acunetix

Affected Items Report

Acunetix Security Audit

2022-08-30

Generated by Acunetix

Scan of rksk.in

Scan details

Scan information	
Start time	2022-08-30T11:00:35.423234+05:30
Start url	rksk.in
Host	rksk.in
Scan time	102 minutes, 18 seconds
Profile	Full Scan
Server information	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.23
Responsive	True
Server OS	Unix
Server technologies	PHP
Scan status	failed

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	36
High	8
Medium	5
Low	10
Informational	13

Affected items

/add_phc.php	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **dist_id** was set to **57'"()&%<acx><ScRiPt >OD2Y(9943) </ScRiPt>**

```
POST /add_phc.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://rksk.in/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 96

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



dist_id=57'"()%26%25<acx><ScRiPt%20>OD2Y(9943)
</ScRiPt>&phc_code=94102&phc_name=wUmrLVWz&submit=
```

/add_phc.php	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **phc_code** was set to **94102'"()&%<acx><ScRiPt >G1D3(9709) </ScRiPt>**

```
POST /add_phc.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://rksk.in/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 96

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



dist_id=25&phc_code=94102'"()%26%25<acx><ScRiPt%20>G1D3(9709)
</ScRiPt>&phc_name=wUmrLVWz&submit=
```

/add_phc.php	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **phc_name** was set to **wUmrLVWz'"()&%<acx><ScRiPt >G1D3(9677)</ScRiPt>**

```
POST /add_phc.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://rksk.in/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 96

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



dist_id=25&phc_code=94102&phc_name=wUmrLVWz'"()%26%25<acx><ScRiPt%20>G1D3(9677)
</ScRiPt>&submit=
```

/add_phc.php	
Alert group	**SQL injection**
Severity	High
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **dist_id** was set to **1'"** Error message found: `You have an error in your SQL syntax`

```
POST /add_phc.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://rksk.in/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 52

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



dist_id=1'"&phc_code=94102&phc_name=wUmrLVWz&submit=
```

/add_phc.php	
Alert group	**SQL injection**
Severity	High
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **phc_code** was set to **1'"** Error message found: `You have an error in your SQL syntax`

```
POST /add_phc.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://rksk.in/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 49

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



dist_id=28&phc_code=1'"&phc_name=wUmrLVWz&submit=
```

/add_phc.php	
Alert group	**SQL injection**
Severity	High
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **phc_name** was set to **1'"** Error message found: `You have an error in your SQL syntax`

```
POST /add_phc.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://rksk.in/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 46

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



dist_id=28&phc_code=94102&phc_name=1'"&submit=
```

/admin_login1.php	
Alert group	**SQL injection (verified)**
Severity	High
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **username** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z** Tests performed: • 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.234** • 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.122** • 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.25** • 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.261** • 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.175** • 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.28** • 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.202** Original value: **wUmrLVWz**

```
POST /admin_login1.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: http://rksk.in/

Cookie: PHPSESSID=3ggicppm56ertiemgot5h1qcpj

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

Accept-Encoding: gzip,deflate

Content-Length: 61

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



save=&username=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
```

/login.php	
Alert group	**SQL injection (verified)**
Severity	High
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **username** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z** Tests performed: • 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.151** • 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.137** • 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.072** • 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.05** • 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.065** • 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.082** • 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.071** Original value: **wUmrLVWz**

```
POST /login.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: http://rksk.in/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 61

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



save=&username=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
```

/marriage.php	
Alert group	**Amazon S3 public bucket**
Severity	Medium
Description	Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. Files within S3 are organized into "buckets", which are named logical containers accessible at a predictable URL. Access controls can be applied to both the bucket itself and to individual objects (files and directories) stored within that bucket. A bucket is considered public if any user can list the contents of the bucket, and private if the bucket's contents can only be listed or written by certain S3 users. This web application is using a public Amazon S3 bucket. This is not recommended, as a public bucket will list all of its files and directories to an any user that asks.
Recommendations	Make sure all the Amazon S3 buckets you are using are marked as private.
Alert variants	
Details	Affected Amazon S3 bucket: **cdn.amcharts.com**. Bucket found on page **http://rksk.in/marriage.php**, original URL was .

```
GET /marriage.php HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Application error messages**
Severity	Medium
Description	This alert requires manual confirmation Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).
Recommendations	Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.
Alert variants	
Details	Application error messages: • http://rksk.in/add_phc.php **Table 'indevcon_rksk.phc' doesn't exist** • http://rksk.in/admin_rksk/changelog.txt **Fatal error** • http://rksk.in/admin_rksk/changelog.txt **Fatal error: Call to a member function cellExists() line: 3327 in calculation.php if referenced worksheet doesn't exist - Bugfix: (MBaker) Work Item GH-290 - AdvancedValueBinder "Division by zero"-error - Bugfix: (MBaker) Work Item CP20604 - Adding Sheet to Workbook Bug - Bugfix: (MBaker) Work item CP20703 - Calculation engine incorrectly evaluates empty cells as #VALUE - Bugfix: (MBaker) Work item CP20760 - Formula references to cell on another sheet in ODS files - Bugfix: (MBaker) Work item GH321,GH158,CP17824 - LibreOffice created XLSX files results in an empty file. - Feature: (amerov) - Implementation of the Excel HLOOKUP() function - Feature: (MBaker) - Added "Quote Prefix" to style settings (Excel2007 Reader and Writer only) - Feature: (MBaker) - Added Horizontal FILL alignment for Excel5 and Excel2007 Readers/Writers, and Horizontal DISTRIBUTED alignment for Excel2007 Reader/Writer - Feature: (trvrnrth) Work Item GH-261 - Add support for reading protected (RC4 encrypted) .xls files - Feature: (LWol) Work Item GH-252 - Adding support for macros, Ribbon in Excel 2007 - General: (cdhutch) Work item CP20055 - Remove array_shift in ReferenceHelper::insertNewBefore improves column or row delete speed - General: (MBaker) - Improve stock chart handling and rendering, with help from Swashata Ghosh - General: (MBaker) - Fix to calculation properties for**

Excel2007 so that the opening application will only recalculate on load if it's actually required - General: (MBaker) - Modified Excel2007 Writer to default preCalculateFormulas to false Note that autosize columns will still recalculate affected formulae internally - General: (dresenhista) Work Item GH-242 - Functionality to getHighestRow() for a specified column, and getHighestColumn() for a specified row - General: (adamriyadi) Work Item GH-247 - Modify PHPExcel_Reader_Excel2007 to use zipClass from PHPExcel_Settings::getZipClass() This allows the use of PCLZip when reading for people that don't have access to ZipArchive - General: (infojunkie) Work Item GH-276 - Convert properties to string in OOCalc reader - Security: (maartenba) Work Item GH-322 - Disable libxml external entity loading by default. This is to prevent XML External Entity Processing (XXE) injection attacks (see http://websec.io/2012/08/27/Preventing-XEE-in-PHP.html for an explanation of XXE injection). Reference CVE-2014-2054 2013-06-02 (v1.7.9): - Feature: (MBaker) Include charts option for HTML Writer - Feature: (MBaker) Added composer file - Feature: (MBaker) Added getStyle() method to Cell object - Bugfix: (Asker) Work item 18777 - Error in PHPEXCEL/Calculation.php script on line 2976 (stack pop check) - Bugfix: (MBaker) Work item 18794 - CSV files without a file extension being identified as HTML - Bugfix: (AndreKR) Work item GH-66 - Wrong check for maximum number of rows in Excel5 Writer - Bugfix: (MBaker) Work item GH-67 - Cache directory for DiscISAM cache storage cannot be set - Bugfix: (MBaker) Work item 17976 - Fix to Excel2007 Reader for hyperlinks with an anchor fragment (following a #), otherwise they were treated as sheet references - Bugfix: (MBaker) Work item 18963 - getSheetNames() fails on numeric (floating point style) names with trailing zeroes - Bugfix: (MBaker) Work item GH-130 - Single cell print area - General: (kea) Work item GH-69 - Improved AdvancedValueBinder for currency - General: (MBaker) Work items 17936 and 17840 - Fix for environments where there is no access to /tmp but to upload_tmp_dir Provided an option to set the sys_get_temp_dir() call to use the upload_tmp_dir; though by default the standard temp directory will still be used - General: (amironov) Work item GH-84 - Search style by identity in PHPExcel_Worksheet::duplicateStyle() - General: (karak) Work item GH-85 - Fill SheetView IO in Excel5 - General: (cfhay) Work item 18958 - Memory and Speed improvements in PHPExcel_Reader_Excel5 - General: (MBaker) Work item GH-78 - Modify listWorksheetNames() and listWorksheetInfo to use XMLReader with streamed XML rather than SimpleXML - General: (dbonsch) Restructuring of PHPExcel Exceptions - General: (MBaker) Work items 16926 and 15145 - Refactor Calculation Engine from singleton to a Multiton Ensures that calculation cache is maintained independently for different workbooks - General: (MBaker) Modify cell's getCalculatedValue() method to return the content of RichText objects rather than the RichText object itself - Bugfix: (techhead) Work item GH-70 - Fixed formula/formatting bug when removing rows - Bugfix: (alexgann) Work item GH-63 - Fix to cellExists for non-existent namedRanges - Bugfix: (MBaker) Work item 18844 - cache_in_memory_gzip "eats" last worksheet line, cache_in_memory doesn't - Feature: (Progi1984) Work item GH-22 - Sheet View in Excel5 Writer - Bugfix: (amironov) Work item GH-82 - PHPExcel_Worksheet::getCellCollection() may not return last cached cell - Bugfix: (teso) Work item 18551 - Rich Text containing UTF-8 characters creating unreadable content with Excel5 Writer - Bugfix: (MBaker) Work item GH-104 - echo statements in HTML.php - Feature: (Progi1984) Work item GH-8/CP11704 : Conditional formatting in Excel 5 Writer - Bugfix: (MBaker) Work item GH-113 - canRead() Error for GoogleDocs ODS files: in ODS files from Google Docs there is no mimetype file - Bugfix: (MBaker) Work item GH-80 - "Sheet index is out of bounds." Exception - Bugfix: (ccorliss) Work item GH-105 - Fixed number format fatal error - Bugfix: (MBaker) - Add DROP TABLE in destructor for SQLite and SQLite3 cache controllers - Bugfix: (alexgann) Work item GH-154 - Fix merged-cell borders on HTML/PDF output - Bugfix: (Shanto) Work item GH-161 - Fix: Hyperlinks break when removing rows - Bugfix: (neclimdul) Work item GH-166 - Fix Extra Table Row From Images and Charts 2012-10-12 (v1.7.8): - Special: (kkamkou) Phar builder script to add phar file as a distribution option - Feature: (MBaker) Refactor PDF Writer to allow use with a choice of PDF Rendering library

	rather than restricting to tcPDF Current options are tcPDF, mPDF, DomPDF tcPDF Library has now been removed from the deployment bundle - Feature: (MBaker) Initial version of HTML Reader - Feature: (Progi1984) & (blazzy) Work items 9605 - Implement support for AutoFilter in PHPExcel_Writer_Excel5 - Feature: (MBaker) Modified ERF and ERFC Engineering functions to accept Excel 2010's modified acceptance of negative arguments - Feature: (k1LoW) Support SheetView `view` attribute (Excel2007) - Feature: (MBaker) Excel compatibility option added for writing CSV files While Excel 2010 can read CSV files with a simple UTF-8 BOM, Excel2007 and earlier require UTF-16LE encoded tab-separated files. The new setExcelCompatibility(TRUE) option for the CSV Writer will generate files with this formatting for easy import into Excel2007 and below. - Feature: (MBaker) Language implementations for Turkish (tr) - Feature: (MBaker) Added fraction tests to advanced value binder - Feature: (MBaker) Allow call to font setUnderline() for underline format to specify a simple boolean for UNDERLINE_NONE or UNDERLINE_SINGLE - General: (alexgann) Add Currency detection to the Advanced Value Binder - General: (MBaker) Work item 18404 - setCellValueExplicitByColumnAndRow()

```
POST /add_phc.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://rksk.in/add_phc.php

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Content-Length: 51

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



dist_id=57&phc_code=94102&phc_name=wUmrLVWz&submit=
```

Web Server	
Alert group	**Directory listings (verified)**
Severity	Medium
Description	Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.
Recommendations	You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.
Alert variants	

Details	Folders with directory listing enabled: • http://rksk.in/assets/ • http://rksk.in/assets/css/ • http://rksk.in/sites/default/files/js/ • http://rksk.in/sites/default/files/ • http://rksk.in/sites/default/ • http://rksk.in/sites/default/files/css/ • http://rksk.in/sites/ • http://rksk.in/assets/js/ • http://rksk.in/api/ • http://rksk.in/images/ • http://rksk.in/sites/all/ • http://rksk.in/sites/all/modules/ • http://rksk.in/sites/all/modules/custom_slideshow_helper/ • http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/ • http://rksk.in/sites/all/modules/custom_slideshow_helper/css/ • http://rksk.in/data/ • http://rksk.in/includes/ • http://rksk.in/sites/all/themes/unfpa_global/ • http://rksk.in/sites/all/themes/unfpa_global/css/ • http://rksk.in/sites/all/themes/unfpa_global/css/fonts/ • http://rksk.in/sites/all/themes/unfpa_global/css/fonts/roboto/

```
GET /assets/ HTTP/1.1

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**User credentials are sent in clear text**
Severity	Medium
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
Recommendations	Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).
Alert variants	

Details	Forms with credentials sent in clear text:
	• http://rksk.in/admin_login1.php
	`Form name: <empty>`
	`Form action: <empty>`
	`Form method: POST`
	`Password input: password`
	• http://rksk.in/admin_login.php
	`Form name: <empty>`
	`Form action: <empty>`
	`Form method: POST`
	`Password input: password`

```
GET /admin_login1.php HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Vulnerable JavaScript libraries**
Severity	Medium
Description	You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	• **jQuery 1.10.2** ◦ URL: http://rksk.in/sites/default/files/js/js_Iu231mfdeiEoaLXCWaLUWEw3lvVKe8tL-KJCcJMguXo.js ◦ Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered. ◦ References: ▪ https://github.com/jquery/jquery/issues/2432 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

```
GET /sites/default/files/js/js_Iu231mfdeiEoaLXCWaLUWEw3lvVKe8tL-KJCcJMguXo.js HTTP/1.1

Host: rksk.in

accept-language: en-US

accept: */*

Referer: http://rksk.in/

Accept-Encoding: gzip,deflate

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36
```

Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	

```
GET / HTTP/1.1

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Cookies with missing, inconsistent or contradictory properties (verified)**

Severity	Low
Description	At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.
Recommendations	Ensure that the cookies configuration complies with the applicable standards.
Alert variants	

Details	List of cookies with missing, inconsistent or contradictory properties:
	• http://rksk.in/admin_login1.php
	Cookie was set via:
	`Set-Cookie: PHPSESSID=3ggicppm56ertiemgot5h1qcpj; path=/`
	This cookie has the following issues:
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`

```
GET /admin_login1.php HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Cookies without HttpOnly flag set (verified)**
Severity	Low
Description	One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HttpOnly flag for these cookies.
Alert variants	

Details	Cookies without HttpOnly flag set: • http://rksk.in/admin_login1.php `Set-Cookie: PHPSESSID=3ggicppm56ertiemgot5h1qcpj; path=/`

```
GET /admin_login1.php HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Documentation files**
Severity	Low
Description	One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.
Recommendations	Remove or restrict access to all documentation file acessible from internet.
Alert variants	

Details	Documentation files:
	• http://rksk.in/admin_rksk/**changelog.txt**
	File contents (first 100 characters):
	`********** * PHPExcel * ...`
	• http://rksk.in/admin_rksk/**license.txt**
	File contents (first 100 characters):
	`GNU LESSER GENERAL PUBLIC LICENSE  TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATI`

```
GET /admin_rksk/changelog.txt HTTP/1.1

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

/admin_login1.php	
Alert group	**Login page password-guessing attack**
Severity	Low
Description	A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
Recommendations	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.
Alert variants	
Details	

```
POST /admin_login1.php HTTP/1.1

Referer: http://rksk.in/admin_login1.php

Cookie: PHPSESSID=8u6t9mh07cbg8bfoi96e85uifr;

Content-Type: application/x-www-form-urlencoded

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

Accept-Encoding: gzip,deflate

Content-Length: 48

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive



username=username&password=testing&login=Log In&
```

Web Server	
Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Pages with potential relative path overwrite: • http://rksk.in/index.php CSS import from a relative path: `<link type="text/css" rel="stylesheet" href="assets/css/find.css` • http://rksk.in/marriage.php CSS import from a relative path: `<link type="text/css" rel="stylesheet" href="assets/css/find.css` • http://rksk.in/afhc_list.php CSS import from a relative path: `<link type="text/css" rel="stylesheet" href="assets/css/find.css` • http://rksk.in/chc_list.php CSS import from a relative path: `<link type="text/css" rel="stylesheet" href="assets/css/find.css`

- http://rksk.in/communicable_disease.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/dashboard_static.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/clientlist.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/injury.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/dashboard_static_srh.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/mental_health.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/outreachlist.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/phc_list.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/static_vulnerable.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/static_ncd.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/static_communication.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/subcenter_list.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/substances_abuse.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/user_list.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/hr_management_list.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/static_cd.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

- http://rksk.in/add_hr_management.php
  CSS import from a relative path:

```
<link type="text/css" rel="stylesheet" href="assets/css/find.css
```

```
GET /index.php/j02ca/ HTTP/1.1

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to these directories or remove them from the website.
Alert variants	
Details	Possible sensitive directories: • http://rksk.in/**includes** • http://rksk.in/admin_rksk/**nbproject** • http://rksk.in/admin_rksk/**includes** • http://rksk.in/manual/**developer**

```
GET /includes/ HTTP/1.1

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Possible sensitive files**
Severity	Low
Description	A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
Recommendations	Restrict access to this file or remove it from the website.
Alert variants	
Details	Possible sensitive files: • http://rksk.in/manual/**logs.html**

```
GET /manual/logs.html HTTP/1.1

Accept: acunetix/wvs

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**TRACE method is enabled**
Severity	Low
Description	HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.
Recommendations	Disable TRACE Method on the web server.
Alert variants	

Details	

```
TRACE /liGDtrpMmo HTTP/1.1

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Unencrypted connection (verified)**
Severity	Low
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```
GET / HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Content Security Policy (CSP) not implemented**
Severity	Informational

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.
	
	Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:
	
	`Content-Security-Policy:`
	`default-src 'self';`
	`script-src 'self' https://code.jquery.com;`
	
	It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

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

Details	Paths without CSP header: • http://rksk.in/ • http://rksk.in/index.php • http://rksk.in/marriage.php • http://rksk.in/images/ • http://rksk.in/api/ • http://rksk.in/admin_login1.php • http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/flexslider-icon-2.html • http://rksk.in/admin_rksk/image/acunetix.txt • http://rksk.in/misc/ • http://rksk.in/data/ • http://rksk.in/includes/ • http://rksk.in/sites/all/themes/unfpa_global/css/fonts/roboto/ • http://rksk.in/login.php • http://rksk.in/manual/ • http://rksk.in/modules/ • http://rksk.in/afhc_list.php • http://rksk.in/chc_list.php • http://rksk.in/communicable_disease.php • http://rksk.in/dashboard_static.php • http://rksk.in/clientlist.php • http://rksk.in/graph.php

```
GET / HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Content type is not specified (verified)**
Severity	Informational
Description	These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.
Recommendations	Set a Content-Type header value for these page(s).
Alert variants	
Details	Pages where the content-type header is not specified: • http://rksk.in/data/error_log

```
GET /data/error_log HTTP/1.1

Referer: http://rksk.in/data/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Email addresses**
Severity	Informational

Description	One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Emails found: • http://rksk.in/icons/ **kevinh@kevcom.com** • http://rksk.in/icons/ **mike@hyperreal.org**

```
GET /icons/ HTTP/1.1

Referer: http://rksk.in/images/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Insecure Referrer Policy**
Severity	Informational
Description	Referrer Policy controls behaviour of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.
Recommendations	Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value
Alert variants	

Details	URLs where Referrer Policy configuration is insecure: • http://rksk.in/ • http://rksk.in/index.php • http://rksk.in/marriage.php • http://rksk.in/images/ • http://rksk.in/api/ • http://rksk.in/admin_login1.php • http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/flexslider-icon-2.html

```
GET / HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Internal IP address disclosure**
Severity	Informational
Description	One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks. The significance of this finding should be confirmed manually.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pages with internal IPs: • http://rksk.in/manual/howto/access.html **10.252.46.165**

```
GET /manual/howto/access.html HTTP/1.1

Referer: http://rksk.in/manual/

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Javascript Source map detected**
Severity	Informational
Description	Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript.
Recommendations	According to the best practices, source maps should not be accesible for an attacker. Consult web references for more information
Alert variants	
Details	URLs where links to SourceMaps were found: • sourceMappingURL in JS body - http://rksk.in/amchart/animated.js • sourceMappingURL in JS body - http://rksk.in/assets/js/highcharts.js

```
GET /amchart/animated.js HTTP/1.1

Referer: http://rksk.in/static_cd.php

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server

Alert group	No HTTP Redirection
Severity	Informational
Description	It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.
Recommendations	It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information
Alert variants	
Details	

```
GET / HTTP/1.1

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	• **Highcharts 7.1.2** ◦ URL: http://rksk.in/assets/js/highcharts.js ◦ Detection method: The library's name and version were determined based on the file's contents. ◦ References: ▪ https://github.com/highcharts/highcharts/releases

```
GET /assets/js/highcharts.js HTTP/1.1

Referer: http://rksk.in/marriage.php

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	

Details	Pages with auto-complete password inputs:
	• http://rksk.in/admin_login1.php
	`Form name: <empty>`
	`Form action: <empty>`
	`Form method: POST`
	`Password input: password`
	• http://rksk.in/login.php
	`Form name: <empty>`
	`Form action: <empty>`
	`Form method: POST`
	`Password input: login`
	• http://rksk.in/admin_login.php
	`Form name: <empty>`
	`Form action: <empty>`
	`Form method: POST`
	`Password input: password`

```
GET /admin_login1.php HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Web Server	
Alert group	**PHP Version Disclosure**
Severity	Informational
Description	The web server is sending the X-Powered-By: response headers, revealing the PHP version.
Recommendations	Configure your web server to prevent information leakage from its HTTP response.
Alert variants	
Details	Version detected: **PHP/7.3.23**.

/afhc_list.php	
Alert group	**Subresource Integrity (SRI) not implemented**
Severity	Informational
Description	Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match. Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512. The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Recommendations	Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).
	
	For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.
	
	`<script src="https://example.com/example-framework.js"`
	`integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HN`
	`crossorigin="anonymous"></script>`

Alert variants	
Details	Pages where SRI is not implemented: • http://rksk.in/afhc_list.php Script SRC: **https://cdn.datatables.net/1.10.19/js/jquery.dataTables.min.js**

```
GET /afhc_list.php HTTP/1.1

Referer: http://rksk.in/marriage.php

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

/dashboard_static.php	
Alert group	**Subresource Integrity (SRI) not implemented**
Severity	Informational

Description	Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match. Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512. The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Recommendations	Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).
	
	For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.
	
	`<script src="https://example.com/example-framework.js"`
	`integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HN`
	`crossorigin="anonymous"></script>`

Alert variants	
Details	Pages where SRI is not implemented: • http://rksk.in/dashboard_static.php Script SRC: **https://maps.googleapis.com/maps/api/js?key=AIzaSyCkiEn37V_FFSkk2jHYTlzOg3YUcb-ak9I&callback=initMap&sensor=false&region=IN**

```
GET /dashboard_static.php HTTP/1.1

Referer: http://rksk.in/marriage.php

Cookie: PHPSESSID=ki0v1t5sveu8qsnujfciadevsg

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

/marriage.php	
Alert group	**Subresource Integrity (SRI) not implemented**
Severity	Informational
Description	Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match. Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512. The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Recommendations	Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).
	
	For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.
	
	`<script src="https://example.com/example-framework.js"`
	`integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HN`
	`crossorigin="anonymous"></script>`

Alert variants	
Details	Pages where SRI is not implemented: • http://rksk.in/marriage.php Script SRC: **https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js** • http://rksk.in/marriage.php Script SRC: **https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js** • http://rksk.in/marriage.php Script SRC: **https://maxcdn.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js** • http://rksk.in/marriage.php Script SRC: **https://code.jquery.com/jquery-3.1.1.min.js** • http://rksk.in/marriage.php Script SRC: **https://code.highcharts.com/highcharts.js** • http://rksk.in/marriage.php Script SRC: **https://cdn.amcharts.com/lib/4/core.js**

```
GET /marriage.php HTTP/1.1

Referer: http://rksk.in/

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

Accept-Encoding: gzip,deflate

Host: rksk.in

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive
```

Scanned items (coverage report)

http://rksk.in/
http://rksk.in/add_hr_management.php
http://rksk.in/add_phc.php
http://rksk.in/add_wifs_monthaly_report.php
http://rksk.in/admin_login.php
http://rksk.in/admin_login1.php
http://rksk.in/admin_rksk/
http://rksk.in/admin_rksk/afc_report.php
http://rksk.in/admin_rksk/afhc.php
http://rksk.in/admin_rksk/ahd_report.php
http://rksk.in/admin_rksk/assets/
http://rksk.in/admin_rksk/assets/css/
http://rksk.in/admin_rksk/assets/css/bootstrap.min.css
http://rksk.in/admin_rksk/assets/css/icons.css
http://rksk.in/admin_rksk/assets/css/style.css
http://rksk.in/admin_rksk/assets/images/
http://rksk.in/admin_rksk/assets/js/
http://rksk.in/admin_rksk/assets/js/bootstrap.bundle.min.js
http://rksk.in/admin_rksk/assets/js/detect.js
http://rksk.in/admin_rksk/assets/js/fastclick.js
http://rksk.in/admin_rksk/assets/js/jquery.app.js
http://rksk.in/admin_rksk/assets/js/jquery.blockUI.js
http://rksk.in/admin_rksk/assets/js/jquery.core.js
http://rksk.in/admin_rksk/assets/js/jquery.min.js
http://rksk.in/admin_rksk/assets/js/jquery.scrollTo.min.js
http://rksk.in/admin_rksk/assets/js/jquery.slimscroll.js
http://rksk.in/admin_rksk/assets/js/modernizr.min.js
http://rksk.in/admin_rksk/assets/js/waves.js
http://rksk.in/admin_rksk/assets/pages/
http://rksk.in/admin_rksk/assets/pages/jquery.dashboard.js
http://rksk.in/admin_rksk/changelog.txt
http://rksk.in/admin_rksk/chc_list.php
http://rksk.in/admin_rksk/client.php
http://rksk.in/admin_rksk/clinical_services.php
http://rksk.in/admin_rksk/core/
http://rksk.in/admin_rksk/core/core.html
http://rksk.in/admin_rksk/core/core.plugin.html
http://rksk.in/admin_rksk/counselling_services.php
http://rksk.in/admin_rksk/coverage.php
http://rksk.in/admin_rksk/dashboard.php
http://rksk.in/admin_rksk/district_listing.php
http://rksk.in/admin_rksk/image/
http://rksk.in/admin_rksk/image/acunetix.txt
http://rksk.in/admin_rksk/includes/
http://rksk.in/admin_rksk/license.txt
http://rksk.in/admin_rksk/list_du_know.php
http://rksk.in/admin_rksk/list_success_story.php
http://rksk.in/admin_rksk/logout.php
http://rksk.in/admin_rksk/mh_report.php
http://rksk.in/admin_rksk/mh_reporting1.php
http://rksk.in/admin_rksk/mpr_report.php
http://rksk.in/admin_rksk/nbproject/
http://rksk.in/admin_rksk/outreach.php
http://rksk.in/admin_rksk/pe_monthly_reporting1.php
http://rksk.in/admin_rksk/plugins/
http://rksk.in/admin_rksk/plugins/counterup/
http://rksk.in/admin_rksk/plugins/counterup/jquery.counterup.min.js
http://rksk.in/admin_rksk/plugins/datatables/

http://rksk.in/admin_rksk/plugins/datatables/buttons.bootstrap4.min.js
http://rksk.in/admin_rksk/plugins/datatables/buttons.html5.min.js
http://rksk.in/admin_rksk/plugins/datatables/buttons.print.min.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.bootstrap4.min.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.buttons.min.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.colVis.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.fixedColumns.min.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.fixedHeader.min.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.keyTable.min.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.responsive.min.js
http://rksk.in/admin_rksk/plugins/datatables/dataTables.scroller.min.js
http://rksk.in/admin_rksk/plugins/datatables/jquery.dataTables.min.js
http://rksk.in/admin_rksk/plugins/datatables/jszip.min.js
http://rksk.in/admin_rksk/plugins/datatables/pdfmake.min.js
http://rksk.in/admin_rksk/plugins/datatables/responsive.bootstrap4.min.js
http://rksk.in/admin_rksk/plugins/datatables/vfs_fonts.js
http://rksk.in/admin_rksk/plugins/morris/
http://rksk.in/admin_rksk/plugins/morris/morris.css
http://rksk.in/admin_rksk/plugins/morris/morris.min.js
http://rksk.in/admin_rksk/plugins/raphael/
http://rksk.in/admin_rksk/plugins/raphael/raphael-min.js
http://rksk.in/admin_rksk/plugins/waypoints/
http://rksk.in/admin_rksk/plugins/waypoints/jquery.waypoints.min.js
http://rksk.in/admin_rksk/program_planning1.php
http://rksk.in/admin_rksk/service_provider.php
http://rksk.in/admin_rksk/users.csv
http://rksk.in/admin_rksk/wifs.php
http://rksk.in/afhc_list.php
http://rksk.in/amchart/
http://rksk.in/amchart/animated.js
http://rksk.in/amchart/charts.js
http://rksk.in/amchart/core.js
http://rksk.in/api/
http://rksk.in/api/api_test.php
http://rksk.in/api/clients_details.php
http://rksk.in/api/config.php
http://rksk.in/api/connection.php
http://rksk.in/api/dashboard_data.php
http://rksk.in/api/download_general.php
http://rksk.in/api/download_general_test.php
http://rksk.in/api/download_test.php
http://rksk.in/api/Image/
http://rksk.in/api/insert_general.php
http://rksk.in/api/insert_general1.php
http://rksk.in/api/jwt/
http://rksk.in/api/language.php
http://rksk.in/api/login.php
http://rksk.in/api/online_search.php
http://rksk.in/api/outreach.php
http://rksk.in/api/register.php
http://rksk.in/api/search_location.php
http://rksk.in/api/test_register.php
http://rksk.in/api/update_service_provider.php
http://rksk.in/assets/
http://rksk.in/assets/css/
http://rksk.in/assets/css/files_founds.css
http://rksk.in/assets/css/find.css
http://rksk.in/assets/css/found_files.css
http://rksk.in/assets/css/icoc.css
http://rksk.in/assets/css/login.css
http://rksk.in/assets/css/style.css

http://rksk.in/assets/css/tooltip.css
http://rksk.in/assets/js/
http://rksk.in/assets/js/analitics.js
http://rksk.in/assets/js/demo.js
http://rksk.in/assets/js/highcharts.js
http://rksk.in/assets/js/moment_timeline_tweet.a20574004ea824b1c047f200045ffa1e.js
http://rksk.in/assets/js/sdk.js
http://rksk.in/chc_list.php
http://rksk.in/clientlist.php
http://rksk.in/communicable_disease.php
http://rksk.in/dashboard.php
http://rksk.in/dashboard_static.php
http://rksk.in/dashboard_static_srh.php
http://rksk.in/data/
http://rksk.in/data/error_log
http://rksk.in/graph.php
http://rksk.in/hr_management_list.php
http://rksk.in/icons/
http://rksk.in/icons/small/
http://rksk.in/images/
http://rksk.in/images/ttc_1.png_jjg_28_07_22
http://rksk.in/includes/
http://rksk.in/includes/admin_rksk/
http://rksk.in/includes/admin_rksk/dashboard.php
http://rksk.in/includes/afhc_list.php
http://rksk.in/includes/assets/
http://rksk.in/includes/assets/css/
http://rksk.in/includes/assets/css/find.css
http://rksk.in/includes/assets/css/icoc.css
http://rksk.in/includes/assets/css/style.css
http://rksk.in/includes/assets/css/tooltip.css
http://rksk.in/includes/assets/js/
http://rksk.in/includes/assets/js/analitics.js
http://rksk.in/includes/assets/js/demo.js
http://rksk.in/includes/assets/js/moment_timeline_tweet.a20574004ea824b1c047f200045ffa1e.js
http://rksk.in/includes/assets/js/sdk.js
http://rksk.in/includes/chc_list.php
http://rksk.in/includes/clientlist.php
http://rksk.in/includes/communicable_disease.php
http://rksk.in/includes/config.php
http://rksk.in/includes/dashboard_static.php
http://rksk.in/includes/dashboard_static_button.php
http://rksk.in/includes/dashboard_static_srh.php
http://rksk.in/includes/footer.php
http://rksk.in/includes/function.php
http://rksk.in/includes/head.php
http://rksk.in/includes/header.php
http://rksk.in/includes/header1.php
http://rksk.in/includes/images/
http://rksk.in/includes/index.php
http://rksk.in/includes/injury.php
http://rksk.in/includes/marriage.php
http://rksk.in/includes/married_less_18.php
http://rksk.in/includes/mental_health.php
http://rksk.in/includes/outreachlist.php
http://rksk.in/includes/phc_list.php
http://rksk.in/includes/sidebar.php
http://rksk.in/includes/sites/
http://rksk.in/includes/sites/default/
http://rksk.in/includes/sites/default/files/
http://rksk.in/includes/sites/default/files/css/

http://rksk.in/includes/sites/default/files/css/css_-7sh1T-NqMBZVwpCKKnx8bGnZNHK7NTf_Gq3Pj_icoc.css
http://rksk.in/includes/sites/default/files/css/css_u2GxgZK34iIP4n4LB9bPc9oqt0tU7WsjT8LgZwCwMt8.css
http://rksk.in/includes/sites/default/files/css/css_Vu_vKom_9Oe8ybFv73ZyWdjTj4w_6esl1dpKj7OlJDQ.css
http://rksk.in/includes/sites/default/files/css/css_xE-rWrJf-fncB6ztZfd2huxqgxu4WO-qwma6Xer30m4.css
http://rksk.in/includes/sites/default/files/js/
http://rksk.in/includes/sites/default/files/js/js_Iu231mfdeiEoaLXCWaLUWEw3lvVKe8tL-KJCcJMguXo.js
http://rksk.in/includes/static_communication.php
http://rksk.in/includes/static_ncd.php
http://rksk.in/includes/static_vulnerable.php
http://rksk.in/includes/subcenter_list.php
http://rksk.in/includes/substances_abuse.php
http://rksk.in/includes/user_list.php
http://rksk.in/index.php
http://rksk.in/injury.php
http://rksk.in/login.php
http://rksk.in/manual/
http://rksk.in/manual/bind.html
http://rksk.in/manual/caching.html
http://rksk.in/manual/configuring.html
http://rksk.in/manual/content-negotiation.html
http://rksk.in/manual/custom-error.html
http://rksk.in/manual/da/
http://rksk.in/manual/de/
http://rksk.in/manual/de/glossary.html
http://rksk.in/manual/de/mod/
http://rksk.in/manual/de/mod/core.html
http://rksk.in/manual/de/mod/directives.html
http://rksk.in/manual/de/mod/mpm_common.html
http://rksk.in/manual/developer/
http://rksk.in/manual/dns-caveats.html
http://rksk.in/manual/dso.html
http://rksk.in/manual/en/
http://rksk.in/manual/en/glossary.html
http://rksk.in/manual/en/howto/
http://rksk.in/manual/en/howto/access.html
http://rksk.in/manual/en/logs.html
http://rksk.in/manual/en/misc/
http://rksk.in/manual/en/misc/perf-tuning.html
http://rksk.in/manual/en/misc/security_tips.html
http://rksk.in/manual/en/mod/
http://rksk.in/manual/en/mod/core.html
http://rksk.in/manual/en/mod/directives.html
http://rksk.in/manual/en/mod/mod_alias.html
http://rksk.in/manual/en/mod/mod_authz_host.html
http://rksk.in/manual/en/mod/mod_cgi.html
http://rksk.in/manual/en/mod/mod_mime.html
http://rksk.in/manual/en/mod/mod_rewrite.html
http://rksk.in/manual/en/mod/mpm_common.html
http://rksk.in/manual/en/sections.html
http://rksk.in/manual/en/urlmapping.html
http://rksk.in/manual/env.html
http://rksk.in/manual/es/
http://rksk.in/manual/es/glossary.html
http://rksk.in/manual/es/mod/
http://rksk.in/manual/es/mod/core.html
http://rksk.in/manual/es/mod/directives.html
http://rksk.in/manual/expr.html
http://rksk.in/manual/filter.html
http://rksk.in/manual/fr/
http://rksk.in/manual/fr/glossary.html
http://rksk.in/manual/fr/howto/

http://rksk.in/manual/fr/howto/access.html
http://rksk.in/manual/fr/logs.html
http://rksk.in/manual/fr/misc/
http://rksk.in/manual/fr/misc/perf-tuning.html
http://rksk.in/manual/fr/misc/security_tips.html
http://rksk.in/manual/fr/mod/
http://rksk.in/manual/fr/mod/core.html
http://rksk.in/manual/fr/mod/directives.html
http://rksk.in/manual/fr/mod/mod_alias.html
http://rksk.in/manual/fr/mod/mod_authz_host.html
http://rksk.in/manual/fr/mod/mod_cgi.html
http://rksk.in/manual/fr/mod/mod_mime.html
http://rksk.in/manual/fr/mod/mod_rewrite.html
http://rksk.in/manual/fr/mod/mpm_common.html
http://rksk.in/manual/fr/sections.html
http://rksk.in/manual/fr/urlmapping.html
http://rksk.in/manual/glossary.html
http://rksk.in/manual/handler.html
http://rksk.in/manual/howto/
http://rksk.in/manual/howto/access.html
http://rksk.in/manual/howto/auth.html
http://rksk.in/manual/howto/cgi.html
http://rksk.in/manual/howto/htaccess.html
http://rksk.in/manual/howto/public_html.html
http://rksk.in/manual/howto/ssi.html
http://rksk.in/manual/images/
http://rksk.in/manual/install.html
http://rksk.in/manual/invoking.html
http://rksk.in/manual/ja/
http://rksk.in/manual/ja/glossary.html
http://rksk.in/manual/ja/howto/
http://rksk.in/manual/ja/logs.html
http://rksk.in/manual/ja/mod/
http://rksk.in/manual/ja/mod/core.html
http://rksk.in/manual/ja/mod/directives.html
http://rksk.in/manual/ja/mod/mod_alias.html
http://rksk.in/manual/ja/mod/mod_cgi.html
http://rksk.in/manual/ja/mod/mod_mime.html
http://rksk.in/manual/ja/mod/mpm_common.html
http://rksk.in/manual/ja/sections.html
http://rksk.in/manual/ja/urlmapping.html
http://rksk.in/manual/ko/
http://rksk.in/manual/ko/glossary.html
http://rksk.in/manual/ko/howto/
http://rksk.in/manual/ko/logs.html
http://rksk.in/manual/ko/misc/
http://rksk.in/manual/ko/misc/perf-tuning.html
http://rksk.in/manual/ko/misc/security_tips.html
http://rksk.in/manual/ko/mod/
http://rksk.in/manual/ko/mod/directives.html
http://rksk.in/manual/ko/mod/mod_alias.html
http://rksk.in/manual/ko/mod/mod_cgi.html
http://rksk.in/manual/ko/sections.html
http://rksk.in/manual/ko/urlmapping.html
http://rksk.in/manual/license.html
http://rksk.in/manual/logs.html
http://rksk.in/manual/misc/
http://rksk.in/manual/misc/password_encryptions.html
http://rksk.in/manual/misc/perf-tuning.html
http://rksk.in/manual/misc/relevant_standards.html
http://rksk.in/manual/misc/security_tips.html

http://rksk.in/manual/mod/
http://rksk.in/manual/mod/core.html
http://rksk.in/manual/mod/directive-dict.html
http://rksk.in/manual/mod/directives.html
http://rksk.in/manual/mod/event.html
http://rksk.in/manual/mod/mod_access_compat.html
http://rksk.in/manual/mod/mod_actions.html
http://rksk.in/manual/mod/mod_alias.html
http://rksk.in/manual/mod/mod_allowmethods.html
http://rksk.in/manual/mod/mod_auth_basic.html
http://rksk.in/manual/mod/mod_auth_digest.html
http://rksk.in/manual/mod/mod_auth_form.html
http://rksk.in/manual/mod/mod_authn_anon.html
http://rksk.in/manual/mod/mod_authn_core.html
http://rksk.in/manual/mod/mod_authn_dbd.html
http://rksk.in/manual/mod/mod_authn_dbm.html
http://rksk.in/manual/mod/mod_authn_file.html
http://rksk.in/manual/mod/mod_authn_socache.html
http://rksk.in/manual/mod/mod_authnz_ldap.html
http://rksk.in/manual/mod/mod_authz_core.html
http://rksk.in/manual/mod/mod_authz_dbd.html
http://rksk.in/manual/mod/mod_authz_dbm.html
http://rksk.in/manual/mod/mod_authz_groupfile.html
http://rksk.in/manual/mod/mod_authz_host.html
http://rksk.in/manual/mod/mod_autoindex.html
http://rksk.in/manual/mod/mod_buffer.html
http://rksk.in/manual/mod/mod_cache.html
http://rksk.in/manual/mod/mod_cache_disk.html
http://rksk.in/manual/mod/mod_cache_socache.html
http://rksk.in/manual/mod/mod_cern_meta.html
http://rksk.in/manual/mod/mod_cgi.html
http://rksk.in/manual/mod/mod_cgid.html
http://rksk.in/manual/mod/mod_charset_lite.html
http://rksk.in/manual/mod/mod_dav.html
http://rksk.in/manual/mod/mod_dav_fs.html
http://rksk.in/manual/mod/mod_dav_lock.html
http://rksk.in/manual/mod/mod_dbd.html
http://rksk.in/manual/mod/mod_deflate.html
http://rksk.in/manual/mod/mod_dialup.html
http://rksk.in/manual/mod/mod_dir.html
http://rksk.in/manual/mod/mod_dumpio.html
http://rksk.in/manual/mod/mod_echo.html
http://rksk.in/manual/mod/mod_env.html
http://rksk.in/manual/mod/mod_example.html
http://rksk.in/manual/mod/mod_expires.html
http://rksk.in/manual/mod/mod_ext_filter.html
http://rksk.in/manual/mod/mod_file_cache.html
http://rksk.in/manual/mod/mod_filter.html
http://rksk.in/manual/mod/mod_headers.html
http://rksk.in/manual/mod/mod_heartbeat.html
http://rksk.in/manual/mod/mod_heartmonitor.html
http://rksk.in/manual/mod/mod_ident.html
http://rksk.in/manual/mod/mod_imagemap.html
http://rksk.in/manual/mod/mod_include.html
http://rksk.in/manual/mod/mod_info.html
http://rksk.in/manual/mod/mod_isapi.html
http://rksk.in/manual/mod/mod_lbmethod_heartbeat.html
http://rksk.in/manual/mod/mod_ldap.html
http://rksk.in/manual/mod/mod_log_config.html
http://rksk.in/manual/mod/mod_log_debug.html
http://rksk.in/manual/mod/mod_log_forensic.html

http://rksk.in/manual/mod/mod_logio.html
http://rksk.in/manual/mod/mod_lua.html
http://rksk.in/manual/mod/mod_macro.html
http://rksk.in/manual/mod/mod_mime.html
http://rksk.in/manual/mod/mod_mime_magic.html
http://rksk.in/manual/mod/mod_negotiation.html
http://rksk.in/manual/mod/mod_nw_ssl.html
http://rksk.in/manual/mod/mod_privileges.html
http://rksk.in/manual/mod/mod_proxy.html
http://rksk.in/manual/mod/mod_proxy_connect.html
http://rksk.in/manual/mod/mod_proxy_express.html
http://rksk.in/manual/mod/mod_proxy_ftp.html
http://rksk.in/manual/mod/mod_proxy_html.html
http://rksk.in/manual/mod/mod_proxy_scgi.html
http://rksk.in/manual/mod/mod_reflector.html
http://rksk.in/manual/mod/mod_remoteip.html
http://rksk.in/manual/mod/mod_reqtimeout.html
http://rksk.in/manual/mod/mod_request.html
http://rksk.in/manual/mod/mod_rewrite.html
http://rksk.in/manual/mod/mod_sed.html
http://rksk.in/manual/mod/mod_session.html
http://rksk.in/manual/mod/mod_session_cookie.html
http://rksk.in/manual/mod/mod_session_crypto.html
http://rksk.in/manual/mod/mod_session_dbd.html
http://rksk.in/manual/mod/mod_setenvif.html
http://rksk.in/manual/mod/mod_so.html
http://rksk.in/manual/mod/mod_speling.html
http://rksk.in/manual/mod/mod_ssl.html
http://rksk.in/manual/mod/mod_status.html
http://rksk.in/manual/mod/mod_substitute.html
http://rksk.in/manual/mod/mod_suexec.html
http://rksk.in/manual/mod/mod_unique_id.html
http://rksk.in/manual/mod/mod_unixd.html
http://rksk.in/manual/mod/mod_userdir.html
http://rksk.in/manual/mod/mod_usertrack.html
http://rksk.in/manual/mod/mod_version.html
http://rksk.in/manual/mod/mod_vhost_alias.html
http://rksk.in/manual/mod/mod_watchdog.html
http://rksk.in/manual/mod/mod_xml2enc.html
http://rksk.in/manual/mod/module-dict.html
http://rksk.in/manual/mod/mpm_common.html
http://rksk.in/manual/mod/mpm_netware.html
http://rksk.in/manual/mod/mpm_winnt.html
http://rksk.in/manual/mod/mpmt_os2.html
http://rksk.in/manual/mod/prefork.html
http://rksk.in/manual/mod/quickreference.html
http://rksk.in/manual/mod/worker.html
http://rksk.in/manual/mpm.html
http://rksk.in/manual/new_features_2_0.html
http://rksk.in/manual/new_features_2_2.html
http://rksk.in/manual/new_features_2_4.html
http://rksk.in/manual/platform/
http://rksk.in/manual/platform/ebcdic.html
http://rksk.in/manual/platform/netware.html
http://rksk.in/manual/platform/rpm.html
http://rksk.in/manual/platform/windows.html
http://rksk.in/manual/programs/
http://rksk.in/manual/programs/apachectl.html
http://rksk.in/manual/programs/apxs.html
http://rksk.in/manual/programs/configure.html
http://rksk.in/manual/programs/httpd.html

http://rksk.in/manual/programs/httxt2dbm.html
http://rksk.in/manual/programs/logresolve.html
http://rksk.in/manual/programs/other.html
http://rksk.in/manual/programs/rotatelogs.html
http://rksk.in/manual/programs/suexec.html
http://rksk.in/manual/pt-br/
http://rksk.in/manual/rewrite/
http://rksk.in/manual/rewrite/flags.html
http://rksk.in/manual/rewrite/intro.html
http://rksk.in/manual/rewrite/rewritemap.html
http://rksk.in/manual/sections.html
http://rksk.in/manual/server-wide.html
http://rksk.in/manual/sitemap.html
http://rksk.in/manual/ssl/
http://rksk.in/manual/ssl/ssl_faq.html
http://rksk.in/manual/stopping.html
http://rksk.in/manual/style/
http://rksk.in/manual/style/css/
http://rksk.in/manual/style/css/manual-loose-100pc.css
http://rksk.in/manual/style/css/manual-print.css
http://rksk.in/manual/style/css/manual.css
http://rksk.in/manual/style/css/prettify.css
http://rksk.in/manual/style/scripts/
http://rksk.in/manual/style/scripts/prettify.js
http://rksk.in/manual/suexec.html
http://rksk.in/manual/tr/
http://rksk.in/manual/tr/glossary.html
http://rksk.in/manual/tr/logs.html
http://rksk.in/manual/tr/misc/
http://rksk.in/manual/tr/misc/perf-tuning.html
http://rksk.in/manual/tr/misc/security_tips.html
http://rksk.in/manual/tr/mod/
http://rksk.in/manual/tr/mod/core.html
http://rksk.in/manual/tr/mod/directives.html
http://rksk.in/manual/tr/mod/mod_alias.html
http://rksk.in/manual/tr/mod/mpm_common.html
http://rksk.in/manual/tr/sections.html
http://rksk.in/manual/tr/urlmapping.html
http://rksk.in/manual/upgrading.html
http://rksk.in/manual/urlmapping.html
http://rksk.in/manual/vhosts/
http://rksk.in/manual/vhosts/fd-limits.html
http://rksk.in/manual/vhosts/name-based.html
http://rksk.in/manual/zh-cn/
http://rksk.in/manual/zh-cn/howto/
http://rksk.in/manual/zh-cn/misc/
http://rksk.in/manual/zh-cn/mod/
http://rksk.in/manual/zh-cn/mod/directives.html
http://rksk.in/marriage.php
http://rksk.in/mental_health.php
http://rksk.in/misc/
http://rksk.in/modules/
http://rksk.in/modules/zingchart-3d.min.js
http://rksk.in/modules/zingchart-animation.min.js
http://rksk.in/modules/zingchart-api-annotations.min.js
http://rksk.in/modules/zingchart-api-rules.min.js
http://rksk.in/modules/zingchart-api.min.js
http://rksk.in/modules/zingchart-area.min.js
http://rksk.in/modules/zingchart-area3d.min.js
http://rksk.in/modules/zingchart-boxplot.min.js
http://rksk.in/modules/zingchart-bubble-legend.min.js

http://rksk.in/modules/zingchart-bubble-pack.min.js
http://rksk.in/modules/zingchart-bubble.min.js
http://rksk.in/modules/zingchart-bubblepie.min.js
http://rksk.in/modules/zingchart-calendar.min.js
http://rksk.in/modules/zingchart-chord.min.js
http://rksk.in/modules/zingchart-color-scale.min.js
http://rksk.in/modules/zingchart-core.min.js
http://rksk.in/modules/zingchart-csv.min.js
http://rksk.in/modules/zingchart-debug.min.js
http://rksk.in/modules/zingchart-depth.min.js
http://rksk.in/modules/zingchart-dragging.min.js
http://rksk.in/modules/zingchart-errorbars.min.js
http://rksk.in/modules/zingchart-export.min.js
http://rksk.in/modules/zingchart-flame.min.js
http://rksk.in/modules/zingchart-gauge.min.js
http://rksk.in/modules/zingchart-grid.min.js
http://rksk.in/modules/zingchart-guide.min.js
http://rksk.in/modules/zingchart-hbar.min.js
http://rksk.in/modules/zingchart-hbar3d.min.js
http://rksk.in/modules/zingchart-hbubble.min.js
http://rksk.in/modules/zingchart-hbullet.min.js
http://rksk.in/modules/zingchart-heatmap.min.js
http://rksk.in/modules/zingchart-hfunnel.min.js
http://rksk.in/modules/zingchart-history.min.js
http://rksk.in/modules/zingchart-hscatter.min.js
http://rksk.in/modules/zingchart-legend.min.js
http://rksk.in/modules/zingchart-line.min.js
http://rksk.in/modules/zingchart-line3d.min.js
http://rksk.in/modules/zingchart-maps-afg.min.js
http://rksk.in/modules/zingchart-maps-ago.min.js
http://rksk.in/modules/zingchart-maps-alb.min.js
http://rksk.in/modules/zingchart-maps-and.min.js
http://rksk.in/modules/zingchart-maps-are.min.js
http://rksk.in/modules/zingchart-maps-arg.min.js
http://rksk.in/modules/zingchart-maps-arm.min.js
http://rksk.in/modules/zingchart-maps-aus.min.js
http://rksk.in/modules/zingchart-maps-aut.min.js
http://rksk.in/modules/zingchart-maps-aze.min.js
http://rksk.in/modules/zingchart-maps-bdi.min.js
http://rksk.in/modules/zingchart-maps-bel.min.js
http://rksk.in/modules/zingchart-maps-ben.min.js
http://rksk.in/modules/zingchart-maps-bfa.min.js
http://rksk.in/modules/zingchart-maps-bgr.min.js
http://rksk.in/modules/zingchart-maps-bih.min.js
http://rksk.in/modules/zingchart-maps-blr.min.js
http://rksk.in/modules/zingchart-maps-bol.min.js
http://rksk.in/modules/zingchart-maps-bra.min.js
http://rksk.in/modules/zingchart-maps-brn.min.js
http://rksk.in/modules/zingchart-maps-btn.min.js
http://rksk.in/modules/zingchart-maps-bwa.min.js
http://rksk.in/modules/zingchart-maps-caf.min.js
http://rksk.in/modules/zingchart-maps-can.min.js
http://rksk.in/modules/zingchart-maps-che.min.js
http://rksk.in/modules/zingchart-maps-chl.min.js
http://rksk.in/modules/zingchart-maps-chn.min.js
http://rksk.in/modules/zingchart-maps-civ.min.js
http://rksk.in/modules/zingchart-maps-cmr.min.js
http://rksk.in/modules/zingchart-maps-cod.min.js
http://rksk.in/modules/zingchart-maps-cog.min.js
http://rksk.in/modules/zingchart-maps-col.min.js
http://rksk.in/modules/zingchart-maps-cri.min.js

http://rksk.in/modules/zingchart-maps-cub.min.js
http://rksk.in/modules/zingchart-maps-cyp.min.js
http://rksk.in/modules/zingchart-maps-cze.min.js
http://rksk.in/modules/zingchart-maps-deu.min.js
http://rksk.in/modules/zingchart-maps-dnk.min.js
http://rksk.in/modules/zingchart-maps-ecu.min.js
http://rksk.in/modules/zingchart-maps-egy.min.js
http://rksk.in/modules/zingchart-maps-esp.min.js
http://rksk.in/modules/zingchart-maps-espL2.min.js
http://rksk.in/modules/zingchart-maps-est.min.js
http://rksk.in/modules/zingchart-maps-eth.min.js
http://rksk.in/modules/zingchart-maps-fin.min.js
http://rksk.in/modules/zingchart-maps-fra.min.js
http://rksk.in/modules/zingchart-maps-fraL2.min.js
http://rksk.in/modules/zingchart-maps-gab.min.js
http://rksk.in/modules/zingchart-maps-gbr.min.js
http://rksk.in/modules/zingchart-maps-gbrL2.min.js
http://rksk.in/modules/zingchart-maps-geojson.min.js
http://rksk.in/modules/zingchart-maps-gha.min.js
http://rksk.in/modules/zingchart-maps-gmb.min.js
http://rksk.in/modules/zingchart-maps-gnb.min.js
http://rksk.in/modules/zingchart-maps-grc.min.js
http://rksk.in/modules/zingchart-maps-gtm.min.js
http://rksk.in/modules/zingchart-maps-guf.min.js
http://rksk.in/modules/zingchart-maps-guy.min.js
http://rksk.in/modules/zingchart-maps-hrv.min.js
http://rksk.in/modules/zingchart-maps-hun.min.js
http://rksk.in/modules/zingchart-maps-ind.min.js
http://rksk.in/modules/zingchart-maps-irl.min.js
http://rksk.in/modules/zingchart-maps-irn.min.js
http://rksk.in/modules/zingchart-maps-isl.min.js
http://rksk.in/modules/zingchart-maps-isr.min.js
http://rksk.in/modules/zingchart-maps-ita.min.js
http://rksk.in/modules/zingchart-maps-jpn.min.js
http://rksk.in/modules/zingchart-maps-kaz.min.js
http://rksk.in/modules/zingchart-maps-ken.min.js
http://rksk.in/modules/zingchart-maps-kor.min.js
http://rksk.in/modules/zingchart-maps-kwt.min.js
http://rksk.in/modules/zingchart-maps-lao.min.js
http://rksk.in/modules/zingchart-maps-lbr.min.js
http://rksk.in/modules/zingchart-maps-lie.min.js
http://rksk.in/modules/zingchart-maps-ltu.min.js
http://rksk.in/modules/zingchart-maps-lux.min.js
http://rksk.in/modules/zingchart-maps-lva.min.js
http://rksk.in/modules/zingchart-maps-mda.min.js
http://rksk.in/modules/zingchart-maps-mex.min.js
http://rksk.in/modules/zingchart-maps-mkd.min.js
http://rksk.in/modules/zingchart-maps-mlt.min.js
http://rksk.in/modules/zingchart-maps-mne.min.js
http://rksk.in/modules/zingchart-maps-moz.min.js
http://rksk.in/modules/zingchart-maps-nam.min.js
http://rksk.in/modules/zingchart-maps-ncl.min.js
http://rksk.in/modules/zingchart-maps-nga.min.js
http://rksk.in/modules/zingchart-maps-nld.min.js
http://rksk.in/modules/zingchart-maps-nor.min.js
http://rksk.in/modules/zingchart-maps-nzl.min.js
http://rksk.in/modules/zingchart-maps-omn.min.js
http://rksk.in/modules/zingchart-maps-pak.min.js
http://rksk.in/modules/zingchart-maps-pan.min.js
http://rksk.in/modules/zingchart-maps-per.min.js
http://rksk.in/modules/zingchart-maps-phl.min.js

http://rksk.in/modules/zingchart-maps-png.min.js
http://rksk.in/modules/zingchart-maps-pol.min.js
http://rksk.in/modules/zingchart-maps-prt.min.js
http://rksk.in/modules/zingchart-maps-qat.min.js
http://rksk.in/modules/zingchart-maps-rou.min.js
http://rksk.in/modules/zingchart-maps-rus.min.js
http://rksk.in/modules/zingchart-maps-rwa.min.js
http://rksk.in/modules/zingchart-maps-sen.min.js
http://rksk.in/modules/zingchart-maps-slv.min.js
http://rksk.in/modules/zingchart-maps-srb.min.js
http://rksk.in/modules/zingchart-maps-sur.min.js
http://rksk.in/modules/zingchart-maps-svk.min.js
http://rksk.in/modules/zingchart-maps-svn.min.js
http://rksk.in/modules/zingchart-maps-swe.min.js
http://rksk.in/modules/zingchart-maps-tha.min.js
http://rksk.in/modules/zingchart-maps-tjk.min.js
http://rksk.in/modules/zingchart-maps-topojson.min.js
http://rksk.in/modules/zingchart-maps-tun.min.js
http://rksk.in/modules/zingchart-maps-tur.min.js
http://rksk.in/myjson.json
http://rksk.in/outreachlist.php
http://rksk.in/phc_list.php
http://rksk.in/sites/
http://rksk.in/sites/all/
http://rksk.in/sites/all/modules/
http://rksk.in/sites/all/modules/custom_slideshow_helper/
http://rksk.in/sites/all/modules/custom_slideshow_helper/css/
http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/
http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/flexslider-icon-2.html
http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/flexslider-icon-3.html
http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/flexslider-icon-4.html
http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/flexslider-icon.html
http://rksk.in/sites/all/modules/custom_slideshow_helper/css/fonts/flexslider-icond41d.html
http://rksk.in/sites/all/modules/custom_slideshow_helper/images/
http://rksk.in/sites/all/modules/unfpa_global_home/
http://rksk.in/sites/all/modules/unfpa_global_home/images/
http://rksk.in/sites/all/modules/unfpa_global_home/images/new-home-page/
http://rksk.in/sites/all/modules/unfpa_global_icpd/
http://rksk.in/sites/all/modules/unfpa_global_icpd/images/
http://rksk.in/sites/all/themes/
http://rksk.in/sites/all/themes/unfpa_global/
http://rksk.in/sites/all/themes/unfpa_global/css/
http://rksk.in/sites/all/themes/unfpa_global/css/font-icons/
http://rksk.in/sites/all/themes/unfpa_global/css/fonts/
http://rksk.in/sites/all/themes/unfpa_global/css/fonts/roboto/
http://rksk.in/sites/all/themes/unfpa_global/css/fonts/slick-fonts/
http://rksk.in/sites/all/themes/unfpa_global/images/
http://rksk.in/sites/all/themes/unfpa_global/images/2016/
http://rksk.in/sites/all/themes/unfpa_global/images/logo_header.html
http://rksk.in/sites/default/
http://rksk.in/sites/default/files/
http://rksk.in/sites/default/files/css/
http://rksk.in/sites/default/files/css/css_-7sh1T-NqMBZVwpCKKnx8bGnZNHK7NTf_Gq3Pj_icoc.css
http://rksk.in/sites/default/files/css/css_u2GxgZK34iIP4n4LB9bPc9oqt0tU7WsjT8LgZwCwMt8.css
http://rksk.in/sites/default/files/css/css_Vu_vKom_9Oe8ybFv73ZyWdjTj4w_6esI1dpKj7OlJDQ.css
http://rksk.in/sites/default/files/css/css_xE-rWrJf-fncB6ztZfd2huxqgxu4WO-qwma6Xer30m4.css
http://rksk.in/sites/default/files/icpd/
http://rksk.in/sites/default/files/icpd/images/
http://rksk.in/sites/default/files/js/
http://rksk.in/sites/default/files/js/js_Iu231mfdeiEoaLXCWaLUWEw3lvVKe8tL-KJCcJMguXo.js
http://rksk.in/static_cd.php

http://rksk.in/static_communication.php
http://rksk.in/static_injuries.php
http://rksk.in/static_mh.php
http://rksk.in/static_ncd.php
http://rksk.in/static_school_health.php
http://rksk.in/static_vulnerable.php
http://rksk.in/subcenter_list.php
http://rksk.in/substances_abuse.php
http://rksk.in/user_list.php
http://rksk.in/wifs_monthaly_reporting.php