



Acunetix Website Audit

22 December, 2013

Affected Items

Scan of https://keyofthesky-se2.rhcloud.com:443/

Scan details

Scan information	
Starttime	12/21/2013 12:39:20 PM
Finish time	12/21/2013 12:47:43 PM
Scan time	8 minutes, 23 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.22 (Red Hat Enterprise Web Server)
Server OS	Unix
Server technologies	PHP

Threat level



Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	35
High	0
Medium	2
Low	7
Informational	26

Affected items

/	
Parameter	
Alert group	Session Cookie without HttpOnly flag set
Severity	Low
Alert variants	
Details	Cookie name: "PHPSESSID" Cookie domain: "keyofthesky-se2.rhcloud.com"
GET / HTTP/1.1 Pragma: no-cache Acunetix-Aspect: enabled Acunetix-Aspect-Password: ***** Acunetix-Aspect-Queries: filelist;aspectalerts Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljf17 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*	
Alert group	Session Cookie without Secure flag set

Severity	Low
Alert variants	
Details	Cookie name: "PHPSESSID" Cookie domain: "keyofthesky-se2.rhcloud.com"
GET / HTTP/1.1 Pragma: no-cache Acunetix-Aspect: enabled Acunetix-Aspect-Password: ***** Acunetix-Aspect-Queries: filelist;aspectalerts Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl7 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*	

/a

Parameter	
Alert group	Broken links
Severity	Informational
Alert variants	
Details	No details are available.
GET /a HTTP/1.1 Pragma: no-cache Referer: https://keyofthesky-se2.rhcloud.com/ Acunetix-Aspect: enabled Acunetix-Aspect-Password: ***** Acunetix-Aspect-Queries: filelist;aspectalerts Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl7; mysheet=style3 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*	

/assets/df1afc51/jquery.min.js

Parameter	
Alert group	Possible username or password disclosure
Severity	Informational
Alert variants	
Details	Pattern found: password:rt
GET /assets/df1afc51/jquery.min.js HTTP/1.1 Pragma: no-cache Referer: https://keyofthesky-se2.rhcloud.com/ Acunetix-Aspect: enabled Acunetix-Aspect-Password: ***** Acunetix-Aspect-Queries: filelist;aspectalerts Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl7 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*	

/bin

Parameter	
Alert group	Possible sensitive directories
Severity	Low

Alert variants	
Details	No details are available.
GET /bin HTTP/1.1 Accept: acunetix/wvs Range: bytes=0-99999 Cookie: PHPSESSID=9a71o1veipm3ket6j9buljfl7; mysheet=style3 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	

/CHANGELOG

Parameter	
Alert group	Source code disclosure
Severity	Medium
Alert variants	
Details	<p>Pattern found: <? in text/html message parts</p> <ul style="list-style-type: none"> - Hide border around radio buttons - Applied patch for attachment download by crichardson (closes #1484198) - Fixed bug in Postgres DB handling (closes #1484068) - Fixed bug of invalid calls to fetchRow() in rcube_db.inc (closes #1484280) - Fixed array_merge bug (closes #1484281) - Fixed flag for deletion in list view (closes #1484264) - Finally support semicolons as recipient separator (closes ##1484251) - Fixed message headers (subject) encoding - check if safe mode is on or not (closes #1484269) - Show "no subject" in message list if subject is missing (closes #1484243) - Solved page caching of message preview (closes #1484153) - Only use gzip compression if configured (closes #1484236) - Fixed priority selector issue (#1484150) - Fixed some CSS issues in default skin (closes #1484210 and #1484161) - Prevent from double quoting of numeric HTML character references (closes #1484253) - Fixed display of HTML message attachments (closes #1484178) - Applied patch for preview caching (closes #1484186) - Added error handling for attachment uploads - Use multibyte safe string functions where necessary (closes #1483988) - Applied security patch to validate the submitted host value (by Kees Cook) - Applied security patch to validate input values when deleting contacts (by Kees Cook) - Applied security patch that sanitizes emoticon paths when attaching them (by Kees Cook) - Applied a patch to more aggressively sanitize a HTML message - Visualize blocked images in HTML messages - Fixed wrong message listing when showing search results (closes #1484131) - Show remote images when opening HTML message part as attachment - Improve memory usage when sending mail (closes #1484098) - Mark messages as read once the preview is loaded (closes #1484132) - Include smtp final response in log (closes #1484081) - Corrected date string in sent message header (closes #1484125) - Correctly choose "To" column in sent and draft mailboxes (closes #1483943) - Changed strong tooltips for message browse buttons (closes #1483930) - Fixed signature delimiter character to be standard (Bug #1484035) - Fixed XSS vulnerability (Bug #1484109) - Remove newlines from mail headers (Bug #1484031) - Selection issues when moving/deleting (Bug #1484044) - Applied patch of Clement Moulin for imap host auto-selection - ISO-encode IMAP password for plaintext login (Bugs #1483977 & #1483886) - Fixed folder name encoding in subscription list (Bug #1484113) - Fixed JS errors in identity list (Bug #1484120) - Translate foldernames in folder form (closes #1484113) - Added first and last buttons to message list, address book and message detail - Pressing Shift-Del bypasses Trash folder - Enable purge command for Junk folder - Fetch all aliases if virtuser_query is used instead

- Re-enabled multi select of contacts (Bug #1484017)
- Enable contact editing right after creation (Bug #1459641)
- Correct UTF-7 to UTF-8 conversion if mbstring is not available
- Fixed IMAP fetch of message body (Bug #1484019)
- Fixed safe_mode problems (Bug #1418381)
- Fixed wrong header encoding (Bug #1483976)
- Made automatic draft saving configurable
- Fixed JS bug when renaming folders (Bug #1483989)
- Added quota display as image (by Brett Patterson)
- Corrected creation of a message-id
- New indentation for quoted message text
- Improved HTML validity
- Fixed URL character set (Ticket #1445501)
- Fixed saving of contact into MySQL from LDAP query results (Ticket #1483820)
- Fixed folder renaming: unsubscribe before rename (Bug #1483920)
- Finalized new message parsing (+ chaching)
- Fixed wrong usage of mbstring (Bug #1462439)
- Set default spelling language (Ticket #1483938)
- Added support for Nox Spell Server
- Re-built message parsing (Bug #1327068)
Now based on the message structure delivered by the IMAP server.
- Fixed some XSS and SQL injection issues
- Fixed charset problems with folder renaming

```
GET /CHANGELOG HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

Alert group	Possible sensitive files
Severity	Low
Alert variants	
Details	No details are available.
<pre>GET /CHANGELOG HTTP/1.1 Accept: acunetix/wvs Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17; mysheet=style3 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)</pre>	
Alert group	Possible username or password disclosure
Severity	Informational
Alert variants	
Details	Pattern found: Password: Support

GET /CHANGELOG HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/css/form.css

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants

Details	Pattern found: qiang.xue@gmail.com
---------	------------------------------------

GET /css/form.css HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants

Details	Tested on URI: /index.php/irO1I8T5Hx.jsp Pattern found in response: iust@comp.iust.ac.ir
---------	---

GET /index.php/irO1I8T5Hx.jsp HTTP/1.1
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants

Details	Tested on URI: /index.php/site/zm2Q1HxLVy.jsp Pattern found in response: iust@comp.iust.ac.ir
---------	--

GET /index.php/site/zm2Q1HxLVy.jsp HTTP/1.1
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/googlemap

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Pattern found: iust@comp.iust.ac.ir

GET /index.php/site/googlemap HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/index

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Pattern found: iust@comp.iust.ac.ir

GET /index.php/site/index HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosquemap/

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Tested on URI: /index.php/site/mosquemap/N7S43TUq2h.jsp Pattern found in response: iust@comp.iust.ac.ir

GET /index.php/site/mosquemap/N7S43TUq2h.jsp HTTP/1.1
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosquemap/ld/

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Tested on URI: /index.php/site/mosquemap/ld/zdgYbai8Om.jsp
	Pattern found in response: iust@comp.iust.ac.ir
GET /index.php/site/mosquemap/ld/zdgYbai8Om.jsp HTTP/1.1 Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*	

/index.php/site/mosquemap/ld/10

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Pattern found: iust@comp.iust.ac.ir
	GET /index.php/site/mosquemap/ld/10 HTTP/1.1 Pragma: no-cache Referer: https://keyofthesky-se2.rhcloud.com/ Acunetix-Aspect: enabled Acunetix-Aspect-Password: ***** Acunetix-Aspect-Queries: filelist;aspectalerts Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*

/index.php/site/mosquemap/ld/3

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Pattern found: iust@comp.iust.ac.ir

GET /index.php/site/mosquemap/Id/3 HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl7
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosquemap/Id/9

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants

Details	Pattern found: iust@comp.iust.ac.ir
---------	-------------------------------------

GET /index.php/site/mosquemap/Id/9 HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl7
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosqueReward/

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants

Details	Tested on URI: /index.php/site/mosqueReward/BUWeUuRvU7.jsp Pattern found in response: iust@comp.iust.ac.ir
---------	---

GET /index.php/site/mosqueReward/BUWeUuRvU7.jsp HTTP/1.1
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl7; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosqueReward/Id/

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants

Details	Tested on URI: /index.php/site/mosqueReward/Id/xBILtM1dix.jsp Pattern found in response: iust@comp.iust.ac.ir
---------	--

GET /index.php/site/mosqueReward/Id/xBILtMldjx.jsp HTTP/1.1
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosqueReward/Id/10

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Pattern found: iust@comp.iust.ac.ir

GET /index.php/site/mosqueReward/Id/10 HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosqueReward/Id/3

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Pattern found: iust@comp.iust.ac.ir

GET /index.php/site/mosqueReward/Id/3 HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/mosqueReward/Id/9

Parameter	
Alert group	Email address found
Severity	Informational
Alert variants	
Details	Pattern found: iust@comp.iust.ac.ir

GET /index.php/site/mosqueReward/Id/9 HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/page/

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants	
----------------	--

Details	Tested on URI: /index.php/site/page/KzXIyYFMXa.jsp
---------	--

	Pattern found in response: iust@comp.iust.ac.ir
--	---

GET /index.php/site/page/KzXIyYFMXa.jsp HTTP/1.1
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/page/view/

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants	
----------------	--

Details	Tested on URI: /index.php/site/page/view/owC686txNF.jsp
---------	---

	Pattern found in response: iust@comp.iust.ac.ir
--	---

GET /index.php/site/page/view/owC686txNF.jsp HTTP/1.1
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/page/view/about

Parameter

Alert group	Email address found
-------------	---------------------

Severity	Informational
----------	---------------

Alert variants	
----------------	--

Details	Pattern found: iust@comp.iust.ac.ir
---------	-------------------------------------

GET /index.php/site/page/view/about HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl7
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/point.php

Parameter

Alert group	Broken links
--------------------	---------------------

Severity	Informational
----------	----------------------

Alert variants

Details	No details are available.
---------	---------------------------

GET /index.php/site/point.php HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/index.php/site/refrencePoint
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl7
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

Alert group	Email address found
--------------------	----------------------------

Severity	Informational
----------	----------------------

Alert variants

Details	Pattern found: iust@comp.iust.ac.ir
---------	-------------------------------------

GET /index.php/site/point.php HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/index.php/site/refrencePoint
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl7
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/index.php/site/refrencePoint

Parameter

Alert group	Email address found
--------------------	----------------------------

Severity	Informational
----------	----------------------

Alert variants

Details	Pattern found: iust@comp.iust.ac.ir
---------	-------------------------------------

GET /index.php/site/referencePoint HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/installer

Parameter

Alert group	Possible sensitive directories
-------------	--------------------------------

Severity	Low
----------	-----

Alert variants	
----------------	--

Details	No details are available.
---------	---------------------------

GET /installer HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)

/js/jquery-1.7.1.min.js

Parameter

Alert group	Possible username or password disclosure
-------------	--

Severity	Informational
----------	---------------

Alert variants	
----------------	--

Details	Pattern found: password:function
---------	----------------------------------

GET /js/jquery-1.7.1.min.js HTTP/1.1
Pragma: no-cache
Referer: https://keyofthesky-se2.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=9a71ol1veipm3ket6jh9buljfl17
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

/phpmyadmin

Parameter

Alert group	Possible sensitive directories
-------------	--------------------------------

Severity	Low
----------	-----

Alert variants	
----------------	--

Details	No details are available.
---------	---------------------------

```
GET /phpmyadmin HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3
Host: keyofthesky-se2.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

/SQL

Parameter	
Alert group	Possible sensitive directories
Severity	Low
Alert variants	
Details	No details are available.
<pre>GET /SQL HTTP/1.1 Accept: acunetix/wvs Range: bytes=0-99999 Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17; mysheet=style3 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)</pre>	

Web Server

Parameter	
Alert group	Apache server-status enabled
Severity	Medium
Alert variants	
Details	Pattern found: <title>Apache Status</title>
<pre>GET /server-status HTTP/1.1 Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*</pre>	

Alert group	Error page Web Server version disclosure
Severity	Informational
Alert variants	
Details	Information disclosure pattern found: Apache/2.2.22 (Red Hat Enterprise Web Server) Server at keyofthesky-se2.rhcloud.com Port 80
<pre>GET /3D7GLaYJvy HTTP/1.1 Cookie: PHPSESSID=9a71o1veipm3ket6jh9buljfl17 Host: keyofthesky-se2.rhcloud.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Accept: */*</pre>	