

Nagios 5.6.11 XSS'd

The image shows a web browser window with the URL https://www.nagios.org/downloads/nagios-xi/vmware/vm7/product. The page header features the Nagios logo and the tagline "The industry standard in IT Infrastructure Monitoring". Below the header, there is a blue banner with the text "Nagios XI 5.6.11-64.ova". A download dialog box is open, titled "Otwieranie nagiosxi-5.6.11-64.ova". It shows the file name "nagiosxi-5.6.11-64.ova" with a file icon, the type "Open Virtualization Format Archive (1,8 GB)", and the address "https://assets.nagios.com". Under the section "Po ukończeniu pobierania:", there are three options: "Otwórz za pomocą VirtualBox Manager (domyślny)", "Zapisz plik" (which is selected with a radio button), and "Pamiętaj tę decyzję dla wszystkich plików tego typu". At the bottom right of the dialog are "OK" and "Anuluj" buttons.

Below you'll find few XSS bugs found for latest Nagios XI (5.6.11). All of them are available for admin user logged-in (so, those are postauth xss bugs). For example:

[illegible][illegible]

The screenshot shows a web browser window with the address bar displaying '760.168.276.53/ldapimportusers/importusers.php'. The page title is 'LDAP / Active Directory Import Users'. The main content area contains a form with the following elements:

- A text input field labeled 'username' containing the value 'jdoe'.
- A text input field labeled 'password'.
- A 'confirm' button.
- Below the form, there are two links: 'add' and 'add all'.

The 'add' link is highlighted with a red box. The 'add all' link is also visible below it.

```

700 }
701
702 // Show us the user
703 Show = false
704 $this->loadModel('User', $this->loadModel('Connection', $connection) => $this->getConnection(), $connection);
705 $? ($this->loadModel()
706     $url = $url;
707
708
709
710 // Once we've checked their details, kick back their admin info if we have it

```

[illegible]

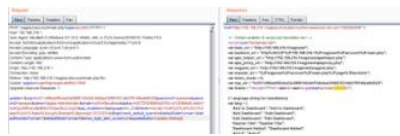
Cody Sixteen

Wyświetl mój pełny profil

► **2022** (16)

- ▶ 02 (6)
- ▶ 01 (7)
- ▶ 2019 (97)
- ▶ 2018 (67)
- ▶ 2017 (58)
- ▶ 2016 (63)

.net
android
binary
crackme
ctf
debug
docker
drones
enll
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc



Hope you'll find it usefull.

More cases (for CVE lovers.):

- 01
- 02
- 03

See you next time!

Cheers

Posted by [code16](#) at 15:28



Labels: [debug](#), [infrastructure](#), [notes](#), [pentest](#), [web](#), [writeup](#)

Brak komentarzy:

Prześlij komentarz



Wpisz komentarz



[Nowszy post](#)

[Strona główna](#)

[Starszy post](#)

Subskrybuj: [Komentarze do posta \(Atom\)](#)

pwn
RE
web
writeup