

Forum:[Hack Forums](#)

Thread: [What can you do with a XSS Vulnerability?](#)

deetex - October 11, 2024, 8:51 am

Hello, like the 6th thread before me I also found a XSS Vulnerability inside of my school website.

I am planning on reporting it to the IT-Team since I actually want to finish school and not get kicked out ?.

But to do this i want to show what someone can do with this type of Vulnerability so my school actually takes it serious, I have found a XSS Vulnerability on my school's website before and i want them to take it more serious now, since i ran "dalfox" (a automated XSS Scanner) and I found another vuln in around 5 minutes. I want my school to take this stuff serious before there are victims or anything else happens.

Do you guys know a good way to show my school that this vulnerability is actually serious and what someone can do with a XSS Vulnerability?

Thank you,
All Love Deetex.

zaya.klum - October 11, 2024, 12:06 pm

I'd suggest reading OWASP's page on this, so that no one accuses you of doing your homework before you actually turn it in ;)

<https://owasp.org/www-community/attacks/xss/>

But as for methods and vulns you could exploit using XSS, the simplest thing you can test for is if you can run a malicious Javascript that intercepts user credentials (even a simple fake Login/Password pop-up box can be made to steal creds). Or a redirect to an external malicious HTML url that further performs attacks (cookie stealing, drive-by download - off the to of my head).

Other stuff is altering web page content to show malicious or misleading content.

If you're open to sharing what the vulnerability actually is, we might be able to give you some more practical advice. See if you can implement the above though.

Good luck!

deetex - October 11, 2024, 12:13 pm

(Oct 11, 2024 12:06 PM)zaya.klum Wrote: [\[CITE\]](#) I'd suggest reading OWASP's page on this, so that no one accuses you of doing your homework before you actually turn it in ;)

(removed link cause i need to have 50 total posts?)

But as for methods and vulns you could exploit using XSS, the simplest thing you can test for is if you can run a malicious Javascript that intercepts user credentials (even a simple fake Login/Password pop-up box can be made to steal creds). Or a redirect to an external malicious HTML url that further performs attacks (cookie stealing, drive-by download - off the to of my head).

Other stuff is altering web page content to show malicious or misleading content.

If you're open to sharing what the vulnerability actually is, we might be able to give you some more practical advice. See if you can implement the above though.

Good luck!

Hello, thank you very much for your reply and i will most definitely check out that OWASP guide. I have already tested the javascript, a alert box works, h1 (text) works, redirect works (so for example what you said 2, redirect it to a phishing page) and i can also make input boxes AKA its a full xss vulnerability and i can put in any html tag i want.

But i got a question, what do you mean with "If you're open to sharing what the vulnerability actually is" do you mean sharing the website or just the payload?

Thank you for your time?,
Deetex.

zaya.klum - October 11, 2024, 12:21 pm

(Oct 11, 2024 12:13 PM)deetex Wrote: [\[CITE\]](#) Hello, thank you very much for your reply and i will most definitely check out that OWASP guide.

I have already tested the javascript, a alert box works, h1 (text) works, redirect works (so for example what you said 2, redirect it to a phishing page) and i can also make input boxes AKA its a full xss vulnerability and i can put in any html tag i want.

But i got a question, what do you mean with "If you're open to sharing what the vulnerability actually is" do you mean sharing the website or just the payload?

Thank you for your time?,
Deetex.

From what you've described, it sounds to me that you have enough material for a case to turn in to the admin/school principal :) An additional idea for you to polish your presentation: the attacker spoofs a staff member (e.g.: similar Gmail email address), sending an email which contains using the malicious school URL you've just crafted with the XSS vuln. It looks innocuous, who would refuse clicking an URL from the school itself?

The surprise is of course the payload on the other side. Could be a malicious download for a Word file, could be a phishing Log-in form (if your school has a Portal for staff or students).

And yes I meant sharing the website and the payload, however I wouldn't advise doing so here publicly for obvious reasons.

You've got this. Good luck!

deetex - October 11, 2024, 12:26 pm

(Oct 11, 2024 12:21 PM)zaya.klum Wrote: [\[CITE\]](#) From what you've described, it sounds to me that you have enough material for a case to turn in to the admin/school principal :) An additional idea for you to polish your presentation: the attacker spoofs a staff member (e.g.: similar Gmail email address), sending an email which contains using the malicious school URL you've just crafted with the XSS vuln. It looks innocuous, who would refuse clicking an URL from the school itself?

The surprise is of course the payload on the other side. Could be a malicious download for a Word file, could be a phishing Log-in form (if your school has a Portal for staff or students).

And yes I meant sharing the website and the payload, however I wouldn't advise doing so here publicly for obvious reasons.

You've got this. Good luck!
Thank you for your reply,

I am thinking of indeed doing that and just mass sending to email's to show what it can do.

I will indeed not be sharing the website/vuln (for obvious opsec reasons lol).

Thank you,
Deetex.

Money- - *October 13, 2024, 4:02 am*

Dalfox huh? This site must be really vulnerable to be able to pick up by the likes of dalfox lol. Report it to your school honestly go get an award for it lol.

deetex - *October 14, 2024, 12:46 pm*

(Oct 13, 2024 04:02 AM)Money- Wrote: [\[CITE\]](#) Dalfox huh? This site must be really vulnerable to be able to pick up by the likes of dalfox lol. Report it to your school honestly go get an award for it lol.
Yeah it really is,

I checked my schools IT Team and it was all old people who looked like they have never written a line of code.

Probably don't even know what a <h1> tag does, so I wasn't to surprised it was vulnerable lol.