Demande n°3193 - ARED

Acronyme :AVF-Deb

Identification

Identification

N°	3193
Année	2023
Statut	Brouillon
Date de création	01/02/2023
Date de modification	01/02/2023
Date de soumission	01/02/2023
Acronyme	AVF-Deb
Intitulé du projet	Automatic vulnerability fixing with debloating
Dispositif	ARED

Priorité régionale

Priorité régionale

Priorité régionale	Cybersécurité

Stratégie régionale de recherche et d’innovation (S3)

Stratégie régionale de recherche et d’innovation (S3)

Domaine d'innovation stratégique	Économie numérique sécurisée et responsable
Levier thématique	Cybersécurité

Organisme de tutelle

Organisme de tutelle

Etablissement	UNIVERSITE BRETAGNE SUD
Commune	LORIENT
Civilité	Madame
Nom	Maffessoli

Prénom	Audrey

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA
Civilité	Monsieur
Nom	Gravier
Prénom	Gullaume
Courriel	dir@irisa.fr

Données complémentaires de l'unité de recherche

Libellé	Valeur
Statut et numéro de l'unité de recherche (UMR, USR, EA?)	UMR 6074
Le cas échéant, nom de l'équipe de recherche	
Le cas échéant, nom du responsable de l'équipe de recherche	
Activités de recherche et points forts de l'équipe	
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Co-directeur de thèse

Civilité	Monsieur
Nom	khelladi
Prénom	Djamel Eddine
Unité de recherche	IRISA
Etablissement de tutelle	CNRS BRETAGNE PAYS LOIRE

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	The goal of the project is to explore the debloating technique for fixing vulnerabilities while also assessing the impact on the original specification and also on the non functional properties other than security, such as test performance or energy consumption of the debloated software.
Porteur du projet : date d'obtention de l'HDR ou dérogation	Octobre 2003
Hypothèses, questions posées, points de blocage, approche méthodologique, technique (4000 car. max)	Description des objectifs et originalité de la thèse When vulnerabilities are identified, applying their fixes may take time. However, for many real-world clients, it is not acceptable to simply keep using the vulnerable code, with its attack surface. We propose to analyze the usage of vulnerable code to help developers to reduce such usage, a process that we refer to as debloating. The principle of debloating is to remove portions of code with the goal of narrowing the attack surface to limit the effects of a vulnerability [1-4]. Debloating can take

	different forms and granularities: from removing a specific function in a single file to removing a high-level functionality spanning different concerns and files.Debloating can have a direct effect here by removing the vulnerable code. Another targeted scenario of debloating is when the vulnerability is not precisely mitigated and understood. For example, vulnerabilities are not yet fixed in a given API. In this case, debloating an API would provide a sub-API that still meets the customers' other functional needs, but with a reduced code and surface attack. Debloating can complicate the task of an attacker and reduce the damage incurred by vulnerable code for two reasons: i) debloating produces a new code variant and attackers have to design specific strategies, ideally for each debloated variant of the code; ii) the attack over the vulnerable code is possible if and only if other parts of the code and entry points can be leveraged: if debloated, some attacks are simply not applicable. Description des principaux verrous et techniques envisagées Beyond the surface attack, one must also ensure that the original functional specification is not impacted entirely, or at least control and identify the impacts so that developers can perform informative decisions on how to use the debloated software. Moreover, the security benefit of debloating can also be coupled with performance benefit. State of the art does not investigate the benefit of debloating on non-functional properties, such as on tests execution in the continuous integration (CI) or the energy consumption of the debloated software. Approche méthodologique et critères de qualité des résultats obtenus We will realize automatic debloating tools operating over source code. The tools will produce debloated versions of applications and libraries that other projects depend on. We plan to leverage databases of vulnerabilities as well as associated patches and tests (based on existing vulnerability databases) to i) guide the debloating strategy (i.e., what to remove in the code); ii) validate and characterize to what extent the system is less vulnerable. Moreover, we will investigate the effect of debloating on test execution in the CI and on the energy consumption of the debloated software variants. We can orient our effort towards 1) libraries and Web applications (e.g., written in JavaScript) and 2) libraries and clients in Java projects on Maven central. We will implement automatic solutions and we will evaluate them with state of the art methods and tools. We will rely on the known use cases of vulnerabilities and their fixes to compare to our debloating solution. For example, the case of Log4shell vulnerability on Log4j will be part of our case studies.
Environnement scientifique, positionnement dans contexte régional/national/international (2000 car.)	
Collaborations scientifiques (nature/partenariat/pays) et partenariat socio-économique envisagé	Résoudre les problèmes liés à la vulnérabilité du code va dans le sens du renforcement de la souveraineté des solutions utilisées. Nous comptons discuter du sujet que nous proposons avec le Dr. Xavier LE Bourdon et Dr. Gurvan LE GUERNIC de la DGA. Nous avons déjà collaboré avec M. Le Bourdon dans le cadre d'une thèse de notre équipe ArchWare, financée par la DGA. Et M. LE GUERNIC est aussi un collaborateur dans l'équipe DiverSE depuis plusieurs années avec qui nous avons discuté à plusieurs reprises du potentiel et l'applicabilité du debloating en génie logiciel.
Adéquation du projet avec le DIS de rattachement (3000 caractères maximum)	
Si priorité régionale, préciser (200 caractères maximum)	
Cotutelle internationale (indiquer "oui" ou "non"; si oui, préciser le pays et l'établissement)	
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	
Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE	
État du cofinancement (indiquer "acquis" ou "demandé")	Co-financement CREACH LABS déjà acuis.
Si demandé, date prévisionnelle de réponse du cofinanceur	
Si cofinancement refusé, autre(s) source(s) de cofinancement identifiée(s)	

Si reversement prévu, préciser (partenaire, montant)	

Candidat

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
01/02/2023	ARED - Dépôt - CV du porteur	Obligatoire - Le CV doit préciser si le porteur est titulaire de l'HDR et, le cas échéant, depuis quand, et mentionner la liste des doctorant·e·s déjà encadré·e·s et des publications associées.	ShortCV_Sadou.pdf	Non traité	
	ARED - Dépôt - Avis directeur·rice d'unité	15 lignes maximum		Non traité	
	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...		Non traité	
	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
01/02/2023	ARED - Dépôt - Pièce complémentaire	Facultatif	CV Short Djamel Khelladi.pdf	Non traité	
	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
	ARED - Instruction - Lettre de saisine	Lettre de l'établissement à transmettre à la Région (utiliser le modèle disponible dans la rubrique "Documents à télécharger")		Non traité	
	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
	ARED - Versement 1/2 - CV doctorant.e	Pour versement tranche 1 (cohortes jusqu'en 2018) Pour versement tranche 2 (cohortes à partir de 2019)		Non traité	
	ARED - Versement 1/2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 1 (cohortes jusqu'en 2018) Pour versement tranche 2 (cohortes à partir de 2019)		Non traité	

	ARED - Versement 1 - Lettre d'approbation école doctorale	Pour versement tranche 1 (cohortes jusqu'en 2018)		Non traité	
	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	
	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3 (à accompagner des pièces justificatives correspondantes pour les cohortes jusqu?en 2018 : avis du jury, attestation de réinscription en ED, justificatif de prolongation ou d'abandon)		Non traité	
	ARED - Versement 4 - Avis du jury si thèse soutenue	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
	ARED - Versement 4 - Attestation de réinscription en ED	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
	ARED - Versement 4 - Justificatif de prolongation	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
	ARED - Versement 4 - Justificatif d'abandon de thèse	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	