

98

Urgent: Server side template injection via Smarty template allows for RCE

Share:

State ○ Resolved (Closed)Disclosed **August 17, 2017 11:55pm +0530**Reported To **Unikrn**Weakness **Code Injection**Bounty **\$400**Severity ○ No Rating (---)

Participants

Visibility **Disclosed (Full)**[Collapse](#)

TIMELINE · EXPORT

**yaworsk** submitted a report to **Unikrn**.

Aug 29th (2 years ago)

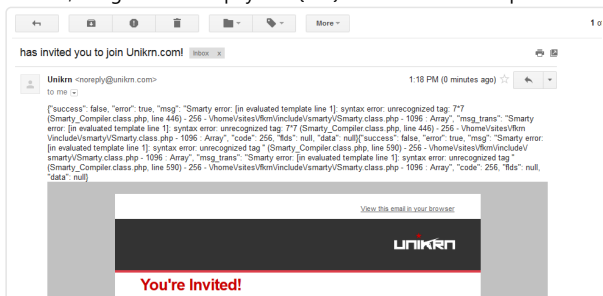
Hi All,

I've found an issue which has allowed me to execute `file_get_contents` and extract your `/etc/passwd` file.

Description

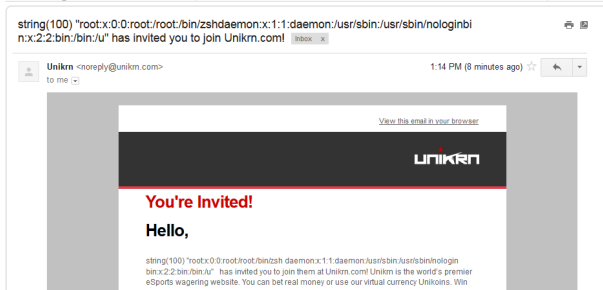
It appears as though you are using smarty on the backend for templating. Entering a malicious payload as my firstname, lastname and nickname and then inviting a user to join the site results in the code being executed.

To start, I began with the payload `{7*7}` and received a template error in the email I received



Recognizing the injection, I then was able to confirm the version of smarty used via `{${smarty.version}} {F115750}` Next I was able to test `{php}` tags by using `{php}print "Hello"{/php} {F115751}`. Finally I used `file_get_contents` to begin extracting the `etc/passwd` file `{php}$s =`

`file_get_contents('/etc/passwd',NULL, NULL, 0, 100); var_dump($s);{/php}`



Steps to reproduce

1. Edit your profile
2. Add the payload `{php}$s = file_get_contents('/etc/passwd',NULL, NULL, 0, 100); var_dump($s);{/php}` as your first name, last name and user name (I'm not sure which field is vulnerable)
3. Invite a friend using another email of yours
4. View the email and you will see part of the etc file dumped

Vulnerability

Since the {php} tags are being parsed and executed, we can execute php functions. In this case, you'll see I'm able to extract the etc/passwd file. While I haven't tried, an attacker can more than likely create a shell on the server.

Please let me know if you have any questions.

Pete

2 attachments:

F115749: [ssti_rce_initial_payload_error.png](#)

F115752: [ssti_rce_etc_passwd.png](#)

 [decrypted](#) changed the status to  **Triaged**. Aug 30th (2 years ago)

 [Unikrn](#) rewarded [yaworsk](#) with a \$250 bounty. Aug 30th (2 years ago)



[decrypted](#) posted a comment.

Aug 30th (2 years ago)

[@yaworsk](#) would you be so kind and add a curl request you used to set your nickname towards an injected value? thx!



[yaworsk](#) posted a comment.

Aug 30th (2 years ago)

Hi [@decrypted](#), I actually didn't use curl, it was all done via your web interface.

After saving the payload, it gets reflected back incorrectly via the web as opposed to what is saved. If it helps I can get the curl command from burp -- let me know if you need that.




[yaworsk](#) posted a comment.

Aug 30th (2 years ago)

And sorry, after step two, be sure to save your profile :)



[decrypted](#) closed the report and changed the status to  **Resolved**.

Aug 30th (2 years ago)

[@yaworsk](#) thx again for the report, not needed anymore. We read something wrong. Nice find - thx again!

Please also confirm the problem exist no more.



[yaworsk](#) posted a comment.

Updated Aug 30th (2 years ago)

Hi All, confirmed, it doesn't look like I can save my profile with the payload any more and the email I receive now says "my friend" has invited me to the site.

Thanks for the quick turn around. That said, I really appreciate the bounty - thank you for that. I recognize you are a small site but I thought, given the max bounty before my report was \$150, my bounty would be a little higher given the potential for attackers to exploit this and the fact this was a full rce.

Thanks again, I'm glad I could help,
pete

 [Unikrn](#) rewarded [yaworsk](#) with a \$150 bonus. Aug 30th (2 years ago)



[decrypted](#) posted a comment.

Aug 30th (2 years ago)

Would love (and then maybe not ;)) to get another report from you soonish.

We will definitely look into other migration bugs we have from our old to the new api.



[yaworsk](#) posted a comment.

Aug 30th (2 years ago)

Thanks for the bonus, I really appreciate it!

And lol re: reports - hopefully (or maybe not?) I'll have some more for you :)

pete



yaworsk requested to disclose this report.
Do you guys mind if we disclose this one?

Jul 30th (2 years ago)



decrypted posted a comment.

Jul 31st (2 years ago)

@yaworsk i think it was a nice and very important find at the time, yet i dont see the benefits of disclosing it now. What would you like to disclose exactly?



decrypted posted a comment.

Jul 31st (2 years ago)

A limited disclosure allows for greater control over sensitive or extraneous information. Only the summary and timeline of activity will be visible.

that option?



yaworsk posted a comment.

Updated Jul 31st (2 years ago)

Hi @decrypted, I was hoping for full disclosure to help others to be honest. While I knew of the issue thanks to the work of James Kettle, I missed a key part of his blog post and worked through the issue myself, hence going from the stack trace -> hello -> version -> /etc/passwd.

I don't think there's anything sensitive in the report any more is there? You can remove the attachments if that helps.

Thanks
Pete



decrypted posted a comment.

Aug 2nd (2 years ago)

Can you remove the attachments? i can not .. without contacting hackerone support.



yaworsk posted a comment.

Aug 2nd (2 years ago)

hi @decrypted, yeah, I spoke with H1 and they only they can delete the attachments. They said support will do it when requested. If you're comfortable doing that, would be awesome if we could leave F115750 and F115751 since they don't disclose anything sensitive but do demonstrate what the testing looked like.

pete



decrypted agreed to disclose this report.

Aug 17th (about 1 year ago)

thx @yaworsk ;) There is a reason you till now got the highest bounty. Skill + good timing :D



This report has been disclosed.

Aug 17th (about 1 year ago)



yaworsk posted a comment.

Aug 17th (about 1 year ago)

Thanks for disclosing @decrypted!! I definitely got lucky on this one :) People reading should note your response time from report to fix -- it was impressive.

Thanks again!
Pete