

بسمه تعالی



## وبسایت دانشگاه علوم پزشکی شهرکرد

### ارزیابی امنیتی وبسایت

نوع سند ..... گزارش فنی  
شماره نگارش ..... ۱  
تاریخ نگارش ..... ۱۳۹۹/۰۲/۱۸

تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران

cert.ir



۴۲۶۵۰۰۰۰۰۲۱



(۰۲۱)۴۲۶۵۰۰۰۰



## فهرست مطالب

۱	معرفی سامانه	۱
۲	شرح آسیب پذیری	۲
۳	نقایص امنیتی موجود در برنامه کاربردی	۳
۳-۱	آسیب پذیری دور زدن مکانیزم کد امنیتی (کپچا)	۳-۱
۳-۲	استفاده از شناسه یکتا کاربر (سشن) با ساختار ساده	۳-۲
۳-۳	عدم مدیریت صحیح خطاها	۳-۳
۳-۴	ذکر مسیرهای غیر ضروری در فایل robots.txt	۳-۴

## ۱ معرفی سامانه

وبسایت تحت بررسی مربوط به دانشگاه علوم پزشکی شهرکرد است که از سال ۱۳۶۵ کار خود را با پذیرش ۲۴۰ دانشجو در سه رشته و دو مقطع تحصیلی در قالب دو دانشکده آغاز کرد. تعداد اعضای هیات علمی دانشگاه در حال حاضر ۲۲۸ نفر و شامل ۱۶ ستاد، ۲۹ دانشیار، ۱۶۳ استادیار و ۲۹ مربی و ۱ نفر استادیار پژوهشی می باشد. بخش سلامت استان زیر نظر دانشگاه علوم پزشکی و خدمات بهداشتی و درمانی استان چهارمحال و بختیاری مدیریت می گردد.



شکل ۱ وبسایت دانشگاه علوم پزشکی شهرکرد

## ۲ شرح آسیب‌پذیری

آنچه در این گزارش ارائه می‌گردد، تعدادی از آسیب‌پذیری‌های یافت شده در وبسایت دانشگاه علوم پزشکی شهرکرد به آدرس اینترنتی <https://www.skums.ac.ir> است. ارزیابی‌های صورت گرفته، حاکی از آن است که در این سامانه، چهار آسیب‌پذیری و مشکل امنیتی وجود دارد که در ادامه به تفصیل در مورد هر یک از این آسیب‌پذیری‌ها، مولفه‌های آسیب‌پذیر، جزئیات و راه‌حل‌های پیشنهادی توضیحاتی ارائه می‌گردد.

بررسی‌ها حاکی از آن است که وبسایت مذکور از DorsaPortal به عنوان سیستم مدیریت محتوای خود استفاده می‌نماید.

185.188.112.6		Ports
Country	Iran	80, 8080, 8443
Organization	Rasaneh Estahan Net	
ISP	Rasaneh Estahan Net	
Last Update	2020-08-30T14:02:42.712922	
ASN	AS42163	

شکل ۲ آدرس ip و پورت‌های باز

**توجه:** بررسی سطحی زیر دامنه‌های این وبسایت نشانگر این است که زیر دامنه‌ها نیاز به بررسی بیشتر داشته و احتمال وجود آسیب‌پذیری‌های جدی در آن‌ها به چشم می‌خورد. لازم به ذکر است که با توجه به عدم امکان ثبت‌نام در این وبسایت، پنل کاربران نیز مورد بررسی قرار نگرفت.

## ۳ نقایص امنیتی موجود در برنامه کاربردی

### ۳-۱ آسیب پذیری دور زدن مکانیزم کد امنیتی (کیچا)

● درجه و نوع خطر: بحرانی

● مؤلفه آسیب پذیر: کدهای کیچای در نظر گرفته شده برای کاربران

● توضیحات تکمیلی:

یکی از مهم ترین اشکالات این وبسایت در بخش فرمها خود را نمایان میسازد. به این شکل که پس از پر کردن فرمهای موجود، از کاربر خواسته می شود کد کیچای در نظر گرفته شده در فرم مربوطه را نیز وارد نماید. پس از پر کردن فرم مربوطه و ارسال درخواست، همانطور که در تصویر زیر نیز مشاهده می شود، علاوه بر کد کیچای وارد شده توسط کاربر، کد کیچای در نظر گرفته شده برای وی نیز در متن درخواست به سمت سرور ارسال می گردد. به عبارت دیگر علاوه بر کد وارد شده توسط کاربر، کدی که به منظور راستی آزمایی و مقایسه برای کاربر در نظر گرفته شده نیز در متن درخواست ارسال می گردد. بررسی های صورت گرفته حاکی از آن است که با تغییر هر دوی این مقادیر به مقدار دلخواه، قادر خواهیم بود این فرآیند را دور زده و عبارتی غیر از مقدار تعیین شده توسط سرور را جعل نماییم.

```
POST //ViewAdvForm.aspx?lang=1&sub=0&tempname=main&code=551&ShowNewForm=False&cap=610835 HTTP/1.1
Host: www.skums.ac.ir
Connection: close
Content-Length: 10057
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://www.skums.ac.ir
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: iframe
Referer: https://www.skums.ac.ir//ViewAdvForm.aspx?lang=1&sub=0&tempname=main&code=551&ShowNewForm=False&cap=610835
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=q74a1m1xxairqipc48b8kx0; eformcap610835=Value=520054

...EVENTTARGET=shc14_EVENTARGUMENT=4_VIEWSTATE=->>>>REDUCT<<<<-4_VIEWSTATEGENERATOR=72A9F0B4s_VIEWSTATEENCRYPTED=4hdiTopURL=
//?lang=1&D=0&sub=1&D=2&tempname=1&Domain=5&formid=1&D=31&txtFabgirsCode=4&txtSequre=4&informaring=1&anner=1&delayreason=114&delayreason_0=on&txtcapl=
520054&CopyOfdelayreason1=14&CopyOfdelayreason1_2=on&CopyOfCopyOfdelayreason11778124&CopyOfCopyOfdelayreason11778_2=on
```

#### شکل ۳ درخواست ارسالی هنگام سابمیت فرمها

این مسئله ناشی از آن است که سمت سرور راستی آزمایی و مقایسه این دو مقدار صورت نمی گیرد. به عبارت دیگر بررسی نمی گردد که آیا مقدار وارد شده توسط کاربر به عنوان کیچا با مقدار در نظر گرفته شده توسط سرور یکسان است یا خیر.

● راه حل:

به عنوان راه حل پیشنهاد می گردد مقدار کیچا سمت سرور ذخیره شده و بررسی صحت عبارت وارد شده توسط کاربر با مقدار در نظر گرفته شده برای وی در سمت سرور انجام پذیرد نه در هدر ارسالی.

## ۳-۲ استفاده از شناسه یکتا کاربر (سشن) با ساختار ساده

- درجه و نوع خطر: متوسط
- مؤلفه آسیب‌پذیر: ساز و کار احراز هویت کاربران
- توضیحات تکمیلی:

همانطور که در تصویر زیر نیز مشاهده می‌شود، بررسی‌ها حاکی از آن است که شناسه در نظر گرفته شده برای هر کاربر، ساختار ساده‌ای داشته و استفاده از این ساختار ساده ممکن است وبسایت مربوطه را با مشکلات متعددی مواجه سازد.

```
GET /CAPTCHA/JpegImage.aspx?SessionName=eforcacp759934&newImage=true&rd=190149 HTTP/1.1
Host: www.skums.ac.ir
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://www.skums.ac.ir/ViewAdvZForm.aspx?code=551&lang=1&web=0&tempname=main&cap=759934
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=qf4a1m1x2mrqlpc4sbbkx0; eforcacp759934=Value=190097
```

شکل ۴ ساختار در نظر گرفته شده به عنوان سشن یکتای کاربر

- راه‌حل:
- در نظر گرفتن ساختار مناسب به عنوان شناسه یکتای کاربر

## ۳-۳ عدم مدیریت صحیح خطاها

- درجه و نوع خطر: متوسط – امکان افشای اطلاعات حساس در پیغام‌های خطا
- مؤلفه آسیب‌پذیر: مدیریت خطاها و پیکربندی برنامه کاربردی تحت وب
- توضیحات تکمیلی:

بررسی‌های صورت گرفته حاکی از آن است که وارد کردن مقادیر غیر استاندارد در فرم ورود، منجر به ایجاد خطا سمت سرور و افشای مسیر و توابع برنامه می‌شود. در تصویر زیر نمونه‌ای از این خطاها مشاهده می‌گردد:



**Server Error in '/' Application.**

*Object reference not set to an instance of an object.*

**Description:** An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

**Exception Details:** System.NullReferenceException: Object reference not set to an instance of an object.

**Source Error:**

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

**Stack Trace:**

```
[NullReferenceException: Object reference not set to an instance of an object.]
Dorsc.Library.UrlRewriter.UrlRewrite_BeingRequest(Object sender, EventArgs args) in D:\Branches\15482\CMS\Library\UrlRewriter.cs:414
System.Web.SyncEventExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +141
System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +48
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +71
```

**Version Information:** Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3535.0

شکل ۵ خطای سرور

در این میان به نظر می‌رسد پارامتر hdnparam نیازمند توجه بیشتری است؛ همانطور که در تصویر زیر نیز مشاهده می‌گردد، دستکاری این مقدار، ممکن است منجر به عدم مدیریت صحیح کد امنیتی گردد.

```
POST /Index.aspx/LoginUser HTTP/1.1
Host: www.skums.ac.ir
Connection: close
Content-Length: 184
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105
Content-Type: application/json; charset=UTF-8
Origin: https://www.skums.ac.ir
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.skums.ac.ir/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=qf4aiamixxs1rqlpc4ebbkx0

{
  CodeNumberTextBox: '0',
  txusername: 'a7',
  txpass: 'ZF8mW4MaXtLLD8Y02iQ==',
  lbllockmsg: 'undefined',
  SubId: '0',
  langid: '1',
  Tempname: 'Main',
  hdnparam: '0_651_0_651_False'
}
```

شکل ۶ درخواست ارسالی



```
{
  "Message": "Invalid object passed in, \u0027:\u0027 or \u0027)\u0027 expected. (40): { CodeNumberTextBox: \u0027\\u0027, txusername: \u0027a\u0027, txpass: \u0027ZF8mW4MaXtLLD8Y02iQ==\u0027, lbllockmsg: \u0027undefined\u0027, SubId : \u00270\u0027, langid : \u00271\u0027, Tempname : \u0027Main\u0027, hdnparam : \u00270_651_0_651_False\u0027 }",
  "StackTrace": " at System.Web.Script.Serialization.JavaScriptObjectDeserializer.DeserializeDictionary(Int32 depth)\r\n at System.Web.Script.Serialization.JavaScriptObjectDeserializer.DeserializeInternal(Int32 depth)\r\n at System.Web.Script.Serialization.JavaScriptObjectDeserializer.BasicDeserialize(String input, Int32 depthLimit, JavaScriptSerializer serializer)\r\n at System.Web.Script.Serialization.JavaScriptSerializer.Deserialize(JavaScriptSerializer serializer, String input, Type type, Int32 depthLimit)\r\n at System.Web.Script.Serialization.JavaScriptSerializer.Deserialize[T](String input)\r\n at System.Web.Script.Services.RestHandler.GetRawParamsFromPostRequest(HttpContext context, JavaScriptSerializer serializer)\r\n at System.Web.Script.Services.RestHandler.GetRawParams(WebServiceMethodData methodData, HttpContext context)\r\n at System.Web.Script.Services.RestHandler.ExecuteWebServiceCall(HttpContext context, WebServiceMethodData methodData)",
  "ExceptionType": "System.ArgumentException"
}
```

شکل ۷ عدم مدیریت صحیح کد امنیتی

## ● راه‌حل:

توجه و دقت در پروسه توسعه و آپدیت سامانه، انجام تست‌ها و ارزیابی‌های دوره‌ای در سامانه به منظور شناسایی خطاها و اشکال در پیکربندی‌های مربوطه، مدیریت خطاها و غیرفعال‌سازی قابلیت نمایش خطا در برنامه کاربردی و سرویس‌دهنده وب.

## ۳-۴ ذکر مسیرهای غیرضروری در فایل robots.txt

- درجه و نوع خطر: متوسط
- مؤلفه آسیب‌پذیر: مسیرهای وبسایت
- توضیحات تکمیلی:

بررسی فایل robots.txt این وبسایت از طریق آدرس زیر:

<https://www.skums.ac.ir/robots.txt>

نشانه‌گر وجود مسیرهایی است که ذکر آن‌ها در فایل robots.txt ضرورتی نداشته و تنها منجر به افشای مسیرهای این وبسایت می‌گردد.

```
User-agent: *
http://www.skums.ac.ir/ShowPage.aspx?page_news&lang=1&tempname=Main&sub=0&isPopUp=false&PageID=10172&PageIDF=357
http://www.skums.ac.ir/ShowPage.aspx?page_news&lang=1&tempname=Main&sub=0&isPopUp=false&PageID=10183&PageIDF=357
Disallow: /attachfile
Disallow: /SDK
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_form&order=show&lang=1&sub=308&PageId=993&codeV=1&tempname=DparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_form&order=show&lang=1&sub=308&PageId=991&codeV=1&tempname=DparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_form&order=show&lang=1&sub=308&PageId=994&codeV=1&tempname=DparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_form&order=show&lang=1&sub=308&PageId=996&codeV=1&tempname=DparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_form&order=show&lang=1&sub=308&PageId=998&codeV=1&tempname=DparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_form&order=show&lang=1&sub=308&PageId=989&codeV=1&tempname=DparastariBroujen
Disallow: /attachfile
Disallow: /SDK
Disallow: /attachfile
Disallow: /SDK
```

شکل ۸ محتوای فایل robots.txt

## ● راه‌حل:

از ذکر مسیرهای غیر ضروری، اضافی، حاوی اطلاعات حساس در فایل robots.txt خودداری گردد.