

Security Assessment Report - Red Hat

Questa analisi di sicurezza è stata condotta utilizzando tecniche di **Google Dorking** per identificare potenziali esposizioni informative nell'infrastruttura web di **Red Hat (redhat.com)**. Il report documenta le vulnerabilità e le informazioni sensibili accessibili pubblicamente attraverso i motori di ricerca, seguendo una metodologia strutturata di information gathering.

1. Comando: **site:redhat.com**

La ricerca generale sul dominio ha permesso di mappare l'ampia superficie pubblica dell'infrastruttura Red Hat. Questo comando è stato fondamentale per identificare tutti i sottodomini, portali aziendali, servizi pubblici e risorse indicizzate dal motore di ricerca. I risultati hanno fornito una panoramica completa dell'ecosistema digitale di Red Hat accessibile pubblicamente.

site:redhat.com

X |

AI Mode **Tutti** Immagini Video Video brevi Libri Web Altro Strumenti

Promozione Google

[Prova la Google Search Console](#)
www.google.com/webmasters/
Sei il proprietario di **redhat.com**? Ottieni dettagli di indicizzazione e ranking da Google.

 **Red Hat Developer**
<https://developers.redhat.com> > ... · [Traduci questa pagina](#) ::

Red Hat Developer
Explore developer resources and tools that help you build, deliver, and manage innovative cloud-native apps and services.

 **Red Hat Customer Portal**
<https://access.redhat.com> · [Traduci questa pagina](#) ::

Red Hat Customer Portal - Access to 24x7 support and ...
Access Red Hat's knowledge, guidance, and support through your subscription. Log in or register.
What can we help you find? Search. Red Hat OpenShift 4.20 is ...

 **Red Hat Research**
<https://research.redhat.com> · [Traduci questa pagina](#) ::

Red Hat Research | Bringing great research ideas to open ...
Red Hat Research connects Red Hat engineers with professors, researchers, and students to bring great research ideas into open source communities. Our ...

 **Red Hat Ecosystem Catalog**
<https://catalog.redhat.com> · [Traduci questa pagina](#) ::

Red Hat Ecosystem Catalog: Home
The Red Hat Ecosystem Catalog is the official source for discovering and learning more about the Red Hat Ecosystem of both Red Hat and certified third-party ...

2. Comando: **inurl:redhat.com**

Questa query ha consentito di identificare specifici percorsi e strutture URL all'interno del dominio. È stato particolarmente utile per mappare i principali punti di accesso, portali di servizio, aree di registrazione e documentazione. La ricerca ha rivelato la presenza di molteplici interfacce utente e punti di ingresso ai servizi Red Hat.

The screenshot shows a search results page with the query "inurl:redhat.com". The results include:

- Create a Red Hat Login**
Create a Red Hat Login. A Red Hat account gives you access to product evaluations, purchasing capabilities and knowledge management content.
Red Hat Customer Portal
https://access.redhat.com · Traduci questa pagina
- Red Hat Customer Portal - Access to 24x7 support and ...**
Access Red Hat's knowledge, guidance, and support through your subscription. Log in or register.
What can we help you find ...
- Contatti per la formazione**
Tutte le informazioni per contattare Red Hat Services e per saperne di più sulla formazione, le certificazioni, i corsi e gli esami disponibili nella tua ...
Red Hat Customer Portal
https://access.redhat.com › services › contact-us · Traduci questa pagina
- Software & Download Center | Red Hat Customer Portal**
Product Downloads, Infrastructure Management, Cloud Computing, Storage, Runtimes, Integration and Automation, Mobile
Red Hat Products and Documentation

3. Comando: **inurl:login site:redhat.com**

La ricerca specifica sulle pagine di login ha identificato portali di autenticazione distribuiti su diversi sottodomini. Questa query ha rivelato i principali **entry point** per l'accesso a sistemi sensibili, incluse piattaforme container e portali partner.

site:redhat.com inurl:login

Click on the Login button and enter **piranha** for the Username and the administrative password you created in the Password field. The Piranha Configuration Tool ...

Red Hat
<https://services.redhat.com> > lo... · Traduci questa pagina · :

Login | PSA - Red Hat

To access this page, you have to log in to PSA. Username. Log In with a Different Username. Password. Remember me. Forgot Your Password?

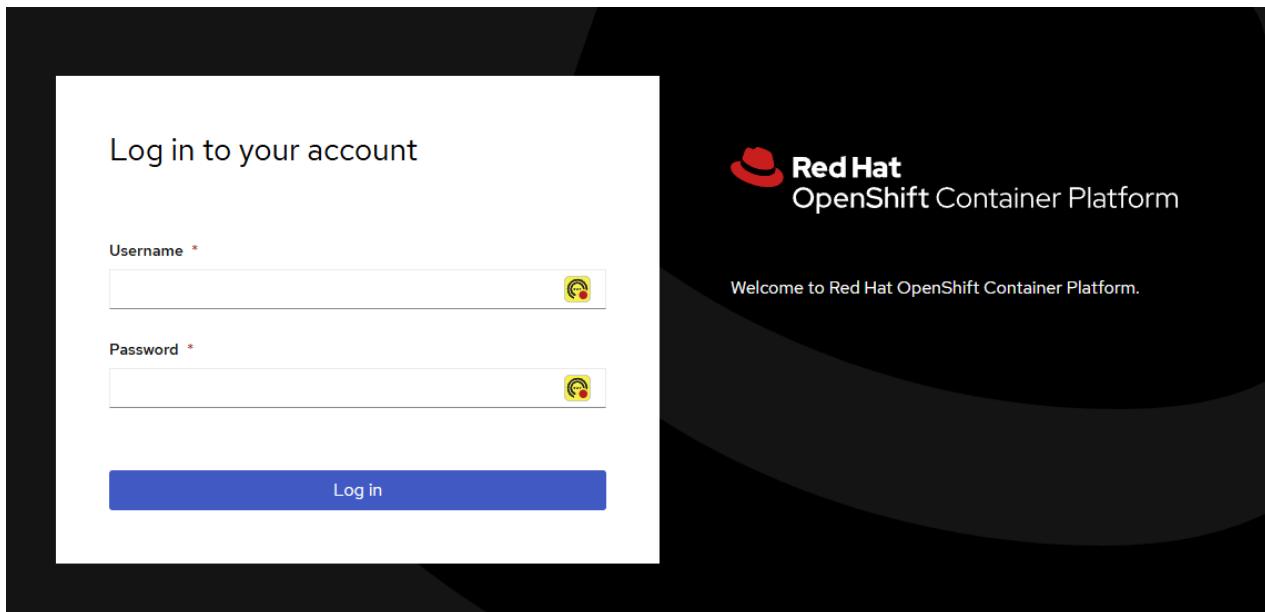
Red Hat
<https://oauth-openshift.apps.ap46r.prod.ole.redhat.com> > ... · Traduci questa pagina · :

Login - Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform logo. Log in to your account. Username *. Password *. Log in. Welcome to Red Hat OpenShift Container Platform.

3.1 Interfaccia Login - OpenShift Container Platform

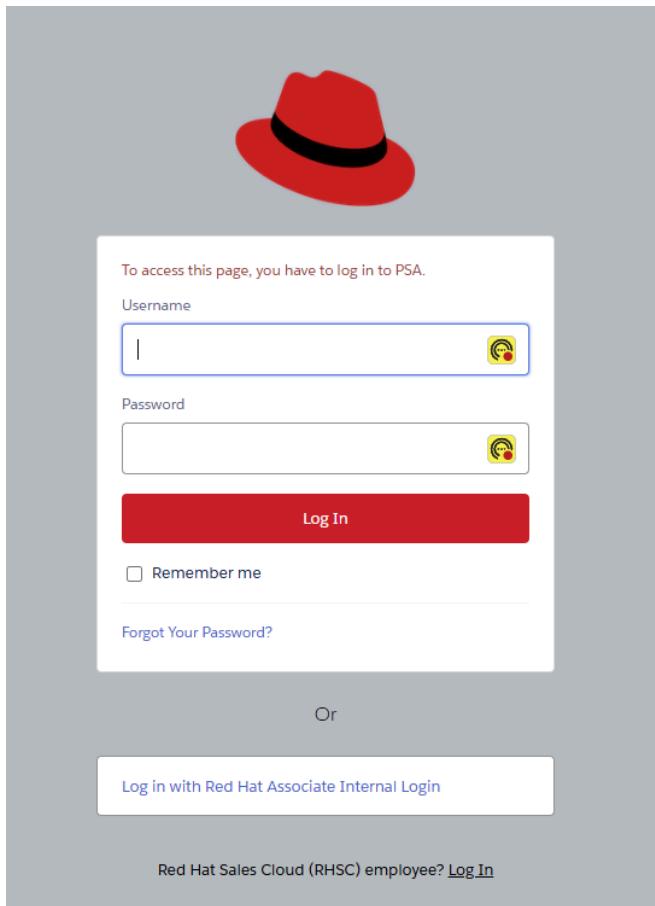
È stata identificata l'interfaccia di autenticazione della **Red Hat OpenShift Container Platform** ospitata su **oauth-openshift.apps.ap46r.prod.ole.redhat.com**. L'interfaccia richiede username e password standard per l'accesso alla piattaforma container di produzione.



3.2 Interfaccia Login - PSA

Il portale PSA su **services.redhat.com** richiede autenticazione obbligatoria con il messaggio "To access this page, you have to log in to PSA". L'interfaccia offre login standard e

accesso alternativo tramite **Red Hat Associate Internal Login**. È anche presente un riferimento specifico per dipendenti Red Hat Sales Cloud.



4. Comando: **intext:admin site:redhat.com**

La ricerca di riferimenti testuali ad **admin** ha identificato documentazione estesa relativa ai pannelli amministrativi. Sono emerse guide per Admin Portal di **Red Hat 3scale API Management** (versioni multiple: 2.7, 2.16, 2.15), documentazione su **Admin Console Access Control and Permissions**, e **Server Administration Guide**.

intext:admin site:redhat.com



 Red Hat Documentation
<https://docs.redhat.com> > documentation > html > admin... ::

Admin Portal Guide | Red Hat 3scale API Management | 2.7

Forniamo soluzioni consolidate che rendono più semplice per le aziende lavorare su piattaforme e ambienti diversi, dal datacenter centrale all'edge della rete.

 Red Hat Documentation
<https://docs.redhat.com> > html · Traduci questa pagina ::

Chapter 11. Admin Console Access Control and Permissions

Users with the admin role are super users and have full access to manage any realm on the server.
Users with the create-realm role are allowed to create new ...

 Red Hat Documentation
<https://docs.redhat.com> > html · Traduci questa pagina ::

Chapter 3. Admin Console | Server Administration Guide

It is the highest level in the hierarchy of realms. Admin accounts in this realm have permissions to view and manage any other realm created on the server ...

 Red Hat Documentation
<https://docs.redhat.com> > documentation > html > admin... ::

Admin Portal Guide | Red Hat 3scale API Management | 2.16

Forniamo soluzioni consolidate che rendono più semplice per le aziende lavorare su piattaforme e ambienti diversi, dal datacenter centrale all'edge della rete.

 Red Hat Documentation
<https://docs.redhat.com> > documentation > html > admin... ::

Admin Portal Guide | Red Hat 3scale API Management | 2.15

Forniamo soluzioni consolidate che rendono più semplice per le aziende lavorare su piattaforme e ambienti diversi, dal datacenter centrale all'edge della rete.

5. Comando: filetype:txt site:redhat.com

La ricerca di file di testo ha identificato il file **robots.txt** pubblicamente accessibile. Questo file espone una mappa dettagliata dell'architettura applicativa con estesi percorsi disallowed per i crawler.

filetype:txt site:redhat.com



Al Mode Tutti Immagini Video Video brevi Libri Web Altro · Strumenti ·

 Red Hat
<https://www.redhat.com> > robots · Traduci questa pagina ::

robots.txt

*Al fine di visualizzare i risultati più pertinenti, sono state omesse alcune voci molto simili alle 1 già visualizzate.
Se vuoi, puoi ripetere la ricerca includendo i risultati omessi.*

5.1 Analisi Dettagliata robots.txt

Il file **robots.txt** rivela una struttura applicativa complessa. I file disallowed includono numerosi **README** di componenti (composer, plugin, template, modules, themes) e web.config. Particolarmente rilevanti sono i percorsi backend PHP esplicativi come [/index.php/admin/](#), [/index.php/user/*](#) e altri endpoint applicativi. Sebbene disallowed per i crawler, questi percorsi rimangono tecnicamente accessibili e forniscono intelligence sulla struttura del sistema.

```
# Files
Disallow: /README.md
Disallow: /composer/Metapackage/README.txt
Disallow: /composer/Plugin/ProjectMessage/README.md
Disallow: /composer/Plugin/Scaffold/README.md
Disallow: /composer/Plugin/VendorHardening/README.txt
Disallow: /composer/Template/README.txt
Disallow: /modules/README.txt
Disallow: /sites/README.txt
Disallow: /themes/README.txt
Disallow: /web.config
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register
Disallow: /user/password
Disallow: /user/login
Disallow: /user/logout
Disallow: /media/oembed
Disallow: /*/media/oembed
# Paths (no clean URLs)
Disallow: /index.php/admin/
Disallow: /index.php/comment/reply/
Disallow: /index.php/filter/tips
Disallow: /index.php/node/add/
Disallow: /index.php/search/
Disallow: /index.php/user/password
Disallow: /index.php/user/register
Disallow: /index.php/user/login
Disallow: /index.php/user/logout
Disallow: /index.php/media/oembed
Disallow: /index.php/*/media/oembed
```

6. Comando: intitle:"Index of" + site:redhat.com

Questa query ha rivelato l'esposizione critica di directory listing.



redhat.com

<https://download1.fedoraproject.org> ... · Traduci questa pagina · :

[Index of /pub/archive/epel/7/x86_64/Packages/n](#)

Note: The Fedora releases here are no longer supported or maintained, so they do not receive bug fixes or security updates. We do not recommend using these ...



Red Hat

<https://people.redhat.com> > lib... · Traduci questa pagina · :

[Index of /jdenemar/libvirt/7.0](#)

[Index of /jdenemar/libvirt/7.0](#) ; [], [libvirt-login-shell-1.2.8-11.el7ost.x86_64.rpm](#), 2015-01-12 13:52 ; [], [libvirt-python-1.2.8-6.el7ost.src.rpm](#), 2015-01-12 13 ...



Red Hat

<https://ftp.redhat.com> > redhat · Traduci questa pagina · :

[Index of /redhat/linux/enterprise/8/Base/en/RHOSE/SRPMS](#)

[Index of /redhat/linux/enterprise/8/Base/en/RHOSE/SRPMS](#) ; [], [NetworkManager-1.26.0-14.1.rhaos4.7.el8.src.rpm](#), 2021-03-18 12:51 ; [], [NetworkManager-1.30.0-16](#).



Red Hat

<https://people.redhat.com> > pos... · Traduci questa pagina · :

[Index of /jdenemar/libvirt/postcopy](#)

[Index of /jdenemar/libvirt/postcopy](#) ; [], [libvirt-lock-sanlock-1.3.1-1.fc23.x86_64.rpm](#), 2016-01-07 09:21 ; [], [libvirt-login-shell-1.3.1-1.fc23.x86_64.rpm](#), 2016 ...

6.1 Root Directory Exposure

L'esposizione della directory root rappresenta una vulnerabilità da mitigare. La pagina "*Index of /*" mostra tre directory principali: **pub/**, **redhat/** e **suse/**. Questa esposizione fornisce una mappa completa della struttura delle directory pubbliche del server.

Index of /

Name	Last modified	Size
pub/	2025-06-23 14:10	-
redhat/	2025-06-13 14:07	-
suse/	2019-09-10 10:22	-

6.2 Public Repository Structure

La directory `/pub/redhat` espone una struttura estesa di sottodirectory per prodotti Red Hat.

Index of /pub/redhat

- [Parent Directory](#)
- [3scale/](#)
- [brms/](#)
- [cdk/](#)
- [client-tools/](#)
- [containers/](#)
- [convert2rhel/](#)
- [dst2007/](#)
- [gnupro/](#)
- [hibernate/](#)
- [jbcp/](#)
- [jbfs/](#)
- [jbmm/](#)
- [jboss-a-mq/](#)
- [jboss-fis/](#)
- [jboss-fuse-ide/](#)
- [jboss-fuse/](#)
- [jboss/](#)
- [jdg/](#)
- [ldapsdk/](#)
- [linux/](#)
- [metamatrix/](#)
- [middleware/](#)
- [mirror-tools/](#)
- [openshift/](#)
- [rhceph-ubuntu/](#)
- [rhceph/](#)
- [rhdevstudio/](#)
- [rhel/](#)
- [rhelatomichost/](#)
- [rhev-m/](#)
- [rhev-power/](#)
- [rhoar/](#)
- [rhscl/](#)
- [satellite/](#)
- [supplementary/](#)
- [support/](#)
- [thincrust/](#)
- [unifiedpush/](#)

Valutazione della Sicurezza

Vulnerabilità Identificate

- Directory listing abilitato su percorsi critici dell'infrastruttura.
- Mappa dettagliata dell'architettura esposta tramite robots.txt.
- Molteplici interfacce di login pubblicamente accessibili.
- Documentazione amministrativa che rivela privilegi e architettura dei sistemi.
- Esposizione di percorsi applicativi backend (endpoint PHP).
- Informazioni pubbliche standard sui portali aziendali.

Raccomandazioni

Priorità Immediata (Alta)

Disabilitare il **directory listing** su tutti i server web per prevenire l'enumerazione della struttura del file system. Rimuovere o proteggere con autenticazione la directory root e le sottodirectory sensibili. Implementare protezioni aggiuntive sui percorsi esposti dal **robots.txt** oltre al semplice disallow.

Priorità Elevata (Media)

Implementare autenticazione a due fattori su tutte le interfacce di login, particolarmente **OpenShift** e **PSA**. Applicare rate limiting e protezione contro attacchi brute-force sui form di autenticazione.

Priorità Standard (Bassa)

Rivedere la documentazione pubblica per valutare quali informazioni architettoniche devono necessariamente essere pubbliche.

Data Report: 05 Dicembre 2025

Metodologia: Google Dorking / OSINT

Target: redhat.com

Scope: Superfici pubblicamente accessibili e indicizzate