Static and Dynamic Analysis

ISTEC-Cyber Security

November 6, 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	**open**
25	smtp	filtered (*Reason: no-response*)
80	http	**open**
9929	nping-echo	**open**
31337	Elite	**open**

4.1 Risk Summary

Risk Level	Number of Findings
Low Risk	204
Medium Risk	130
High Risk	1
Critical Risk	0

Table 2: Summary of Risk Findings

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
- 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

Vulnerability 1	
Risk Level	High (High)
Vulnerability Name	Cross Site Scripting (DOM Based)

Description	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.

Instances	**URI**
Instance 1	http://testphp.vulnweb.com/#jaVasCript: /*-/*\unhbox\voidb@x\bgroup\let\unhbox\ voidb@x\setbox\@tempboxa\hbox{/\global\ mathchardef\accent@spacefactor\spacefactor}\ let\begingroup\let\typeout\protect\ begingroup\def\MessageBreak{Ω(Font)}\let\ protect\immediate\write\m@ne{LaTeXFontInfo: oninputline157.}\endgroup\endgroup\relax\ let\ignorespaces\relax\accent18/\egroup\ spacefactor\accent@spacefactor*\‘/*’/*"/ **/(/**/oNcliCk=alert(5397))//%0D%0A%0d%0a/ /</stYle/</titLe/</teXtarEa/</scRipt/--!>sVg/ <sVg/oNloAd=alert(5397)//>

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

Description	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: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site.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.
Instances	**URI**
Instance 1	`http://testphp.vulnweb.com/`
Instance 2	`http://testphp.vulnweb.com/artists.php`
Instance 3	`http://testphp.vulnweb.com/artists.php?artist=1`
Instance 4	`http://testphp.vulnweb.com/artists.php?artist=2`
Instance 5	`http://testphp.vulnweb.com/artists.php?artist=3`
Instance 6	`http://testphp.vulnweb.com/cart.php`
Instance 7	`http://testphp.vulnweb.com/categories.php`
Instance 8	`http://testphp.vulnweb.com/disclaimer.php`
Instance 9	`http://testphp.vulnweb.com/guestbook.php`
Instance 10	`http://testphp.vulnweb.com/guestbook.php`

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

Instance 38	http://testphp.vulnweb.com/guestbook.php
Instance 39	http://testphp.vulnweb.com/guestbook.php
Instance 40	http://testphp.vulnweb.com/search.php?test=query

Vulnerability 3	
Risk Level	Medium (High)
Vulnerability Name	Content Security Policy (CSP) Header Not Set
Description	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.
Instances	**URI**
Instance 1	http://testphp.vulnweb.com/
Instance 2	http://testphp.vulnweb.com/AJAX/index.php
Instance 3	http://testphp.vulnweb.com/artists.php
Instance 4	http://testphp.vulnweb.com/artists.php?artist=1
Instance 5	http://testphp.vulnweb.com/artists.php?artist=2
Instance 6	http://testphp.vulnweb.com/artists.php?artist=3
Instance 7	http://testphp.vulnweb.com/cart.php
Instance 8	http://testphp.vulnweb.com/categories.php
Instance 9	http://testphp.vulnweb.com/disclaimer.php
Instance 10	http://testphp.vulnweb.com/guestbook.php

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

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

Vulnerability 4	
Risk Level	Medium (Medium)
Vulnerability Name	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
Instances	**URI**
Instance 1	http://testphp.vulnweb.com/AJAX/index.php
Instance 2	http://testphp.vulnweb.com/artists.php
Instance 3	http://testphp.vulnweb.com/artists.php?artist=1

Instance 4	http://testphp.vulnweb.com/artists.php?artist=2
Instance 5	http://testphp.vulnweb.com/artists.php?artist=3
Instance 6	http://testphp.vulnweb.com/cart.php
Instance 7	http://testphp.vulnweb.com/categories.php
Instance 8	http://testphp.vulnweb.com/disclaimer.php
Instance 9	http://testphp.vulnweb.com/guestbook.php
Instance 10	http://testphp.vulnweb.com/hpp/
Instance 11	http://testphp.vulnweb.com/hpp/?pp=12
Instance 12	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Instance 13	http://testphp.vulnweb.com/index.php
Instance 14	http://testphp.vulnweb.com/listproducts.php?artist=1
Instance 15	http://testphp.vulnweb.com/listproducts.php?artist=2
Instance 16	http://testphp.vulnweb.com/listproducts.php?artist=3
Instance 17	http://testphp.vulnweb.com/listproducts.php?cat=1
Instance 18	http://testphp.vulnweb.com/listproducts.php?cat=2
Instance 19	http://testphp.vulnweb.com/listproducts.php?cat=3
Instance 20	http://testphp.vulnweb.com/listproducts.php?cat=4
Instance 21	http://testphp.vulnweb.com/login.php
Instance 22	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Instance 23	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Instance 24	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Instance 25	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

Instance 26	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Instance 27	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Instance 28	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Instance 29	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Instance 30	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Instance 31	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Instance 32	http://testphp.vulnweb.com/product.php?pic=1
Instance 33	http://testphp.vulnweb.com/product.php?pic=2
Instance 34	http://testphp.vulnweb.com/product.php?pic=3
Instance 35	http://testphp.vulnweb.com/product.php?pic=4
Instance 36	http://testphp.vulnweb.com/product.php?pic=5
Instance 37	http://testphp.vulnweb.com/product.php?pic=6
Instance 38	http://testphp.vulnweb.com/product.php?pic=7
Instance 39	http://testphp.vulnweb.com/signup.php
Instance 40	http://testphp.vulnweb.com/cart.php
Instance 41	http://testphp.vulnweb.com/guestbook.php
Instance 42	http://testphp.vulnweb.com/search.php?test=query
Instance 43	http://testphp.vulnweb.com/secured/newuser.php

Vulnerability 5	
Risk Level	Low (Medium)
Vulnerability Name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Instances	**URI**
Instance 1	`http://testphp.vulnweb.com/`
Instance 2	`http://testphp.vulnweb.com/AJAX/index.php`
Instance 3	`http://testphp.vulnweb.com/artists.php`
Instance 4	`http://testphp.vulnweb.com/artists.php?artist=1`
Instance 5	`http://testphp.vulnweb.com/artists.php?artist=2`
Instance 6	`http://testphp.vulnweb.com/artists.php?artist=3`
Instance 7	`http://testphp.vulnweb.com/cart.php`
Instance 8	`http://testphp.vulnweb.com/categories.php`
Instance 9	`http://testphp.vulnweb.com/disclaimer.php`
Instance 10	`http://testphp.vulnweb.com/guestbook.php`
Instance 11	`http://testphp.vulnweb.com/hpp/`
Instance 12	`http://testphp.vulnweb.com/hpp/?pp=12`
Instance 13	`http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12`
Instance 14	`http://testphp.vulnweb.com/index.php`
Instance 15	`http://testphp.vulnweb.com/listproducts.php?artist=1`
Instance 16	`http://testphp.vulnweb.com/listproducts.php?artist=2`
Instance 17	`http://testphp.vulnweb.com/listproducts.php?artist=3`
Instance 18	`http://testphp.vulnweb.com/listproducts.php?cat=1`
Instance 19	`http://testphp.vulnweb.com/listproducts.php?cat=2`

Instance 20	http://testphp.vulnweb.com/listproducts.php?cat=3
Instance 21	http://testphp.vulnweb.com/listproducts.php?cat=4
Instance 22	http://testphp.vulnweb.com/login.php
Instance 23	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Instance 24	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Instance 25	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Instance 26	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Instance 27	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Instance 28	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Instance 29	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Instance 30	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Instance 31	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Instance 32	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Instance 33	http://testphp.vulnweb.com/privacy.php
Instance 34	http://testphp.vulnweb.com/product.php?pic=1
Instance 35	http://testphp.vulnweb.com/product.php?pic=2
Instance 36	http://testphp.vulnweb.com/product.php?pic=3
Instance 37	http://testphp.vulnweb.com/product.php?pic=4
Instance 38	http://testphp.vulnweb.com/product.php?pic=5
Instance 39	http://testphp.vulnweb.com/product.php?pic=6
Instance 40	http://testphp.vulnweb.com/product.php?pic=7
Instance 41	http://testphp.vulnweb.com/showimage.php?file=’%20+%20pict.item(0).firstChild.nodeValue%20+%20’

Instance 42	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Instance 43	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Instance 44	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Instance 45	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Instance 46	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Instance 47	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Instance 48	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Instance 49	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Instance 50	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Instance 51	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Instance 52	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Instance 53	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Instance 54	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Instance 55	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Instance 56	http://testphp.vulnweb.com/signup.php
Instance 57	http://testphp.vulnweb.com/userinfo.php
Instance 58	http://testphp.vulnweb.com/cart.php
Instance 59	http://testphp.vulnweb.com/guestbook.php
Instance 60	http://testphp.vulnweb.com/search.php?test=query
Instance 61	http://testphp.vulnweb.com/secured/newuser.php
Instance 62	http://testphp.vulnweb.com/userinfo.php

Vulnerability 6	
Risk Level	Low (High)
Vulnerability Name	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Instances	**URI**
Instance 1	`http://testphp.vulnweb.com/`
Instance 2	`http://testphp.vulnweb.com/AJAX/index.php`
Instance 3	`http://testphp.vulnweb.com/AJAX/styles.css`
Instance 4	`http://testphp.vulnweb.com/artists.php`
Instance 5	`http://testphp.vulnweb.com/artists.php?artist=1`
Instance 6	`http://testphp.vulnweb.com/artists.php?artist=2`
Instance 7	`http://testphp.vulnweb.com/artists.php?artist=3`
Instance 8	`http://testphp.vulnweb.com/cart.php`
Instance 9	`http://testphp.vulnweb.com/categories.php`
Instance 10	`http://testphp.vulnweb.com/disclaimer.php`
Instance 11	`http://testphp.vulnweb.com/Flash/add.swf`
Instance 12	`http://testphp.vulnweb.com/guestbook.php`
Instance 13	`http://testphp.vulnweb.com/high`
Instance 14	`http://testphp.vulnweb.com/hpp/`
Instance 15	`http://testphp.vulnweb.com/hpp/?pp=12`
Instance 16	`http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12`
Instance 17	`http://testphp.vulnweb.com/images/logo.gif`
Instance 18	`http://testphp.vulnweb.com/images/remark.gif`

Instance 19	http://testphp.vulnweb.com/index.php
Instance 20	http://testphp.vulnweb.com/listproducts.php?artist=1
Instance 21	http://testphp.vulnweb.com/listproducts.php?artist=2
Instance 22	http://testphp.vulnweb.com/listproducts.php?artist=3
Instance 23	http://testphp.vulnweb.com/listproducts.php?cat=1
Instance 24	http://testphp.vulnweb.com/listproducts.php?cat=2
Instance 25	http://testphp.vulnweb.com/listproducts.php?cat=3
Instance 26	http://testphp.vulnweb.com/listproducts.php?cat=4
Instance 27	http://testphp.vulnweb.com/login.php
Instance 28	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Instance 29	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Instance 30	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Instance 31	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Instance 32	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Instance 33	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Instance 34	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Instance 35	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Instance 36	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Instance 37	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Instance 38	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html

Instance 39	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Instance 40	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Instance 41	http://testphp.vulnweb.com/privacy.php
Instance 42	http://testphp.vulnweb.com/product.php?pic=1
Instance 43	http://testphp.vulnweb.com/product.php?pic=2
Instance 44	http://testphp.vulnweb.com/product.php?pic=3
Instance 45	http://testphp.vulnweb.com/product.php?pic=4
Instance 46	http://testphp.vulnweb.com/product.php?pic=5
Instance 47	http://testphp.vulnweb.com/product.php?pic=6
Instance 48	http://testphp.vulnweb.com/product.php?pic=7
Instance 49	http://testphp.vulnweb.com/robots.txt
Instance 50	http://testphp.vulnweb.com/secured/style.css
Instance 51	http://testphp.vulnweb.com/showimage.php?file=%27%20+%20pict.item(0).firstChild.nodeValue%20+%20%27
Instance 52	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Instance 53	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Instance 54	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Instance 55	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Instance 56	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Instance 57	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Instance 58	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Instance 59	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Instance 60	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg

Instance 61	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Instance 62	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Instance 63	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Instance 64	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Instance 65	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Instance 66	http://testphp.vulnweb.com/signup.php
Instance 67	http://testphp.vulnweb.com/sitemap.xml
Instance 68	http://testphp.vulnweb.com/style.css
Instance 69	http://testphp.vulnweb.com/userinfo.php
Instance 70	http://testphp.vulnweb.com/cart.php
Instance 71	http://testphp.vulnweb.com/guestbook.php
Instance 72	http://testphp.vulnweb.com/search.php?test=query
Instance 73	http://testphp.vulnweb.com/secured/newuser.php
Instance 74	http://testphp.vulnweb.com/userinfo.php

Vulnerability 7	
Risk Level	Low (Medium)
Vulnerability Name	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Instances	**URI**
Instance 1	http://testphp.vulnweb.com/
Instance 2	http://testphp.vulnweb.com/AJAX/index.php
Instance 3	http://testphp.vulnweb.com/AJAX/styles.css
Instance 4	http://testphp.vulnweb.com/artists.php
Instance 5	http://testphp.vulnweb.com/artists.php?artist=1
Instance 6	http://testphp.vulnweb.com/artists.php?artist=2
Instance 7	http://testphp.vulnweb.com/artists.php?artist=3
Instance 8	http://testphp.vulnweb.com/cart.php
Instance 9	http://testphp.vulnweb.com/categories.php
Instance 10	http://testphp.vulnweb.com/disclaimer.php
Instance 11	http://testphp.vulnweb.com/Flash/add.swf
Instance 12	http://testphp.vulnweb.com/guestbook.php
Instance 13	http://testphp.vulnweb.com/hpp/
Instance 14	http://testphp.vulnweb.com/hpp/?pp=12
Instance 15	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Instance 16	http://testphp.vulnweb.com/images/logo.gif
Instance 17	http://testphp.vulnweb.com/images/remark.gif
Instance 18	http://testphp.vulnweb.com/index.php
Instance 19	http://testphp.vulnweb.com/listproducts.php?artist=1
Instance 20	http://testphp.vulnweb.com/listproducts.php?artist=2
Instance 21	http://testphp.vulnweb.com/listproducts.php?artist=3
Instance 22	http://testphp.vulnweb.com/listproducts.php?cat=1
Instance 23	http://testphp.vulnweb.com/listproducts.php?cat=2
Instance 24	http://testphp.vulnweb.com/listproducts.php?cat=3

Instance 25	http://testphp.vulnweb.com/listproducts.php?cat=4
Instance 26	http://testphp.vulnweb.com/login.php
Instance 27	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Instance 28	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Instance 29	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Instance 30	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Instance 31	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Instance 32	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Instance 33	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Instance 34	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Instance 35	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Instance 36	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Instance 37	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Instance 38	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Instance 39	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Instance 40	http://testphp.vulnweb.com/product.php?pic=1
Instance 41	http://testphp.vulnweb.com/product.php?pic=2
Instance 42	http://testphp.vulnweb.com/product.php?pic=3
Instance 43	http://testphp.vulnweb.com/product.php?pic=4
Instance 44	http://testphp.vulnweb.com/product.php?pic=5
Instance 45	http://testphp.vulnweb.com/product.php?pic=6
Instance 46	http://testphp.vulnweb.com/product.php?pic=7
Instance 47	http://testphp.vulnweb.com/secured/style.css

Instance 48	http://testphp.vulnweb.com/showimage.php?file=’%20+%20pict.item(0).firstChild.nodeValue%20+%20’
Instance 49	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Instance 50	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Instance 51	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Instance 52	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Instance 53	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Instance 54	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Instance 55	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Instance 56	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Instance 57	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Instance 58	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Instance 59	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Instance 60	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Instance 61	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Instance 62	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Instance 63	http://testphp.vulnweb.com/signup.php
Instance 64	http://testphp.vulnweb.com/style.css
Instance 65	http://testphp.vulnweb.com/cart.php
Instance 66	http://testphp.vulnweb.com/guestbook.php
Instance 67	http://testphp.vulnweb.com/search.php?test=query

Instance 68	`http://testphp.vulnweb.com/secured/newuser.php`

Vulnerability 8	
Risk Level	Informational (Low)
Vulnerability Name	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
Instances	**URI**
Instance 1	`http://testphp.vulnweb.com/secured/newuser.php`

Vulnerability 9	
Risk Level	Informational (Low)
Vulnerability Name	Charset Mismatch (Header Versus Meta Content-Type Charset)
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.

Instances	**URI**
Instance 1	http://testphp.vulnweb.com/
Instance 2	http://testphp.vulnweb.com/AJAX/index.php
Instance 3	http://testphp.vulnweb.com/artists.php
Instance 4	http://testphp.vulnweb.com/artists.php?artist=1
Instance 5	http://testphp.vulnweb.com/artists.php?artist=2
Instance 6	http://testphp.vulnweb.com/artists.php?artist=3
Instance 7	http://testphp.vulnweb.com/cart.php
Instance 8	http://testphp.vulnweb.com/categories.php
Instance 9	http://testphp.vulnweb.com/disclaimer.php
Instance 10	http://testphp.vulnweb.com/guestbook.php
Instance 11	http://testphp.vulnweb.com/index.php
Instance 12	http://testphp.vulnweb.com/listproducts.php?artist=1
Instance 13	http://testphp.vulnweb.com/listproducts.php?artist=2
Instance 14	http://testphp.vulnweb.com/listproducts.php?artist=3
Instance 15	http://testphp.vulnweb.com/listproducts.php?cat=1
Instance 16	http://testphp.vulnweb.com/listproducts.php?cat=2
Instance 17	http://testphp.vulnweb.com/listproducts.php?cat=3
Instance 18	http://testphp.vulnweb.com/listproducts.php?cat=4
Instance 19	http://testphp.vulnweb.com/login.php
Instance 20	http://testphp.vulnweb.com/product.php?pic=1
Instance 21	http://testphp.vulnweb.com/product.php?pic=2
Instance 22	http://testphp.vulnweb.com/product.php?pic=3
Instance 23	http://testphp.vulnweb.com/product.php?pic=4
Instance 24	http://testphp.vulnweb.com/product.php?pic=5

Instance 25	http://testphp.vulnweb.com/product.php?pic=6
Instance 26	http://testphp.vulnweb.com/product.php?pic=7
Instance 27	http://testphp.vulnweb.com/signup.php
Instance 28	http://testphp.vulnweb.com/cart.php
Instance 29	http://testphp.vulnweb.com/guestbook.php
Instance 30	http://testphp.vulnweb.com/search.php?test=query
Instance 31	http://testphp.vulnweb.com/secured/newuser.php

Vulnerability 10	
Risk Level	Informational (Low)
Vulnerability Name	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Instances	**URI**
Instance 1	http://testphp.vulnweb.com/AJAX/index.php

Vulnerability 11	
Risk Level	Informational (Medium)
Vulnerability Name	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Instances	**URI**
Instance 1	http://testphp.vulnweb.com/AJAX/index.php

Instance 2	http://testphp.vulnweb.com/artists.php
Instance 3	http://testphp.vulnweb.com/artists.php?artist=1
Instance 4	http://testphp.vulnweb.com/artists.php?artist=2
Instance 5	http://testphp.vulnweb.com/artists.php?artist=3
Instance 6	http://testphp.vulnweb.com/listproducts.php?artist=1
Instance 7	http://testphp.vulnweb.com/listproducts.php?artist=2
Instance 8	http://testphp.vulnweb.com/listproducts.php?cat=1
Instance 9	http://testphp.vulnweb.com/listproducts.php?cat=2

Vulnerability 12	
Risk Level	Informational (Low)
Vulnerability Name	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
Instances	**URI**
Instance 1	http://testphp.vulnweb.com/guestbook.php
Instance 2	http://testphp.vulnweb.com/search.php?test=query
Instance 3	http://testphp.vulnweb.com/search.php?test=query