



DIGITAL TRANSFORMATION SPECIALISTS

# SECURITY TESTING REPORT

<https://stage.sadashrijewelkart.com//>

[www.iiiQbets.com](http://www.iiiQbets.com)

# SECURITY REPORT OF

[HTTPS://STAGE.SADASHRIJEWELKART.COM/](https://stage.sadashrijewelkart.com/)



RINGS

EARRINGS

BRACELETS  
&  
BANGLES

SOLITAIRES

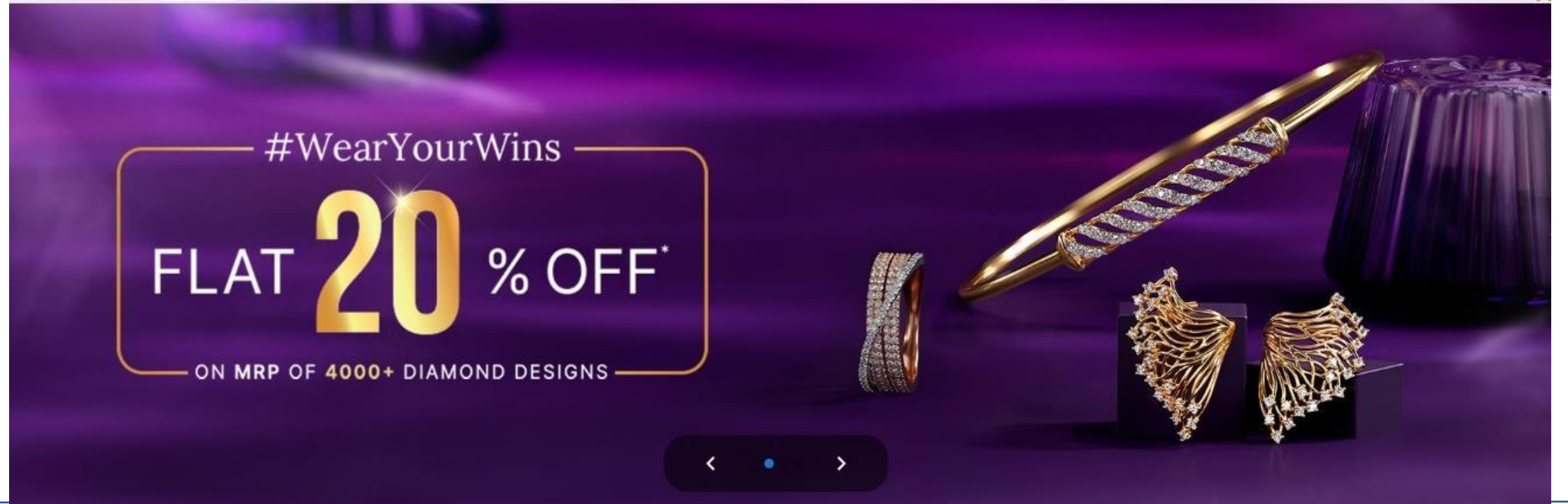
MANGALSUTRAS

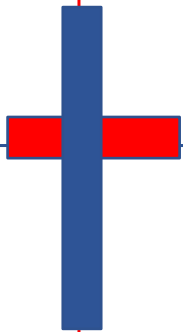
NECKLACES

MORE  
JEWELLERY

GAZAB  
CATEGORY

Search for Jewellery...





# SECURITY REPORT OF HTTPS://STAGE.SADASHRIJEWELKART.COM//

Scan Stats & Info

Vulnerabilities

Site Structure

Events

This scan failed



### Acunetix Threat Level 1




One or more low-severity type vulnerabilities have been discovered by the scanner.

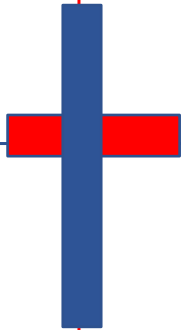
### Activity

Processing

Overall progress

100%

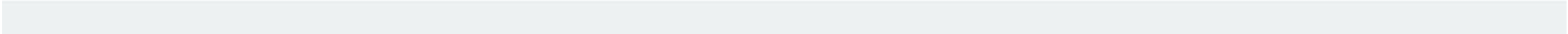
-  Scanning of stage.sadashrijewelkart.com started Oct 7, 2024 4:48:49 PM
-  Scanning of stage.sadashrijewelkart.com was abort... Oct 7, 2024 4:48:56 PM
-  Scanning of stage.sadashrijewelkart.com completed Oct 7, 2024 4:49:15 PM



# SECURITY REPORT OF

## HTTPS://STAGE.SADASHRIJEWELKART.COM/

Scan Duration	Requests	Avg. Response Time	Locations
2m 13s	3,513	104ms	8
Target Information		Latest Alerts	
Address	stage.sadashrijewelkart.com	<div><div>0</div><div>0</div><div>2</div><div>1</div></div>	
Server	Unknown	Clickjacking: X-Frame-Options header missing	Oct 7, 2024 4:38:49 PM
Operating System	Unknown	Content type is not specified	Oct 7, 2024 4:39:09 PM
Identified Technologies	—	OPTIONS method is enabled	Oct 7, 2024 4:39:09 PM
Responsive	Yes		



# SECURITY REPORT OF

[HTTPS://STAGE.SADASHRIJEWELKART.COM//](https://stage.sadashrijewelkart.com//)

```
(kali@kali)-[~]
$ nikto -h 89.117.188.176
- Nikto v2.5.0

+ Target IP:      89.117.188.176
+ Target Hostname: 89.117.188.176
+ Target Port:    80
+ Start Time:     2024-10-07 08:21:00 (GMT-4)

+ Server: LiteSpeed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'platform' found, with contents: hostinger.
+ /: Uncommon header 'panel' found, with contents: hpanel.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /ypoCSpf9.htaccess~: Server may leak inodes via ETags, header found with file /ypoCSpf9.htaccess~, inode: 999, size: 63d7e5b3, mtime: 3fa4519c8b7f9799;;;. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

# SECURITY REPORT OF

**[HTTPS://STAGE.SADASHRIJEWELKART.COM/ /](https://stage.sadashrijewelkart.com/)**

## Scan of <https://stage.sadashrijewelkart.com/>

### Scan details

Scan information	
Start time	07/10/2024, 16:55:42
Start url	<a href="https://stage.sadashrijewelkart.com/">https://stage.sadashrijewelkart.com/</a>
Host	<a href="https://stage.sadashrijewelkart.com/">https://stage.sadashrijewelkart.com/</a>
Scan time	55 seconds
Profile	Full Scan

### Threat level

#### Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

### Alerts distribution

Total alerts found	1
 High	0
 Medium	0
 Low	1
 Informational	0



# SECURITY REPORT OF

[HTTPS://STAGE.SADASHRLJEWELKART.COM/](https://stage.sadashrljewelkart.com/)

## Affected items

Web Server	
Alert group	Clickjacking: X-Frame-Options header missing
Severity	Low
Description	<p>Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.</p> <p>The server didn't return an <b>X-Frame-Options</b> header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.</p>
Recommendations	Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

### Scanned items (coverage report)

---

<https://stage.sadashrijewelkart.com/>

<https://stage.sadashrijewelkart.com/assets>

<https://stage.sadashrijewelkart.com/favicon.ico>

<https://stage.sadashrijewelkart.com/manifest.json>

<https://stage.sadashrijewelkart.com/static>

<https://stage.sadashrijewelkart.com/static/css>

<https://stage.sadashrijewelkart.com/static/css/main.323efbdf.css>

<https://stage.sadashrijewelkart.com/static/js>

<https://stage.sadashrijewelkart.com/static/js/main.9c0367ed.js>





# SECURITY REPORT OF

## [HTTPS://STAGE.SADASHRIJEWELKART.COM//](https://stage.sadashrijewelkart.com/)



jewellery

Mon, 07 Oct 2024 17:48:16 India Standard Time

### TABLE OF CONTENTS

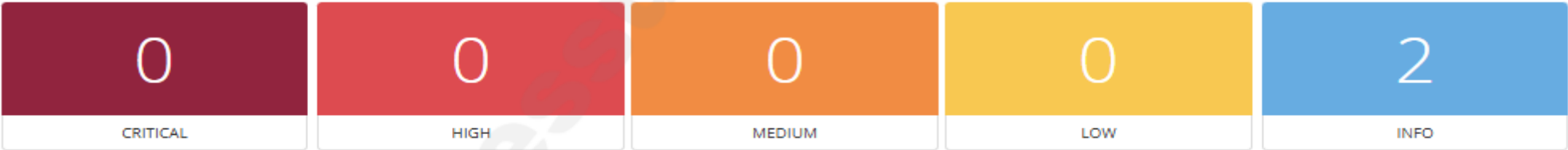
#### Vulnerabilities by Host

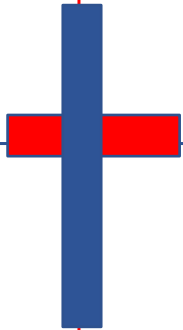
- 89.117.188.176

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

89.117.188.176



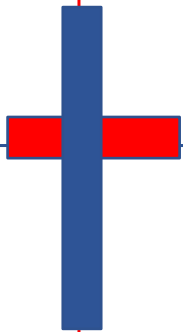


*SECURITY REPORT OF*  
*HTTPS://STAGE.SADASHRIJEWELKART.COM//*



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

\* indicates the v3.0 score was not available;  
the v2.0 score is shown



# SECURITY REPORT OF

## [HTTPS://STAGE.SADASHRIJEWELKART.COM//](https://stage.sadashrijewelkart.com//)

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

---

Protect your target with an IP filter.

### Plugin Details

---

**Severity:** Info

**ID:** 11219

**File Name:** nessus\_syn\_scanner.nbin

**Version:** 1.60

**Type:** remote

**Family:** Port scanners

**Published:** 2/4/2009

**Updated:** 5/20/2024



# SECURITY REPORT OF

## [HTTPS://STAGE.SADASHRIJEWELKART.COM/](https://stage.sadashrijewelkart.com/)

Information

Dependencies

Dependents

Changelog

## Synopsis

This plugin displays information about the Nessus scan.

## Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.

## Plugin Details

**Severity:** Info

**ID:** 19506

**File Name:** scan\_info.nasl

**Version:** 1.127

**Type:** summary

**Agent:** windows, macosx, unix

**Family:** [Settings](#)

**Published:** 8/26/2005

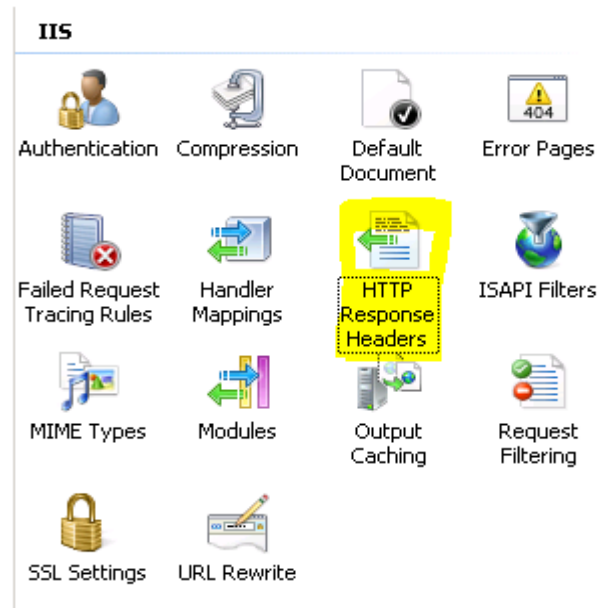
**Updated:** 10/4/2024

**Configuration:** Enable thorough checks

### X FRAME OPTION HEADER TO CONTROL AGAINST CLICKJACKING ATTACK

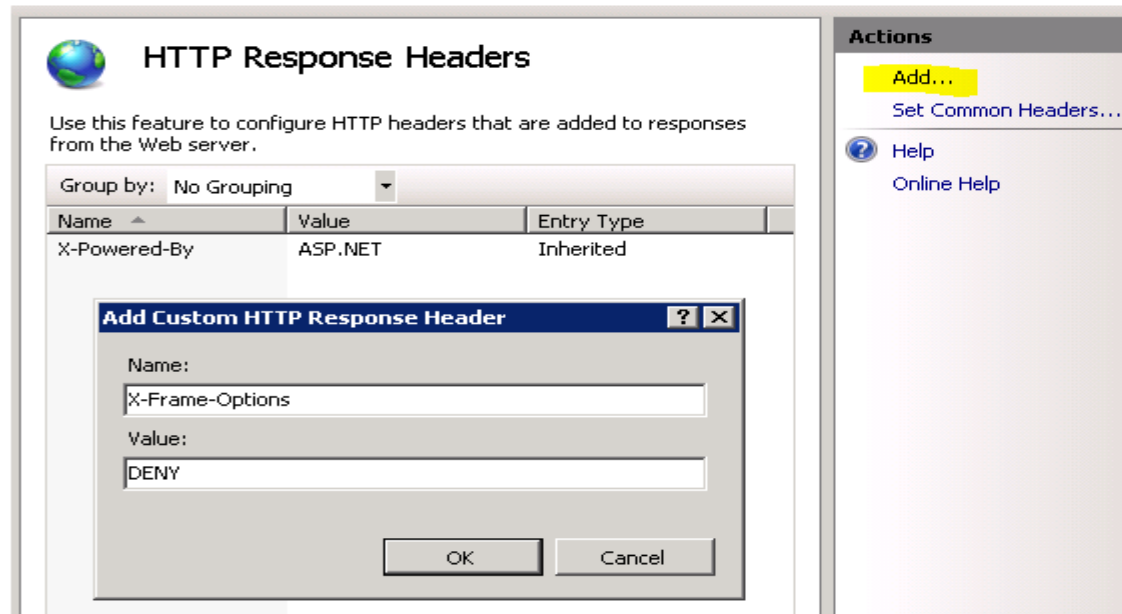
To configure IIS to add an X-Frame-Options header to all responses for a given site, follow these steps:

- Open Internet Information Services (IIS) Manager.
- In the Connections pane on the left side, expand the Sites folder and select the site that you want to protect.
- Double-click the HTTP Response Headers icon in the feature list in the middle



### X FRAME OPTION HEADER TO CONTROL AGAINST CLICKJACKING ATTACK

- In the Actions pane on the right side, click Add.
- In the dialog box that appears, type X-Frame-Options in the Name field and type SAMEORIGIN or DENY in the Value field.





### X FRAME OPTION HEADER TO CONTROL AGAINST CLICKJACKING ATTACK

To configure IIS to send the X-Frame-Options header, add the following code to your site's Web.config file:

```
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <add name="X-Frame-Options" value="SAMEORIGIN" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

```
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <add name="X-Frame-Options" value="SAMEORIGIN" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

# *SECURITY REPORT OF*

***HTTPS://STAGE.SADASHRIJEWELKART.COM//***

THANK YOU

**“The Best Way To Get Started Is To Quit Talking And Begin Doing.”**