



Developer Report

Scan of http://exide16.allindia.com:80/

Scan details

Scan information	
Start time	28-09-2016 15:25:05
Finish time	28-09-2016 17:16:43
Scan time	1 hours, 51 minutes
Profile	Default
Server information	
Responsive	True
Server banner	Microsoft-IIS/8.5
Server OS	Windows









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	56
 High	14 
 Medium	9 
 Low	25 
 Informational	8 

Knowledge base

List of file extensions

File extensions can provide information on what technologies are being used on this website.

List of file extensions detected:

- css => 15 file(s)
- js => 21 file(s)
- png => 22 file(s)
- jpg => 5 file(s)
- gif => 3 file(s)
- aspx => 23 file(s)

- html => 2 file(s)
- appcache => 1 file(s)
- woff2 => 3 file(s)

List of client scripts

These files contain Javascript code referenced from the website.

- /js/common.js
- /js/jpreloader.js
- /js/home.js
- /js/jquery.mousewheel.min.js
- /js/slick.min.js
- /js/jquery.min.js
- /js/jquery.mcustomscrollbar.js
- /js/jquery.fullpage.js
- /js/scrolloverflow.min.js
- /js/common1.js
- /js/registerbattery.js
- /blog/scripts/jquery.min.js
- /blog/scripts/jpreloader.js
- /blog/scripts/scrolloverflow.min.js
- /blog/scripts/jquery.fullpage.js
- /blog/scripts/common.js
- /assets/js/exideshop.lib.min.js
- /assets/js/exideshop.min2.js
- /assets/lib/bootstrap-datepicker.js

List of files with inputs

These files have at least one input (GET or POST).

- / - 6 inputs
- /getsocialfeed.aspx - 1 inputs
- /buy-exide.html - 2 inputs
- /assets/fonts/fontawesome-webfont.woff2 - 1 inputs
- /service.aspx - 7 inputs

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed. (Configuration-> Scan Settings ->Scanning Options-> List of hosts allowed).

- fonts.googleapis.com
- www.exidecare.com
- www.googletagmanager.com
- graph.facebook.com
- ajax.googleapis.com
- maps.google.com
- www.google-analytics.com
- csi.gstatic.com
- maps.googleapis.com
- scontent.xx.fbcdn.net
- www.twitter.com

- www.google.com
- www.facebook.com
- www.youtube.com
- www.exideindustries.com

Alerts summary

Blind SQL Injection

Classification	
CVSS	Base Score: 6.8 <ul style="list-style-type: none"> - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 10 <ul style="list-style-type: none"> - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Changed - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-89
Affected items	Variation
/service.aspx	6

! SQL injection

Classification	
CVSS	Base Score: 6.8 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Medium- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: Partial
CVSS3	Base Score: 10 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Changed- Confidentiality Impact: High- Integrity Impact: High- Availability Impact: None
CWE	CWE-89
Affected items	Variation
/service.aspx	8

! Application error message

Classification	
CVSS	Base Score: 5.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
/	5

! ASP.NET error message

Classification	
CVSS	Base Score: 5.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
Web Server	1

! HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: High- Authentication: None- Confidentiality Impact: None- Integrity Impact: Partial- Availability Impact: None
CVSS3	Base Score: 4.3 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: Required- Scope: Unchanged- Confidentiality Impact: None- Integrity Impact: Low- Availability Impact: None
CWE	CWE-352
Affected items	Variation
/buy-exide.html (4ddc8f9de53cd6e674cb10d552ed1c63)	1

! Vulnerable Javascript library

Classification	
CVSS	Base Score: 6.4 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: None
CVSS3	Base Score: 6.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: Low- Integrity Impact: Low- Availability Impact: None
CWE	CWE-16
Affected items	Variation
/blog/scripts/jquery.min.js	1
/js/jquery.min.js	1

! Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Medium- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: Partial
CWE	CWE-693
Affected items	Variation
Web Server	1

! Cookie(s) without HttpOnly flag set

Classification		
CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None	
CWE	CWE-16	
Affected items		Variation
/		1

! Insecure response with wildcard '*' in Access-Control-Allow-Origin

Classification		
CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None	
CWE	CWE-16	
Affected items		Variation
/		1
/blog		1
/blog/battery-care		1
/blog/content		1
/blog/emergency-services		1
/blog/images		1
/css		1
/images		1
/js		1

ⓘ Possible relative path overwrite

Classification	
CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CWE	CWE-20
Affected items	Variation
/batmobile.aspx	1
/battery-care.aspx	1
/call-to-buy-exide.aspx	1
/company-information.aspx	1
/copyright-policy.aspx	1
/disclaimer.aspx	1
/diy-tips.aspx	1
/faq.aspx	1
/know-your-battery.aspx	1
/terms-conditions.aspx	1
/warranty-terms.aspx	1

Possible sensitive directories

Classification	
CVSS	Base Score: 5.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
/includes	1
/log	1

Session token in URL

Classification	
CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
/getsocialfeed.aspx (7f349109f2bfda17c3c3f274caf8b234)	1

Broken links

Classification	
CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CWE	CWE-16
Affected items	Variation
/blog/fonts/itf-rupee-webfont.woff2	1
/link%20to%20http://www.exideindustries.com/products/automotive-batteries/two-wheeler-batteries-warranty.aspx	1

Email address found

Classification	
CVSS	Base Score: 5.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
/	1

Error page web server version disclosure

Classification	
CVSS	Base Score: 5.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
Web Server	1

Microsoft IIS version disclosure

Classification	
CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
/	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
/buy-exide.html (4ddc8f9de53cd6e674cb10d552ed1c63)	2

Possible username or password disclosure

Classification	
CVSS	Base Score: 5.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None
CVSS3	Base Score: 7.5 <ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None
CWE	CWE-200
Affected items	Variation
/assets/css/exideshop.lib.min.css	1

Alert details

Blind SQL Injection

Severity	High
Type	Validation
Reported by module	Scripting (Blind_Sql_Injection.script)

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.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

- [VIDEO: SQL Injection tutorial](#)
- [OWASP Injection Flaws](#)
- [How to check for SQL injection vulnerabilities](#)
- [SQL Injection Walkthrough](#)
- [OWASP PHP Top 5](#)
- [Acunetix SQL Injection Attack](#)

Affected items

/service.aspx

Details

URL encoded GET input id was set to -1; waitfor delay '0:0:0' --

Tests performed:

```
--1; waitfor delay '0:0:7.532' -- => 9.75 s
--1; waitfor delay '0:0:3.766' -- => 6.547 s
--1; waitfor delay '0:0:11.298' -- => 11.969 s
--1; waitfor delay '0:0:0' -- => 0.218 s
--1; waitfor delay '0:0:0' -- => 0.172 s
--1; waitfor delay '0: ... (line truncated)
```

Request headers

```
GET
/service.aspx?{}&cmd=Cust_staticContent&commandType=LoadStatic&id=-1;%20waitfor%20delay%
20'0:0:0:0'%20--%20&NoLoginRequire=true&Updatetimestamp=&version=0.781978048151359
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://exidel16.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel16.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input makVal was set to 3lAOjCg0'; waitfor delay '0:0:0' --

Tests performed:

```
- relmq3Mc'; waitfor delay '0:0:12' -- => 12.157 s
- RgFlnysW'; waitfor delay '0:0:8' -- => 8.172 s
- 77B8yicg'; waitfor delay '0:0:0' -- => 0.156 s
- 2QIOOLDm'; waitfor delay '0:0:4' -- => 4.156 s
- BFNXG03h'; waitfor delay '0:0:0' -- => 0.531 s/ ... (line truncated)
```

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelfFuel&makVal=3lAOjCg0';%20waitfor%20delay%
20'0:0:0:0'%20--%20&NoLoginRequire=true&segment=CAR/SUV/MUV&vehModel=Select%20Model&_=1475
056690706 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://exidel16.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel16.allindia.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: */*
```


/service.aspx

Details

URL encoded GET input makVal was set to fGHU9cRh'; waitfor delay '0:0:0' --

Tests performed:

- G7pdC00X'; waitfor delay '0:0:3' -- => 3.187 s
- S1mmDs8X'; waitfor delay '0:0:0' -- => 0.156 s
- GaYB4rhO'; waitfor delay '0:0:6' -- => 6.203 s
- j9QjhPFz'; waitfor delay '0:0:9' -- => 9.172 s
- FwRiukMh'; waitfor delay '0:0:0' -- => 0.485 s[bo ... (line truncated)

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelModel&makVal=fGHU9cRh';%20waitfor%20delay%20'0:0:0'%20--%20&NoLoginRequire=true&segment=CAR/SUV/MUV&_=1475056690665 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://exidel16.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel16.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input segment was set to RYiIGxaX'; waitfor delay '0:0:0' --

Tests performed:

- BKfw80qh'; waitfor delay '0:0:9' -- => 9.187 s
- 0lljSNfX'; waitfor delay '0:0:3' -- => 3.172 s
- DYzQlvns'; waitfor delay '0:0:6' -- => 6.218 s
- n5udCskz'; waitfor delay '0:0:0' -- => 0.188 s
- loQYnp0q'; waitfor delay '0:0:0' -- => 0.156 s[b ... (line truncated)

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelModel&makVal=ASHOK%20LEYLAND%20NISSAN&NoLoginRequire=true&segment=RYiIGxaX';%20waitfor%20delay%20'0:0:0'%20--%20&_=1475056690665 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://exidel16.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel16.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input vehModel was set to WVudvbrH'; waitfor delay '0:0:0' --

Tests performed:

- 71EW7qa5'; waitfor delay '0:0:12' -- => 12.156 s
- yzjlbzre'; waitfor delay '0:0:0' -- => 0.172 s
- YiDmTspa'; waitfor delay '0:0:4' -- => 4.687 s
- LyeX3B97'; waitfor delay '0:0:8' -- => 8.734 s
- lyCCEfbK'; waitfor delay '0:0:0' -- => 0.172 s ... (line truncated)

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelFuel&makVal=&NoLoginRequire=true&segment=
CAR/SUV/MUV&vehModel=WVudvbrH';%20waitfor%20delay%20'0:0:0'%20--%20&_=1475056690706
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input vtype was set to BkDQ4bay'; waitfor delay '0:0:0' --

Tests performed:

- 4qDqs6Vw'; waitfor delay '0:0:9' -- => 9.172 s
- nO8cDG9S'; waitfor delay '0:0:6' -- => 6.188 s
- jMFXYrWh'; waitfor delay '0:0:3' -- => 3.688 s
- ckP2Tu43'; waitfor delay '0:0:0' -- => 0.141 s
- eEBlp24i'; waitfor delay '0:0:0' -- => 0.671 s/bol ... (line truncated)

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelMake&NoLoginRequire=true&vtype=BkDQ4bay';
%20waitfor%20delay%20'0:0:0'%20--%20&_=1475056690628 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

SQL injection

Severity	High
Type	Validation
Reported by module	Scripting (Sql_Injection.script)

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.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

[SQL Injection Walkthrough](#)

[OWASP PHP Top 5](#)

[How to check for SQL injection vulnerabilities](#)

[OWASP Injection Flaws](#)

[VIDEO: SQL Injection tutorial](#)

[Acunetix SQL Injection Attack](#)

Affected items

/service.aspx
Details
URL encoded GET input id was set to 1" Error message found: Unclosed quotation mark
Request headers

```
GET
/service.aspx?{}&cmd=Cust_staticContent&commandType=LoadStatic&id=1'"&NoLoginRequire=true&Updatetimestamp=&version=0.781978048151359 HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input makVal was set to 1"

Error message found: Unclosed quotation mark

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelFuel&makVal=1'"&NoLoginRequire=true&segment=CAR/SUV/MUV&vehModel=Select%20Model&_=1475056690685 HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input makVal was set to 1"

Error message found: Unclosed quotation mark

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelModel&makVal=1'"&NoLoginRequire=true&segment=CAR/SUV/MUV&_=1475056690665 HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input segment was set to 1"

Error message found: Unclosed quotation mark

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelModel&makVal=ASHOK%20LEYLAND%20NISSAN&NoLoginRequire=true&segment=1'&_=1475056690665 HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input segment was set to 1"
Error message found: Unclosed quotation mark

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelFuel&makVal=&NoLoginRequire=true&segment=1'&vehModel=Select%20Model&_=1475056690685 HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input vehModel was set to 1"
Error message found: Unclosed quotation mark

Request headers

```
GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelFuel&makVal=&NoLoginRequire=true&segment=CAR/SUV/MUV&vehModel=1'&_=1475056690685 HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/service.aspx

Details

URL encoded GET input vtype was set to 1"
Error message found: Unclosed quotation mark

Request headers

POST
/service.aspx?cmd=Cust_DynamicLookupCallForLookup&function=FillVARating&NoLoginRequire=true&vtype=1'" HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.com
Content-Length: 0
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: */*

/service.aspx

Details

URL encoded GET input vtype was set to 1"
Error message found: Unclosed quotation mark

Request headers

GET
/service.aspx?cmd=Cust_GetLookupData&lktype=SelMake&NoLoginRequire=true&vtype=1'"&_=1475056690628 HTTP/1.1
Referer: http://exidel6.allindia.com:80/
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*

Application error message

Severity	Medium
Type	Validation
Reported by module	Scripting (Error_Message.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

[PHP Runtime Configuration](#)

Affected items

/
Details
Path Fragment (suffix .aspx) input /[*.aspx] was set to Error message found: ASP.NET is configured to show verbose error messages
Request headers
GET /.aspx HTTP/1.1 Referer: http://exide16.allindia.com:80/ Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt Host: exide16.allindia.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: */*
/
Details
Path Fragment (suffix .aspx) input /[*.aspx] was set to RDNvMWtWMTdYWA== Error message found: ASP.NET is configured to show verbose error messages
Request headers
GET /RDNvMWtWMTdYWA==.aspx HTTP/1.1 Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt Host: exide16.allindia.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: */*

/

Details

Path Fragment (suffix .aspx) input `[/<*>]<s>.aspx` was set to
`acu10076%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10076`
Error message found: ASP.NET is configured to show verbose error messages

Request headers

GET `/acu10076%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10076/battery-care.aspx` HTTP/1.1
Referer: `http://exidel16.allindia.com:80/`
Cookie: `ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt`
Host: `exidel16.allindia.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: */*

/

Details

Path Fragment (suffix .aspx) input `[/<*>]<s>/<s>.aspx` was set to
`acu6500%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6500`
Error message found: ASP.NET is configured to show verbose error messages

Request headers

GET `/acu6500%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6500/battery-care/battery-care.aspx` HTTP/1.1
Referer: `http://exidel16.allindia.com:80/`
Cookie: `ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt`
Host: `exidel16.allindia.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: */*

/

Details

Path Fragment (suffix .aspx) input `[/<*>]<s>/<s>.aspx` was set to
Error message found: ASP.NET is configured to show verbose error messages

Request headers

GET `//battery-care/battery-care.aspx` HTTP/1.1
Referer: `http://exidel16.allindia.com:80/`
Cookie: `ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt`
Host: `exidel16.allindia.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: */*

! ASP.NET error message

Severity	Medium
Type	Validation
Reported by module	Scripting (ASP_NET_Error_Message.script)

Description

By requesting a specially crafted URL is possible to generate an ASP.NET error message. The message contains the complete stack trace and Microsoft .NET Framework Version.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Adjust web.config to enable custom errors for remote clients. Set customErrors mode to RemoteOnly. customErrors is part of system.web Element. RemoteOnly specifies that custom errors are shown only to the remote clients, and that ASP.NET errors are shown to the local host. This is the default value.

```
<configuration>
  <system.web>
    <customErrors mode="RemoteOnly" />
  </system.web>
</configuration>
```

References

[customErrors Element \(ASP.NET Settings Schema\)](#)

Affected items

Web Server
Details
Error message pattern found: <title>Illegal characters in path.</title> Version information found: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.6.1069.1
Request headers
GET / ~.aspx HTTP/1.1 Host: exide16.allindia.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: */*

🚨 HTML form without CSRF protection

Severity	Medium
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/buy-exide.html (4ddc8f9de53cd6e674cb10d552ed1c63)

Details

Form name: <empty>
Form action: http://exide16.allindia.com/buy-exide.html?referforcontact
Form method: GET

Form inputs:

- firstname [Text]

Request headers

```
GET /buy-exide.html?referforcontact HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exide16.allindia.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exide16.allindia.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: */*

Vulnerable Javascript library

Severity	Medium
Type	Configuration
Reported by module	Scripting (Javascript_Libraries_Audit.script)

Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult Web References for more information.

Recommendation

Upgrade to the latest version.

References

<http://bugs.jquery.com/ticket/11290>

<http://research.insecurelabs.org/jquery/test/>

Affected items

/blog/scripts/jquery.min.js

Details

Detected Javascript library jquery version 1.8.3.
The version was detected from file content.

Request headers

```
GET /blog/scripts/jquery.min.js HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer:
http://exidel16.allindia.com/blog/emergency-services/getting-quick-on-road-emergency-service
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel16.allindia.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: */*
```

/js/jquery.min.js

Details

Detected Javascript library jquery version 1.8.3.
The version was detected from file content.

Request headers

```
GET /js/jquery.min.js HTTP/1.1
Accept: */*
Referer: http://exidel16.allindia.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Connection: Keep-Alive
Accept-Encoding: gzip,deflate
Accept-Language: en-IN,*
Host: exidel16.allindia.com
```

Clickjacking: X-Frame-Options header missing

Severity	Low
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

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.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

- [The X-Frame-Options response header](#)
- [Clickjacking](#)
- [OWASP Clickjacking](#)
- [Defending with Content Security Policy frame-ancestors directive](#)
- [Frame Buster Buster](#)

Affected items

Web Server
Details
No details are available.
Request headers
GET / HTTP/1.1 Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc Host: exidel16.allindia.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: */*

Cookie(s) without HttpOnly flag set

Severity	Low
Type	Informational
Reported by module	Crawler

Description

This cookie does not 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.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/
Details
Cookies found: - Name: ASP.NET_SessionId, Domain: exide16.allindia.com
Request headers
GET / HTTP/1.1 Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc Host: exide16.allindia.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: */*

Insecure response with wildcard '*' in Access-Control-Allow-Origin

Severity	Low
Type	Configuration
Reported by module	Scripting (Access_Control-Allow-Origin_Dir.script)

Description

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based by returning the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHttpRequest) requests to your site and access the responses. It's not recommended to use the Access-Control-Allow-Origin: * header.

Impact

Any website can make XHR requests to your site and access the responses.

Recommendation

Is recommended not to use Access-Control-Allow-Origin: *. Instead the Access-Control-Allow-Origin header should contain the list of origins that can make COR requests.

References

[Test Cross Origin Resource Sharing \(OTG-CLIENT-007\)](#)

[CrossOriginRequestSecurity](#)

[Cross-Origin Resource Sharing](#)

[Cross-origin resource sharing](#)

Affected items

/
Details
No details are available.
Request headers
GET / HTTP/1.1 Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc Host: exidel16.allindia.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: */*
/blog

Details

No details are available.

Request headers

```
GET /blog/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/blog
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*
```

/blog/battery-care

Details

No details are available.

Request headers

```
GET /blog/battery-care HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*
```

/blog/content

Details

No details are available.

Request headers

```
GET /blog/content/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/blog/content/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*

/blog/emergency-services

Details

No details are available.

Request headers

GET /blog/emergency-services HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*

/blog/images

Details

No details are available.

Request headers

GET /blog/images/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/blog/images/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*

/css

Details

No details are available.

Request headers

GET /css/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/css/

Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*

/images

Details

No details are available.

Request headers

GET /images/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/images/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*

/js

Details

No details are available.

Request headers

GET /js/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/js/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*

Possible relative path overwrite

Severity	Low
Type	Configuration
Reported by module	Scripting (Relative_Path_Overwrite.script)

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.

Impact

On older versions of Internet Explorer it's possible to execute arbitrary JavaScript code using Internet Explorer's expression() function. An attacker can also extract the page source and potentially steal CSRF tokens using CSS selectors.

Recommendation

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.

References

[Relative Path Overwrite](#)

Affected items

/batmobile.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /batmobile.aspx/aIGuA/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel16.allindia.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: */*
```

/battery-care.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /battery-care.aspx/IrrbF/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exide16.allindia.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: */*
```

/call-to-buy-exide.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /call-to-buy-exide.aspx/RrFzg/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exide16.allindia.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: */*
```

/company-information.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /company-information.aspx/0XQFz/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exide16.allindia.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: */*
```

/copyright-policy.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /copyright-policy.aspx/Vtt29/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exide16.allindia.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: */*
```

/disclaimer.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /disclaimer.aspx/3lrbY/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/diy-tips.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /diy-tips.aspx/7tdkp/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/faq.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /faq.aspx/LAsNZ/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/know-your-battery.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /know-your-battery.aspx/v7ARq/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/terms-conditions.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /terms-conditions.aspx/kj0B0/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

/warranty-terms.aspx

Details

A CSS import from a relative path was found on this page: <link rel="stylesheet" type="text/css" href="css/style.css" />The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /warranty-terms.aspx/LhhUa/ HTTP/1.1
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```


Possible sensitive directories

Severity	Low
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive directory has been found. This directory is 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.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

[Web Server Security and Database Server Security](#)

Affected items

/includes
Details
No details are available.
Request headers
GET /includes HTTP/1.1 Accept: acunetix/wvs Range: bytes=0-99999 Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt Host: exide16.allindia.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

/log
Details
No details are available.
Request headers
GET /log HTTP/1.1 Accept: acunetix/wvs Range: bytes=0-99999 Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt Host: exide16.allindia.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
```

Session token in URL

Severity	Low
Type	Informational
Reported by module	Crawler

Description

This application contains a session token in the query parameters. A session token is sensitive information and should not be stored in the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The session should be maintained using cookies (or hidden input fields).

Affected items

/getsocialfeed.aspx (7f349109f2bfda17c3c3f274caf8b234)

Details

<http://exide16.allindia.com/GetSocialFeed.aspx?sid=31&feedtype=all>

Request headers

```
GET /GetSocialFeed.aspx?sid=31&feedtype=all HTTP/1.1
Referer: http://exide16.allindia.com/
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: */*
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en-IN, *
Host: exide16.allindia.com
```

Broken links

Severity	Informational
Type	Informational
Reported by module	Crawler

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/blog/fonts/itf-rupee-webfont.woff2

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /blog/fonts/itf-rupee-webfont.woff2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exide16.allindia.com/blog/content/content.css
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exide16.allindia.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: */*
```

/link%20to%20http://www.exideindustries.com/products/automotive-batteries/two-wheeler-batteries-warranty.aspx

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET
/link%20to%20http://www.exideindustries.com/products/automotive-batteries/two-wheeler-ba
```

```
tteries-warranty.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=3yhe4ojztqbfwr3ax0xquokt
Host: exidel6.allindia.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: */*
```

Email address found

Severity	Informational
Type	Informational
Reported by module	Scanner

Description

One or more email addresses have been found on this page. 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.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

Affected items

/

Details

List of all email addresses found on this host.

- customercare@exidecare.com

/

- grievance@exidecare.com

/

Error page web server version disclosure

Severity	Informational
Type	Configuration
Reported by module	Scripting (Error_Page_Path_Disclosure.script)

Description

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

Impact

Possible sensitive information disclosure.

Recommendation

If you are using Apache, you can setup a custom 404 page by following the instructions provided in the References section.

References

[Creating Custom Error Pages on Apache Servers](#)

[Custom error responses](#)

Affected items

Web Server
Details
Information disclosure pattern found: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.6.1069.1
Request headers
GET /0lIFUtexXB.aspx HTTP/1.1 Host: exidel6.allindia.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: */*

Microsoft IIS version disclosure

Severity	Informational
Type	Configuration
Reported by module	Scripting (ASP_NET_Error_Message.script)

Description

The HTTP responses returned by this web application include a header named Server. The value of this header includes the version of Microsoft IIS server.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.

References

[Remove Unwanted HTTP Response Headers](#)

Affected items

/
Details
Version information found: Microsoft-IIS/8.5
Request headers
GET / ~.aspx HTTP/1.1 Host: exidel6.allindia.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: */*

Password type input with auto-complete enabled

Severity	Informational
Type	Informational
Reported by module	Crawler

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.

Impact

Possible sensitive information disclosure.

Recommendation

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">

Affected items

/buy-exide.html (4ddc8f9de53cd6e674cb10d552ed1c63)

Details

Password type input(s): "" from unnamed form with action 4ddc8f9de53cd6e674cb10d552ed1c63 have autocomplete enabled.

Request headers

```
GET /buy-exide.html?referforcontact HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exide16.allindia.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exide16.allindia.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: */*
```

/buy-exide.html (4ddc8f9de53cd6e674cb10d552ed1c63)

Details

Password type input(s): "" from unnamed form with action javascript:void(0) have autocomplete enabled.

Request headers

```
GET /buy-exide.html?referforcontact HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel6.allindia.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel6.allindia.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: */*
```

Possible username or password disclosure

Severity	Informational
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/assets/css/exideshop.lib.min.css

Details

Pattern found: pass:before

Request headers

```
GET /assets/css/exideshop.lib.min.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://exidel16.allindia.com/buy-exide.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=1b0oejth4hbwyhcm4fxkoxsc
Host: exidel16.allindia.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: */*
```

Scanned items (coverage report)

Scanned 138 URLs. Found 26 vulnerable.

URL: <http://exide16.allindia.com/>

Vulnerabilities have been identified for this URL

11 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
<code>[/[*]]/<s>/<s>.aspx</code>	Path Fragment (suffix .aspx)
<code><s>/[[*]]/<s>.aspx</code>	Path Fragment (suffix .aspx)
<code><s>/<s>/[[*]].aspx</code>	Path Fragment (suffix .aspx)

Input scheme 2

Input name	Input type
<code>[[*]].aspx</code>	Path Fragment (suffix .aspx)

Input scheme 3

Input name	Input type
<code>[[*]]/<s>/<s></code>	Path Fragment
<code><s>/[[*]]/<s></code>	Path Fragment
<code><s>/<s>/[[*]]</code>	Path Fragment

Input scheme 4

Input name	Input type
<code>[[*]]/<s>.aspx</code>	Path Fragment (suffix .aspx)
<code><s>/[[*]].aspx</code>	Path Fragment (suffix .aspx)

Input scheme 5

Input name	Input type
<code>[[*]].html</code>	Path Fragment (suffix .html)

Input scheme 6

Input name	Input type
Host	HTTP Header

URL: <http://exide16.allindia.com/css/>

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://exide16.allindia.com/css/style.css>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://exide16.allindia.com/css/slick.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/css/jquery.fullpage.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/css/home.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/css/jpreloader.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/css/jquery.mcustomscrollbar.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/css/content.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/css/style2.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/css/fonts
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/common.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/jpreloader.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/home.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://exide16.allindia.com/js/jquery.mousewheel.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/slick.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/jquery.min.js
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/jquery.mcustomscrollbar.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/jquery.fullpage.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/scrolloverflow.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/common1.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/js/registerbattery.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/exide-care-logo.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/batmobilecar.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/snabtn.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://exide16.allindia.com/images/icon-ec.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/redbg.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/home-blog3.jpg
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/pin_red.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/pin_grey.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/bdbg.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/signupbg2.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/socialbg.jpg
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/pin_orange.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/social-active.gif
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/batmobile-icon.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/logo.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://exide16.allindia.com/images/icon-contactno.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/downarrow.gif
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/radio-selected.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/pin_deepred.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/arrow.gif
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/batmobilebg.jpg
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/scrolldown.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/icon-facebook.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/smoverlay.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/icon-twitter.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/icon-smedia2.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/images/icon-contactno2.png
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://exide16.allindia.com/images/icon-smedia.png	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/images/home-blog1.jpg	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/images/home-blog2.jpg	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/getsocialfeed.aspx	
No vulnerabilities have been identified for this URL	
2 input(s) found for this URL	
Inputs	
Input scheme 1	
Input name	Input type
feedtype	URL encoded GET
sid	URL encoded GET
URL: http://exide16.allindia.com/blog/	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/blog/emergency-services	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/blog/emergency-services/introducing-exide-care	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/blog/emergency-services/getting-quick-on-road-emergency-service	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/blog/emergency-services/battery-care.aspx	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/blog/emergency-services/know-your-battery.aspx	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	

URL: http://exide16.allindia.com/blog/battery-care
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/battery-care/environment-friendly-recycle-used-battery
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/battery-care/battery-care.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/battery-care/know-your-battery.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/content/
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/content/style.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/content/content.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/content/jpreloader.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/content/jquery.fullpage.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/images/
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/scripts/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/scripts/jquery.min.js
Vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://exide16.allindia.com/blog/scripts/jpreloader.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/scripts/scrolloverflow.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/scripts/jquery.fullpage.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/scripts/common.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/emergency%20services
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/emergency%20services/introducing-exide-care
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/emergency%20services/battery-care.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/emergency%20services/know-your-battery.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/exide-batteries
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/exide-batteries/know-your-battery
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/exide-batteries/battery-care.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/exide-batteries/know-your-battery.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://exide16.allindia.com/blog/uploadblogimages/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/uploadblogimages/blog/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/uploadblogimages/bigimages/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/uploadblogimages/thumbimages/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/battery-care.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/know-your-battery.aspx
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/fonts/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/blog/fonts/itf-rupee-webfont.woff2
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/faq.aspx
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/diy-tips.aspx
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/buy-exide.html
No vulnerabilities have been identified for this URL
2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

Input scheme 2	
Input name	Input type
firstname	URL encoded GET
URL: http://exide16.allindia.com/batmobile.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/disclaimer.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/battery-care.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/warranty-terms.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/know-your-battery.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/terms-conditions.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/copyright-policy.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/call-to-buy-exide.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/company-information.aspx	
Vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/exidecustomer.appcache	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://exide16.allindia.com/assets/	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	

URL: http://exide16.allindia.com/assets/images/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/images/mobileapp/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/images/images/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/css/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/css/exideshop.min.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/css/exideshop.lib.min.css
Vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/css/fonts
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/css/images/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/css/jquery.animateSlider.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/js/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/js/exideshop.lib.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://exide16.allindia.com/assets/js/exideshop.min2.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/assets/js/appjs/>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/assets/js/appjs/marketplace.js>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/assets/lib/>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/assets/lib/bootstrap-datepicker.js>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: http://exide16.allindia.com/assets/lib/lightbox.js?_=1475056690627
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/assets/img>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/assets/fonts/>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/assets/fonts/fontawesome-webfont.woff2>
No vulnerabilities have been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
v	URL encoded GET

URL: <http://exide16.allindia.com/assets/templates/>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/fonts/>
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: <http://exide16.allindia.com/service.aspx>
Vulnerabilities have been identified for this URL
37 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET
cmd	URL encoded GET
commandType	URL encoded GET
NoLoginRequire	URL encoded GET

Input scheme 2	
Input name	Input type
-	URL encoded GET
cmd	URL encoded GET
lktype	URL encoded GET
NoLoginRequire	URL encoded GET
vtype	URL encoded GET

Input scheme 3	
Input name	Input type
	URL encoded GET
cmd	URL encoded GET
commandType	URL encoded GET
id	URL encoded GET
NoLoginRequire	URL encoded GET
Updatetimestamp	URL encoded GET
version	URL encoded GET

Input scheme 4	
Input name	Input type
cmd	URL encoded GET
function	URL encoded GET
NoLoginRequire	URL encoded GET
vtype	URL encoded GET

Input scheme 5	
Input name	Input type
-	URL encoded GET
cmd	URL encoded GET
lktype	URL encoded GET
makVal	URL encoded GET
NoLoginRequire	URL encoded GET
segment	URL encoded GET

Input scheme 6	
Input name	Input type

-	URL encoded GET
cmd	URL encoded GET
lktype	URL encoded GET
makVal	URL encoded GET
NoLoginRequire	URL encoded GET
segment	URL encoded GET
vehModel	URL encoded GET

Input scheme 7

Input name	Input type
UserName	JSON
cmd	URL encoded GET
cnt	URL encoded GET
NoLoginRequire	URL encoded GET

URL: <http://exide16.allindia.com/exidecustomer.html>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://exide16.allindia.com/link%20to%20http:>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://exide16.allindia.com/link%20to%20http://www.exideindustries.com>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://exide16.allindia.com/link%20to%20http://www.exideindustries.com/products>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://exide16.allindia.com/link%20to%20http://www.exideindustries.com/products/automotive-batteries>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL:
<http://exide16.allindia.com/link%20to%20http://www.exideindustries.com/products/automotive-batteries/two-wheeler-batteries-warranty.aspx>

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://exide16.allindia.com/includes/>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://exide16.allindia.com/log/>

No vulnerabilities have been identified for this URL

No input(s) found for this URL