Bộ môn An toàn Thông tin – Khoa MMT&TT

Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: Lập trình ứng dụng web

Kỳ báo cáo: Buổi 06 (Session 6)

Tên chủ đề: CTF

GV: Nguyễn Bùi Kim Ngân

Ngày báo cáo: 28/05/2025

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT208.P22.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Hữu Hoàng Huy	21522154	21522154@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Task 01	100%
2	Task 02	100%
3	Task 03	100%
4	Task 04	0%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Challenge 1

a. *Thông tin chung.*

Tên challenge: Admin has the power

Độ khó: Dễ

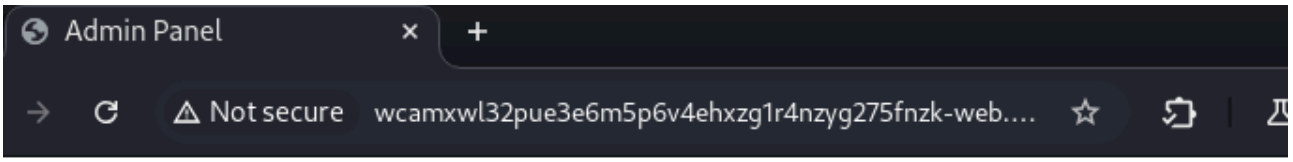
b. *Phân tích ban đầu.*

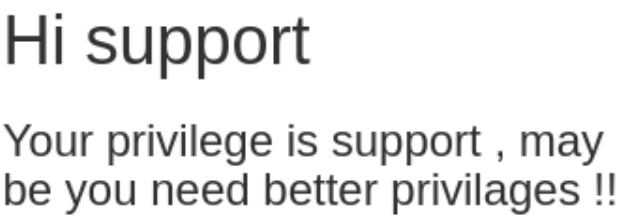
Sử dụng Burp Suite để tiến hành phân tích trang web.

Quan sát được thông tin sau:

```
    src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"
    /script>
    <![endif]-->
    <!-- TODO: remove this line ,  for maintenance purpose us
    this info (user:support password:x34245323)-->
  </head>
  <body>
```

Tiến hành đăng nhập thử:





Đăng nhập thành công nhưng ta muốn muốn chiếm quyền admin thay vì support.

c. Quá trình khai thác.

Sau khi đăng nhập thành công với user là “support”:

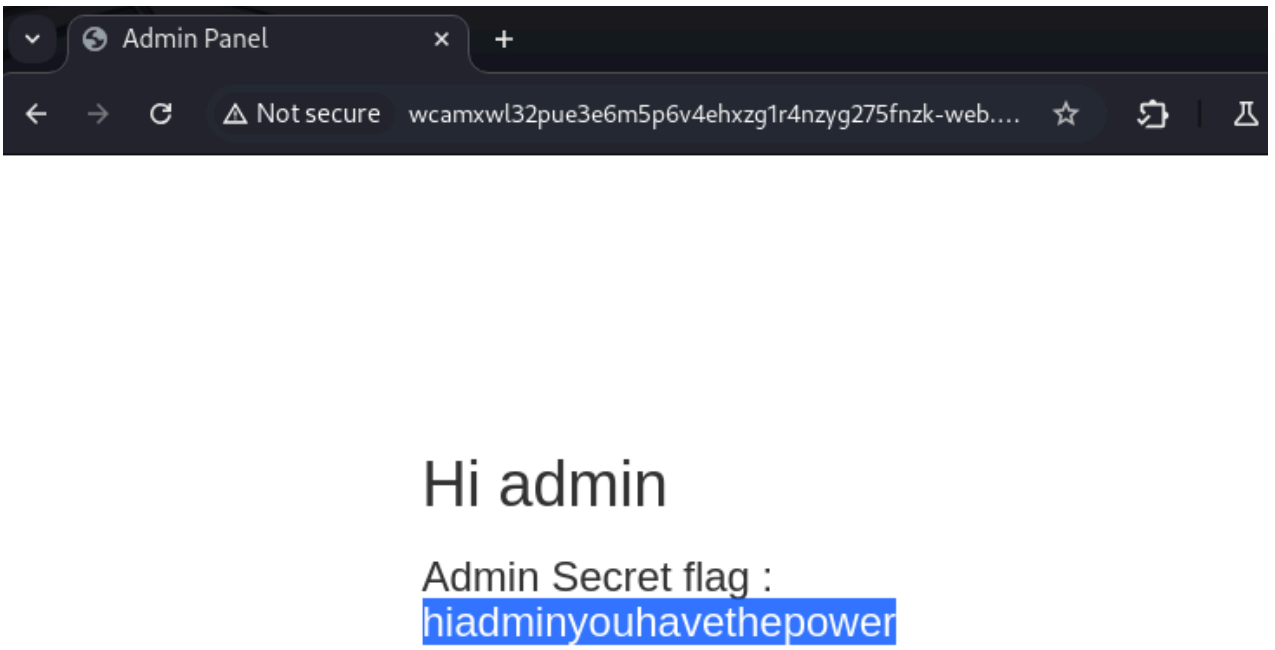
Request

Pretty Raw Hex

```
1  POST / HTTP/1.1
2  Host: wcamxwl32pue3e6m5p6v4ehxzg1r4nzyg275fnzk-web.cybertalentslabs.com
3  Content-Length: 35
4  Cache-Control: max-age=0
5  Accept-Language: en-US,en;q=0.9
6  Origin: http://wcamxwl32pue3e6m5p6v4ehxzg1r4nzyg275fnzk-web.cybertalentslabs.com
7  Content-Type: application/x-www-form-urlencoded
8  Upgrade-Insecure-Requests: 1
9  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/133.0.0.0 Safari/537.36
10 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
   png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://wcamxwl32pue3e6m5p6v4ehxzg1r4nzyg275fnzk-web.cybertalentslabs.com/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: role=support; PHPSESSID=hhu2os3te8s0nfi5m9dknrrh0c
14 Connection: keep-alive
15
16 username=support&password=x34245323
```

Ta thấy ở phần cookie có role, và PHPSESSIONID. Lợi dụng điều này ta thay đổi role của request thành “admin” nhưng sử dụng cùng một PHPSESSTIONID khi ta đăng nhập thành công ở role “support”.

Kết quả ta sẽ chiếm được quyền admin.



d. Mức độ ảnh hưởng.

Đây là lỗ hổng Broken Access Control. Đây là lỗ hổng bảo mật cực kỳ nghiêm trọng khi, lỗ hổng này đã leo lên top 1 OWASP.

Lỗ hổng này cho phép người dùng truy cập tài nguyên không hợp lệ mà không kiểm tra quyền truy cập của người đó.

e. Cách khắc phục.

- Không nên lưu role trong cookie, hãy lưu role trong session trên server.
- Bên phía server cần phải có code để kiểm tra role tại mọi nơi phân quyền.

2. Challenge 2

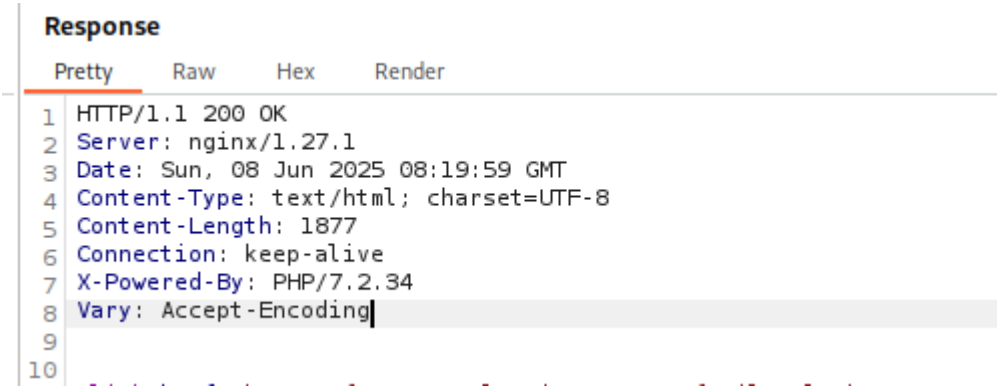
a. Thông tin chung.

Tên challenge: This is Sparta

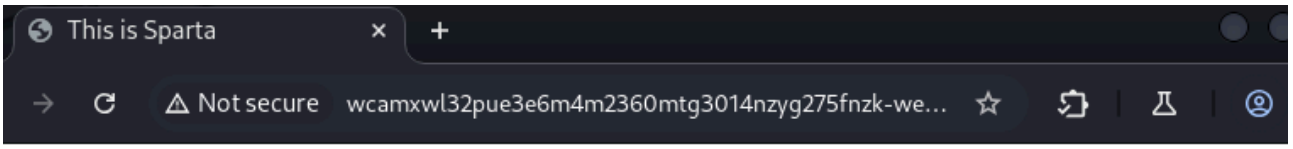
Mức độ: Easy.

b. Phân tích ban đầu.

Sử dụng Burp Suite để phân tích request/respone.



Server này sử web server là NginX version 1.27.1, backend là PHP version 7.2.34.

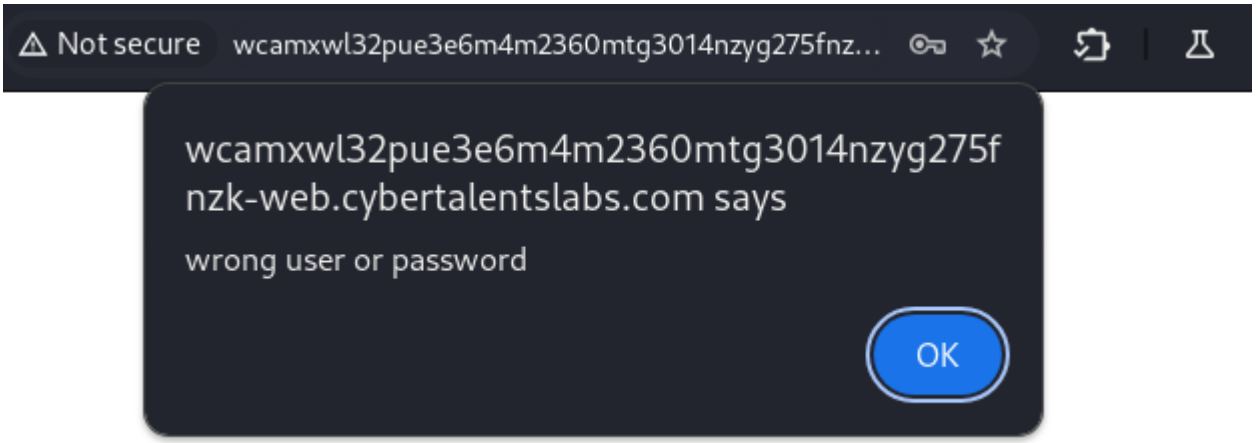


c. *Quá trình khai thác.*

Có đoạn javascript ở phần response

```
<script>
  var _0xae5b=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72",
  "\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64",
  "\x70\x61\x73\x73","\x43\x79\x62\x65\x72\x2d\x54\x61\x6c\x65\x6e\x74",
  "\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
  x20\x20\x20\x20\x43\x6F\x6E\x67\x72\x61\x74\x7A\x20\x0A\x0A",
  "\x77\x72\x6F\x6E\x67\x20\x50\x61\x73\x73\x77\x6F\x72\x64"];
  function check(){
    var _0xeb80x2=document[_0xae5b[2]](_0xae5b[1])[_0xae5b[0]];
    var _0xeb80x3=document[_0xae5b[2]](_0xae5b[3])[_0xae5b[0]];
    if(_0xeb80x2==_0xae5b[4]&&_0xeb80x3==_0xae5b[4]){
      alert(_0xae5b[5]);
    }
     else {
      alert(_0xae5b[6]);
    }
  }
</script>
```

Tiến hành đăng nhập thử.



Vậy khi ta đang nhập thì trang web sẽ gọi hàm check(). Nếu nhập sai username hoặc password sẽ gọi alert()

Giải mã mảng *_0xae5b* bằng CyberChef ta được mảng như sau:

```
2
3 var _0xae5b=["value", "user", "getElementById", "pass", "Cyber-Talent", "                    Congratz ",  "wrong Password"]
```

Trong hàm check() có 2 biến là *_0xeb80x2* và *_0xeb80x3* có giá trị là các phần tử của mảng *_0xae5b* tiến hành giải mã bằng CyberChef:

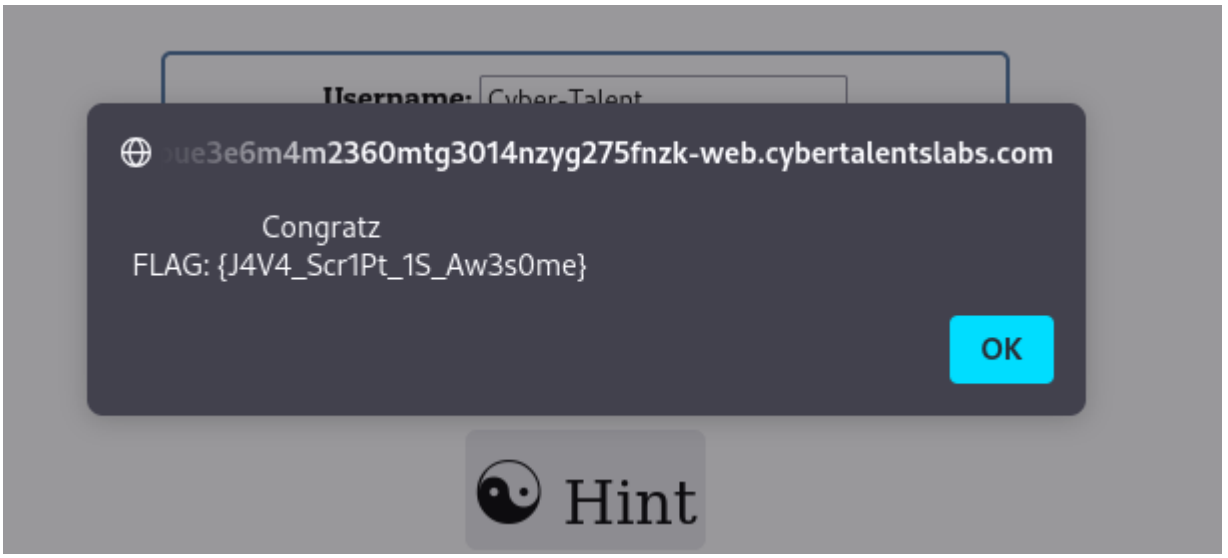
```
5 var _0×eb80×2=document[_0×ae5b[2]](_0×ae5b[1])[_0×ae5b[0]];
6
7 var _0×eb80×2 = document[getElementById](user)[value];
8 ⟹ var _0×eb80×2 = document.getElementById("user").value
9
10 var _0×eb80×3=document[_0×ae5b[2]](_0×ae5b[3])[_0×ae5b[0]];
11
12 var _0×eb80×3 = document[getElementById](pass)[value];
13 ⟹ var _0×eb80×3 = document.getElementById("pass").value
```

Vậy 2 biến *_0xeb80x2* và *_0xeb80x3* là 2 biến chứa username và password mà người dùng nhập vào.

Tiếp tục phân tích code If-else như sau:

```
15 if(_0×eb80×2=="Cyber-Talent" && _0×eb80×3=="Cyber-Talent"){
16         alert("                    Congratz ");
17 }
18 else {
19         alert(wrong Password);
20 }
```

Vậy từ code if-else trên t có thể suy ra username và password là Cyber-Talent.



d. *Mức độ ảnh hưởng.*

Đây là lỗ hổng vô cùng nghiêm trọng nó có thể dẫn đến **bỏ qua hoàn toàn cơ chế đăng nhập**, lộ **thông tin nhạy cảm** và chiếm đoạt quyền truy cập.

Kẻ tấn công có thể:

- Xem **tên đăng nhập và mật khẩu hardcoded** ngay trong mã JavaScript.
- Bỏ qua **xác thực server**, nếu nó **chỉ dựa vào logic phía client**.
- Giả mạo bất kỳ người dùng nào (thường là admin) nếu hệ thống dùng cookie/flag đơn giản.
- Khai thác thêm nếu đoạn mã này bảo vệ các tính năng admin, upload file,...

e. Cách khắc phục.

- Xác thực phải được thực hiện trên server
- Không để lộ thông tin nhạy cảm trong client.
- Ẩn logic quan trọng khỏi client

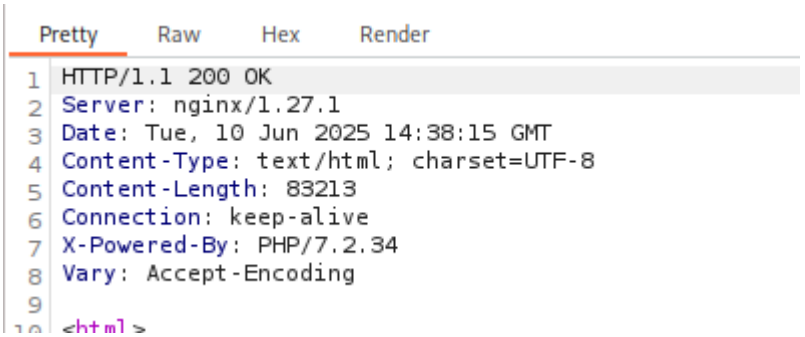
3. Challenge 3

a. Thông tin chung.

Tên challenge: Iam Legend

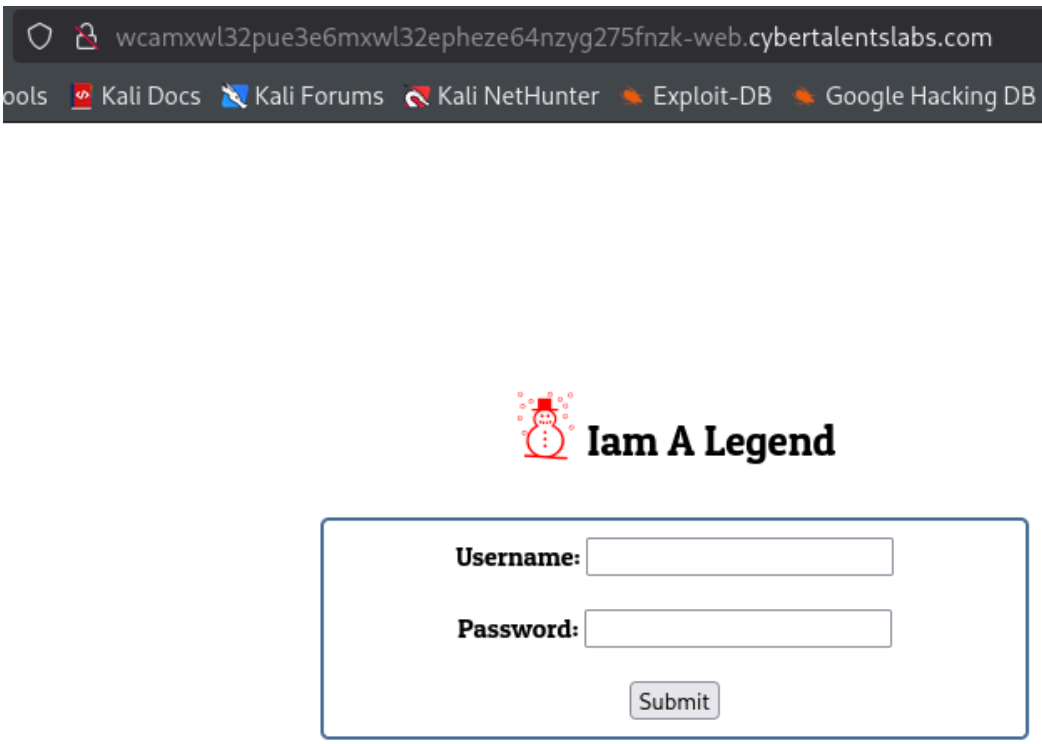
Mức độ: Easy.

b. Phân tích ban đầu.

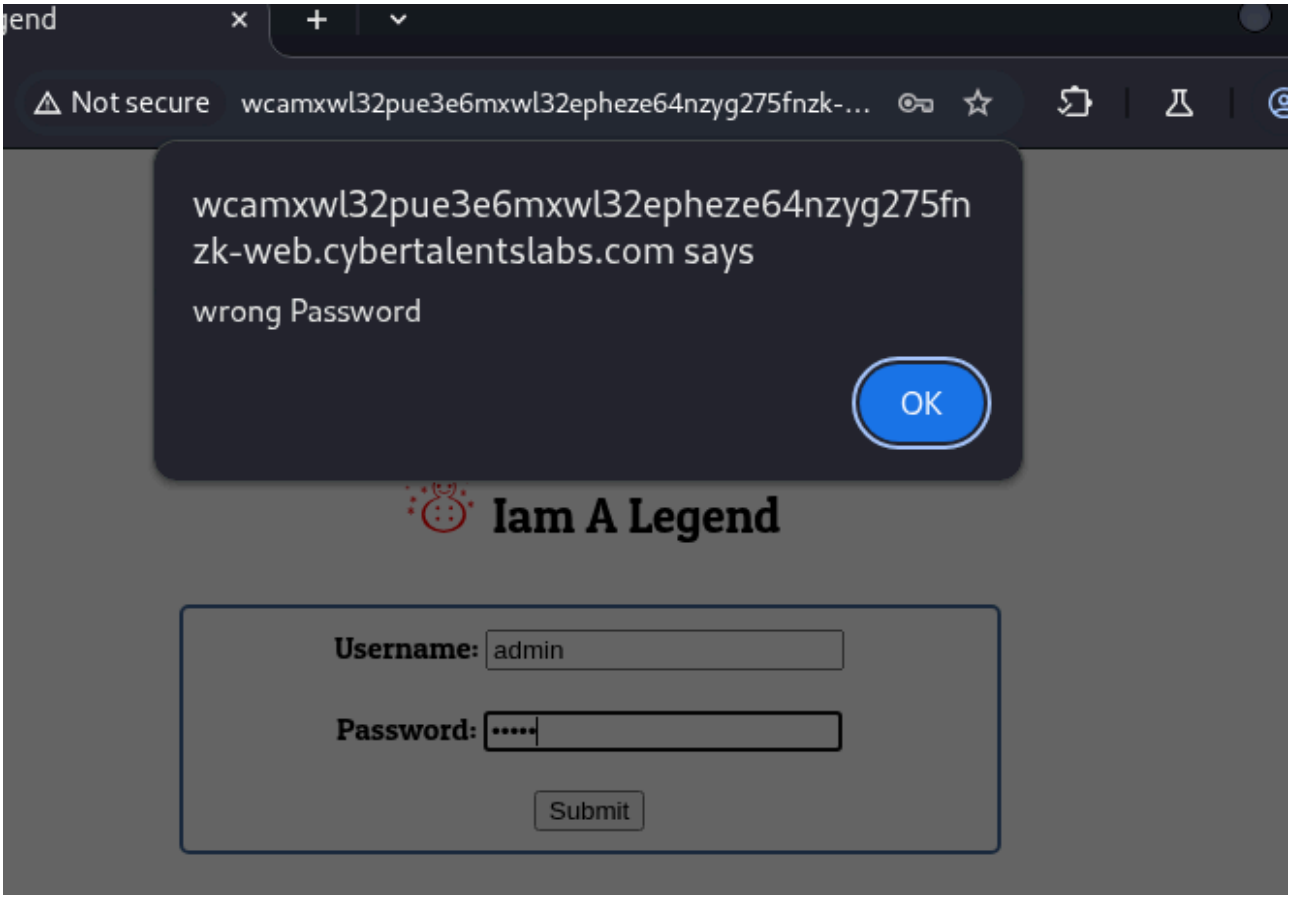


Sử dụng Burp Suite để phân tích request/response, ta thấy trang web này sử web server là NginX version 1.27.1, backend là PHP version 7.2.34

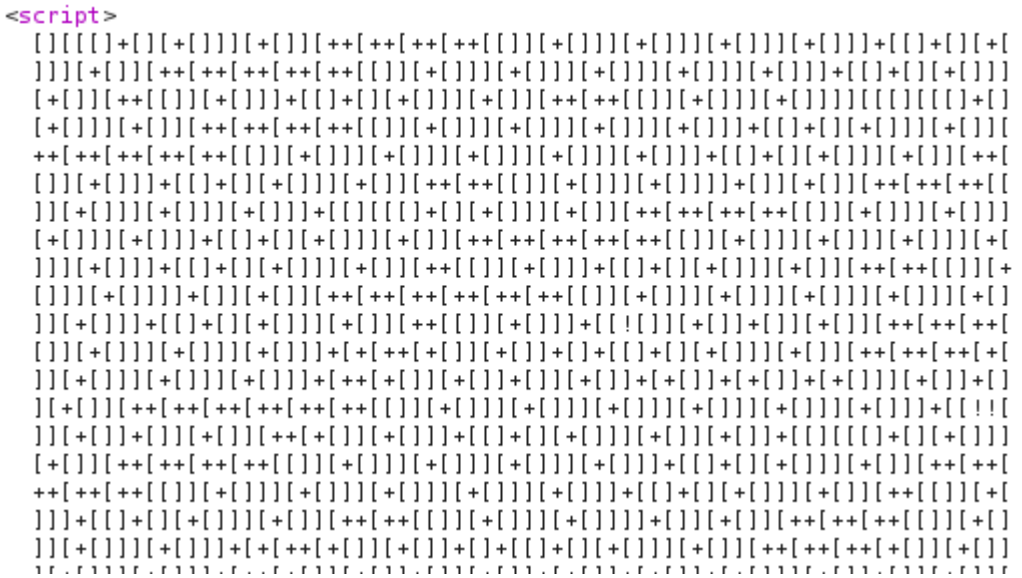
Giao diện login của trang web:



Thử nhập username/password là admin/admin



Tiếp tục quan sát, có một đoạn mã lạ ở tag <script> của response



Đây là một loại làm rối mã của Javascript gọi là JSFuck.

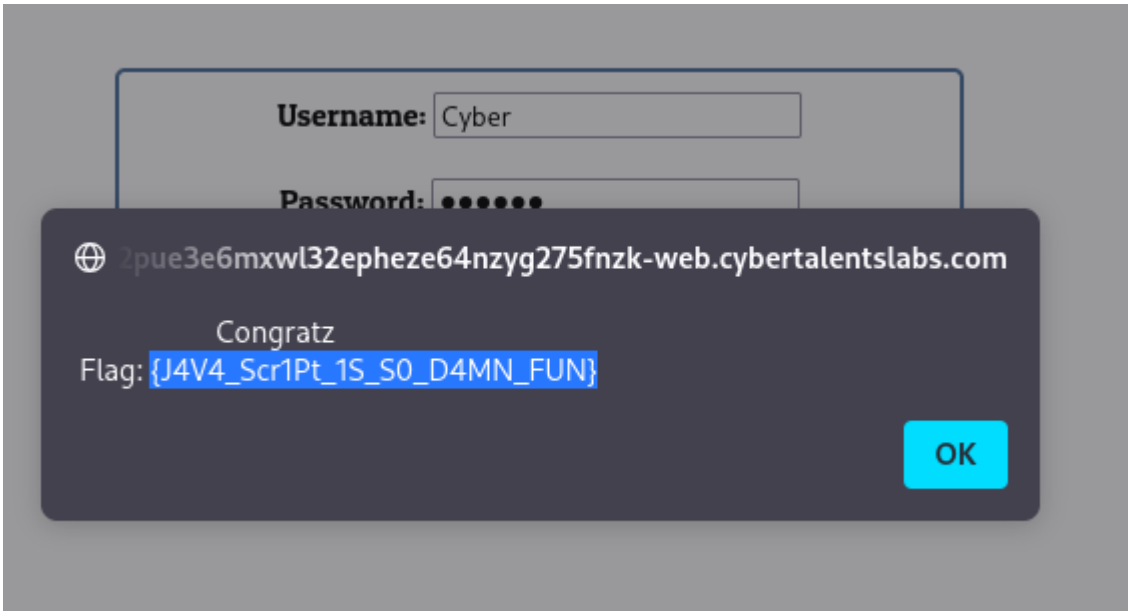
JSFuck là một kỹ thuật mã hóa code JavaScript hoàn toàn chỉ sử dụng các ký tự:

- ()
- []
- +
- !

c. *Quá trình khai thác.*

Sử dụng tool de4js để deobfuscate đoạn mã trên. Khi giải mã sẽ có một đoạn code If (user == Cyber && pass == Talent)

Vậy có thể kết luận là username/password là Cyber/Talent



d. Mức độ ảnh hưởng.

Tương tự challenge 2. Dù được code đã được làm rối nhưng vẫn lưu trên client nên hoàn có thể bị giải mã.

e. Cách khắc phục.

Tương tự challenge 2.

4. Challenge 4

a. Thông tin chung.

Tên challenge: Cool Name Effect

Mức độ: Easy.

b. Phân tích ban đầu.

Giao diện của trang web.

Sử dụng Burp Suit để phân tích Request và Response. Ở phần response, trong phần tag <script> khá đáng ngờ

```
(
'6($,12){$.1b.N=6(25,5){7 T={\'1L\':1W.2b,\'1K\':1W.2a};d 4.p(6(){7 $4=$(4);
7 1T=25||1;b(5){$.1H(T,5)}7 1m=6(){$4.W(\'2c-2d\',n.2f(n.29($4.2e()/(1T*10),2
2(T.1K)),22(T.1L)))};1m();$(X).1u(1m)})};6 Y(t,23,1Q,1P){7 a=t.2A().2u(23),1g
=\'\',S;b(a.2t){$(a).p(6(i,V){S=\'\';b(V===\' \'){S=\' 1O\';V=\'&2s;\'}1g+=\'
<1k 2h="\'+1Q+(i+1)+S+\'">\'+V+\'</1k>\'+1P});t.1O().2y(1g)}}7 O={1n:6(){d 4.
p(6(){Y($(4),\'\',\'2x\',\'\')})},2r:6(){d 4.p(6(){Y($(4),\' \',\'2q\',\' \')
})},2k:6(){d 4.p(6(){7 r="2j";Y($(4).2i("2l").2p(r).2n(),r,\'2v\',\'\')})}};$
.1b.1h=6(q){b(q&&O[q]){d O[q].1j(4,[].1d.K(1e,1))}1R b(q===\'F\'||!q){d O.1n.
1j(4,[].1d.K(1e,0))}$.1Y(\'2o \'+q+\' 2m 2z 2w 18 1f.1h\');d 4};$.L=6(5,1x){4
.$E=$(1x);4.1y(5)};$.L.1E={9:0,C:1,D:R,N:J};$.L.21={1y:6(5){4.5=$.1H(R,{},$.L
.1E,5);4.1w();4.$E.k(\'c\',R);4.Z();4.P();4.1q()},1w:6(){4.$E.1h();b(4.5.N)4.
$E.N();4.$F=4.$E.26(\'1k\').W(\'27\',\'28-2g\')},Z:6(){b(4.5.9===-1)d J;4.1B(
);4.1p()},1B:6(){4.B=0;7 8=4;4.$F.p(6(i){7 $e=$(4),14=$e.1o(R);8.B+=14;$e.k(\
'1l\',8.B-14/2)});7 1c=4.B/2;b(4.5.9<1c)4.5.9=1c;4.1X=4.B;7 M=2*n.1I(4.1X/(2*
4.5.9));4.1t=4.5.9*M},1p:6(){7 8=4,G=0;4.$F.p(6(i){7 $e=$(4),1v=($e.1o(R)/8.B
)*8.1t,19=1v/8.5.9,h=8.5.9*(n.1F(19/2)),1s=n.2F((8.B/2-G)/8.5.9),17=1s+19/2,x
=n.1F(17)*h,y=n.38(17)*h,15=G+n.34(8.B/2-x-G),1r=0|15-$e.k(\'1l\'),1i=0|8.5.9
-y,M=(8.5.D)?0|-n.1I(x/8.5.9)*(2Z/n.32):0;G=2*15-G;$e.k({x:1r,y:(8.5.C===1)?1
i:-1i,a:(8.5.C===1)?M:-M})})},P:6(Q){b(!4.$E.k(\'c\'))d J;7 8=4;4.$F.p(6(i){7
 $e=$(4),H=(8.5.9===-1)?\'1A\':\'2X(\'+$e.k(\'x\')+\'1G) 2Y(\'+$e.k(\'y\')+\'
```

```
1G) D(\'+$e.k(\'a\')+\'37)\',m=(Q)?\'2B \'+(Q.39||0)+\'13 \'+(Q.3d||\'3b\'):\
'1A\';$e.W({\'-1C-m\':m,\'-1D-m\':m,\'-o-m\':m,\'-13-m\':m,\'m\':m}).W({\'-1C
-I\':H,\'-1D-I\':H,\'-o-I\':H,\'-13-I\':H,\'I\':H})})},1q:6(){b(4.5.N){7 8=4;
$(X).18(\'1u.c\',6(){8.Z();8.P()})}},1z:6(v){b(!v.9&&!v.C&&v.D===\'12\'){d J}
4.5.9=v.9||4.5.9;4.5.C=v.C||4.5.C;b(v.D!==12){4.5.D=v.D}4.Z();4.P(v.Q)},3a:6(
){4.5.9=-1;4.P();4.$F.20(\'x y a 1l\');4.$E.20(\'c\');$(X).2V(\'.c\')}};7 16=
6(1J){b(4.1Z){1Z.1Y(1J)}};$.1b.c=6(5){b(2I 5===\'2J\'){7 1S=2K.21.1d.K(1e,1);
4.p(6(){7 A=$.k(4,\'c\');b(!A){16("2H K O 18 c 2G 11 2C; "+"2D 11 K q \'"+5+"
\'");d}b(!$.2E(A[5])||5.2W(0)==="2L"){16("2M 2S q \'"+5+"\' 2T c A");d}A[5].1
j(A,1S)})}1R{4.p(6(){7 A=$.k(4,\'c\');b(!A){$.k(4,\'c\',2Q $.L(5,4))}})}d 4}}
)(1f);(6(j,w){7 24=1U;7 U=6(){7 z=[\'y\',\'o\',\'u\',\'r\',\' \',\'f\',\'l\',
\'a\',\'g\',\' \',\'i\',\'s\',\':\'];7 f=([]["2N"]+"")[3];f+=([J]+12)[10];f+=
(1N+[1V])[10];f+=(1N+[1V])[10];f+=(+(20))["11"+1M["1a"]](31)[1];f+=([]["2P"](
)+"")[3];f+=(+(35))["11"+1M["1a"]](36);24(z.2R(\'\')+f)};w.1U=U;w.2U=U;w.33=U
;j(6(){$x=j(\'#1a\');$x.c({9:3c});$x.c(\'1z\',{9:30,C:1})})})(1f,X);',62,200,
'||||this|options|function|var|_self|radius||if|arctext|return|letter||||||da
ta||transition|Math||each|method|||||opts|||||instance|dtWord|dir|rotate|el|l
etters|iteratorX|transformation|transform|false|call|Arctext|angle|fitText|me
thods|_rotateWord|animation|true|emptyclass|settings|newAlert|item|css|window
|injector|_calc||to|undefined|ms|letterWidth|xpos|logError|theta|on|beta|name
|fn|centerWord|slice|arguments|jQuery|inject|lettering|yval|apply|span|center
|resizer|init|outerWidth|_calcLetters|_loadEvents|xval|alpha|dtArc|resize|dtA
rcLetter|_applyLettering|element|_init|set|none|_calcBase|webkit|moz|defaults
|cos|px|extend|asin|message|maxFontSize|minFontSize|String|NaN|empty|after|kl
ass|else|args|compressor|alert|Infinity|Number|dtArcBase|error|console|remove

Data|prototype|parseFloat|splitter|legacyAlert|kompressor|find|display|inline
|min|POSITIVE_INFINITY|NEGATIVE_INFINITY|font|size|width|max|block|class|chil
dren|eefec303079ad17405c889e092e105b0|lines|br|does|end|Method|replaceWith|wo
rd|words|nbsp|length|split|line|exist|char|append|not|text|all|initialization
|attempted|isFunction|acos|prior|cannot|typeof|string|Array|_|no|fill|211|ent
ries|new|join|such|for|prompt|off|charAt|translateX|translateY|180|140||PI|co
nfirm|abs|||deg|sin|speed|destroy|linear|400|easing'.split('|'),0,{
}
));\n
\n
\n
\n
\n
\n
\n
</script>\n
```

Sau khi tìm hiểu, đây là đoạn mã đã bị làm rối bằng kỹ thật PACKER (do Dean Edwards phát triển). Trong tag <script> cũng có đoạn code để giải mã nó

```
eval(function(p,a,c,k,e,d){
  e=function(c){
    return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29)
    toString(36))
  };
  if(!''.replace(/^/,String)){
    while(c--){
      d[e(c)]=k[c]||e(c)
    }
    k=[function(e){
      return d[e]
    }
    ];
    e=function(){
      return'\\w+'
    };
    c=1
  };
  while(c--){
    if(k[c]){
      p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])
    }
  }
  return p
```

c. *Quá trình khai thác.*

Tiến hành copy toàn bộ code trong tag <script> vào một file .js và format code để dễ nhìn hơn. Ta sẽ được code như hình dưới.

```
eval(
    function (p, a, c, k, e, d) {
        e = function (c) {
            return (c < a ? '' : e(parseInt(c / a))) + ((c = c % a) > 35 ? String.fromCharCode(c + 29
        };
        if (!''.replace(/^/, String)) {
            while (c--) {
                d[e(c)] = k[c] || e(c)
            }
            k = [function (e) {
                return d[e]
            }];
            e = function () {
                return '\\w+'
            };
            c = 1
        };
        while (c--) {
            if (k[c]) {
                p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c])
            }
        }
        return p
    }
('(6($,12){$.1b.N=6(25,5){7 T={\'1L\':1W.2b,\'1K\':1W.2a};d 4.p(6(){7 $4=$(4);7 1T=25||1;b(5){$.1H(T,
);
```

Hàm eval() trong JS sẽ thực thi một chuỗi bên trong nó như thể nó là một code JS. Vì vậy ta có thể thực thi đoạn code trên để có thể giải mã.

Ta phải chỉnh sửa code một chút bằng cách thay dòng code “return p” thành “console.log(p)”. Đây là kết quả:

```
huynnh@Desktop:~$ node decode.js
(function($,undefined){$.fn.fitText=function(kompressor,options){var settings={'minFontSize':Number.NEGATIVE_I
axFontSize':Number.POSITIVE_INFINITY};return this.each(function(){var $this=$(this);var compressor=kompressor
ons){$.extend(settings,options)}var resizer=function(){$this.css('font-size',Math.max(Math.min($this.width()/(
*10),parseFloat(settings.maxFontSize)),parseFloat(settings.minFontSize)))};resizer();$(window).resize(resizer
on injector(t,splitter,klass,after){var a=t.text().split(splitter),inject='',emptyclass;if(a.length){$(a).each
i,item){emptyclass='';if(item===' '){emptyclass=' empty';item=' '}inject+='<span class="'+klass+(i+1)+emp
>'+item+'</span>'+after});t.empty().append(inject)}}var methods={init:function(){return this.each(function(){i
this),'','char','')})},words:function(){return this.each(function(){injector($(this),' ','word',' ')})},lines
{return this.each(function(){var r="eefec303079ad17405c889e092e105b0";injector($(this).children("br").replaceW
(),r,'line','')})}};$.fn.lettering=function(method){if(method&&methods[method]){return methods[method].apply(this,[].sli
ce.call(arguments,1))}else if(method==='letters'||!method){return methods.init.apply(this,[].slice.call(arguments,0))}$.
error('Method '+method+' does not exist on jQuery.lettering');return this};$.Arctext=function(options,element){this.$el=
$(element);this._init(options)};$.Arctext.defaults={radius:0,dir:1,rotate:true,fitText:false};$.Arctext.prototype={_init
:function(options){this.options=$.extend(true,{},$.Arctext.defaults,options);this._applyLettering();this.$el.data('arcte
xt',true);this._calc();this._rotateWord();this._loadEvents()},_applyLettering:function(){this.$el.lettering();if(this.op
tions.fitText)this.$el.fitText();this.$letters=this.$el.find('span').css('display','inline-block')},_calc:function(){if(
this.options.radius===-1)return false;this._calcBase();this._calcLetters()},_calcBase:function(){this.dtWord=0;var _self
=this;this.$letters.each(function(i){var $letter=$(this),letterWidth=$letter.outerWidth(true);_self.dtWord+=letterWidth;
$letter.data('center',_self.dtWord-letterWidth/2)});var centerWord=this.dtWord/2;if(this.options.radius<centerWord)this.
options.radius=centerWord;this.dtArcBase=this.dtWord;var angle=2*Math.asin(this.dtArcBase/(2*this.options.radius));this.
dtArc=this.options.radius*angle},_calcLetters:function(){var _self=this,iteratorX=0;this.$letters.each(function(i){var $
```

```
letter=$(this),dtArcLetter=($letter.outerWidth(true)/_self.dtWord)*_self.dtArc,beta=dtArcLetter/_self.options.radius,h=_
self.options.radius*(Math.cos(beta/2)),alpha=Math.acos((_self.dtWord/2-iteratorX)/_self.options.radius),theta=alpha+beta
/2,x=Math.cos(theta)*h,y=Math.sin(theta)*h,xpos=iteratorX+Math.abs(_self.dtWord/2-x-iteratorX),xval=0|xpos-$letter.data(
'center'),yval=0|_self.options.radius-y,angle=(_self.options.rotate)?0|-Math.asin(x/_self.options.radius)*(180/Math.PI):
0;iteratorX=2*xpos-iteratorX;$letter.data({x:xval,y:(_self.options.dir===1)?yval:-yval,a:(_self.options.dir===1)?angle:-
angle})})},_rotateWord:function(animation){if(!this.$el.data('arctext'))return false;var _self=this;this.$letters.each(f
unction(i){var $letter=$(this),transformation=(_self.options.radius===-1)?'none':'translateX('+$letter.data('x')+'px) tr
anslateY('+$letter.data('y')+'px) rotate('+$letter.data('a')+'deg)',transition=(animation)?'all '+(animation.speed||0)+'
ms '+(animation.easing||'linear'):'none';$letter.css({'-webkit-transition':transition,'-moz-transition':transition,'-o-t
ransition':transition,'-ms-transition':transition,'transition':transition}).css({'-webkit-transform':transformation,'-mo
z-transform':transformation,'-o-transform':transformation,'-ms-transform':transformation,'transform':transformation})})}
,_loadEvents:function(){if(this.options.fitText){var _self=this;$(window).on('resize.arctext',function(){_self._calc();_
self._rotateWord()})}},set:function(opts){if(!opts.radius&&!opts.dir&&opts.rotate==='undefined'){return false}this.optio
ns.radius=opts.radius||this.options.radius;this.options.dir=opts.dir||this.options.dir;if(opts.rotate!==undefined){this.
options.rotate=opts.rotate}this._calc();this._rotateWord(opts.animation)},destroy:function(){this.options.radius=-1;this
._rotateWord();this.$letters.removeData('x y a center');this.$el.removeData('arctext');$(window).off('.arctext')}};var l
ogError=function(message){if(this.console){console.error(message)}};$.fn.arctext=function(options){if(typeof options==='
string'){var args=Array.prototype.slice.call(arguments,1);this.each(function(){var instance=$.data(this,'arctext');if(!i
nstance){logError("cannot call methods on arctext prior to initialization; "+"attempted to call method '"+options+"'");r
eturn}if(!$.isFunction(instance[options])||options.charAt(0)==="_"){logError("no such method '"+options+"' for arctext i
nstance");return}instance[options].apply(instance,args)})}else{this.each(function(){var instance=$.data(this,'arctext');
if(!instance){$.data(this,'arctext',new $.Arctext(options,this))})}return this}})(jQuery);(function(j,w){var legacyAler
t=alert;var newAlert=function(){var z=['y','o','u','r',' ','f','l','a','g',' ','i','s',':'];var f=([]["fill"]+"")[3];f+=
([false]+undefined)[10];f+=(NaN+[Infinity])[10];f+=(NaN+[Infinity])[10];f+=(+(211))["to"+String["name"]](31)[1];f+=([]["
entries"]()+"")[3];f+=(+(35))["to"+String["name"]](36);legacyAlert(z.join('')+f)};w.alert=newAlert;w.prompt=newAlert;w.c
onfirm=newAlert;j(function(){$x=j('#name');$x.arctext({radius:400});$x.arctext('set',{radius:140,dir:1})})})(jQuery,wind
ow);
```

Copy output trên ra một file js khác vì đây là code JS gốc sau khi được giải mã.

Ta format code lại cho dễ nhìn.

Quan sát code sau khi được format, ta thấy một hàm có vẻ là chứa flag.

```
(function(j, w) {
    var legacyAlert = alert;
    var newAlert = function() {
        var z = ['y', 'o', 'u', 'r', ' ', 'f', 'l', 'a', 'g', ' ', 'i', 's',
        var f = ([]["fill"] + "")[3];
        f += ([false] + undefined)[10];
        f += (NaN + [Infinity])[10];
        f += (NaN + [Infinity])[10];
        f += (+(211))["to" + String["name"]](31)[1];
        f += ([]["entries"]() + "")[3];
        f += (+(35))["to" + String["name"]](36);
        legacyAlert(z.join('') + f)
    };
    w.alert = newAlert;
    w.prompt = newAlert;
    w.confirm = newAlert;
    j(function() {
        $x = j('#name');
        $x.arctext({
            radius: 400
        });
        $x.arctext('set', {
            radius: 140,
            dir: 1
        })
    })
})(jQuery, window);
```

Ta tiếp tục copy code này sang một file js khác, chỉnh sửa code để có thể chạy bằng NodeJS.

```
var legacyAlert = console.log;
var newAlert = function() {
        var z = ['y', 'o', 'u', 'r', ' ', 'f', 'l', 'a', 'g', ' ', 'i', 's', ':'];
        var f = ([]["fill"] + "")[3];
        f += ([false] + undefined)[10];
        f += (NaN + [Infinity])[10];
        f += (NaN + [Infinity])[10];
        f += (+(211))["to" + String["name"]](31)[1];
        f += ([]["entries"]() + "")[3];
        f += (+(35))["to" + String["name"]](36);
        // legacyAlert(z.join('') + f)
        legacyAlert(z.join('') + f)
};

newAlert();
```

Khi chạy code bằng NodeJS

```
huynnh@Desktop:~$ node test.js
your flag is:ciyypjz
huynnh@Desktop:~$
```

d. *Mức độ ảnh hưởng.*

Tương tự Challenge 2

e. *Cách khắc phục.*

Tương tự Challenge 2

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-LabX_NhomY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT208.P22.ANTT*]-Lab1_Nhom1.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT