SERVER-SIDE REQUEST FORGERY (SSRF)

Λίγα λόγια…

- Πρόκειται για ευπάθεια μίας web εφαρμογής η οποία δίνει τη δυνατότητα σε έναν επιτιθέμενο να πυροδοτήσει requests από την πλευρά του server (server-side), σε μη επιθυμητά locations.

- Για παράδειγμα, ένα σύνηθες σενάριο είναι ο επιτιθέμενος να προκαλέσει τον server να πραγματοποιήσει request σε internal-only υπηρεσίες εντός κάποιου οργανισμού (μέρος του οποίου συνιστά ο server).

- Με τον τρόπο αυτόν είναι εφικτό:
  - Να διαρρεύσουν ευαίσθητα στοιχεία ενός server (ή μιας επιχείρησης)
  - Η σύνδεση με εξωτερικά συστήματα ενός επιτιθέμενου
  - Σε σπάνιες περιπτώσεις να επιτευχθεί arbitrary command execution

Παράδειγμα

Ας υποθέσουμε πως μία εφαρμογή με προϊόντα επιτρέπει σε έναν χρήστη να ελέγξει εάν ένα αντικείμενο είναι σε απόθεμα. Προς τούτο, η εφαρμογή επικοινωνεί (URL requests) με άλλα internal back-end APIs. Για παράδειγμα όταν ο χρήστης επιθυμεί να μάθει για ένα προϊόν, πραγματοποιεί το ακόλουθο POST request.

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118

stockApi=http://stock.weliketoshop.net:8080/product/stoc
k/check%3FproductId%3D6%26storeId%3D1
```

Παράδειγμα (1)

Το προηγούμενο θα έχει ως αποτέλεσμα ο server να πραγματοποιήσει request στο εκάστοτε URL της μεταβλητής stockApi, προκειμένου να ανακτήσει τις ζητούμενες πληροφορίες και να τις επιστρέψει στον χρήστη.

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118

stockApi=http://stock.weliketoshop.net:8080/product/stock/check%3FproductId%3D6%26storeId%3D1
```

Σε ένα τέτοιο σενάριο, ο επιτιθέμενος μπορεί να τροποποιήσει το POST request του ως εξής:

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118

stockApi=http://localhost/admin
```

Παράδειγμα (2)

Το γεγονός αυτό θα αναγκάσει τον server να ζητήσει τη σελίδα του admin και να επιστρέψει τα περιεχόμενά της στον χρήστη.

Ε και; Σελίδες σαν και αυτές του admin είναι προσβάσιμες μόνο από authenticated ή privileged χρήστες της εφαρμογής (πιθανόν να σκεφτεί κανείς και να έχει και δίκαιο). Άρα πολύ απλά ο χρήστης εν τέλει δε θα δει τίποτα.

Έλα όμως που το request για τη σελίδα */admin* δεν πραγματοποιείται από τον απλό χρήστη αλλά από τον server ο οποίος πολύ πιθανόν να θεωρείται έμπιστος και άρα να έχει τα κατάλληλα δικαιώματα. Σε αυτήν την περίπτωση, στον χρήστη θα επιστραφεί κανονικά το περιεχόμενο της privileged σελίδας.

WOW SLAY!!

Resources

- https://portswigger.net/web-security/ssrf
- https://owasp.org/www-community/attacks/Server_Side_Request_Forgery
- https://academy.hackthebox.com/module/details/145 (το κομμάτι για SSRF)
- https://tryhackme.com/room/ssrfhr