

# Static and Dynamic Analysis

ISTEC-Cyber Security

November 7, 2024

## Description

This report contains static and dynamic analysis of the target. It uses Semgrep for static analysis and OWASP ZAP, Nmap, and SQLMap for dynamic analysis.

Provided by



# 1 Static Analysis

Details about static analysis...

## 2 Analysis Report

### 2.1 Risk Summary

Risk Level	Number of Findings
Low Risk	42
Medium Risk	28
High Risk	0
Critical Risk	0

Table 1: Summary of Risk Findings

### 2.2 Vulnerability Categories

- Category 1: Denial-of-Service (DoS) — 28
- Category 2: Improper Encoding — 4
- Category 3: Mass Assignment — 4
- Category 4: Cross-Site-Scripting (XSS) — 4
- Category 5: Cryptographic Issues — 29
- Category 6: Mishandled Sensitive Information — 1

### 2.3 Vulnerabilities by Page

## 3 Dynamic Analysis

Details about dynamic analysis...

## 4 Analysis Report

### Nmap Scan Results

Host: **scanme.nmap.org**, **scanme.nmap.org** (45.33.32.156)

Scan Duration: *4.46 seconds*

Port	Service	State
22	ssh	<b>open</b>
25	smtp	filtered ( <i>Reason: no-response</i> )
80	http	
9929	nping-echo	<b>open</b>
31337	Elite	<b>open</b>

### SQLMap Injection Points

Injection Point 1:

- **Parameter:** artist (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Type: time-based blind

Title: MySQL  $\geq$  5.0.12 AND time-based blind (query SLEEP)

Type: UNION query

Title: MySQL UNION query (NULL) - 3 columns

### 4.1 Risk Summary

### 4.2 Vulnerability Categories

- Category 1: Cross Site Scripting (DOM Based) — 1
- Category 2: Absence of Anti-CSRF Tokens — 40
- Category 3: Content Security Policy (CSP) Header Not Set — 47
- Category 4: Missing Anti-clickjacking Header — 43

<b>Risk Level</b>	<b>Number of Findings</b>
Low Risk	204
Medium Risk	130
High Risk	1
Critical Risk	0

Table 2: Summary of Risk Findings

- Category 5: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) — 62
- Category 6: Server Leaks Version Information via "Server" HTTP Response Header Field — 74
- Category 7: X-Content-Type-Options Header Missing — 68
- Category 8: Authentication Request Identified — 1
- Category 9: Charset Mismatch (Header Versus Meta Content-Type Charset) — 31
- Category 10: Information Disclosure - Suspicious Comments — 1
- Category 11: Modern Web Application — 9
- Category 12: User Controllable HTML Element Attribute (Potential XSS) — 3

### 4.3 Vulnerabilities by Page

#### Site 1: <http://testphp.vulnweb.com>

Host: testphp.vulnweb.com, Port: 80, SSL: false

<b>Vulnerability 1</b>	
<b>Risk Level</b>	High (High)
<b>Vulnerability Name</b>	Cross Site Scripting (DOM Based)

<p><b>Description</b></p>	<p>Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.</p>
---------------------------	---

Instances	URI
Instance 1	<pre>http://testphp.vulnweb.com/#jaVaScRipt: /*-/*\unhbox\voidb@x\bgroup\let\unhbox\ voidb@x\setbox\@tempboxa\hbox{/global\ mathchardef\accent@spacefactor\spacefactor}\ let\beginngroup\let\typeout\protect\ beginngroup\def\MessageBreak{\Omega(Font)}\let\ protect\immediate\write\m@ne{LaTeXFontInfo: oninputline170.}\endgroup\endgroup\relax\ let\ignorespaces\relax\accent18/\egroup\ spacefactor\accent@spacefactor*\'/*\'/*"/ **/(**/oNcliCk=alert(5397))//%0D%0A%0d%0a/ /&lt;/stYle/&lt;/titLe/&lt;/teXtarEa/&lt;/scRipt/--!&gt;sVg/ &lt;sVg/oNloAd=alert(5397)//&gt;</pre>

Vulnerability 2	
Risk Level	Medium (Low)
Vulnerability Name	Absence of Anti-CSRF Tokens

<b>Description</b>	<p>No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"> <li>* The victim has an active session on the target site.</li> <li>* The victim is authenticated via HTTP auth on the target site.</li> <li>* The victim is on the same local network as the target site.</li> </ul> <p>CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.</p>
<b>Instances</b>	<b>URI</b>
Instance 1	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Instance 2	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Instance 3	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Instance 4	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Instance 5	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Instance 6	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Instance 7	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Instance 8	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Instance 9	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Instance 10	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>

Instance 11	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Instance 12	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Instance 13	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Instance 14	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Instance 15	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Instance 16	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Instance 17	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Instance 18	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Instance 19	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Instance 20	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Instance 21	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Instance 22	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Instance 23	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Instance 24	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Instance 25	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Instance 26	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Instance 27	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Instance 28	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Instance 29	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Instance 30	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Instance 31	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Instance 32	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Instance 33	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Instance 34	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Instance 35	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Instance 36	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Instance 37	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>



Instance 38	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Instance 39	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Instance 40	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>

Vulnerability 3	
<b>Risk Level</b>	Medium (High)
<b>Vulnerability Name</b>	Content Security Policy (CSP) Header Not Set
<b>Description</b>	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. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
<b>Instances</b>	<b>URI</b>
Instance 1	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Instance 2	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Instance 3	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Instance 4	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Instance 5	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Instance 6	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Instance 7	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Instance 8	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Instance 9	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Instance 10	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>

Instance 11	<a href="http://testphp.vulnweb.com/high">http://testphp.vulnweb.com/high</a>
Instance 12	<a href="http://testphp.vulnweb.com/hpp/">http://testphp.vulnweb.com/hpp/</a>
Instance 13	<a href="http://testphp.vulnweb.com/hpp/?pp=12">http://testphp.vulnweb.com/hpp/?pp=12</a>
Instance 14	<a href="http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12">http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12</a>
Instance 15	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Instance 16	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Instance 17	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Instance 18	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Instance 19	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Instance 20	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Instance 21	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Instance 22	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Instance 23	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Instance 24	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/</a>
Instance 25	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/</a>
Instance 26	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/</a>
Instance 27	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/</a>
Instance 28	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/</a>
Instance 29	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/</a>
Instance 30	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/</a>
Instance 31	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html</a>

Instance 32	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html</a>
Instance 33	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html</a>
Instance 34	<a href="http://testphp.vulnweb.com/privacy.php">http://testphp.vulnweb.com/privacy.php</a>
Instance 35	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Instance 36	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Instance 37	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Instance 38	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Instance 39	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Instance 40	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Instance 41	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Instance 42	<a href="http://testphp.vulnweb.com/robots.txt">http://testphp.vulnweb.com/robots.txt</a>
Instance 43	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Instance 44	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Instance 45	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Instance 46	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Instance 47	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>