



WRITE-UP

Injektion - Web

Alexis GIROMAGNY

HACKY'NOV

Hacky'Nov est une association créée dans le cadre des YDAYS organisés par l'école YNOV qui organise chaque année un CTF afin d'initier le grand public aux différentes problématiques de cybersécurité.

L'événement est organisé par les étudiants du campus YNOV d'Aix-en-Provence et se décompose en trois parties.

La première partie est l'organisation d'un Capture The Flag (CTF). Chaque étudiant, de bachelor 1 à master 2 propose des challenges de cybersécurité, afin que les participants puissent en résoudre le maximum et gagner la compétition ! Les challenges sont axés de sorte que même les débutants puissent en résoudre un maximum tout en sachant faire plaisir aux plus expérimentés

La deuxième partie est dédiée à l'organisation de conférences autour de problématiques et sujets de cybersécurité. Elles sont proposées soit par des étudiants volontaires, soit par des intervenants externes afin de former et de sensibiliser les participants sur des sujets ciblés.

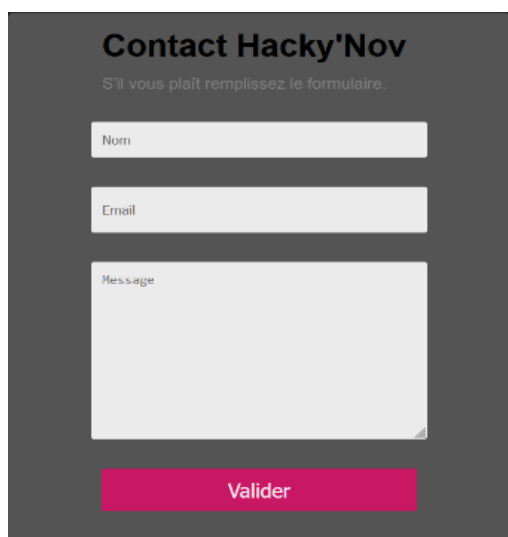
La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants, qui sont pour la plupart, des étudiants en cybersécurité.

<https://hackynov.fr/>

Table des matières

Partie 1 : Présentation du challenge	4
Partie 2 : Sources	4
Partie 3 : Résolution.....	5

Partie 1 : Présentation du challenge



The screenshot shows a web form titled "Contact Hacky'Nov" with the instruction "S'il vous plaît remplissez le formulaire." (Please fill out the form). The form contains three input fields: "Nom" (Name), "Email", and "Message". Below these fields is a red button labeled "Valider" (Validate).

Nom du challenge : Injektion.

Domaine : Web

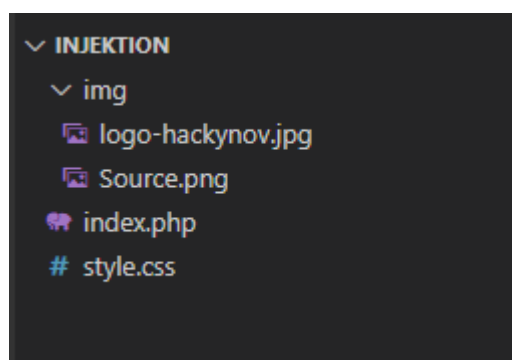
Difficulté ★ ★ ★ ★ ★

Auteur : Alexis GIROMAGNY

Description : Un site internet pour contacter l'équipe de Hacky'Nov vient d'être créée,.

Partie 2 : Sources

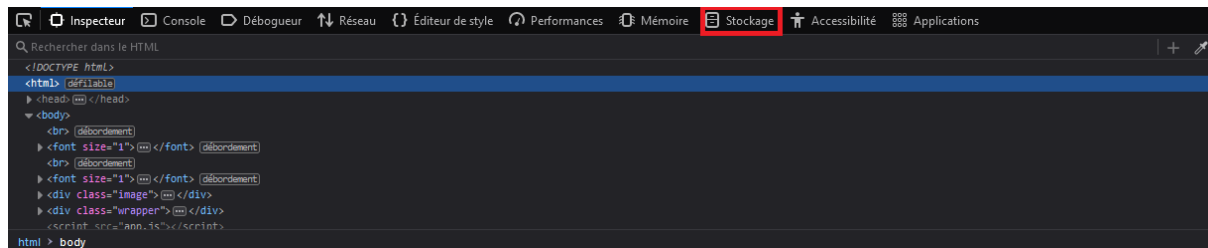
Le challenge comporte les fichiers suivants :



Tous les fichiers du challenge sont disponibles dans le dossier de ce write-up.

Partie 3 : Résolution

Pour résoudre ce challenge, nous allons devoir nous rendre dans l'inspecteur **f12** ou encore cliquer droit inspecteur.



Ensuite, il va falloir cliquer sur **Stockage**, pour ensuite aller dans les **Cookies**.

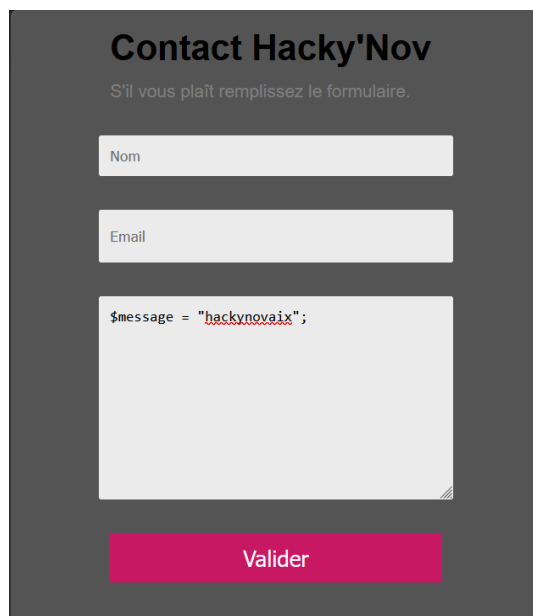
	Nom	Valeur	Domain	Path	Expiration / Durée maximum	Taille
Indexed DB	1n3i6SLG8cn0uuDCmDQr3XS4iaxb69gnwmb7WnP	6543	localhost	/Hacknov%201	Session	44
Stockage de session	1QrawJ074Y2WJj42EPeIUWZ86ZkuaZTM57aRX	4652	localhost	/Hacknov%201	Session	44
Stockage cache	2aYkzIqLHGcQdXIV8De04WjOW9mXNlog3SJaBA	9786	localhost	/Hacknov%201	Session	44
Stockage local	3j5H4JzcNoc8X7ETG77IKVmeOnS6XbnYK04PUB5B	8257	localhost	/Hacknov%201	Session	44
	5YPGu8mwfAmUzrB0cBI88tJID00Lw7MyyPEgVpPE	0115	localhost	/Hacknov%201	Session	44
	6BXoFrAHJOLKlnS9oZF1DvVt5bIF8nNmfWaNiEK	4557	localhost	/Hacknov%201	Session	44
	6jvZBSRw3qtU2hDYN1IN8yShsIRZD9ZrXv4qTMaT	0328	localhost	/Hacknov%201	Session	44
	36pGGQWMNueQg1FoERsmTk8GCCFOKJVLlCuto3Ha	3819	localhost	/Hacknov%201	Session	44

Une fois que vous êtes sur la page des Cookies, il faudra cliquer sur Valeur pour tirer. Vous allez avoir les trois premières lignes avec les valeurs suivantes :

- 1%3D%22hack%22 -> 1= "hack".
- 2%3D%22ynov%22 -> 2="ynov".
- 3%3D%22aix%22 -> 3="aix".

	Nom	Valeur
Indexed DB	L9gnhUrT2kDinxYGOpiYlQd5GUS43ny4ZSgmCeTQ	1%3D%22hack%22
Stockage de session	O3vg3kq7Rn2aLoTgBwXCKcyTpZkbLYOxbfoLLWec	2%3D%22ynov%22
Stockage cache	YoT5x94SCiknhjka4eSQECBI3KJSC8u0NNAeGZOQ	3%3D%22aix%22
Stockage local	5YPGu8mwfAmUzrB0cBI88tJID00Lw7MyyPEgVpPE	0115
	6jvZBSRw3qtU2hDYN1IN8yShsIRZD9ZrXv4qTMaT	0328
	zegMZIVAvFO0tSotm3Vwgi2vNzxN5kkPlv2wYc9T	0329
	oiYXeEpU7nrxn8KEndPdRzVPWqYfFixH3MNwAPEwIE	0437
	M30pp8x4ogNvPwYsw8AuilwDAI4Q0X7SguAe0Bw4	0952

Pour finir, il faudra retourner sur la page principal, vous allez ensuite dans la case des messages pour enfin taper la commande suivante « \$message = "hackynovaix" ; ».



Contact Hacky'Nov

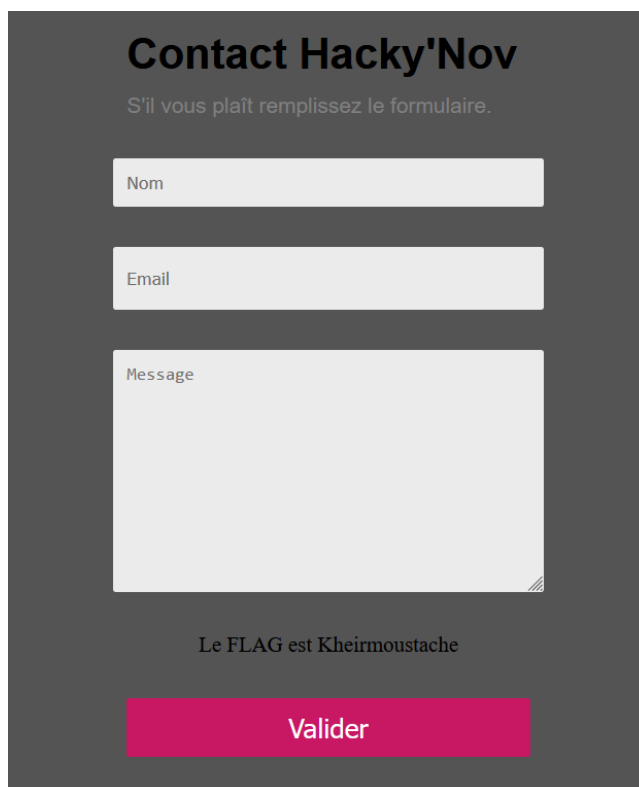
S'il vous plaît remplissez le formulaire.

Nom

Email

`$message = "hackynovaix" ;`

Valider



Contact Hacky'Nov

S'il vous plaît remplissez le formulaire.

Nom

Email

Message

Le FLAG est Kheirmoustache

Valider

Et pour confirmer que vous avez bien réussie le challenge, il affichera un message « Le flag est Kheirmoustache ».

HN0x02{ Kheirmoustache }