



usd HeroL



Technisch erforderlich



Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)



## Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analysezwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

**Advisory ID:** usd-2020-0048  
**CVE Number:** CVE-2020-24708  
**Affected Product:** Gophish  
**Affected Version:** v0.10.1  
**Vulnerability Type:** Stored Cross-Site Scripting  
**Security Risk:** Medium  
**Vendor URL:** <https://getgophish.com/>  
**Vendor Status:** Fixed

## Description

Gophish is vulnerable to stored self-XSS. In v0.10.1 Gophish introduced an impersonation button, which allows normal users to exploit administrative users.

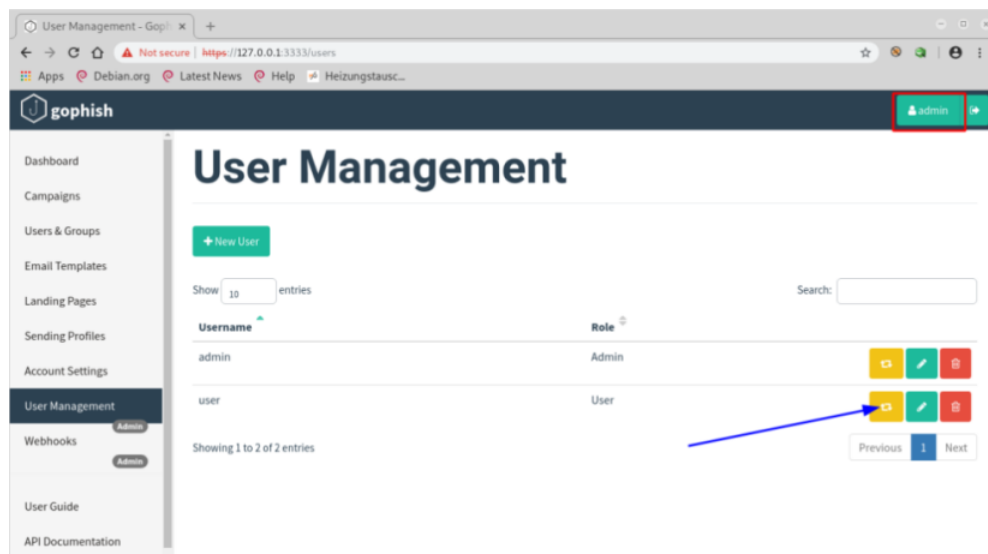
The new sending profile form's "Host" input field is vulnerable to XSS. The payload executes when sending a test email. The XSS gets stored when saving the profile. A rogue user could exploit an admin by asking him to impersonate him and test his broken sending profile.

## Proof of Concept (PoC)

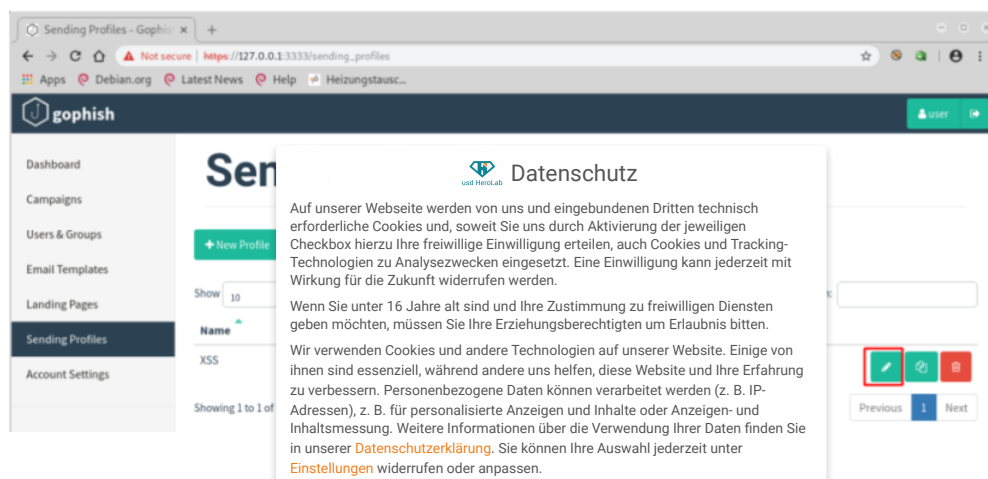
The rogue user injects an XSS payload into a new Sending Profile (/sending\_profiles). By saving the Sending Profile, also the injected XSS payload gets stored. The rogue user then requests assistance from an admin user to check out his "broken" sending profile.



The admin user impersonates the user that he wants to assist



The admin user edits the user's Sending Profile





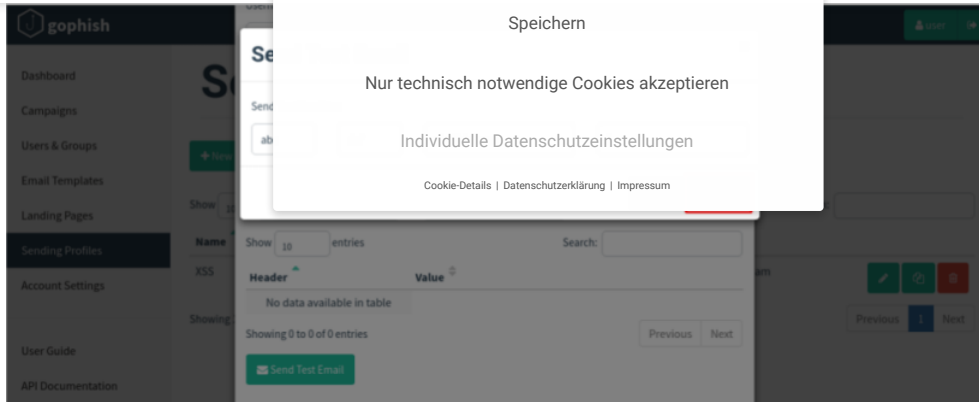
Alle akzeptieren

Speichern

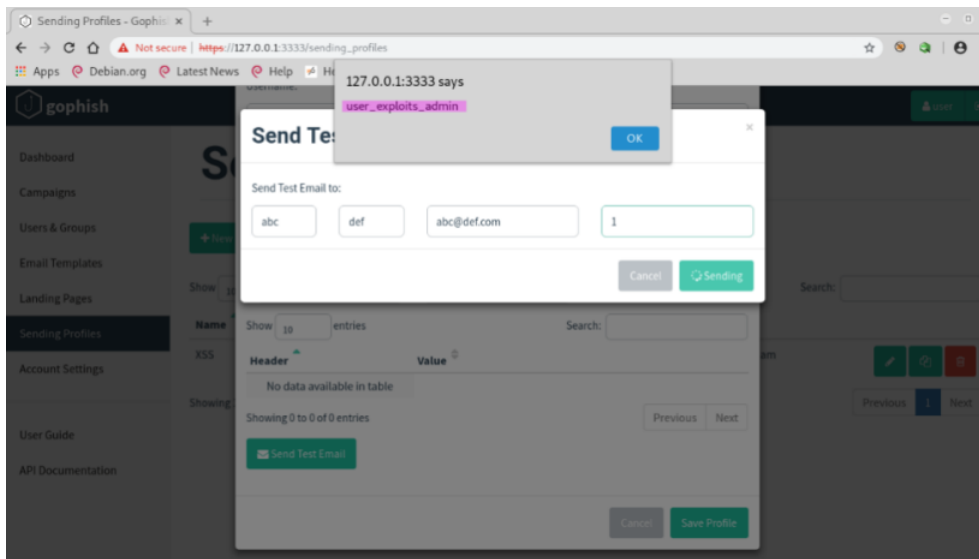
Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)



The XSS payload executes in the admin user's browser



## Fix

It is recommended to treat all input on the website as potentially dangerous. Hence, all output that is dynamically generated based on user-controlled data should be encoded according to its context. The majority of programming languages support standard procedures for encoding meta characters. For example, PHP has the built-in function `htmlspecialchars()`.

Additionally, all input should be validated on the server-side. Where possible, whitelist filters should be used. The more restrictive a filter can be specified, the better the protection it provides. Whitelisting is especially recommended if input values have a well defined format or a list of valid input values exists. Invalid values should not be sanitized and forwarded to the application. Instead, requests with invalid values should be rejected.

## Timeline

- 2020-06-18 First contact request via [security@getgophish.com](mailto:security@getgophish.com)
- 2020-06-22 Vendor responds to initial contact
- 2020-08-07 Vendor publishes a fix on <https://github.com/gophish/gophish/commit/90fed5a575628b89eaf941e1627b49e0f3693812>
- 2020-09-29 Security advisory released

## Credits

This security vulnerabilities were found



### Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technische erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse Zwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



usd HeroLab

☒ Technisch erforderlich

☐ Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)



In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our **CST Academy** and our **usd HeroLab** are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the **usd HeroLab** publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security.“

to usd AG

In accordance with usd AG's **Responsible Disclosure Policy**, all vendors have been notified of the existence of these vulnerabilities.

## Disclaimer

The information provided in this security advisory is provided „as is“ and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.

[usd AG](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz](#)

[AGB](#)

© 2022 usd AG

[Meldung einer Schwachstelle oder eines Bugs](#)

[Code of Ethics](#)



[LabNews](#)

[Security Advisory zu GitLab](#)

**Dez 15, 2022**

[Security Advisory zu Acronis Cyber Protect](#)

**Nov 9, 2022**

[Security Advisories zu Apache Tomcat](#)

**Nov 24, 2022**