Authenticated POST XSS Report

State	● New (Open)
Reported To	Bot Testing Environment
Asset	Add
References	Edit
Weakness	None Edit
Severity	No Rating (---) Add
Participants	(Add participant)
Notifications	Enabled
Visibility	Private Redact

Collapse

ADD SUMMARY

ADD HACKER SUMMARY

TIMELINE · EXPORT

ddworken_sfdc submitted a report to **Bot Testing Environment**. Aug 17th (9 mins ago)

Authenticated POST XSS Report

BOT: hackbot posted an internal comment. Aug 17th (9 mins ago)

Hey there! I am Hackbot, I help find possible duplicates and related reports. Here are my top suggestions:

- (100%) Report #261131 by ddworken_sfdc (new): Authenticated POST XSS Report (Aug 2017 - 2 minutes)
- (100%) Report #260102 by ddworken_sfdc (new): Authenticated POST XSS Report (Aug 2017 - 3 days)
- (83%) Report #240863 by ddworken_sfdc (triaged): Authenticated XSS Report (Jun 2017 - 2 months)
- (83%) Report #249506 by ddworken_sfdc (triaged): Authenticated XSS report (Jul 2017 - about 1 month)
- (83%) Report #240855 by ddworken_sfdc (new): Authenticated XSS Report (Jun 2017 - 2 months)
- (82%) Report #251028 by ddworken_sfdc (triaged): Unauthenticated POST XSS Report (Jul 2017 - 30 days)
- (74%) Report #251877 by ddworken_sfdc (triaged): Authenticated POST SQLi Report (Jul 2017 - 28 days)
- (60%) Report #260164 by ddworken_sfdc (new): Unauthenticated GET XSS Report (Aug 2017 - 3 days)
- (60%) Report #260056 by ddworken_sfdc (new): Unauthenticated GET XSS Report (Aug 2017 - 3 days)
- (52%) Report #240851 by ddworken_sfdc (new): Authenticated XSS Report (Jun 2017 - 2 months)

BOT: autotriagebot_dev posted a comment. Aug 17th (8 mins ago)

We have detected that this report is about an XSS vulnerability.

To triage this bug quicker, this bot can automatically verify vulnerabilities.

Try either:

- Posting a URL that will pop up an alert box containing `"YYLMJRIW"`
- Use the JSON structure below to change the method and/or add cookies

Examples:

Option 1: Unauthenticated GET

If it can be exploited without authentication via simply loading a URL, respond with a link that when visited will pop up an alert box containing `"YYLMJRIW"`. The link should either be specified as a markdown link (`[text](https://example.com)` or inside a code block (`` `https://example.com` ``).

Option 2: Authenticated GET

If doing so requires authentication, then please copy and paste the below into JSON a code block and fill in the blanks:

```
{
    "URL": "<Fill in the URL here>",
    "cookies": {"CookieOneName":   "CookieOneValue",
                "CookieTwoName":   "CookieTwoValue",
                "CookieThreeName": "CookieThreeValue"},
    "type": "get"
}
```

Option 3: Authenticated POST

If the exploit requires authentication and is done via POST, then please copy and paste the below into a code block and fill in the blanks:

```
{
    "URL": "<Fill in the URL here>",
    "cookies": {"CookieOneName":   "CookieOneValue",
                "CookieTwoName":   "CookieTwoValue",
                "CookieThreeName": "CookieThreeValue"},
    "type": "post",
    "data": {"ArgumentOneName":   "ArgumentOneValue",
             "ArgumentTwoName":   "ArgumentTwoValue",
             "ArgumentThreeName": "ArgumentThreeValue"}
}
```

If this is not possible, there is no need to reply and a human will verify your report as soon as possible.

Metadata: `{"token": "YYLMJRIW"}`

To disable AutoTriageBot, reply with STOP TRIAGEBOT

ddworken_sfdc posted a comment. (Edit message) Aug 17th (7 mins ago)

Not a URL

BOT: autotriagebot_dev posted a comment. Aug 17th (7 mins ago)

We failed to find any URLs in your comment. Please include the link in either a markdown link (for example: `[link text](https://example.com)`) or in a code block (for example: `` `https://example.com` ``).

To disable AutoTriageBot, reply with STOP TRIAGEBOT

ddworken_sfdc posted a comment. (Edit message) Aug 17th (6 mins ago)

{Not: JSON}

BOT: autotriagebot_dev posted a comment. Aug 17th (6 mins ago)

Failed to parse JSON! Please try again.

To disable AutoTriageBot, reply with STOP TRIAGEBOT

ddworken_sfdc posted a comment. (Edit message) Aug 17th (5 mins ago)

{
"URL": "http://vulnserver/xssIfCookiePost.php",
"cookies": {"NAME": "VALUE"},
"type": "post",
"data": {"q": "<script>alert('YYLMJRIW')</script>"}
}

BOT: autotriagebot_dev posted a comment. Aug 17th (3 mins ago)

Successfully found and confirmed an XSS at `http://vulnserver/xssIfCookiePost.php`!

Results:

Driver	Results
Firefox	XSS confirmed working!
Chrome	No alert box found!

Metadata: {"vulnDomain": "vulnserver"}

To disable AutoTriageBot, reply with STOP TRIAGEBOT

BOT: autotriagebot_dev posted an internal comment. 🔒 Aug 17th (3 mins ago)

Internal Metadata:

```
{
    "alertBrowsers": [
        "Firefox"
    ],
    "confirmedBrowsers": [
        "Firefox"
    ],
    "cookies": {
        "NAME": "VALUE"
    },
    "exploitURL": "http://vulnserver/xssIfCookiePost.php",
    "httpType": "post",
    "id": "261133",
    "method": "unstructured",
    "reportedTime": "2017-08-17 16:50:32.802000+00:00",
    "title": "Authenticated POST XSS Report",
    "type": "XSS",
    "verifiedTime": "2017-08-17 16:55:55.820347"
}
```

BOT: autotriagebot_dev posted an internal comment. 🔒 Aug 17th (3 mins ago)

Suggested bounty: xxx.xx with a σ of xx.xx

Add comment ▾ > Post to: **None selected** ▾ **Request Mediation** ▾

Add a comment...

Write | Common Responses | Parsed with Markdown

Drag & drop or select more files from your computer (max. 50MB per file)

Post comment