Unauthenticated POST SQLi 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 (about 1 hr ago)

Unauthenticated POST SQLi Report

BOT: hackbot posted an internal comment.   🔒 Aug 17th (about 1 hr ago)

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

- (82%) Report #251877 by ddworken_sfdc (triaged): Authenticated POST SQLi Report (Jul 2017 - 28 days)
- (75%) Report #251028 by ddworken_sfdc (triaged): Unauthenticated POST XSS Report (Jul 2017 - 30 days)
- (61%) Report #261133 by ddworken_sfdc (new): Authenticated POST XSS Report (Aug 2017 - 11 minutes)
- (61%) Report #260102 by ddworken_sfdc (new): Authenticated POST XSS Report (Aug 2017 - 3 days)
- (61%) Report #261131 by ddworken_sfdc (new): Authenticated POST XSS Report (Aug 2017 - 13 minutes)
- (56%) Report #260056 by ddworken_sfdc (new): Unauthenticated GET XSS Report (Aug 2017 - 3 days)
- (56%) Report #260164 by ddworken_sfdc (new): Unauthenticated GET XSS Report (Aug 2017 - 3 days)
- (51%) Report #240864 by ddworken_sfdc (new): Unauthenticated open redirect report (Jun 2017 - 2 months)
- (51%) Report #240880 by ddworken_sfdc (new): Unauthenticated open redirect report (Jun 2017 - 2 months)
- (51%) Report #240866 by ddworken_sfdc (new): Unauthenticated open redirect report (Jun 2017 - 2 months)

BOT: autotriagebot_dev posted a comment.   Aug 17th (about 1 hr ago)

We have detected that this report is about a SQLi vulnerability.

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

Try either:

- Posting a URL that delays loading for `"14"` seconds due to a call to the sleep function
- 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 take `14` seconds to load due to a call to the sleep function. 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": "14"}`

To disable AutoTriageBot, reply with STOP TRIAGEBOT

---

ddworken_sfdc posted a comment.   Updated Aug 17th (about 1 hr ago)

```
{
"URL": "http://vulnserver/sqliPost.php ↗",
"type": "post",
"data": {"q": "14"}
}
```

BOT: **autotriagebot_dev** posted a comment.   Aug 17th (about 1 hr ago)

Successfully found and confirmed SQLi at `http://vulnserver/sqliPost.php` !

Metadata: {"vulnDomain": "vulnserver"}

To disable AutoTriageBot, reply with STOP TRIAGEBOT

BOT: **autotriagebot_dev** posted an internal comment.   🔒 Aug 17th (about 1 hr ago)

Internal Metadata:

```
{
    "cookies": {},
    "delay": 14,
    "exploitURL": "http://vulnserver/sqliPost.php",
    "httpType": "post",
    "id": "261135",
    "method": "structured",
    "reportedTime": "2017-08-17 17:01:17.177000+00:00",
    "title": "Unauthenticated POST SQLi Report",
    "type": "SQLi",
```

    "verifiedTime": "2017-08-17 17:04:36.227446"
}

BOT: autotriagebot_dev posted an internal comment.   🔒 Aug 17th (about 1 hr ago)
Suggested bounty: xxxx.xx with a σ of xxx.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

Directory   Security

Leaderboard   Blog

Help   Disclosure Guidelines

Press   Privacy

Terms   🐦