VAPT REPORT

August 2023

Confidential

DOCUMENT DETAILS

Document Properties

Title	Vulnerability Assessment & Penetration Testing
URL	https://ww\
Start time	2023-08-21T01:20:30.207276+06:00
Report type	Manual scan
Profile	Full Scan
Version	V1.0
Validity	30 days
Author	Rifat
Pen-testers	Rifat
Reviewed By	Rifat
Approved By	Rifat
Classification	Confidential

Version Control

Version	Date	Author	Description
V1.0	21-08-23	Rifat	Final Draft

Contact

Name	Rifat
Phone	
Email	

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This assessment aimed to identify weaknesses in security, mistakes in how the business logic was set up, and any areas where the best security practices were missing.

1.1 Scope of Testing

The following URL was the scope covered under the security audit:

Application 1: **https://wwv**

1.2 Threat level Summary

The visual representations VAPT dashboard offer a comprehensive overview of the outcomes of the security audit scan. These graphics provide a summary encompassing various aspects.

- **Threat Level 3**

Vulnerability Severity	No. of Vulnerability found
High	2
Medium	10
Low	8
Informational	4

1.3 List of Executive summary

#	Alert group	Severity	Alert count
1	SQLi	High	2
2	Access Control	Medium	3
3	Cryptographic Failures	Low	1
4	Insecure Design	Medium	3
5	Security Misconfiguration	High	12
6	Vulnerable and Outdated Components	Medium	13
7	Software and Data Integrity Failures	Medium	3
8	Broken Link Hijacking	Medium	1
9	Cookies without HttpOnly flag set	Low	1
10	Clickjacking: X-Frame-Options header	Low	1
11	Possible virtual host found	Low	1
12	Reverse proxy detected	Informational	1
13	Web Application Firewall detected	Informational	1
14	Broken Link Hijacking	Low	1
15	Vulnerable JavaScript libraries	Medium	1
16	Insecure Inline Frame (iframe)	Low	1
17	Cookies without Secure flag set	Low	1
18	HTTP Strict Transport Security (HSTS) not implemented	Low	1
19	Content Security Policy (CSP) not implemented	Informational	1
20	Outdated JavaScript libraries	Informational	1

2. DISCOVERED VULNERABILITIES DETAILS

VULNERABILITY	SQLi
SEVERITY	High
IMPACT	High
CVSS SCORE	7.5

Affected URL: https://www news-details.php?Id=8

Details of Vulnerability:
SQL injection (SQLi) is a type of injection attack that allows an attacker to execute malicious SQL statements on a database server. This can be done by inserting malicious code into a vulnerable web application.SQLi vulnerabilities can occur in a variety of places, such as:

- User input fields: This is the most common place for SQLi vulnerabilities to occur. User input fields are often used to enter data into a database, such as usernames, passwords, and email addresses. If this data is not properly sanitized, an attacker can inject malicious code into the field.
- Parameterised queries: Parameterised queries are a way of preventing SQLi vulnerabilities. However, if they are not implemented correctly, they can still be vulnerable.
- Stored procedures: Stored procedures are a way of grouping together SQL statements. They can be used to improve performance and security. However, if stored procedures are not properly designed, they can be vulnerable to SQLi attacks.

Impact: The impact of a successful SQLi attack can be severe. An attacker can use SQLi to:

- Read sensitive data from the database, such as passwords, credit card numbers, and personal information.
- Modify data in the database, such as changing account balances or deleting records.
- Create new records in the database, such as adding new users or accounts.
- Execute arbitrary commands on the database server, such as installing malware or deleting files.

Recommendation: To prevent SQLi attacks, it is important to:

- Sanitize all user input. This means removing any special characters that could be used to inject malicious code.
- Use parameterised queries. This will prevent attackers from injecting malicious code into the query.

- Design stored procedures carefully. Make sure that they are not vulnerable to SQLi attacks.
- Use a web application firewall (WAF). A WAF can help to block SQLi attacks.

Additional References: https://portswigger.net/web-security/sql-injection

VULNERABILITY	Clickjacking: X-Frame-Options header
SEVERITY	MEDIUM
IMPACT	LOW
CVSS SCORE	3

Affected URL: Sitewide

Details of Vulnerability:

GET / HTTP/1.1
Refere https://
Accep ext/htm' pli ir nl;q=0.9,*/*;q=0.8
Accep ncor g: gzip, ate,br
User-A en' ozilla/5.0 Windows NT 10.0; Win64; x64) App 37.36 (KHTM e Gecko)
Chron 08.0.0.0 Safari/537.36
Host: www.
Connection: Keep-alive

Paths without secure XFO hea er: https://ww /
https://ww /1200- rnace.php
https://www /1200- i-Tube F hp
https://www. /1200-Split-Tube-Furnace.php

Impact: The impact depends on the affected web application.

Recommendation:
Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

Additional References:
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html
https://en.wikipedia.org/wiki/Clickjacking

VULNERABILITY	Possible virtual host found
SEVERITY	MEDIUM
IMPACT	Low
CVSS SCORE	3.5

Affected URL: Virtual host: r), webmai

Details of Vulnerability:

Virtual host: mai'

Response:

```
<!DOC  'PE HTML PU  "-//IET  TD HTML 2.0//EN">
<html:  ead>
<title>  1 M  Permanently</title>
</hea  <'  y>
<h1>  d Permanently</h1>
<p>T  document has moved <a href="http://  ./">here</a>.</p>
</body></html>
```

Virtual host: web

Response:

```
<!DOCTYPE HTML PUB  DTD HTML 2.0//EN">
<html  head>
<title>  1 Moved  manently</title>
</hea  <body
<h1>M  ved  manently</h1>
<p>Th  d  ment has moved <a
href="  www.  /
proxy_subdomain_webmail/proxy_subdomain_webmail/">he re</a>.</p>
</body></html>
```

Impact:

Possible sensitive information disclosure.

Recommendation:

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

Additional References: https://en.wikipedia.org/wiki/Virtual_hosting

VULNERABILITY	Broken Link Hijacking
SEVERITY	MEDIUM
IMPACT	MEDIUM
CVSS SCORE	5.5

Affected URL: ww\ 'assets/img/banner/

Details of Vulnerability: This page contains a script tag with the src attribute (http://cdn.jsinit.directfwd.com/sk-jspark_init.php) pointing to the domain cdn.jsinit.directfwd.com. This domain does currently not resolve to an IP address and can potentially be taken over by an attacker.

```
GET /assets/img/banner/ HTTP/1.1

Referer: h  s://ww\

Cookie: PHP  SID=  4af64e3613476414278a8b  4b

Accept: text  ml,  pl.  tion/xb  ,apj  cat.  'xml;q=0.9,*/*;q=0.8

Accept-Encodi  :  ip,de  te,

User-Agent: M  a/5.0 (W  ws NT 10.0,  n64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/  .0.0.0 Safari/537.36

Host: ww\

Connection: Keep-alive
```

Impact: An attacker can potentially register the expired domain and serve a malicious file that will be loaded in the context of your web application.

Suggested Fixes: Replace the scripts/frames that are loaded from non-resolving domains with new links that are pointing to valid domains.

Additional References: https://edoverflow.com/2017/broken-link-hijacking/

VULNERABILITY	Clickjacking: X-Frame-Options header
SEVERITY	Low
IMPACT	MEDIUM
CVSS SCORE	5.8

Details of Vulnerability: 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. The server did not return an X-Frame-Options header with the value DENY or SAMEORIGIN, 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 untrusted sites.

Paths without secure XFO header:

https://www ' https://www. '1200-Mini-Muffle-Furnace.php
https://www . 1200-Mini-Tube-Furnace.php
https://www. 1200-Sp -Tube-Furnace.php
https://www. 1700-Li ype-Bel ar-Furnace.php
https://www /1700-M le- mos ere-Furnace.php
https://www /1700-M le- rna .php
https://www '1700-V ur -urn e.php
https://www 3-rods-(D- ster hp
https://www 3-rods-(aph e-(wth-system.php
https://ww Therma VI hp tps://www.' about-us.php
https://ww advanc em ol or-nano-analysis.php
https://ww area-co gu io st-5-10-20ln.php
https://ww astar-te to(-r notechnology.php
https://ww auto-strain-m p g.php
https://www. big-size-split-tube-furnace.php

```
GET / HTTP/1.1

Referer: https://ww

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: www

Connection: Keep-alive
```

Impact: The impact depends on the affected web application.

Recommendation: Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

VULNERABILITY	Cookies without Secure flag set
SEVERITY	Medium
IMPACT	High
CVSS SCORE	7

Details of Vulnerability:

```
GET / HTTP/1.1
Referer: https://www.
Accept:
text/html application/xhtml+xml,
applic .on/xml;q= q=0.8
Accept ncodir gzi eflat
User-A +• /5.0 (Windows N  0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0
Safari/537.36
Host : www
Connection: keep_alive
```

Impact: Cookies could be sent over unencrypted channels.

VULNERABILITY	Malware Identified (verified)
SEVERITY	High
IMPACT	Medium
CVSS SCORE	4

Details of Vulnerability:
A malicious file was detected on your web server. This could be that you either uploaded the file by accident or an attacker was able to write arbitrary files to your web server.
Threats found by Windows Defender: Trojan:HTML/Phish!MSR

Recommendation:

It is advisable to contact an information security company with experience in malware removal. They may help or instruct you to take the following steps:

- Immediate removal of the malicious file.

- Find out whether additional steps need to be taken to ensure that the malicious files were completely removed from your server.
- Where applicable, replacement of the file with a clean copy that does not contain the malicious code. You should make sure to locally scan the new file with an antivirus tool or submit it to VirusTotal before you upload it again.
- They may help you to ensure that the malicious file is no longer accessible. If you use caching server such as Varnish, Squid or Nginx, they might tell you to make sure that they don't serve a copy of the infected file from memory.
- They will tell you to notify your users and the appropriate authorities. This may include law enforcement and data protection authorities depending on your local laws.

VULNERABILITY	Vulnerable JavaScript libraries
SEVERITY	MEDIUM
IMPACT	MEDIUM
CVSS SCORE	5.5

Details of Vulnerability:

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

```
GET / HTTP/1.1

Referer: https://w

Accep   text/htm.   oplic      'xht.                                    .8

Accept-   coding: gz.   lef   ce,z

User-Age.   Mozilla/5.(      dows NT 1(      ;4; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Ch.   e/108.0.0.0      ri/537.36

Host: www

Connection: Keep-alive
```

- jQuery 1.12.4
- URL: https://ww
- Detection method: The library's name and version were determined based on its dynamic behavior.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023

- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Recommendation: Upgrade to the latest version.

Additional References:
https://jquery.com/upgrade-guide/3.5/ https://api.jquery.com/jQuery.htmlPrefilter/
https://www.cvedetails.com/cve/CVE-2020-11022/
https://github.com/advisories/GHSA-gxr4-xjj5-5px2

VULNERABILITY	Cookies without HttpOnly flag set (verified)
SEVERITY	Low
IMPACT	MEDIUM
CVSS SCORE	3.5

Details of Vulnerability:
One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies

Cookies without HttpOnly flag set:

- https://www Set-Cookie: PHPSESSID=34e044af64e3 3476414278a8bb1e4b; path=/
- https www Set-Cookie: PHPSESSID c309f65 8b94 29f5 adc6; path=/
- http //www p Set-Cookie: PHPSESSID=6577829e7c33a49f4b7a49ceeeb5429c; path=/

VULNERABILITY	Cookies without Secure flag set (verified)
SEVERITY	MEDIUM
IMPACT	MEDIUM
CVSS SCORE	3.5

Details of Vulnerability:
One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Cookies without Secure flag set:

- https://www Set ookie: PHF 4e 1347 4278a8bb1 ; path=/
- https://www / Set- ok PHPSESSID=3c309f65899 9 42 122 adc6; path=/
- https://www /supp dsubp .php Set-Cookie: PHPSESSID=6577829e7c33 f4b7a49 eb5429c; path=/

VULNERABILITY	HTTP Strict Transport Security (HSTS) not implemented
SEVERITY	Low
IMPACT	MEDIUM
CVSS SCORE	4

Details of Vulnerability:
HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

URLs where HSTS is not enabled:

https://www http /www. 120 ace.php
https://www 120 hp
https://www. 1200- lit-Tube hp
https://www. /1700-L ell-Jar-F ace.php
https://www. /1700-Muffle-Atmosphere-F nace.php

https://www 1700-M https://www /700-Vacuum-Furnace.p https://www 3-rod CVD-system.php https://www 3-rod Graphen rowth- stem.php https://www 3d-pr ssion-d tion-t ography.php https://www CNT- n.php //ww -CVD.php https://www PEC\ D-pr ss uipn dia.php https://www Therr l-C\ .php ps:/ /about-us.php https://www adva -tools- -na analysis.php https://www. /area- f uration- -5- 20ln.php https://www.t /astar-t ools-nan chnology.php https://www.t /auto-strain-mapping.php https://www. /big- .ce.php
Recommendation: It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

VULNERABILITY	Content Security Policy (CSP) not implemented
SEVERITY	**Informational**
IMPACT	**MEDIUM**
CVSS SCORE	**5.2**

Details of Vulnerability:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. Content Security Policy (CSP) can be implemented by adding a Content-Security-Policy header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' http
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Paths without CSP header:

https://www
https://www.t '120 Mir nace.php
https://www 120 Mini-Tube-Furnace.php
https://www 120 ube-Fu ce.php
https://www 1 ace.php
https://www . 0 uffle-Atmosphe -Furnace.php
https://www 170 luffle-Furnace p
https://www . 170 e.php
https://www . 3-rc
https://www . 3-rc -Grap growth- tem.php
https://www . 3d-p ession-diffraction-to graphy.php
https://www. . CN arn.php https://ww /Hot-Wire- /D.php
https://www. . PE(ED-process-equi o
https://www. . The al-CVD.php h ww /a ut-us.php
https://www. . advanc -analysis.ph
https://www. . are st-/ 0-20ln.ph
https://www. . a ote holo
https://www. . aut
https://www.t big-size .php

Recommendation:

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

VULNERABILITY	Outdated JavaScript libraries
SEVERITY	Informational
IMPACT	MEDIUM
CVSS SCORE	4.5

Details of Vulnerability:

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

- bootstrap.js 3.3.7
- URL: https://www

- Detection method: The library's name and version were determined based on its dynamic behavior.

Recommendation:

- Upgrade to the latest version.

Additional References:

- https://github.com/twbs/bootstrap/releases

VULNERABILITY	Reverse proxy detected
SEVERITY	Informational
IMPACT	MEDIUM
CVSS SCORE	4.5

Details of Vulnerability:
This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.
Detected reverse proxy: Apache httpd

```
GET / HTTP/1.1

Max-Forwards: 0

Accept: text/h                                    :ion/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: ww

Connection: Keep-alive
```

Recommendation: None

VULNERABILITY	Web Application Firewall detected
SEVERITY	Informational
IMPACT	MEDIUM
CVSS SCORE	4.5

Details of Vulnerability:
This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Detected ModSecurity from the response body.

```
GET /?page=../../../../../../../../../etc/passwd%00.jpg HTTP/1.1

Cookie:

Accept: t                          tml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: ww

Connection: Keep-alive
```

Recommendation: If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

3. LIST OF VAPT TESTS PERFORMED

3.1 OWASP Top 10

#	OWASP Top 10
	For Web Applications
1	SQL Injection
2	Broken Authentication
3	Sensitive Data Exposure
4	XML External Entities (XXL)
5	Broken Access Control
6	Security Misconfiguration
7	Cross-Site Scripting (XSS)
8	Insecure Deserialization
9	Using Components with Known Vulnerabilities
10	Insufficient Logging and Monitoring

3.2 SANS 25 Software Errors/Tests

#	SANS 25
1	Improper Restriction of Operations within the Bounds of a Memory Buffer
2	Improper Neutralization of Input During Web Page Generation ('XSS')
3	Improper Input Validation
4	Information Exposure
5	Out-of-bounds Read
6	Improper Neutralization of Special Elements used in an SQL Command (SQLi)
7	Use After Free
8	Integer Overflow or Wraparound
9	Cross-Site Request Forgery (CSRF)
10	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
11	Improper Neutralization of Special Elements used in an OS Command
12	Out-of-bounds Write
13	Improper Authentication
14	NULL Pointer Dereference
15	Incorrect Permission Assignment for Critical Resource
16	Unrestricted Upload of File with Dangerous Type
17	Improper Restriction of XML External Entity Reference
18	Improper Control of Generation of Code ('Code Injection')
19	Use of Hard-coded Credentials
20	Uncontrolled Resource Consumption
21	Missing Release of Resource after Effective Lifetime
22	Untrusted Search Path
23	Deserialization of Untrusted Data
24	Improper Privilege Management
25	Improper Certificate Validation

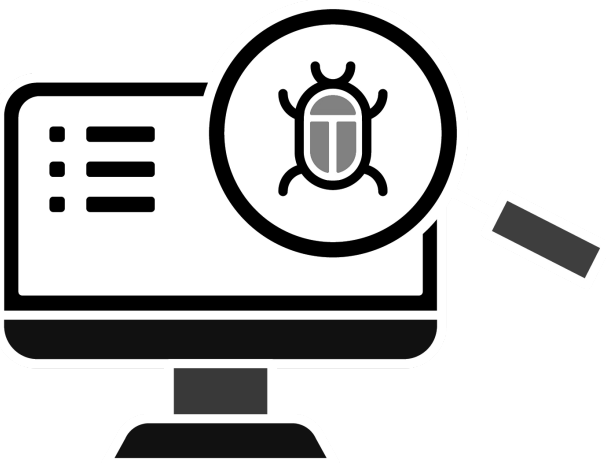
3.3 Scanned items

https://www
https://www /1200-Mini-Muffle-Furnace.php
https://www '1200-Mini-Tube-Furn php
https://www '1200-S -Tube-Fu
https://www '1700-L Type-B r-Fu ace.php
https://www '1700-M le-A phere-Furnace.php
https://www '1700-M nace.php
https://www '1700-Vacuum-Furnace.php
https://www '3-rods-CVD-system.php
https://www '3-rods-Graphene-gro -system.php
https://www '3d-prcessio -diffrac ography.php
https://www 'about-us.p
https://www 'advance-t -f ano-a sis.php
https://www 'area-confi ati -10-20ln.php
https://www 'assets/ htt /ww /assets/css/
https://www 'assets/css otsnav.css
https://ww /assets/css/ tstrap.min.css
https://ww /assets/css/ t-awesome.min.css
https://www
https://www 'as 'css/ css
https://www 'as ss/ .video.play.html
https://www /as s ponsive.css
https://www /as
https://www /ass 'fo a-branc 00.html
https://www /asse nts/fa-regul 00.html
https://www /asset nts/fa-solid .html
https://ww /assets/ s/glyphic -halflings - r e g ula r - 2.h t ml
https://ww in/assets/fo lyphi s-halflings-regular-3.html
https://www /' phi s-halfling -4.html
https://www sets/fo s-halfling eg html
https://www asse o s-halfling egula
https://www asse /pl alflin egularde t ml
https://www ass os ww /assets/in nner/
https://www. ss g/ nt ttps://w in/asse img/demo/
https://www.t ss g/ ar t.jfif https://w .in/assets/img/product/
https://ww s g/ vi https://www.t /assets/js/
https://ww s/bo n s
https://ww js/boots min.js
https://ww /js/jquery- 2.4.min.js
https://ww s/js/jquery. gnific-popup.min.js
https://ww 'a s/js/main.j
https://ww 'a ts/js/owl.carousel.min.js
https://ww 'a
https://ww 'astar-tem-tools-nanotechnology.php
https://ww 'auto-strain-mapping.php
https://ww big-size-split-tube-furnace.php
https://ww .in/bio-equipments.php
https://ww vices.php
https://ww rs.php
https://www .in/bwf-17.php
https://www in/bwf-serial-data-transmission.php
https://www. .in/cgi-sys/

https://ww 'single-raman-spectrometer.php https://www /sitemap.xml
https://www.' sliding-furnace.php
https://www.t spectroscopy-and-micro-analysis-accessories.php
https://www.t split-tube-furnace php in/support/
https://www.t support/find .php https. in/survey-ir.php
https://www tab' n-series.php
https://www proc -equipments.php
https://www -robo education.php
https://www d-f ohene-foam-synthesis.php
https://www for-nanowire-synthesis.php
https://www /Ther ee-zone-1600-cvd.php
https://www /tpx- ttps://www nace.php
https://www /ubg ang ensor.php
https://www /ubgo in-range-sensor.php n/uploads/
https://www nloads/banner/ https://ww /banner/thumb/
https://www ads/clients/ https://ww n/uploa clients/thumb/
https://www /u lx-ug-01.php
https://www /urg ange-sensor.php
https://www /urg04l ge-sensor.php
https://www /utm-30lx- n-30lx-f-ew.p
https://www /utm30lx-se php
https://www.' /uxm-30lxh-eh m-30lah a.php
https://www.' /uxm30lnp-range sor.pl
https://www.' vacuum-furnace-h d-sy n.php
https://www.' vacuum-oven-for-dy tes-system.php
https://www n variable- -ez-slice
https://www vertical-f php https://ww ay-lynx.php
https://www ec sy n- 200-P80V10.php
https://www E cess-equipments-india.php
https://www ex nsor.php
https://www fx- sor.php
https://www ho .php
https://www lx- t hp
https://www ort e-ram ter.php
https://www re ion-el ion.php
https://www roc s-com pen-networks.php
https://www roc s.php
https://www vf-p o-sens hp
https://ww ang .php
https://ww bot stem.php
https://ww boti
https://ww afety- ner-uam-05lp-t301.php
https://ww ample
https://ww ample- accessory.php
https://ww canning-la e-finder.php
https://ww scientific-in n nera.php
https://ww sensor-for-s i lication.php
https://ww sensors-for- eel-industry.php
https://ww /sensors-for- ile-industry.php
https://ww /sensors.php
https://ww serial-paralle ata-converter.php
https://www./serial-type-data-transmission-devices.php

https://www /indiram-handy-handheld-raman-spectrometer.php
https://www sp- -converter.php
https://www br·
https://www ab fu s-process-solutions.php
https://ww as
https://ww da ip
https://ww e) ip
https://w ansmittance-cell-cryostat-190.php
https://w sor.php
https://w l/l sor.php
https://w l/n n
https://w l/r archives/
https://ww n/r ch-pick-pen.php
https://ww /n ce-sliceir-easy-cross-sectioning.php
https://www 'mi ce.php
https://ww r tr-vis php
https://w -p e.p
https:// ti-c h
https:/ w-si- sur -s is.php
https://ww n-des e· o
https://ww ical-d an ic ip
https://w ical-remote-c er.php
https:/ er
https .php
https: s2.php
https://www .php
https://www -data-transmission-devices.php
https://www r.p
https://ww d sor.p
https://ww
https://ww ecvd-f e nts.php
https://ww ecvd- ensity php
https://ww ecvd· cluster-s apher nthesis.php
https://ww cvd te -l ip- ner
https://ww vd-sv -c arrier
https://ww t- r-solar-cell-ar·
https://ww ita-transmissi ce
https://w c
https://w e-data-devices
https://w dical- or vices.php
https://ww data on- php
https://ww ip
https://ww parall sion-devices.php
https://ww -ene ami -ray.php
https://ww ounte
https://ww -ch
https://ww ianc x-edx-spectroscopy.php
https://www uiry.php
https://www pick.php
https://www.t 0.php
https://w 20bw.php

https://www grazing-angle-objective.php
https://www. anabi-metaphase-chromosome-spreader.php
https://www ter.php
https://www ter.php
https://www an .php
https://www -spreader.php
https://www. preader.php
https://www -compact-stage.php
https://www p
https://www -spectrometer.php
https://ww -chamber-250r-dr.php
https://ww .php
https://ww
https://ww .pnp
https://www on-guns.php
https://www.
https://www
https://www gi-sys/
https://www gi-sys/js/
https://www quipments.php
https://www quipments.php
https://www
https://www p
https:// -silicon-layer.php
https:// ng-spectroscopy.php
https://
https://
https://w
https://w p
https://ww rometer.php
https://ww p
https://www /contact
https://www.t s-equipments.php
https://www.t -data-transmission.php
https://ww device.php
https://ww iamond plate.php
https://ww g-furnace.php
https://ww -ray- pection-system.php
https://ww an 00-b 2.php
https://ww an 0d.
https://ww ana 0d p
https://ww ana 40.
https://ww ana- -v2 php
https://ww iond-express-II.php
https://www.t iamond-window.php
https://ww istance-data-output-ust-10-20-30-lx.php



END

August 21, 2023