

# ■ SDV Toolbox - Rapport de Sécurité

Outil:	OWASP Amass
Date:	07/06/2025 à 17:09:17
Cible:	isrp.fr
Opérateur:	SDV Security Team

## ■ Résultats de la Reconnaissance Amass

### ■ EXPOSITION ÉLEVÉE

Métrique	Valeur
■ Domaine cible	isrp.fr
■ Sous-domaines découverts	116
■ Adresses IP uniques	43
■ Sous-domaines sensibles	6
■ Niveau d'exposition	ÉLEVÉ

### ■ SOUS-DOMAINES SENSIBLES DÉTECTÉS

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

### ■ Analyse des adresses IP :

Adresse IP	Occurrences	Services détectés
95.128.40.112	8	Unknown
185.75.140.0	3	Unknown
52.20.0.0	3	Unknown
217.74.96.0	3	Unknown
95.128.40.0	2	Unknown
185.75.141.215	2	Unknown
37.97.66.126	2	Unknown
37.97.64.0	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)
eye.emailing.isrp.fr (FQDN) --> cname_record --> eye.customizedurl.com (FQDN)
eye.customizedurl.com (FQDN) --> cname_record --> hub08.sarbatech.com (FQDN)
hub.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
www.old.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
www.dpc.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
forms.emailing.isrp.fr (FQDN) --> cname_record --> forms.customizedurl.com (FQDN)
www.assistant-medical.isrp.fr (FQDN) --> cname_record --> webredir.gandi.net (FQDN)
alternance-psychomotricite.isrp.fr (FQDN) --> cname_record --> isrp.fr (FQDN)
isrp.fr (FQDN) --> a_record --> 95.128.40.112 (IPAddress)
moodle.isrp.fr (FQDN) --> cname_record --> isrp.fr (FQDN)
master-psychomotricite.isrp.fr (FQDN) --> cname_record --> isrp.fr (FQDN)
dpc.isrp.fr (FQDN) --> a_record --> 95.128.40.112 (IPAddress)
95.128.40.0/21 (Netblock) --> contains --> 95.128.40.112 (IPAddress)
41653 (ASN) --> managed_by --> AQUARAY (RIROrganization)
41653 (ASN) --> announces --> 95.128.40.0/21 (Netblock)
hub08.sarbatech.com (FQDN) --> a_record --> 185.75.141.215 (IPAddress)
hub08.sarbatech.com (FQDN) --> a_record --> 37.97.66.126 (IPAddress)
landings.customizedurl.com (FQDN) --> cname_record --> hub06.sarbatech.com (FQDN)
extranet.isrp.fr (FQDN) --> cname_record --> isrp.fr (FQDN)
cnia.isrp.fr (FQDN) --> a_record --> 95.128.40.112 (IPAddress)
185.75.140.0/22 (Netblock) --> contains --> 185.75.141.215 (IPAddress)
37.97.64.0/19 (Netblock) --> contains --> 37.97.66.126 (IPAddress)
35625 (ASN) --> managed_by --> EURAFIBRE-AS (RIROrganization)
35625 (ASN) --> announces --> 185.75.140.0/22 (Netblock)
8399 (ASN) --> managed_by --> SEWAN- (RIROrganization)
8399 (ASN) --> announces --> 37.97.64.0/19 (Netblock)
ns-247-b.gandi.net (FQDN) --> a_record --> 213.167.230.248 (IPAddress)

```

... et 87 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