

■ SDV Toolbox - Rapport de Sécurité

Outil:	OWASP Amass
Date:	06/06/2025 à 21:52:44
Cible:	isrp.fr
Opérateur:	SDV Security Team

■ Résultats de la Reconnaissance Amass

■ EXPOSITION ÉLEVÉE

Métrique	Valeur
■ Domaine cible	isrp.fr
■ Sous-domaines découverts	125
■ Adresses IP uniques	46
■ Sous-domaines sensibles	5
■ Niveau d'exposition	ÉLEVÉ

■ SOUS-DOMAINES SENSIBLES DÉTECTÉS

Sous-domaine	Type	Niveau de Risq
emailing.isrp.fr	MAIL	MOYEN
preprod.isrp.fr	PROD	ÉLEVÉ
eye.emailing.isrp.fr	MAIL	MOYEN
landings.emailing.isrp.fr	MAIL	MOYEN
click.emailing.isrp.fr	MAIL	MOYEN

■ Analyse des adresses IP :

Adresse IP	Occurrences	Services détectés
95.128.40.112	10	Unknown
52.20.0.0	4	Unknown
217.74.111.248	3	Mail
217.74.96.0	3	Unknown
185.75.140.0	3	Unknown
37.97.64.0	3	Unknown
95.128.40.0	2	Unknown
217.70.187.77	2	Unknown

■ Échantillon des découvertes :

```
isrp.fr (FQDN) --> ns_record --> ns-106-a.gandi.net (FQDN)
isrp.fr (FQDN) --> ns_record --> ns-76-c.gandi.net (FQDN)
isrp.fr (FQDN) --> ns_record --> ns-247-b.gandi.net (FQDN)
```

```
isrp.fr (FQDN) --> a_record --> 95.128.40.112 (IPAddress)
emailing.isrp.fr (FQDN) --> a_record --> 217.74.111.248 (IPAddress)
hub.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
ticketing.isrp.fr (FQDN) --> cname_record -->
b341f0f596d3e617f4e08b003a285807d66999bb6cc7b437e238fc06724f.desk365.io (FQDN)
moodle.isrp.fr (FQDN) --> cname_record --> isrp.fr (FQDN)
extranet.isrp.fr (FQDN) --> cname_record --> isrp.fr (FQDN)
www.hub.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
217.74.96.0/20 (Netblock) --> contains --> 217.74.111.248 (IPAddress)
95.128.40.0/21 (Netblock) --> contains --> 95.128.40.112 (IPAddress)
8399 (ASN) --> managed_by --> SEWAN- (RIROrganization)
8399 (ASN) --> announces --> 217.74.96.0/20 (Netblock)
41653 (ASN) --> managed_by --> AQUARAY (RIROrganization)
41653 (ASN) --> announces --> 95.128.40.0/21 (Netblock)
ns-76-c.gandi.net (FQDN) --> a_record --> 217.70.187.77 (IPAddress)
ns-76-c.gandi.net (FQDN) --> aaaa_record --> 2604:3400:aaac::4d (IPAddress)
ns-247-b.gandi.net (FQDN) --> a_record --> 213.167.230.248 (IPAddress)
ns-247-b.gandi.net (FQDN) --> aaaa_record --> 2001:4b98:aaab::f8 (IPAddress)
www.isrp.fr (FQDN) --> cname_record --> isrp.fr (FQDN)
preprod.isrp.fr (FQDN) --> a_record --> 95.128.40.112 (IPAddress)
www.cnia.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
webredir.gandi.net (FQDN) --> a_record --> 217.70.184.56 (IPAddress)
webredir.gandi.net (FQDN) --> aaaa_record --> 2001:4b98:e01::38 (IPAddress)
www.old.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
marseille.isrp.fr (FQDN) --> a_record --> 95.128.40.112 (IPAddress)
dpc.isrp.fr (FQDN) --> a_record --> 95.128.40.112 (IPAddress)
www.dpc.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
forms.customizedurl.com (FQDN) --> cname_record --> hub06.sarbatech.com (FQDN)
```

... et 96 autres sous-domaines découverts

■ ■ Recommandations de sécurité prioritaires :

- URGENT : Surface d'attaque très étendue détectée
- Auditez immédiatement tous les sous-domaines sensibles (admin, dev, api)
- Désactivez ou sécurisez les sous-domaines non essentiels
- Examinez en priorité les sous-domaines d'administration et de développement
- Considérez l'implémentation d'un WAF pour protéger vos nombreux sous-domaines
- Surveillez régulièrement l'apparition de nouveaux sous-domaines avec des outils de monitoring
- Implémentez des certificats SSL/TLS valides sur tous les sous-domaines exposés
- Configurez une politique de sous-domaines stricte et documentée
- Effectuez des audits périodiques de votre surface d'attaque externe
- Mettez en place des alertes automatiques pour les nouveaux sous-domaines détectés