Jasa Test, Note [removed]alert('tes')[removed], Status Perbaikan Pengajuan, and File 20220208133540.png. The table has pagination controls at the bottom.

No	Tgl Penyerahan	Tgl Selesai	Nomor Aset	Serial Number	Nama Aset	Pengelola Aset	Note	Status	File	A
1	08-02-2022		123	123456789	Aset Test	Peminta Jasa Test	[removed]alert('tes')[removed]	Perbaikan Pengajuan	20220208133540.png	

10. Bypass blocked extension file upload to Remote Code Execution

Sudah diperbaiki untuk Bypass Blocked Extension File upload to Remote Code Execution ketika diintercept dan melakukan pergantian nama file melalui burp suite maka ketika format file tidak sesuai dengan ketentuan file tidak tersimpan di sistem

10.1.1 Bypass blocked extension file upload to Remote Code Execution “sample request”

The screenshot shows a 'Sample Request' form with various fields for sample submission. The 'PIC Pengirim Sample' field contains a JavaScript payload: `<script>alert('test pentest')</script>`. Other fields include 'Peminta Jasa' (Peminta Jasa Test), 'Jenis Sample' (Kalibrasi Wet Test), 'Jenis Pekerjaan' (Pekerjaan Test), 'Tgl Pengajuan' (08-02-2022 13:13:44), 'Tgl Memo' (08-02-2022 00:00:00), 'Nomor Memo' (1), 'Identitas' (Kalibrasi Wet Test), 'Ext Pengirim Sample' (1), 'Jumlah Sample' (1), 'Parameter' (1), 'Note' (123), and 'Foto Sample' (Screenshot_3.png). A red warning message states: '* jika identitas tidak ada silahkan pilih sesuai jenis sample & tuliskan identitas sample anda di NOTE'. The form has 'Close', 'Simpan', and 'Tambah' buttons.

Sample Request

Peminta Jasa* Peminta Jasa Test

Jenis Sample* Kalibrasi Wet Test

Jenis Pekerjaan* Pekerjaan Test

PIC Pengirim Sample <script>alert('test pentest')</script>

Ext Pengirim Sample* 1

Jumlah Sample* 1

Tgl Pengajuan 08-02-2022 13:13:44

Tgl Memo* 08-02-2022 00:00:00

Nomor Memo* 1

Identitas* Kalibrasi Wet Test

* jika identitas tidak ada silahkan pilih sesuai jenis sample & tuliskan identitas sample anda di NOTE

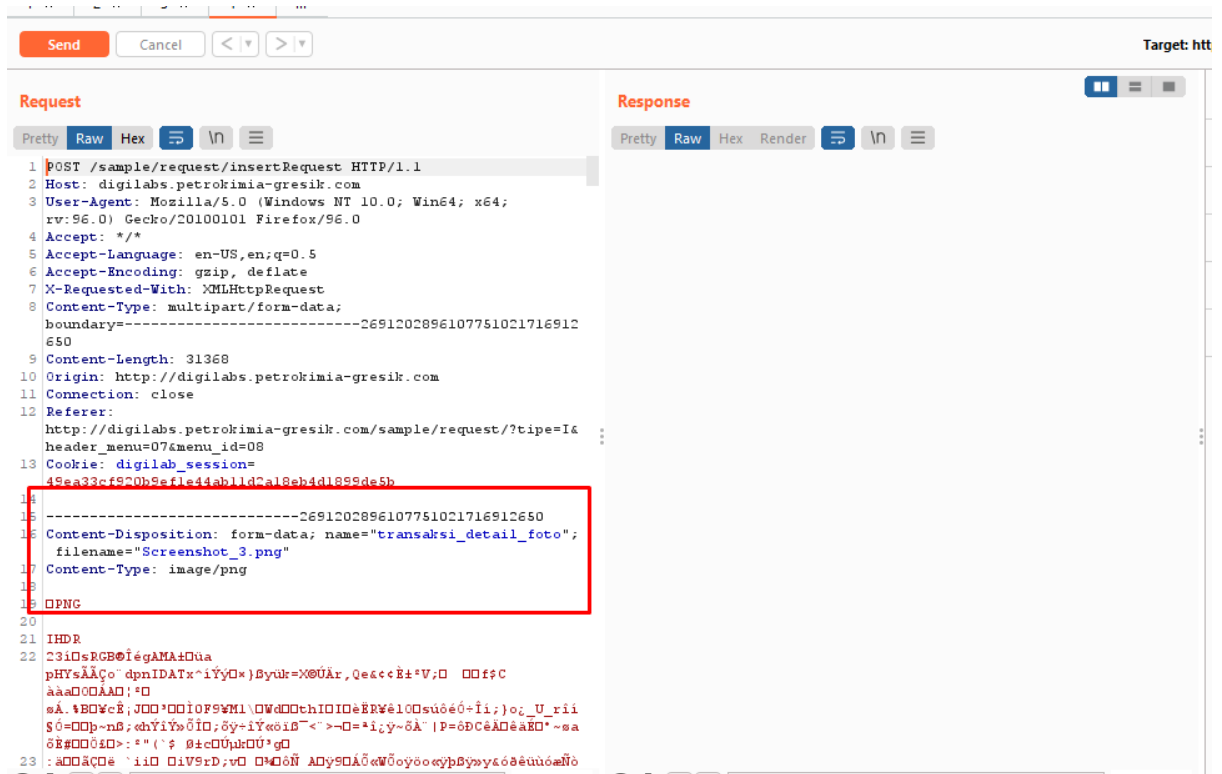
Parameter* 1

Note 123

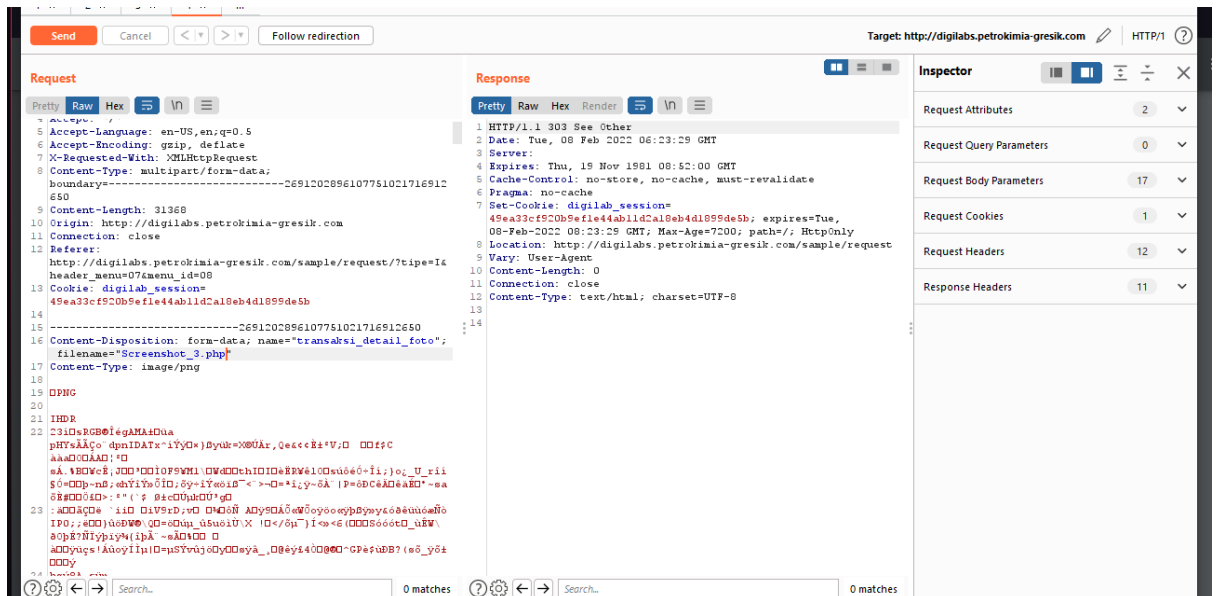
Foto Sample* Browse... Screenshot_3.png

Close Simpan Tambah

10.1.2 Bypass blocked extension file upload to Remote Code Execution “sample request” sebelum di intercept



10.1.3 Bypass blocked extension file upload to Remote Code Execution “sample request” setelah di intercept



10.1.4 File tidak mengalami perubahan / bertambah

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..					
9c474cc23d425da3e48...	28.889	PNG File	02/08/22 13:16:...	-rw-r--r--	daemon da...
44276997_2202080907...	41.515	PDF Docu...	02/08/22 09:07:...	-rw-r--r--	daemon da...
42137729_2202080807...	17.340	PDF Docu...	02/08/22 08:07:...	-rw-r--r--	daemon da...
93981693_2202070309...	15.535	PDF Docu...	02/07/22 15:09:...	-rw-r--r--	daemon da...
73838708_2202070307...	42.127	PDF Docu...	02/07/22 15:07:...	-rw-r--r--	daemon da...
32133706_2202070236...	12.134	PDF Docu...	02/07/22 14:36:...	-rw-r--r--	daemon da...
72309331_2202070959...	35.034	PDF Docu...	02/07/22 09:59:...	-rw-r--r--	daemon da...
41246317_2202070843...	19.871	PDF Docu...	02/07/22 08:43:...	-rw-r--r--	daemon da...
65232147_2202070841...	15.965	PDF Docu...	02/07/22 08:41:...	-rw-r--r--	daemon da...

10.2.1 Bypass blocked extension file upload to Remote Code Execution “pengajuan perbaikan”

digilabs.petrokimia-gresik.com/material/pengajuan_perbaikan/?&header_menu=32&menu_id=34

90%

Tgl Penyerahan * 8-2-2022

Nomor Aset * 123

Nama Aset * Aset Test

Serial Number * 123456789

Jenis Pekerjaan * Perbaikan

Pengelola Aset * Peminta Jasa Test

Vendor * <script>alert('tes')</script>

Note * <script>alert('tes')</script>

File * Screenshot_4.png

10.2.2 Bypass blocked extension file upload to Remote Code Execution “pengajuan perbaikan” sebelum di intercept

The screenshot shows a web browser's developer tools with the 'Network' tab selected. The target URL is `http://digilabs.petrokimia-gresik.com`. The 'Request' pane shows a POST request to `/aset_perbaikan_file` with a file named `Screenshot_4.png`. The 'Response' pane shows a 200 OK status. The 'Inspector' pane shows the request attributes, query parameters, body parameters, cookies, and headers. The request body is a multipart/form-data payload containing a file upload and a status update.

```
35 -----62939593239263967561747564379
36 Content-Disposition: form-data; name="aset_perbaikan_vendor"
37
38 <script>alert('tes')</script>
39 -----62939593239263967561747564379
40 Content-Disposition: form-data; name="aset_perbaikan_note"
41
42 <script>alert('tes')</script>
43 -----62939593239263967561747564379
44 Content-Disposition: form-data; name="id_user"
45
46 1
47 -----62939593239263967561747564379
48 Content-Disposition: form-data; name="aset_perbaikan_status"
49
50 n
51 -----62939593239263967561747564379
52 Content-Disposition: form-data; name="aset_perbaikan_file";
53 filename="Screenshot_4.png"
54 Content-Type: image/png
55
56
57 IHDRb0An/sRGB0iegAMA4Dua pHYsAAQo' deZIDATx~iYD\AQ(m0e0Dy
i~$000' OnD0i1i0K Ylnw ~y06~i00If00RvwieN"0h"0UeI'kU'~a-YeI\0
f0i1lgy0A8Dx04'w0Dy~uies00Tu00r0S0U000000:0T0~eyes'~a0pao0B!
00h'~aA_0z0A/TIAA0000'~A044uu:00R00' iU'00iU00wviD000U0)~LNN0000
0000AA 000
58 D'~J0000DqIf\0,S\IiI0R0'~'cklp=0>oJ&W)D,W3SSpIf\0.C\IiI0R0'
~U
59 tA042\0.C\IiI0R0'~EU
60 0i0i4Y2\IcI0R0'~EU
61 tD-$,h300(r\IAC)0A'~(-imjlp=FO000J&(W)xpuQSAA000'00k((i\Y'~x0)00-
'00000000
62 t,0(W0YehDyQ0b000000~Ye00eiU'3u'0KAc0]
```

10.2.3 Bypass blocked extension file upload to Remote Code Execution “pengajuan perbaikan” setelah di intercept

The screenshot shows a web browser's developer tools with the 'Network' tab selected. The target URL is `http://digilabs.petrokimia-gresik.com`. The 'Request' pane shows a POST request to `/aset_perbaikan_file` with a file named `Screenshot_4.php`. The 'Response' pane shows a 200 OK status. The 'Inspector' pane shows the request attributes, query parameters, body parameters, cookies, and headers. The request body is a multipart/form-data payload containing a file upload and a status update.

```
35 -----62939593239263967561747564379
36 Content-Disposition: form-data; name="aset_perbaikan_vendor"
37
38 <script>alert('tes')</script>
39 -----62939593239263967561747564379
40 Content-Disposition: form-data; name="aset_perbaikan_note"
41
42 <script>alert('tes')</script>
43 -----62939593239263967561747564379
44 Content-Disposition: form-data; name="id_user"
45
46 1
47 -----62939593239263967561747564379
48 Content-Disposition: form-data; name="aset_perbaikan_status"
49
50 n
51 -----62939593239263967561747564379
52 Content-Disposition: form-data; name="aset_perbaikan_file";
53 filename="Screenshot_4.php"
54 Content-Type: image/png
55
56
57 IHDRb0An/sRGB0iegAMA4Dua pHYsAAQo' deZIDATx~iYD\AQ(m0e0Dy
i~$000' OnD0i1i0K Ylnw ~y06~i00If00RvwieN"0h"0UeI'kU'~a-YeI\0
f0i1lgy0A8Dx04'w0Dy~uies00Tu00r0S0U000000:0T0~eyes'~a0pao0B!
00h'~aA_0z0A/TIAA0000'~A044uu:00R00' iU'00iU00wviD000U0)~LNN0000
0000AA 000
58 D'~J0000DqIf\0,S\IiI0R0'~'cklp=0>oJ&W)D,W3SSpIf\0.C\IiI0R0'
~U
59 tA042\0.C\IiI0R0'~EU
60 0i0i4Y2\IcI0R0'~EU
61 tD-$,h300(r\IAC)0A'~(-imjlp=FO000J&(W)xpuQSAA000'00k((i\Y'~x0)00-
'00000000
62 t,0(W0YehDyQ0b000000~Ye00eiU'3u'0KAc0]
```

10.2.4 File tidak mengalami perubahan / bertambah

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
20220208133540.png	29.893	PNG File	02/08/22 13:35:...	-rw-r--r--	daemon da...
155225-IKPENET.DOC	135.168	Microsoft ...	02/07/22 15:52:...	-rw-r--r--	daemon da...
155225-IK-39-4414 Int...	588.224	PDF Docu...	02/07/22 15:52:...	-rw-r--r--	daemon da...
154812-IK-39-4413 Int...	570.944	PDF Docu...	02/07/22 15:48:...	-rw-r--r--	daemon da...
154812-4413 IK GWOR...	137.728	Microsoft ...	02/07/22 15:48:...	-rw-r--r--	daemon da...
153949-IK-39-4412 Int...	802.534	PDF Docu...	02/07/22 15:39:...	-rw-r--r--	daemon da...
153949-4412 IK FLASH...	211.968	Microsoft ...	02/07/22 15:39:...	-rw-r--r--	daemon da...
153428-IK-39-4411 Int...	571.430	PDF Docu...	02/07/22 15:34:...	-rw-r--r--	daemon da...
153428-4411 IK COLO...	209.920	Microsoft ...	02/07/22 15:34:...	-rw-r--r--	daemon da...

556 files. Total size: 472.899.705 bytes