20 FEB 2021

PERSIS HIGH-LEVEL HUMAN RESOURCE SOFTWARE - ONLINE APPLICANT PORTAL SECURITY ADVISORY (CVE-2020-35753)

Today I am publishing a another write up by my good friend **user_x73x76x6E** - have fun reading!

Although this vulnerability again was not your typical JavaScript XSS it was categorized as such, because HTML could be inserted to manipulate content. This write up should show yet another time that even with no script execution, a vulnerability can have a relevant impact.

TL;DR

The online applicant portal as part of the Persis High-Level Human Resource Software was prone to an HTML-injection. The form for recommending a job posting could be used to send spam mails with nearly any arbitrary content to any recipient. A short search revealed a large number of publicly available portals with open job postings. The Parameter `ABSENDER` could be used to inject HTML, which resulted in a mail sent from *noreply@domain.TLD* with the attacker defined content to the attacker defined recipient.

Product: Online applicant portal with enabled job recommendation feature
Affected Versions: 17.2.00 through 17.2.35 and 19.0.00 through 19.0.20
Fixed Versions: 17.2.36, 19.0.21
Operating Systems: Linux, Windows
Workaround (QuickFix): Deactivate the function "Stellenausschreibung weiterempfehlen" (job recommendation feature) in the settings and replacing it with "einfache Browserfunktionalität (teilen)" (use simple browser functionality)
Responsible: Michael Barth CEO Persis GmbH
CVE ID: CVE-2020-35753

Vulnerability Scoring

Vulnerability Class: Improper neutralization of user supplied input

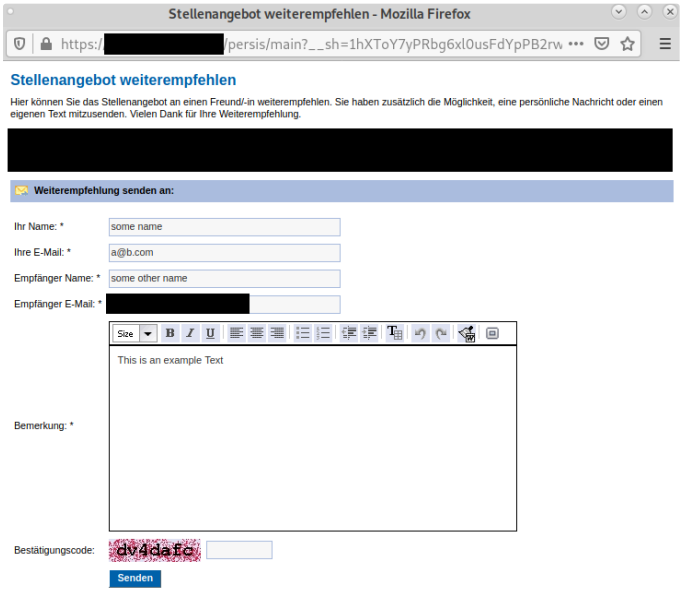
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSS 2
Score 6.4 (Medium)
Vector AV:N/AC:L/Au:S/C:N/I:P/A:P

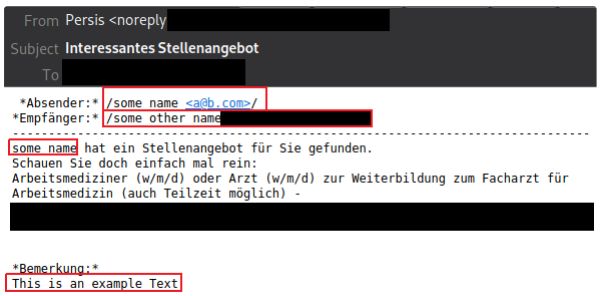
CVSS 3.1
Score: 7.2 (High)
Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L

Detailed Description - Walkthrough

During a domain flyover of several client domains, an instance of the Persis High-Level Human Resource Software was identified and checked fairly quickly. Except for the login, there was one job posting which seemed to be empty. However, even that empty job posting had a function to recommend the posting to a friend (Stellenangebot weiterempfehlen). Using this feature, an e-mail was sent from noreply@domain.TLD to the provided e-mail recipient.



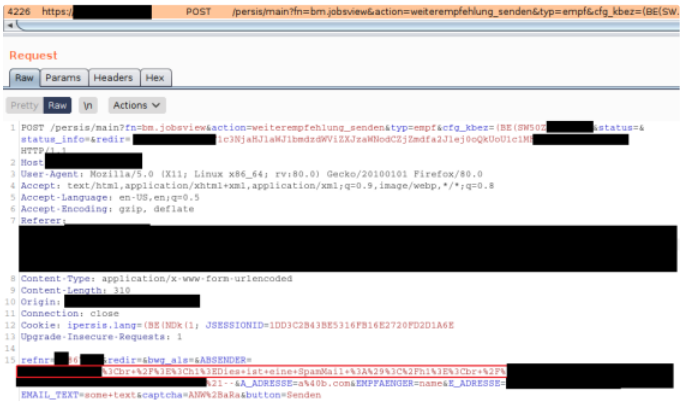
The received mail looked similar to the following:



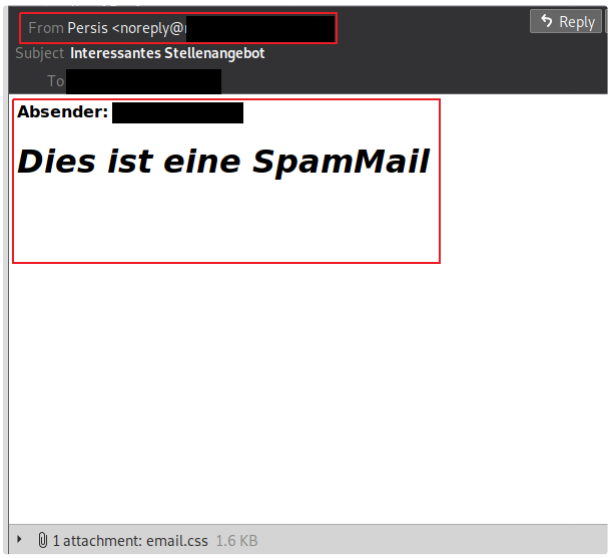
The first field in the form was the senders name (Ihr Name: *). After checking the input validation, it was discovered that there was none. Consequently, this field could already be used to manipulate the future HTML e-mail. The following POST request shows a mail with the manipulated Parameter `ABSENDER`.

Plain text parameter and value

```
ABSENDER=some name<br /><h1>Dies ist eine SpamMail</h1><br />
```



Afterwards the mail was received with the manipulated content.



One caveat was that the subject of the mail could not be changed and there was a file *email.css* attached to every mail. Furthermore, links were not interpreted and the first word `Absender:` could not be changed as well, limiting the versatility of the attack.

Conclusion

The missing input validation of the job recommendation form led to an indirect compromise of the mail address **noreply@domain.TLD**.
The content of mails could be changed nearly arbitrary. Thus, it was possible to craft targeted or generic spam mails and send them to the regarding victims.

The implemented CAPTCHA prevented immediate automated large-scale attacks but did not stop the attack from happening. Furthermore, a simple script e. g. with selenium could automate the attack and use human resource as an element to just solve one CAPTCHA after another. The security of the CAPTCHA and possible automated attacks on solving the CAPTCHA were not researched.

An update is provided via the internal notification to the administrators. If the update cannot be installed, deactivating the function "Stellenausschreibung weiterempfehlen" (job recommendation feature) in the settings and replacing it with "einfache Browserfunktionalität (teilen)" (use simple browser functionality) also stops this behavior.

Potential Damage and Attack Scenarios

There are several security implications for this kind of attack, especially when thinking of a larger company with many active users.

Denial of Service

The issue may be used to send triggering spam mails to spam mail protected clients resulting in blacklisting the domain and thus in a Denial of Service (DoS) of the mail service. This could affect sending mails from inside the company as well as receiving mails from external customers.

Targeted Attacks

Sending mails from a valid and reputational domain can overcome spam mail protection mechanisms for internal staff and external customers alike. This issue could potentially be used to send crafted mails to target specific individuals.

References

- Persis GmbH
- Responsible: Michael Barth CEO Persis GmbH
- MITRE Entry for CVE-2020-35753
- Official blog post by it.sec GmbH

This work is licensed under a Creative Commons Attribution 4.0 International License. In other words, share generously but provide attribution.