

Authenticated GET open redirect via window.location


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](#).
Authenticated GET open redirect via window.location

Aug 17th (8 mins ago)



BOT: hackbot posted an internal comment.

Aug 17th (7 mins ago)

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

- (92%) Report [#261161](#) by [ddworken_sfdc](#) (new): Authenticated GET open redirect via window.location (Aug 2017 - 7 minutes)
- (70%) Report [#250992](#) by [ddworken_sfdc](#) (triaged): Authenticated open redirect via GET (Jul 2017 - about 1 month)
- (62%) Report [#260105](#) by [ddworken_sfdc](#) (new): Authenticated GET Open Redirect (Aug 2017 - 3 days)



BOT: autotriagebot_dev posted a comment.

Aug 17th (7 mins ago)

We have detected that this report is about an Open Redirect vulnerability.

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

Try either:

- Posting a URL that will redirect to a domain containing `"QKVPJHPM"`
- 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 redirect to a domain containing `"QKVPJHPM"`. 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": "QKVPJHPM"}

To disable AutoTriageBot, reply with STOP TRIAGEBOT



ddworken_sfdc posted a comment. ([Edit message](#))

Updated Aug 17th (< 1 min ago)

```
{
"URL": "http://vulnserver/xssIfCookie.php?q=<script>window.location='http://QKVPJHPM.example.com'</script>",
"cookies": {"NAME": "VALUE"}
}
```



BOT: autotriagebot_dev posted a comment.

Aug 17th (4 mins ago)

Successfully found and confirmed an open redirect from `http://vulnserver/xssIfCookie.php?q=<script>window.location='http://QKVPJHPM.example.com'</script>` to `http://qkvpjhp.example.com/!`
Metadata: {"vulnDomain": "vulnserver"}

To disable AutoTriageBot, reply with STOP TRIAGEBOT



BOT: autotriagebot_dev posted an internal comment.

Aug 17th (4 mins ago)

Internal Metadata:

```
{
  "cookies": {
    "NAME": "VALUE"
  },
  "exploitURL": "http://vulnserver/xssIfCookie.php?q=<script>window.location='http://QKVPJHPM.example.cc",
  "httpType": "GET",
  "id": "261163",
  "method": "structured",
  "redirect": "http://qkvpjhp.example.com/",
  "reportedTime": "2017-08-17 18:50:24.968000+00:00",
  "title": "Authenticated GET open redirect via window.location",
  "type": "Open Redirect",
  "verifiedTime": "2017-08-17 18:53:41.948759"
}
```

BOT: autotriagebot_dev posted an internal comment.

Aug 17th (4 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

© HackerOne

[Directory](#)
[Leaderboard](#)
[Help](#)
[Press](#)
[Terms](#)

[Security](#)
[Blog](#)
[Disclosure Guidelines](#)
[Privacy](#)
