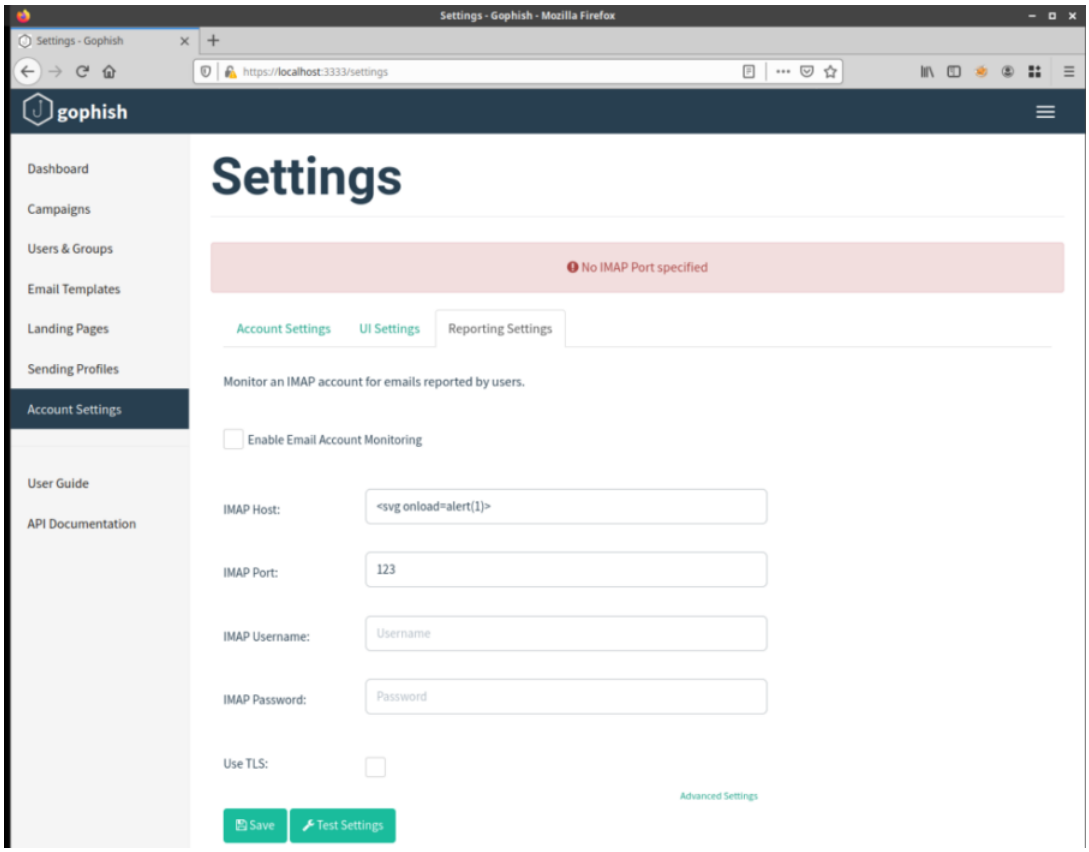
**Advisory ID**: usd-2020-0050
**CVE Number**: CVE-2020-24712
**Affected Product**: Gophish
**Affected Version**: v0.10.1
**Vulnerability Type**: non-persistent self
**Security Risk**: Low
**Vendor URL**: https://getgophish.com/
**Vendor Status**: Fixed

## Description

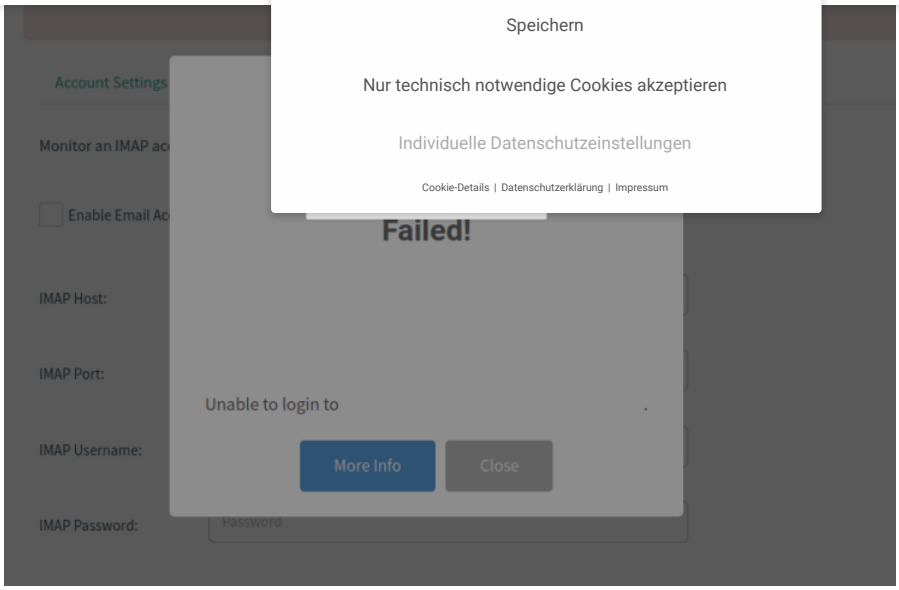
The "IMAP Host" input field is vulnerable to Self-XSS when combined with pressing the "Test Settings" button. It was however not possible during the pentest to save an XSS payload with a "Reporting Settings".

## Proof of Concept (PoC)

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




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




## 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
- 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 ... late. Thus, security research is just as important for our work as is building u... security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLa... in our practical work and our research through training courses and publicati... abilities and current security issues.

Always for the sake of our mission: „m...

to usd AG

## Disclaimer

The information provided in this securi ecurity advisory may be updated in order to provide as accurate informati



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