Cross-Site Request Forgery (CSRF)

Kus leidub oht

Kõikidel veebilhetedel või siis HTML feede millele kasutaja saab ligi.

Kuidas toimub rünne

Kasutaja petetaks ära saatma võtlsitud http päring kas image tagis, XSS või mõnel muul viisil.

Ning see päring sooritab midagi tegevuse ilma ohvri tegeliku nõusolekuta, ega aplikatsioon ei tee vahet kas see on saadetud http päring või kasutaja poolt klickitud link kui kasutaja on autoriseeritud.

Üldiselt lähevad rünnakud läbi siis kui ründaja teab kasutaja autoriseeritud ning kasutaja on kindlasti sisse logitud süsteemi ning esined süsteemis nõrkus mis ei soovi kasutaja autentimist peale iga tehingut.

Turva nõrkus

Kui on veebilehel lihtne leida operatsiooni detaile. Kasutaja andmeid saadetakse automaatselt ja tänu sellele on võimalik teha pahatahtlik veebileht mis saadab võltsitud pärnguid mida pole võimalik eristada tõestest. Kõik aplikatsioonid on ohus mis nõustuvad http päringutega kui pole võimalust tõestada et konkreetne päring on seotud kindla kasutajaga sessiooniga .Ainult unikaalsest session ID pole kasu kuna http päringus on lisatud juba kehtid sessioon ID sest kasutaja on autenditud.

Nõrkused saab leida kas oled ohus penetration testiga või code analysistiga.

Tagajärg

Võimalik on muuta ära kõiksugused andmed mida on kasutajal õigus muuta.Või funktsioone.

Vältimine

Ettearvamatu sümbol litsatud lehe url-i. Võiksid olla unikaalsed kas vähemalt igas sessioonis või siis ka päringus.Kasutatakse ka nii et , lisatakse html body sse pedetud välja siis ei ole vaja seda url i panna.

1. A list is complied prior to delivering the page to the user. The list contains all valid unique IDs generated for all links on a given page. The unique ID could be derived from a secure random generator such as SecureRandom for J2EE. .
2. A unique ID is appended to each link/form on the requested page prior to being displayed to the user.
3. Maintaining a list of unique IDs in the user session, the application checks if the unique ID passed with the HTTP request is valid for a given request. if the unique ID passed with the HTTP request is valid for a given request.

4. If the unique ID is not present, terminate the user session and display an error to the user.

Näide

1.

The application allows a user to submit a state changing request that does not include anything secret. Like so:

```
http://example.com/app/transferFunds?amount=1500&destinationAcc
ount=4673243243
```

So, the attacker constructs a request that will transfer money from the victim's account to their account, and then embeds this attack in an image request or iframe stored on various sites under the attacker's control.

```
<img
src="http://example.com/app/transferFunds?amount=1500&destinati
onAccount=attackersAcct#" width="0" height="0" />
```

If the victim visits any of these sites while already authenticated to example.com, any forged requests will include the user's session info, inadvertently authorizing the request.

2.Testkeskond csrft Tester:

Testimiseks

https://www.owasp.org/index.php/CSRFTester_Usage

Kasutatud kirjandus:

https://www.owasp.org/index.php/Top_10_2010-A5