Vtop Scan

Report generated by Nessus™ Tue, 24 Oct 2023 21:11:24 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

-
-

Vulnerabilities by Host

115.240.194.17

0	0	0	0	8
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Oct 24 20:26:14 2023

End time: Tue Oct 24 21:11:24 2023

Host Information

IP: 115.240.194.17

OS: Nutanix

Vulnerabilities

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03
a9a
http://www.nessus.org/u?b019c
bdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
  Based on tests of each method
 :

   - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
     BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
     INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
     OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
     RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
 UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

     /
    - Invalid/unknown HTTP methods are allowed on
 :

     /
```

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2015/09/04, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The server supports direct HTTP/2 connections   without encryption.
```

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP KeepAlive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
```

```
Options allowed : (Not implemented) Headers :

  content-length: 0   location: https://115.240.194.17/   cache-control:
no-cache   connection: close   Response Body :
```

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
  Request         : http://115.240.194.17/
```

```
  HTTP response   : HTTP/1.1 302 Found
  Redirect to     : https://115.240.194.17/
  Redirect type   : 30x redirect
```

```
Note that Nessus did not receive a 200 OK response from the last
examined redirect.
```

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.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

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.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

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.
- The number of checks done in parallel.

Solution

---

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

---

tcp/0

```
Information about this scan :

Nessus version : 10.6.0
Nessus build : 20103
Plugin feed version : 202310212203
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : VtopC
```

```
Scan policy used : Web Application Tests
Scanner IP : 192.168.0.134
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 31.756 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5
minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/24 20:26 India Standard Time
Scan duration : 2699 sec
Scan for malware : no
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds to requests for non-existent
URLs with HTTP code 302 rather than 404. The requested URL was :

    http://115.240.194.17/K1QIlbt6fwhs.html
```

122.187.117.185

0	0	0	0	8
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Tue Oct 24 20:26:14 2023
End time:	Tue Oct 24 21:09:53 2023

Host Information

DNS Name:	nsg-corporate-185.117.187.122.airtel.in
IP:	122.187.117.185
OS:	Nutanix

Vulnerabilities

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
  Based on tests of each method
 :

   - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
     CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL
     LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
     ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
     RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
 UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

     /
    - Invalid/unknown HTTP methods are allowed on
 :

     /
```

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2015/09/04, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The server supports direct HTTP/2 connections   without encryption.
```

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP KeepAlive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 302 Found
```

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented) Headers :

  content-length: 0   location: https://122.187.117.185/   cache-
control: no-cache   connection: close   Response Body :
```

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
  Request         : http://nsg-corporate-185.117.187.122.airtel.in/
  HTTP response   : HTTP/1.1 302 Found
  Redirect to     : https://nsg-corporate-185.117.187.122.airtel.in/
  Redirect type   : 30x redirect


Note that Nessus did not receive a 200 OK response from the
last examined redirect.
```

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.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

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.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

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.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.0
Nessus build : 20103
Plugin feed version : 202310212203
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : VtopC
```

```
Scan policy used : Web Application Tests
Scanner IP : 192.168.0.134
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 31.499 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5
minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/24 20:26 India Standard Time
Scan duration : 2609 sec
Scan for malware : no
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds to requests for non-existent
URLs with HTTP code 302 rather than 404. The requested URL was :

    http://nsg-corporate-185
```

The scan for the main website has shown there are only info level vulnerabilities therefore for proper penetration testing we use another website.

Alternate website: http://testphp.vulnweb.com/

1. Cross-Site Scripting (Stored)

CWE: CWE-79

OWASP Category: A03:2021 – Injection

Description: The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Business Impact: The most common attack performed with cross-site scripting involves the disclosure of information stored in user cookies. Typically, a malicious user will craft a client-side script, which -- when parsed by a web browser -- performs some activity (such as sending all site cookies to a given E-mail address). This script will be loaded and run by each user visiting the web site. Since the site requesting to run the script has access to the cookies in question, the malicious script does also.

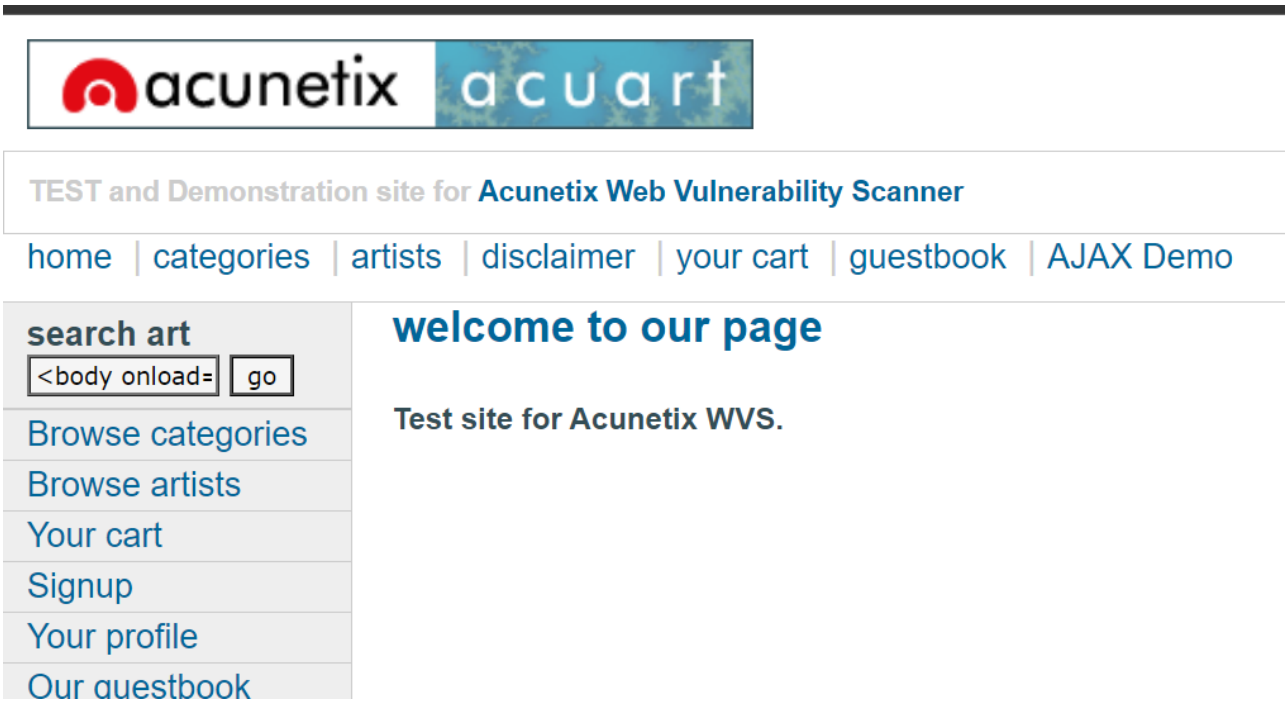
Vulnerability Path : http://testphp.vulnweb.com

Vulnerability Parameter: http://testphp.vulnweb.com/search.php?test=query

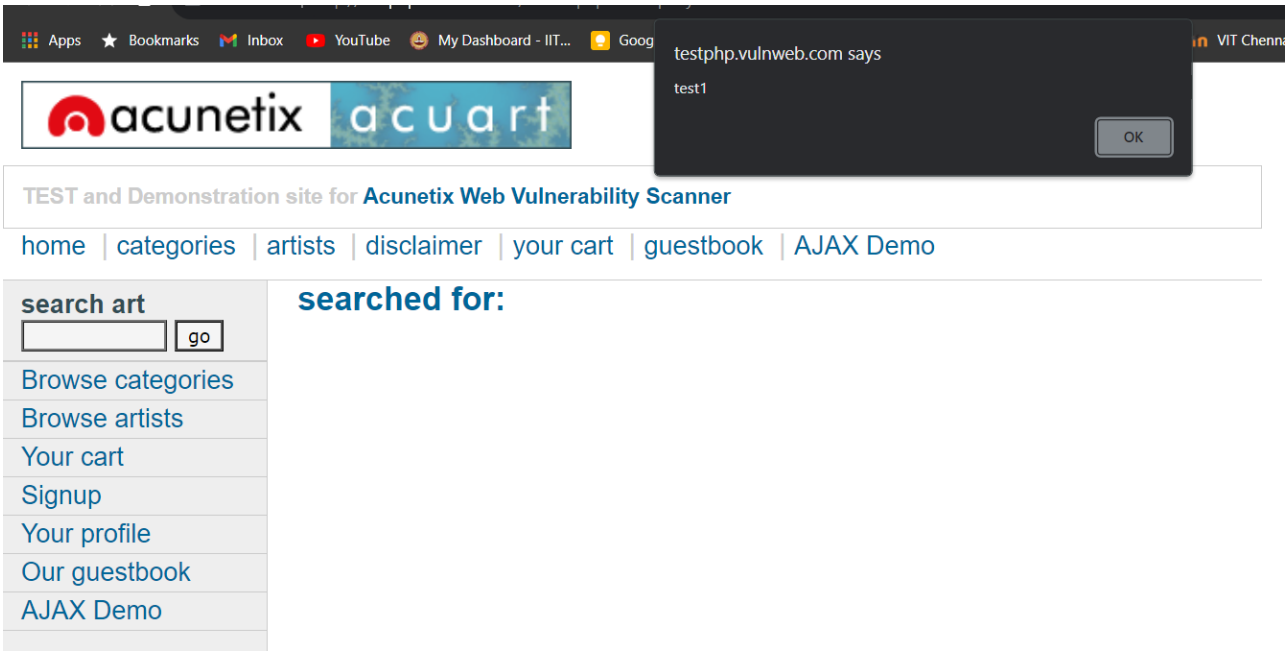
Steps to Reproduce :

Step 1. Access the URL

Step 2: enter the script in the search box <body onload=alert('test1')>



Step 3:-after entering the script content like” hacked” u will find the dialogue box as shown below.



Recommendation:

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

2. Html injection

CWE: CWE-80

OWASP Category: A03:2021 – Injection

Description: The product receives input from an upstream component, but it does not neutralize or incorrectly neutralizes special characters such as "<", ">", and "&" that could be interpreted as web-scripting elements when they are sent to a downstream component that processes web pages.

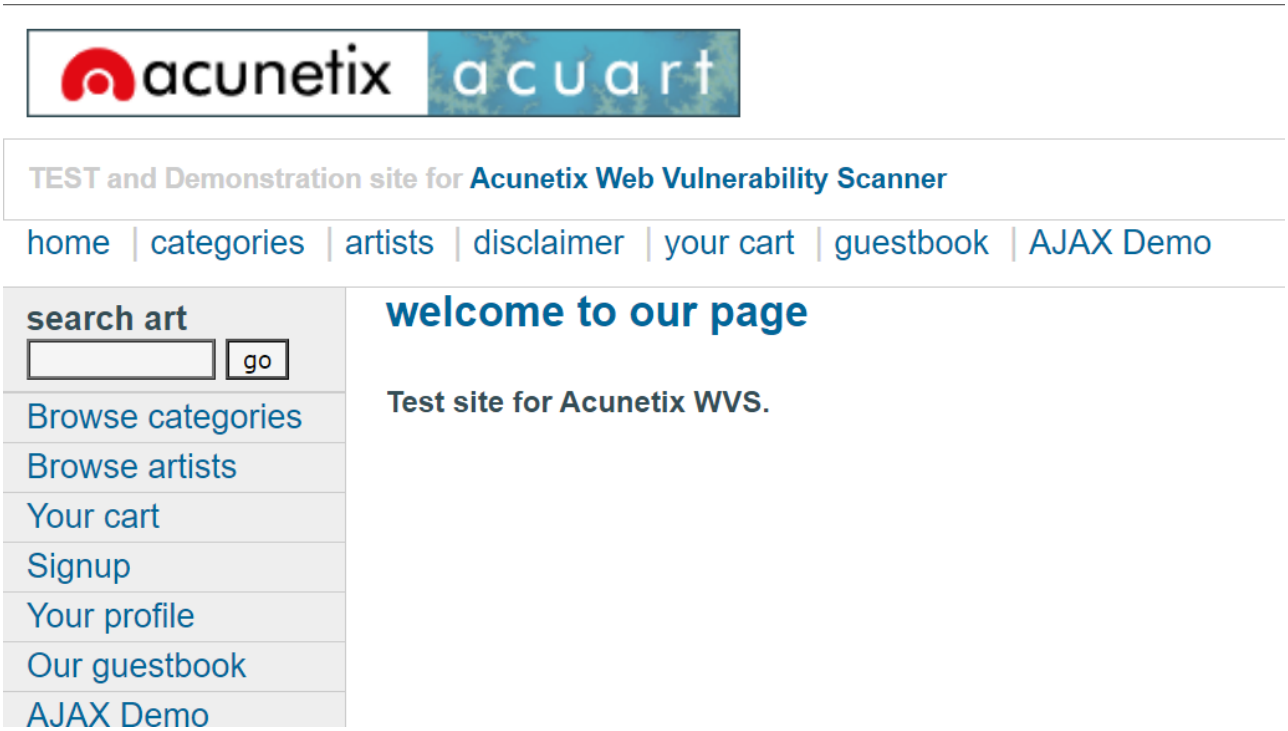
Business Impact: In some circumstances it may be possible to run arbitrary code on a victim's computer when cross-site scripting is combined with other flaws.

Vulnerability Path : http://testphp.vulnweb.com

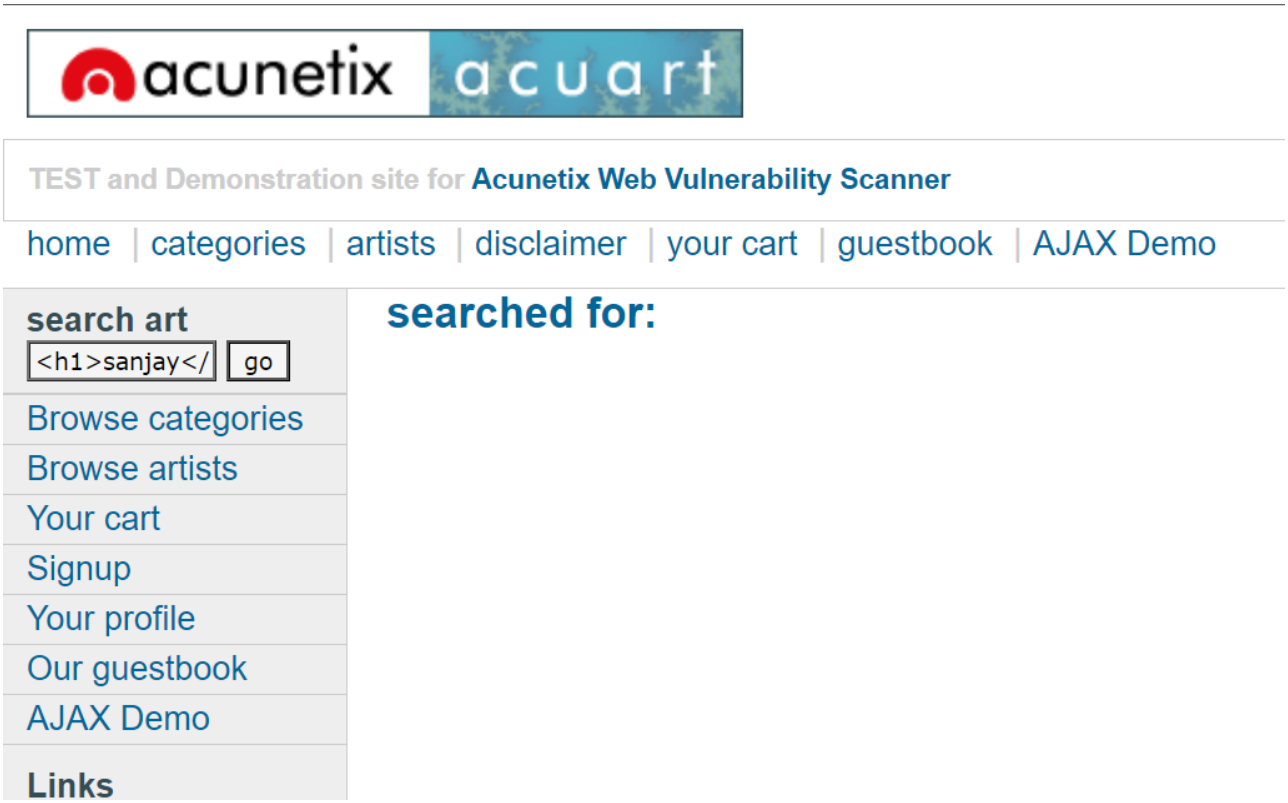
Vulnerability Parameter: http://testphp.vulnweb.com/search.php?test=query

Steps to Reproduce :

Step 1. Access the URL



Step 2: type the html script in the search box



Step 3: The script affects the webpage

3. No Session Management

CWE: CWE-384

OWASP Category: A07:2021 –Identification and Authentication Failures

Description: An attacker is able to force a known session identifier on a user so that, once the user authenticates, the attacker has access to the authenticated session.

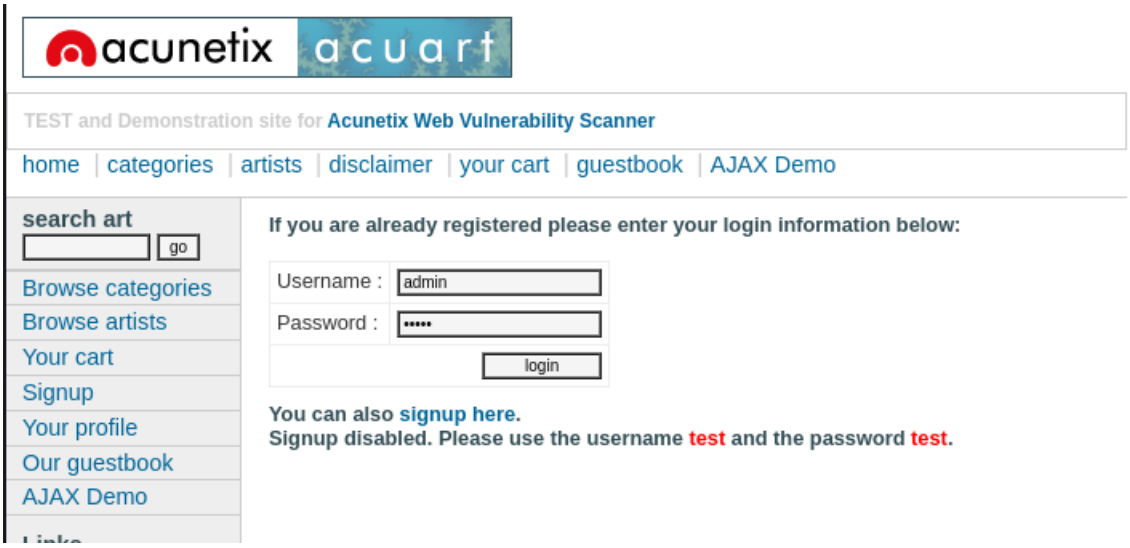
Business Impact: Without appropriate session management, you can run into several security problems, putting your users at risk. Common vulnerabilities caused by a lack of or poorly implemented session management include: Session hijacking

Vulnerability Path : http://testphp.vulnweb.com/logon.jsp

Vulnerability Parameter: http://testphp.vulnweb.com/login.jsp

Steps to Reproduce :

Step 1. Access the URL



Step 2.without the proper session management the burp can still access the request of session as shown.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 × +

Send Cancel < > Follow redirection Target: htt

Request

Pretty Raw Hex

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 22
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
  0.7
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 uname=admin&pass=admin
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.19.0
3 Date: Fri, 27 Oct 2023 19:51:18 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
7 Location: login.php
8 Content-Length: 14
9
10 you must login
```

Recommendation:

- Invalidate any existing session identifiers prior to authorizing a new user session.

4. Default Credentials

CWE : CWE-1392

OWASP Category:A07:2021-Identification and Authentication Failures

Description:It is common practice for products to be designed to use default keys, passwords, or other mechanisms for authentication. The rationale is to simplify the manufacturing process or the system administrator's task of installation and deployment into an enterprise. However, if admins do not change the defaults, it is easier for attackers to bypass authentication quickly across multiple organizations.

Business Impact:Attackers can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet.

Vulnerability Path : http://testphp.vulnweb.com/login.jsp

Vulnerability Parameter: http://testphp.vulnweb.com/login.jsp

Steps to Reproduce :

Step 1. Access the URL

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

If you are already registered please enter your login information below:

Username :	admin
Password :	•••••
	login

You can also signup here.
Signup disabled. Please use the username test and the password test.

Step 2: The website is based on apache tomcat server so we are able to login using a default user and password .

Recommendation:

- Prohibit use of default, hard-coded, or other values that do not vary for each installation of the product - especially for separate organizations.

5. Clickjacking (Improper Restriction of Rendered UI Layers or Frames)

CWE :CWE-1021

OWASP Category: A04-2021- insecure design

Description:it occurs whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

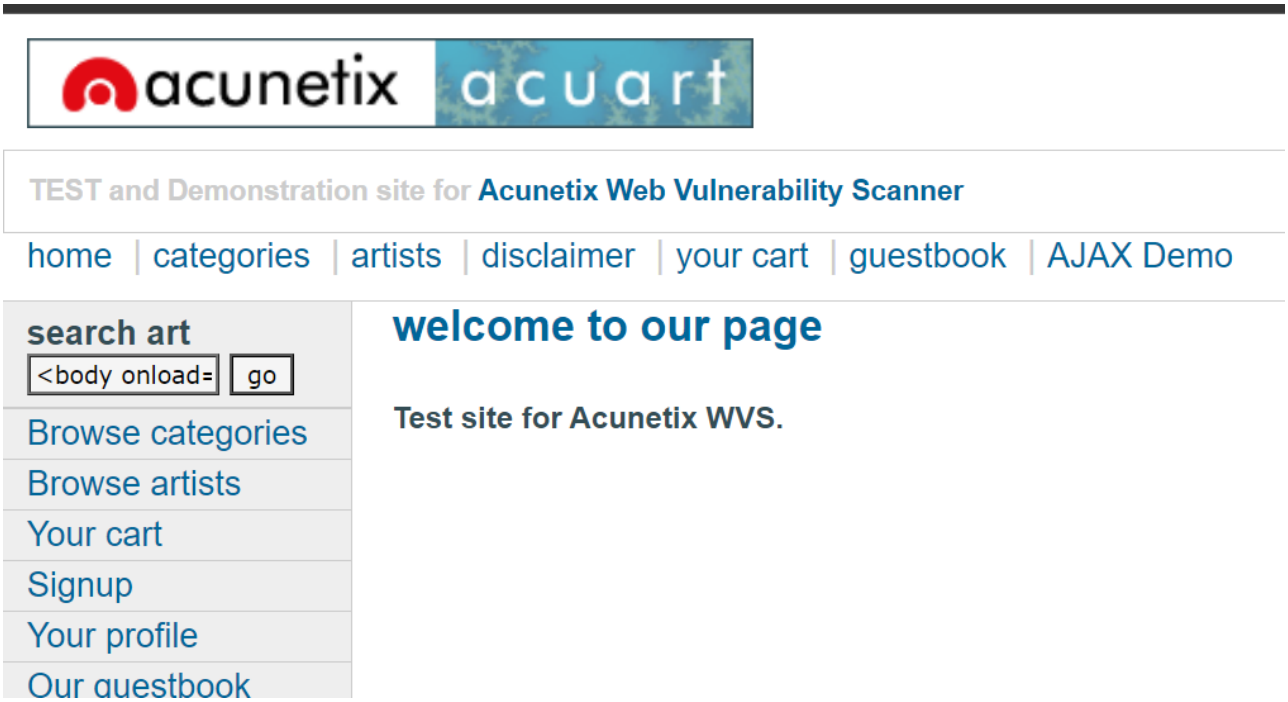
Business Impact: The common consequences of clickjacking include unauthorized actions, data theft, phishing, cookie theft, social engineering, reputation damage, legal and regulatory consequences, and user frustration. To prevent these, organizations should implement security headers, frame-busting techniques, user education, and regular security testing.

Vulnerability Path : http://testfire.net/index.jsp

Vulnerability Parameter: **http://testfire.net/index.jsp**

Steps to Reproduce :

Step 1:- Access the URI

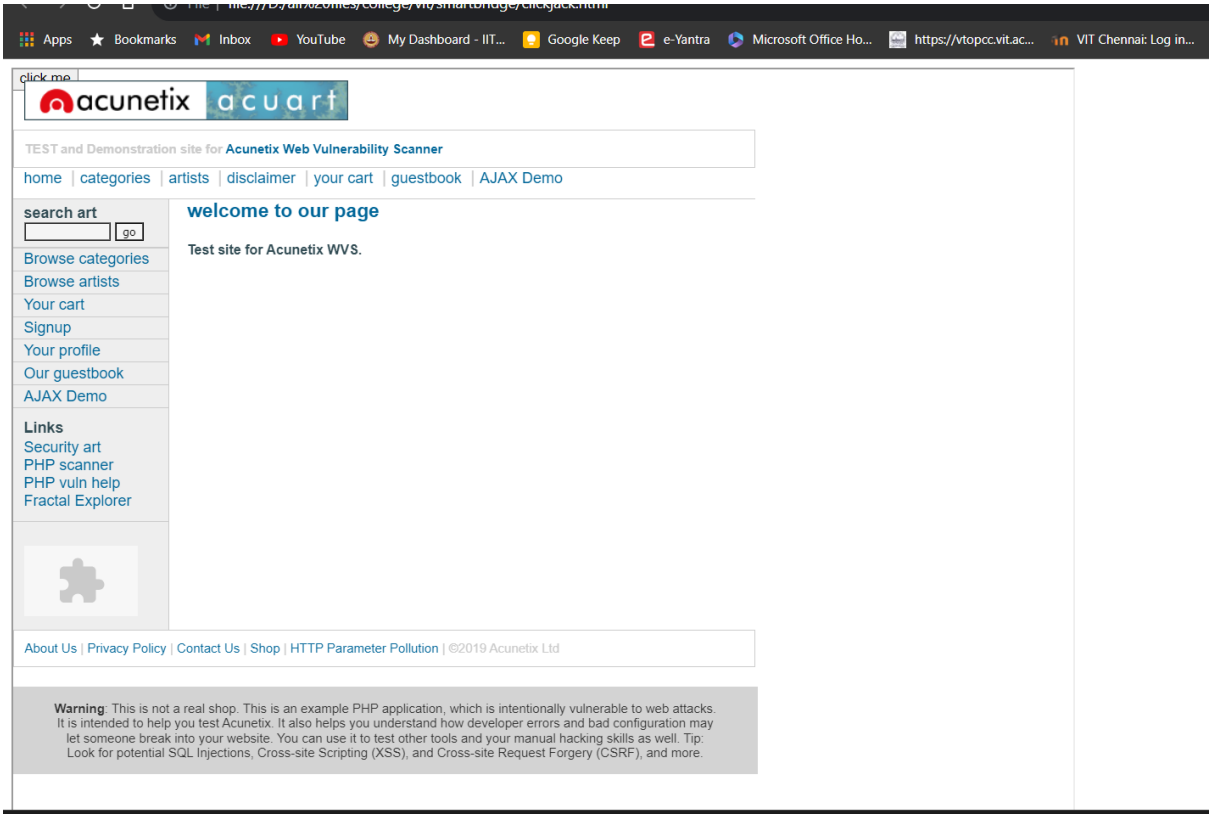


Step 2:- we write a html code as shown below when we run with the web address .

```
<head>
    <style>
        #target_website {
            position:relative;
            width:1000px;
            height:1000px;
            opacity:;
            z-index:2;
            }
        #decoy_website {
            position:absolute;
            width:300px;
            height:400px;
            z-index:1;
            }
    </style>
</head>

<body>
    <div id="decoy_website">
    <button>click me
    </button>
    </div>
    <iframe id="target_website" src="http://testfire.net/index.jsp">
    </iframe>
</body>
```

Step 3:- this will be the output of clickjacking the website with html code .



Recommendation:

- Segment remote resource access functionality in separate networks to reduce the impact of SSRF
- Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic.
- Enforce the URL schema, port, and destination with a positive allow list
- Do not send raw responses to clients
- Disable HTTP redirection