セキュリティ・コアャンプ2017参加応募用紙

|  |  |  |  |
| --- | --- | --- | --- |
| ふりがな | 　 | 性別 | * 男　　□　女
 |
| 氏名 | ­ | 生年月日・年齢 | 　　　　　　　　年　　　月　　　日　　　　　歳 |
| 住所 | 〒　　　　　－ |
| 学校名・学部学科名 |  | 学　年 | 　　　　　　　　　　年 |
| 電話番号 |  | Emailアドレス |  |
| セキュリティ・キャンプ（セキュリティ＆プログラミングキャンプ）に参加した年と2015-6年以外は参加したクラスをお答えください。参加年：参加したクラス（2015-6年参加者は除く）： |
| 質問事項　　回答は本用紙に記述いただくか、「別紙参照」として Office（word、excel、powerpoint）互換ファイル、画像ファイル等を添付していただいてもかまいません。 |
| 1 | マルウェア解析は、動的解析や静的解析手法などが存在しますが、それらは手法に過ぎず、実際にはそれぞれの手法のうち簡易にできるものから実施し効率良く解析していくことになります。あなた自身がマルウェア解析をしなければならない状況下であると想定した上で、マルウェア解析手法の調査や既存ツール・環境の調査・比較を行い、マルウェア解析をどのような環境・ツールを用いて、どのような順序で実施すれば効率良くマルウェア解析を進められるか検討し、その検討結果を10,000文字以内で記述してください。なお、調査の結果判明した各種ツール・環境の問題点や制限事項（解析できないマルウェアが存在する、等）およびその解決方法（他のツールなら解決可能であった、等）を忘れずに含めてください。 |
| 回答： |
| 2 | https://secure.example.com/ ドメインを https://sub.example.com/ ドメインのXSS脆弱性を利用することで攻撃できるとき、どのような攻撃が考えられますか。 sub.example.com のXSS脆弱性を介すことではじめて攻撃できるものであれば、 2つのドメインのレスポンス内容は自由に決めて構いません。攻撃の概要、ドメインの前提条件、攻撃方法を以下の例に従って好きなだけ書いてください。 |
| 回答：[攻撃パターン1] (これは回答例です。回答時には削除して、これ以外の回答を記入してください。)▽攻撃の概要: Cookieを介したXSS▽前提条件: secure.example.com上に test という名前のCookieの値を書き出しているページがある。▽攻撃方法: XSSを使って、example.comに対してタグ文字列を含むCookieをつけるための以下のようなスクリプトを実行する。document.cookie="test=<script>alert(1)</script>;domain=example.com;path=/";Cookieを書き出しているページにアクセスしたとき、secure.example.com上でXSSが可能。[攻撃パターン2](以下同様に考えられるだけ増やして構いません。) |
| 3 | セキュリティ・キャンプの講師を担当したらやってみたいテーマを[タイトル]、[概要（200～400字程度）]に分けて書いてください。 |
| 回答：[タイトル][概要] |

■個人情報の取り扱いについて

セキュリティ・キャンプ実施協議会（以下、当会）は、セキュリティ・コアキャンプ2017参加応募において、個人情報保護の重要性を認識し、ご提供いただく個人情報を慎重に取り扱い、プライバシーの保護に努めております。当会では申込者の個人情報を以下の目的に利用し、他の目的では利用しません。また当会以外の第三者には一切開示しません。

(1) 応募者からのイベントの申込み手続きを受付けるため　　(2) 当会に関わるイベント情報などを提供するため

当会に対して個人情報を与えるか否かは、応募者がご判断ください。

個人情報をご提供いただけない場合には、イベントへの参加申込をお受けすることができなくなりますのでご了承ください。

本告知に関する個人情報管理責任者　セキュリティ・キャンプ実施協議会　会長　西本　逸郎　　E-Mail : info@ security-camp.org

※本書に記載の「個人情報の取り扱いについて」に同意された場合のみお申込みください。

※回答が書ききれない場合は他の用紙に記入下さい。書式は問いません。 Emailでの申し込みの場合は、メール本文に必要事項をご記入いただいても構いません。