Vulnerability assessment

Conduct a *web application vulnerability assessment on http://testphp.vulnweb.com/* and create a report documenting identified vulnerabilities and their potential impact.

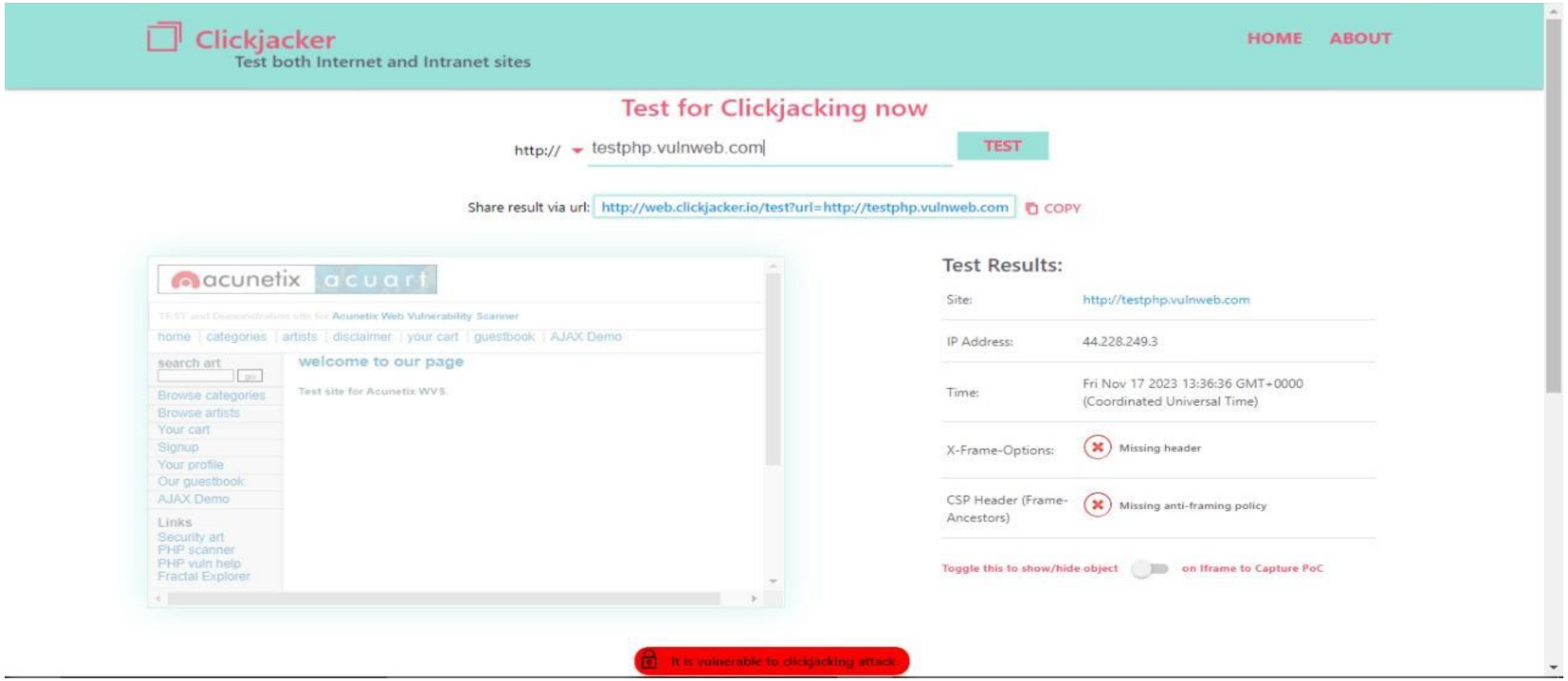
Introduction

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Vulnerabilities founded

I frame is disabled in the current website.

- If iframe is disabled , it can be reproduced in another website.



Test both Internet and Intranet sites

Test for Clickjacking now

http:// testphp.vulnweb.com

Share result via url: http://web.clickjacker.io/test?url=http://testphp.vulnweb.com

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

welcome to our page

Test site for Acunetix WVS.

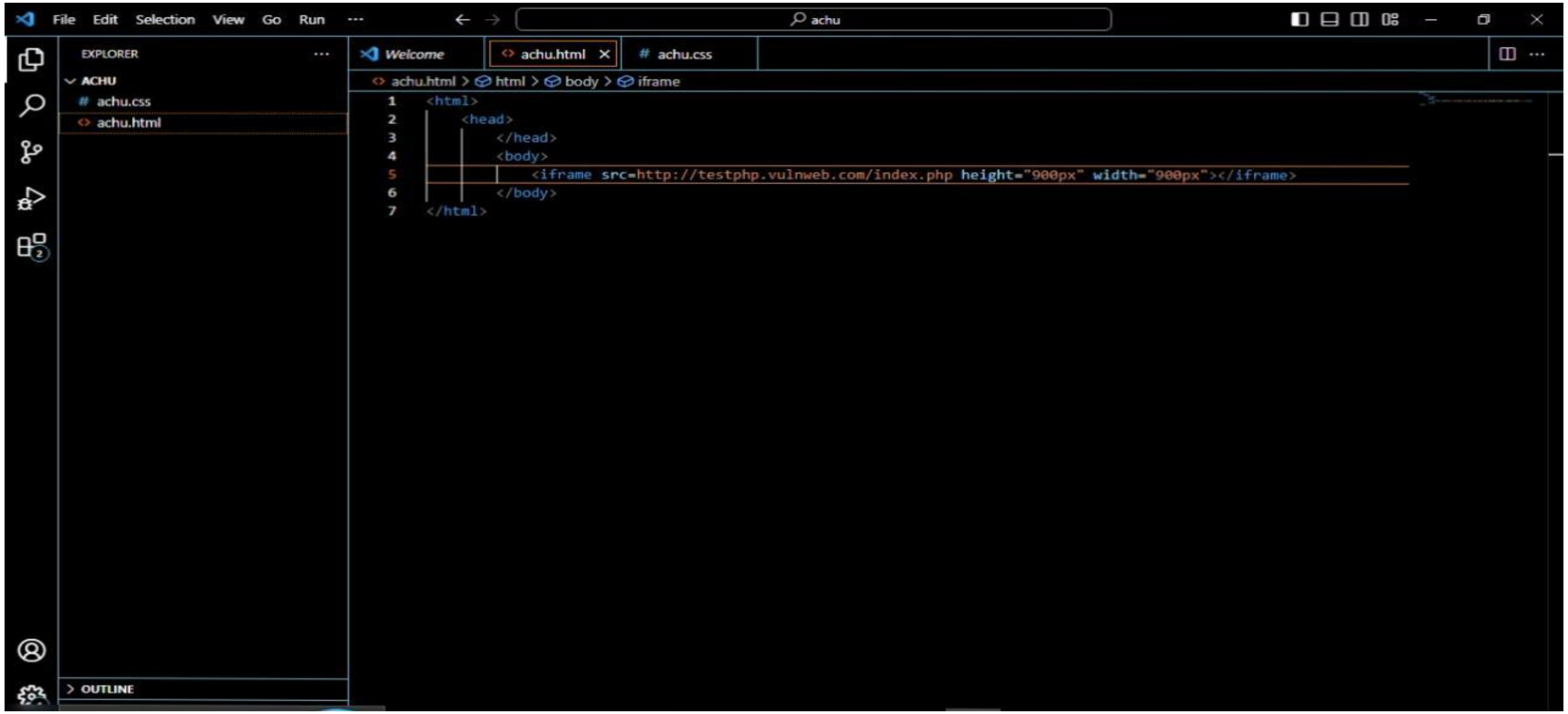
Test Results:

Site:	http://testphp.vulnweb.com
IP Address:	44.228.249.3
Time:	Fri Nov 17 2023 13:36:36 GMT+0000 (Coordinated Universal Time)
X-Frame-Options:	☒ Missing header
CSP Header (Frame-Ancestors)	☒ Missing anti-framing policy

Toggle this to show/hide object on Iframe to Capture PoC

It is vulnerable to clickjacking attack

- In the above case,we checked the vulnerability using click jacker and found the absence of iframe so that the given website can be reproduced by any other sites.
- Here the vulnerability is checked automatically.
- We can also find this vulnerability manually using html.

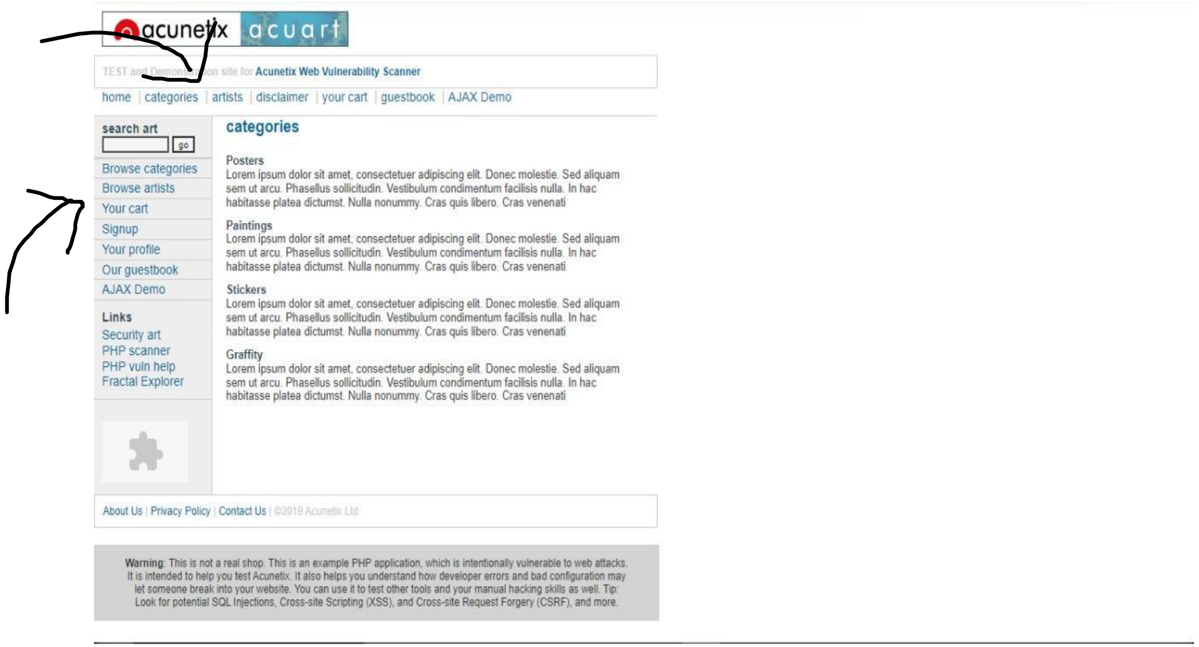


```
<html>
    <head>
        </head>
        <body>
            <iframe src=http://testphp.vulnweb.com/index.php height="900px" width="900px"></iframe>
        </body>
</html>
```

- Hence the vulnerability is shown manually and automatically.

Repetition of icons/elements

- Icons are repeated on the page with the same content.



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

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

categories

Posters
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

Paintings
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

Stickers
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

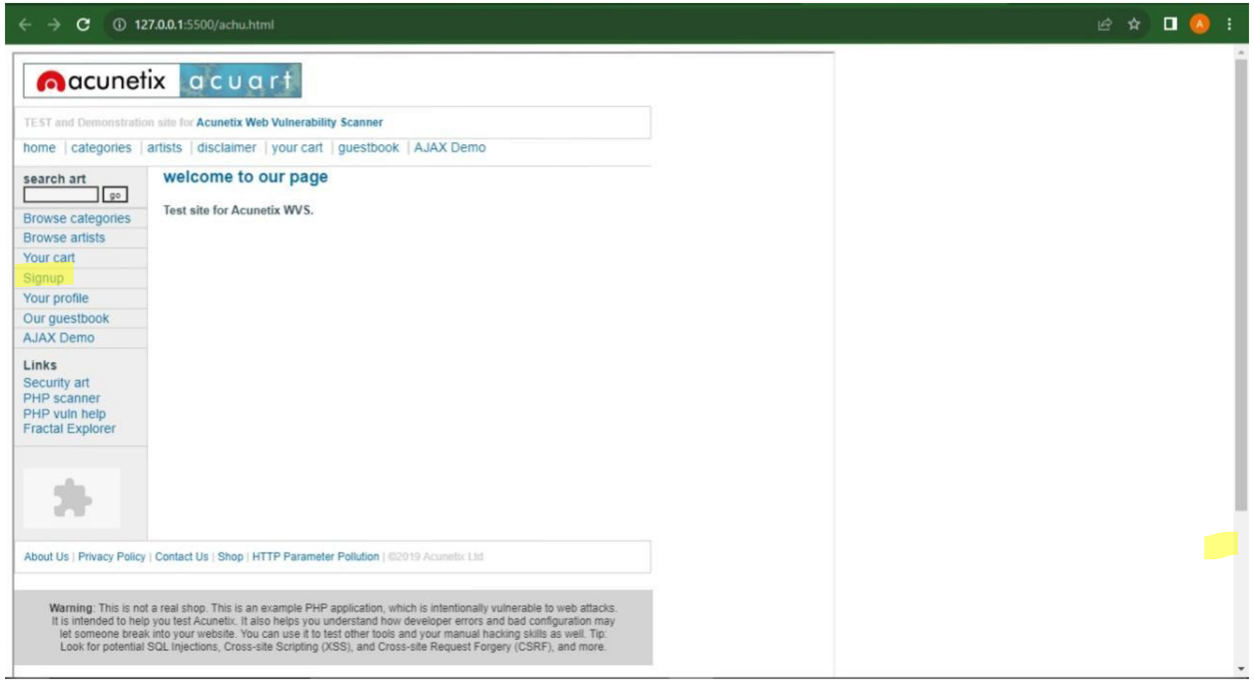
Graffity
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Absence of sign in or sign up at the entry time itself

- We directly enters into the website without any sign in or sign up.
- It is available after we entered into the site.
- This shows threat to the security of website.


127.0.0.1:5500/achu.html
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
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

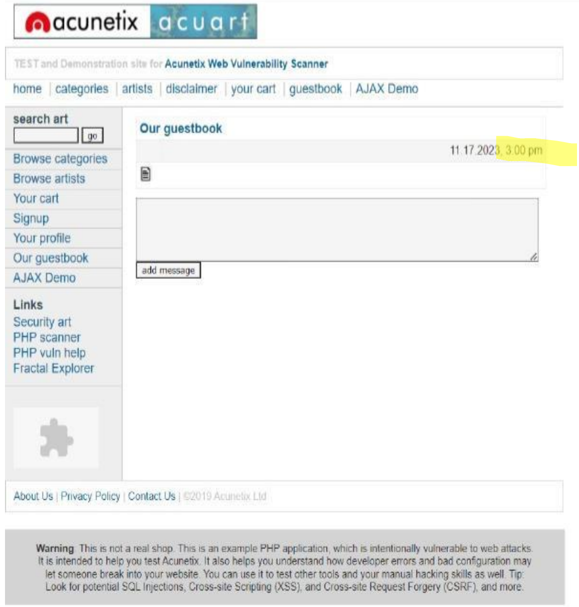
welcome to our page

Test site for Acunetix WVS.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Default time for message is not correct

- The given time showing the time of sending our message is incorrect in the given website.



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

Our guestbook

11.17.2023, 3:00 pm

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Summary

The given website contains many vulnerabilities and those are identified and mentioned. It helps us to understand how vulnerabilities affect the functioning of a website and how it can be identified.

References

- Youtube
- Google