

**ATTACK**

**DEFENSE**

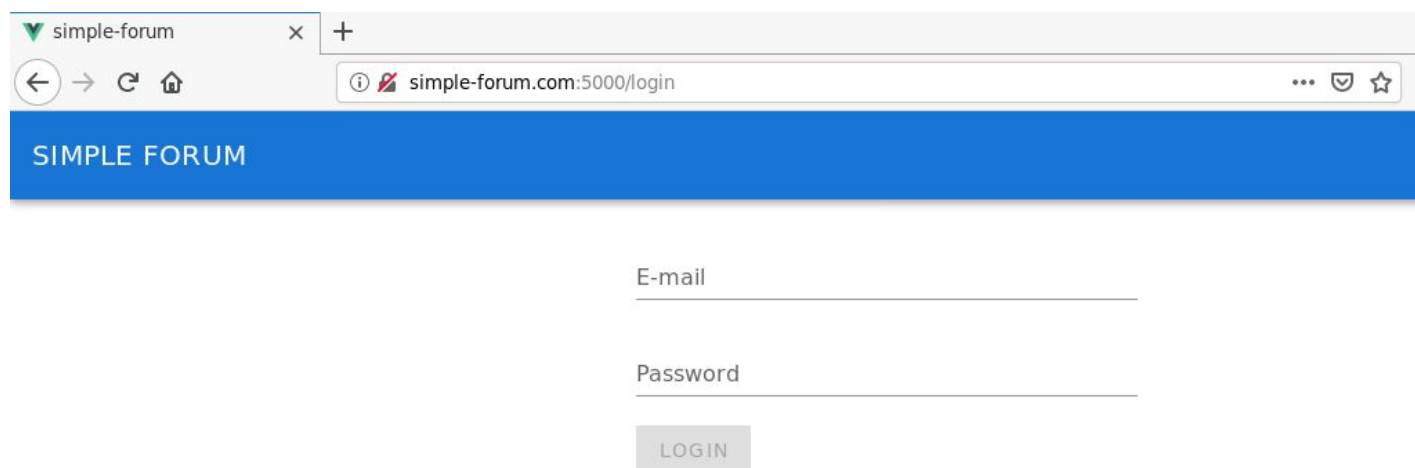
by PentesterAcademy

<b>Name</b>	Vulnerable Forum - XSS
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=1973">https://attackdefense.com/challengedetails?cid=1973</a>
<b>Type</b>	REST: API Security

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Interacting with the Forum webapp.

When the lab starts up, the webapp opens up in the browser:



simple-forum

simple-forum.com:5000/login

SIMPLE FORUM

E-mail

Password

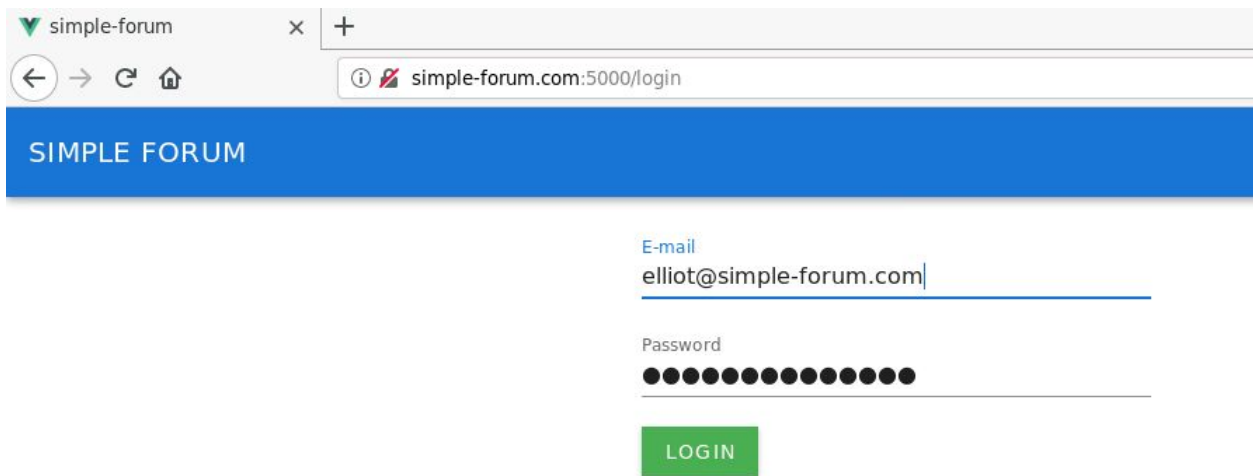
LOGIN

Login into the forum.

Login into the forum using the provided credentials:

**Email:** `elliott@simple-forum.com`

**Password:** `elliottalderson`



simple-forum x +

← → ↻ 🏠

simple-forum.com:5000/login

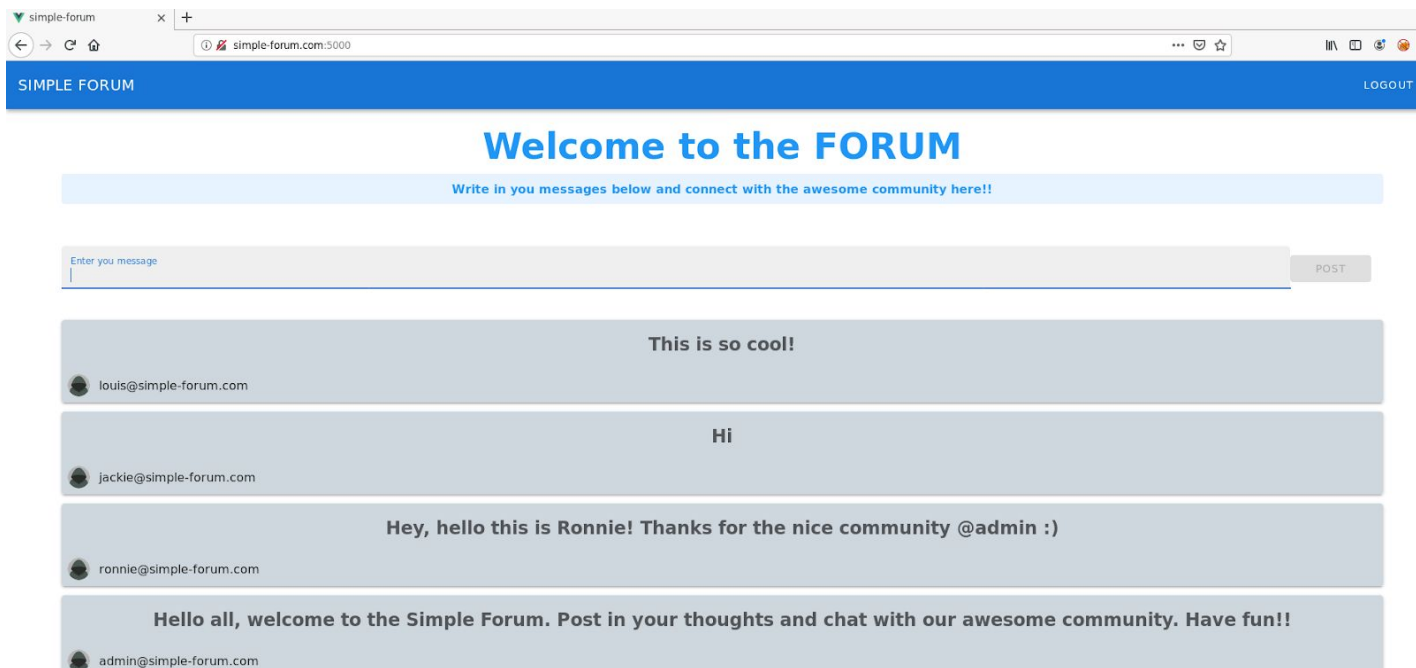
SIMPLE FORUM

E-mail  
elliott@simple-forum.com

Password  
●●●●●●●●●●●●●●●●

LOGIN

After login the following screen appears:



simple-forum x +

← → ↻ 🏠

simple-forum.com:5000

SIMPLE FORUM

LOGOUT

Welcome to the FORUM

Write in you messages below and connect with the awesome community here!!

Enter your message

POST

This is so cool!

louis@simple-forum.com

Hi

jackie@simple-forum.com

Hey, hello this is Ronnie! Thanks for the nice community @admin :)

ronnie@simple-forum.com

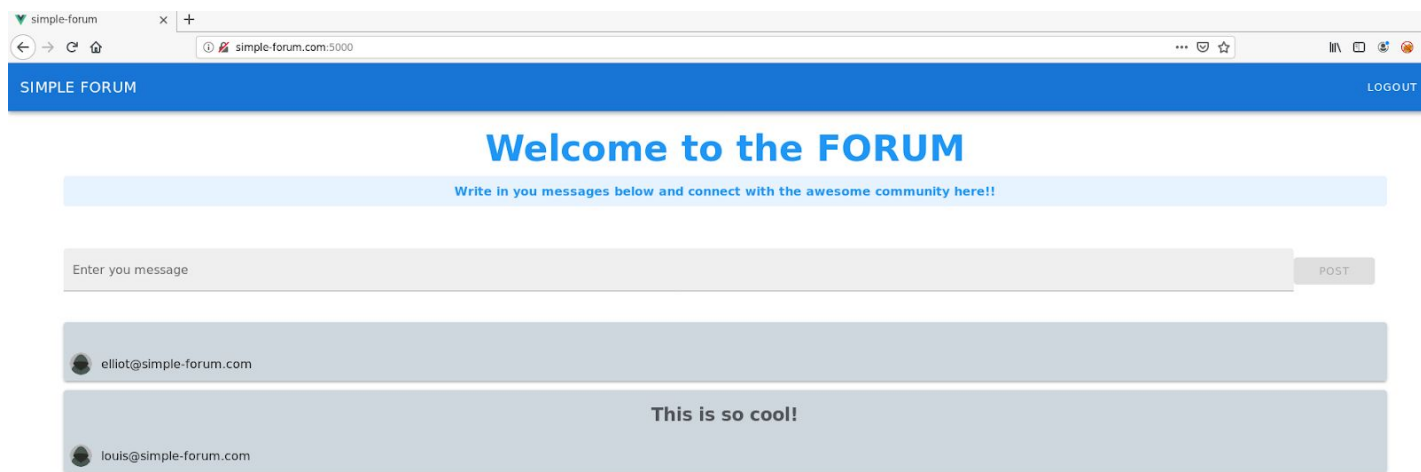
Hello all, welcome to the Simple Forum. Post in your thoughts and chat with our awesome community. Have fun!!

admin@simple-forum.com

**Step 2:** Perform XSS Attack on the Forum.

Posting XSS payload on the forum:

**Payload:** `<script>alert(1234);</script>`



Notice that a new message entry appears on the top.

But the XSS wasn't successful (even after refreshing the page).

Inspect the message that appears on the top:

```
<div class="my-3">
  <div class="mx-auto v-card v-sheet theme--light" style="background-color:
    <div class="v-card__text headline font-weight-bold">
      <script>alert(1234);</script>
    </div>
    <div class="v-card__actions">... </div> flex
  </div>
</div>
```

Notice that the payload is there but it is not being executed.

**Reason:** JavaScript inserted as DOM text will not execute.

#### References:

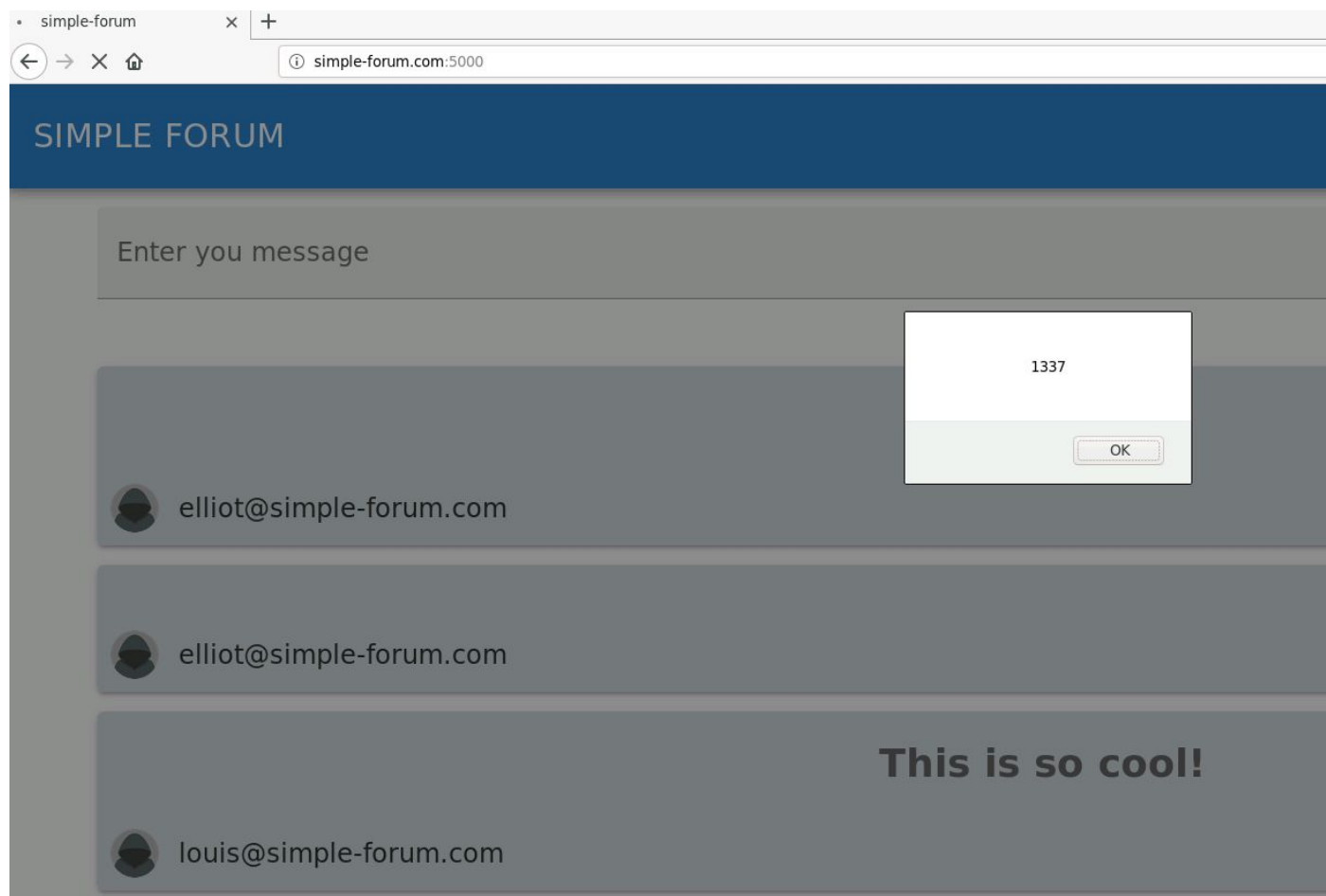
<https://stackoverflow.com/questions/4619668/executing-script-inside-div-retrieved-by-ajax/16278107>

<https://stackoverflow.com/questions/13390588/script-tag-create-with-innerhtml-of-a-div-doesnt-work>

Try using the following payload:

**Payload:** ``

The above payload would try to get an image from a non-existent source and since that request will fail the payload would get executed!



Notice that after the above payload is sent, after some time, XSS payload gets executed (after the request to load the image failed)!

### Conclusion:

Sanitize user input before placing it on a web page. Make sure to encode the content and filter / block malicious content to avoid such issues!

## References:

1. OWASP Top 10 (<https://owasp.org/www-project-top-ten/>)
2. XSS  
([https://owasp.org/www-project-top-ten/OWASP\\_Top\\_Ten\\_2017/Top\\_10-2017\\_A7-Cross-Site\\_Scripting\\_\(XSS\)](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS)))