



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](#)

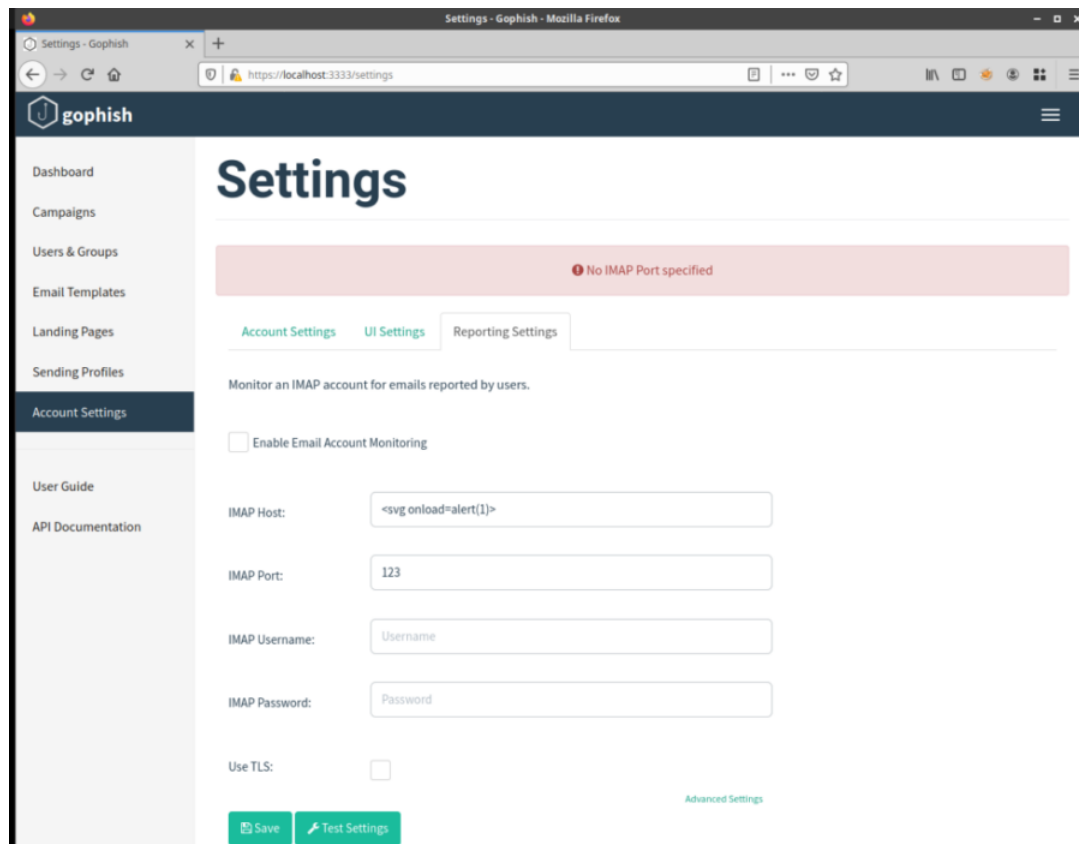
**Advisory ID:** usd-2020-0050  
**CVE Number:** CVE-2020-24712  
**Affected Product:** Gophish  
**Affected Version:** v0.10.1  
**Vulnerability Type:** non-persistent self-XSS  
**Security Risk:** Low  
**Vendor URL:** <https://getgophish.com/>  
**Vendor Status:** Fixed

## Description

The "IMAP Host" input field is vulnerable to Self-XSS when combined with pressing the "Test Settings" button. It was however not possible during the pentest to save an XSS payload with a "Reporting Settings".

## Proof of Concept (PoC)

Visit /settings and enter an XSS payload as „IMAP Host“



Press „Test Settings“ and observe that the JavaScript is executed



## 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](#)

**Failed!**

Unable to login to

More Info

Close

## 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
- 2020-07-18 Vendor fixes vulnerability <https://github.com/gophish/gophish/commit/4e9b94b641755f359542b246cc0c555fa3bc6715>
- 2020-09-29 Security advisory released

## Credits

This security vulnerability was found by Marcus Nilsson of usd AG.

## About usd Security Advisories



In order to protect businesses against security risks, it is important for our work as is building up a strong security culture. Individuals take on the task.

Our CST Academy and our usd HeroLab are important for our work as is building up a strong security culture through training courses and publications.

Always for the sake of our mission: „Protect your data“

to usd AG



## 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 [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.

late. Thus, security research is just as important as security can only be achieved if many

in our practical work and our research on security vulnerabilities and current security issues.



## Disclaimer

The information provided in this security advisory may be updated in order to provide as accurate information as possible.

The information provided in this security advisory may be updated in order to provide as accurate information as possible.

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

[HeroLabs](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz](#)

[AGB](#)

© 2022 HeroLabs 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