SOWA.OPAC Reflected Cross Site Scripting

From: hacker () marekholka pl
Date: Tue, 17 Nov 2020 22:06:04 +0100

```
# Title: SOWA.OPAC Reflected Cross Site Scripting
# Vulnerability
Type: Cross Site Scripting (XSS)
# Attack Type: Account Hijacking,
Credential Theft, Data Leakage
# Author: Marek Holka
# Date:
2020-11-08
# Vendor: SOKRATES-software
# Software Link:
https://www.demo.sowwwa.pl/sowacgi.php
# Version: SOWA.OPAC all versions
up to 5.6.2
# CVE: CVE-2020-28350
# Description: A Cross Site Scripting
(XSS) vulnerability exists in Sokrates SOWA
SowaSQL via the sowacgi.php
"typ" parameter which means that this parameter did not sanitize HTML
characters. The module
SOWA.WWW was fixed in 4.8.16, whereas the module
SOWA.OPAC was fixed
in 5.6.2.
# Attack Vectors: To use this
vulnerability victim needs to open crafted URL which inject a Javascript
code to url parameter
"typ":
https://www.demo.sowwwa.pl/sowacgi.php?KatID=0&typ=test%3C/script%3E%3Cscript%3Ealert(document.domain)%3C/script%3E
#
Reference OWASP top 10: https://owasp.org/www-community/attacks/xss/
```

```
_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

- **SOWA.OPAC Reflected Cross Site Scripting** *hacker (Nov 18)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License