Gmail **Maurice Lambert <mauricelambert434@gmail.com>**

[Vulnerability] simpletouchsoftware boxingtimerpro

Maurice Lambert <mauricelambert434@gmail.com> 26 octobre 2021 à 20:14
À : contact@chrisbiron.com, amber@simpletouchsoftware.com

Hello,

i am contacting you because i found a **vulnerability** in your *Boxing Timer Pro*.

I am a developer and security researcher, I use your application regularly and yesterday I found a vulnerability in your application. The vulnerability is *Cross-Site-Scripting (XSS) reflected* in the page title. This vulnerability **is very easy to exploit** (example (open this URL in your web browser): https://www.simpletouchsoftware.com/timers/boxingtimerpro/?name=</title><script>alert("Demontration: XSS Reflected... You are hacked !")</script>&rounds=45&prep=56&round=2&warning=25&rest=89).

What about the **severity** of the vulnerability:

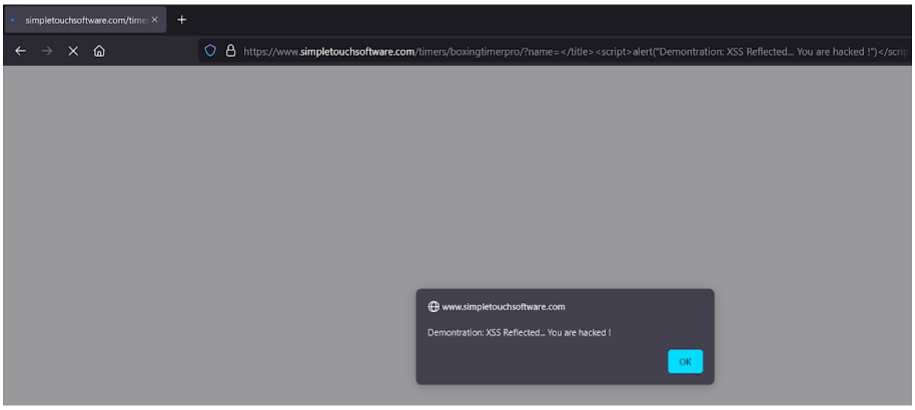
1. **CRITICAL**: If you have an admin page on simpletouchsoftware.com, a hacker can steal your session and use the admin features and permissions on your server.
2. **HIGHT**: If you have an authentication system on simpletouchsoftware.com, a hacker can steal a user session and spoof their account.
3. **MEDIUM**: [no conditions] a hacker can use your website to control your users' web browser. It can exploit a *Cross-Site-Request-Forgery (CSRF) vulnerability* on another website or implement a redirect on a *phishing URL* from your web application (and your users will see your application as an un trusted or malicious website).

Protection against XSS:

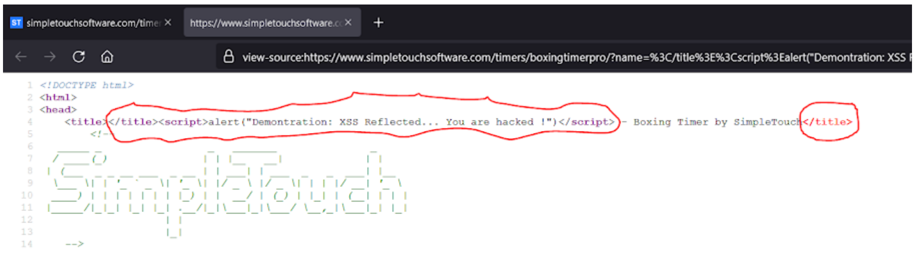
- *PHP*: `<title><?php echo htmlspecialchars($title); ?></title>`
- *NodeJS*: ``const escape = str => str.replace(/&/g, '&amp;').replace(/</g, '&lt;').replace(/>/g, '&gt;').replace(/'/g, "&#x27;").replace(/"/g, '&quot;'); `<title>${escape(title)}</title>` ``
- *Python*: `f"<title>{html.escape(title)}</title>"`

Best regards,
Maurice LAMBERT.

Contact: contact@chrisbiron.com, amber@simpletouchsoftware.com
Date: 2021-10-26


simpletouchsoftware.com/timer
https://www.simpletouchsoftware.com/timers/boxingtimerpro/?name=</title><script>alert("Demontration: XSS Reflected... You are hacked !")</scrip
www.simpletouchsoftware.com
OK

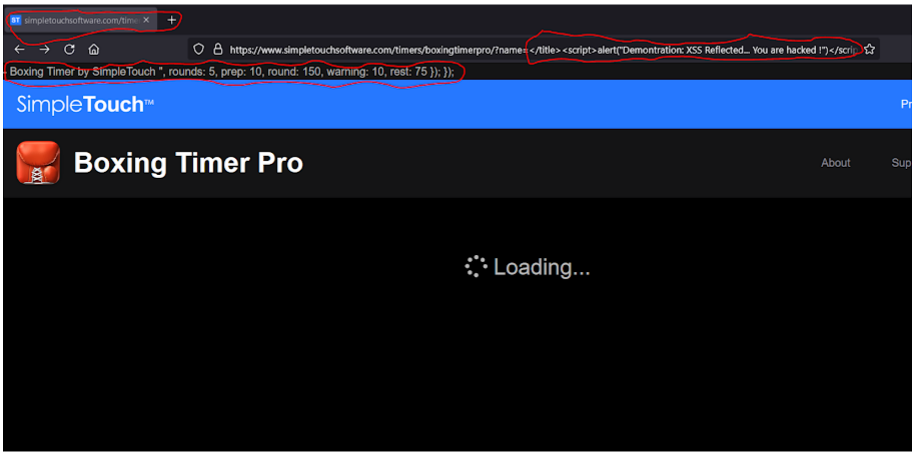
Demontration: XSS Reflected... You are hacked !



simpletouchsoftware.com/timer ×
https://www.simpletouchsoftware.c ×

view-source:https://www.simpletouchsoftware.com/timers/boxingtimerpro/?name=%3C/title%3E%3Cscript%3Ealert("Demontration: XSS

```
<!DOCTYPE html>
<html>
<head>
    <title></title><script>alert("Demontration: XSS Reflected... You are hacked !")</script> - Boxing Timer by SimpleTouch</title>
        <!--
    -->
```



https://www.simpletouchsoftware.com/timers/boxingtimerpro/?name=</title><script>alert("Demontration: XSS Reflected... You are hacked !")</scrip

Boxing Timer by SimpleTouch ", rounds: 5, prep: 10, round: 150, warning: 10, rest: 75 }); });