New issue

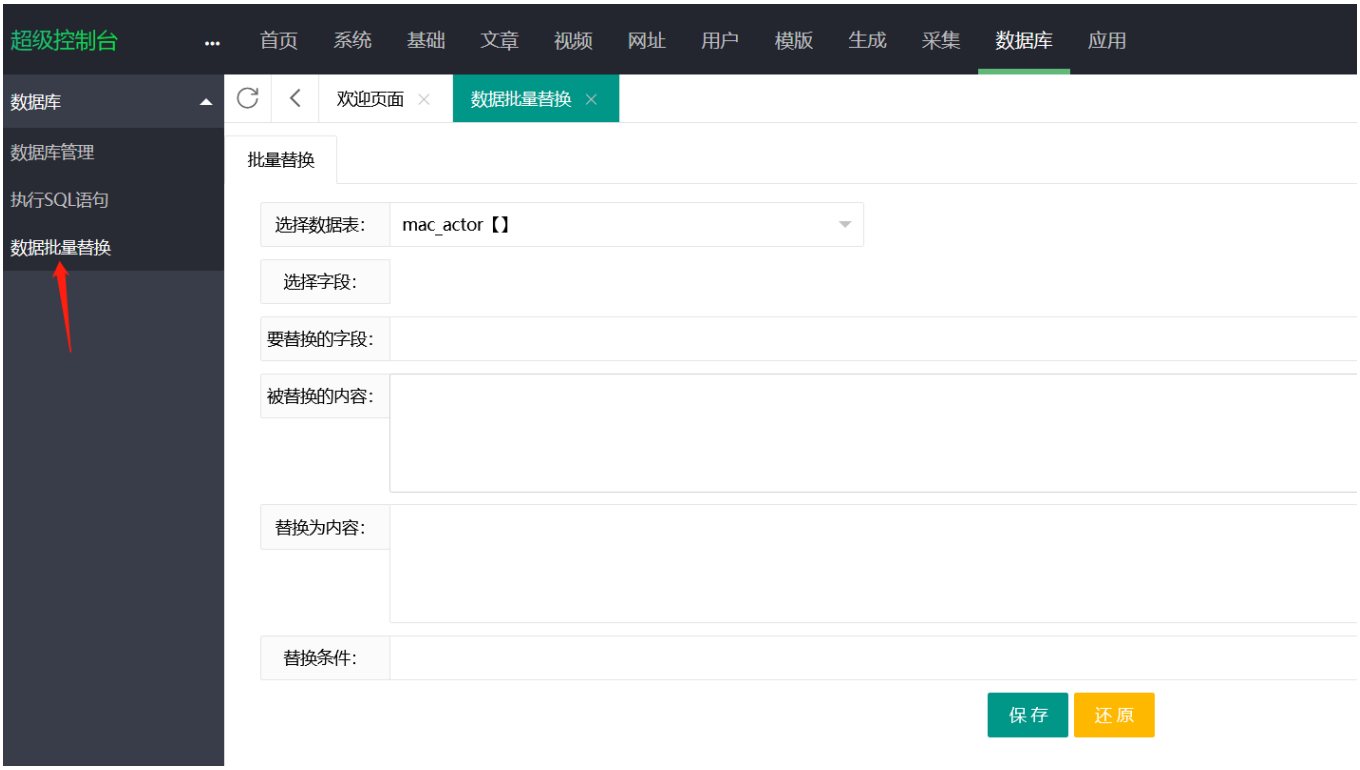
Jump to bottom

SQL injection vulnerability in maccms10 background #931

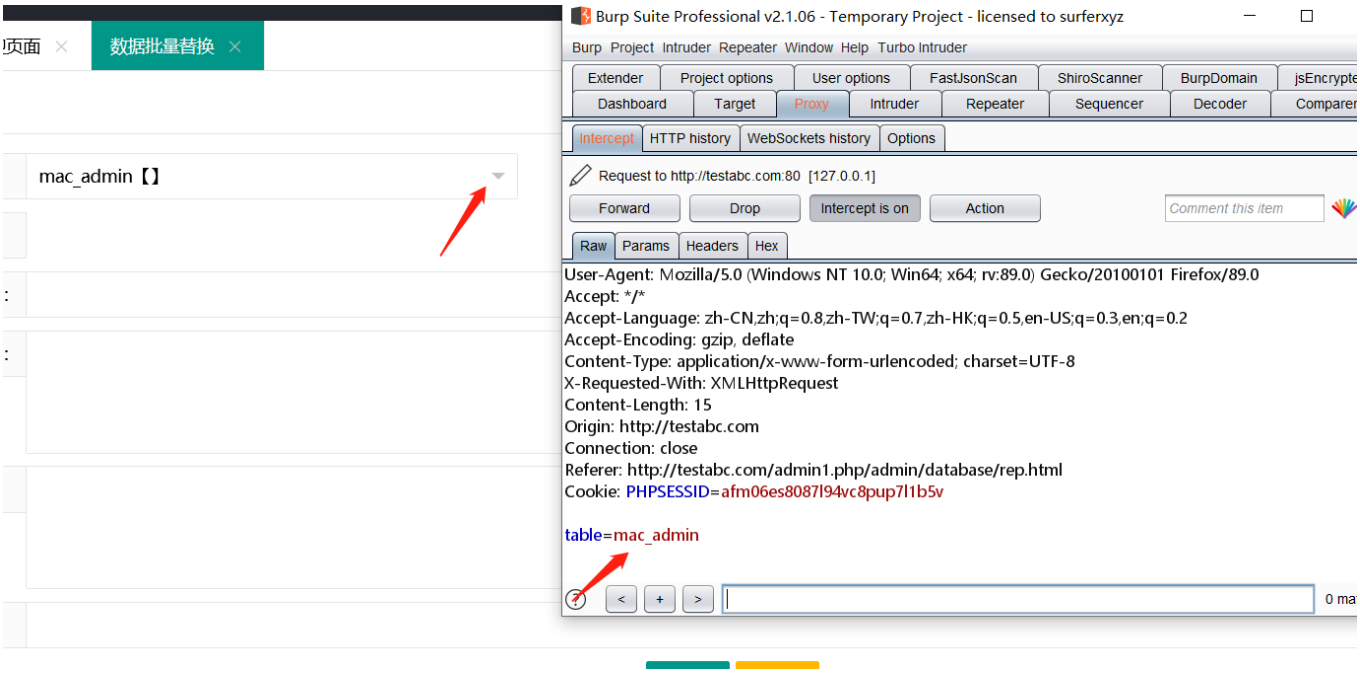
Closed **GxBSXUKing** opened this issue on Jul 1 · 1 comment

GxBSXUKing commented on Jul 1

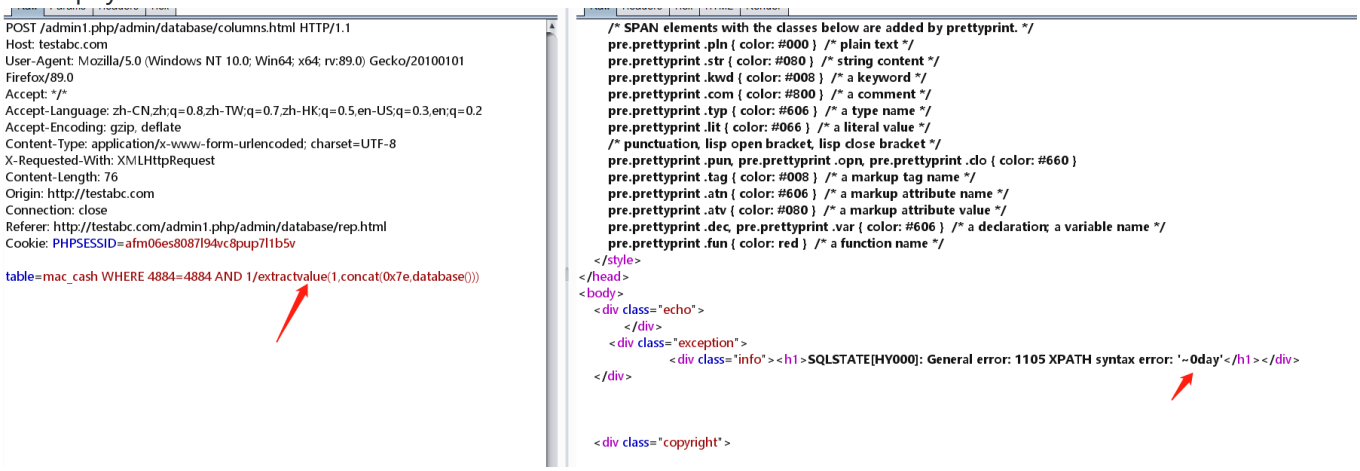
Vulnerability name：SQL injection
Vulnerability level：Medium risk
Affected version：v2021.1000.1081<=v2022.1000.3031
Vulnerability location：
Log in to the background and click the database function module to select the data batch replacement function



Intercept selection data table



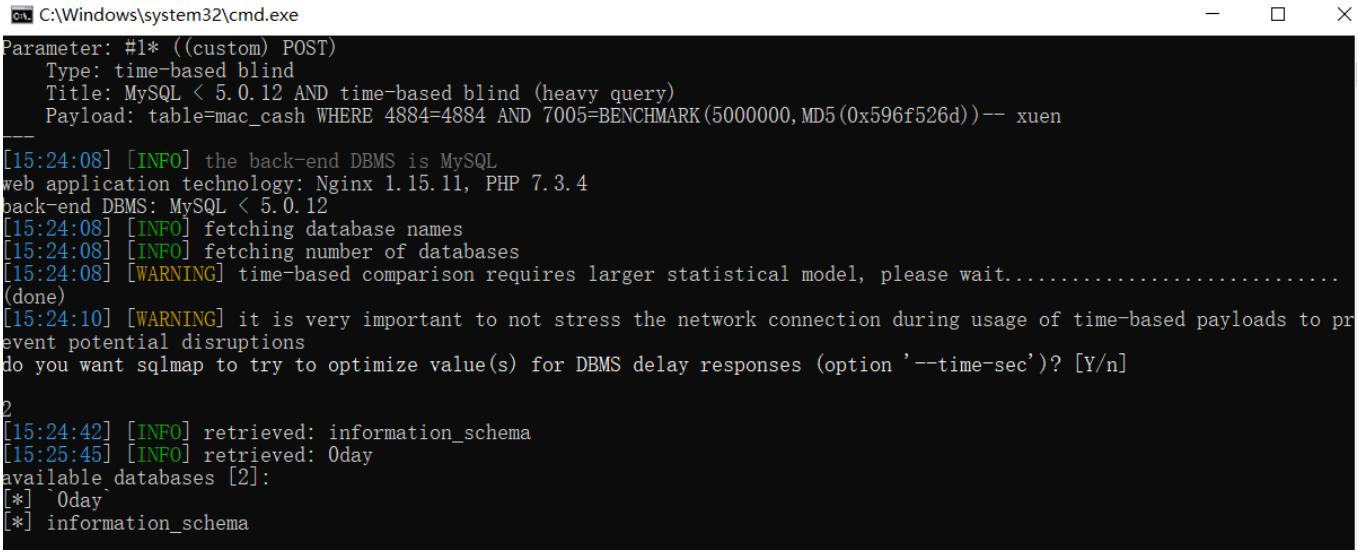
Enter payload to attack



Audit the code. There is no restriction on the type and length of the parameter tables, and there is no token verification

```
public function columns()
{
    $param = input();
    $table = $param['table'];
    if(!empty($table)){
        $list = Db::query('SHOW COLUMNS FROM '.$table);
        $this->success(lang('obtain_ok'),null, $list);
    }
    $this->error(lang('param_err'));
}
```

This vulnerability can obtain a large amount of data



magicblack closed this as completed in 9375d42 on Jul 14

---

magicblack commented on Jul 14 — Owner

Fixed, thanks for your hard work.

magicblack closed this as completed on Jul 14

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants