acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

2 July, 2015

Developer Report

Generated by Acunetix WVS Reporter (v10.0 Build 20150623)

Scan of https://18f-ads.noblis.org

Scan details

Scan information	
Start time	7/2/2015 4:05:51 PM
Finish time	7/2/2015 4:14:01 PM
Scan time	8 minutes, 11 seconds
Profile	High_Risk_Alerts
Server information	
Responsive	True
Server banner	Apache/2.2.15 (CentOS)
Server OS	Unix

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	**10**
High	2
Medium	4
Low	2
Informational	2

Knowledge base

SSL server running [443]

A TLS1 server is running on TCP port 443.

-
SSL server information:
Ciphers suported:
- TLS1_CK_RSA_WITH_3DES_EDE_CBC_SHA(OpenSSL ciphername: DES-CBC3-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA(OpenSSL ciphername: EDH-RSA-DES-CBC3-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: AES128-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: DHE-RSA-AES128-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: AES256-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: DHE-RSA-AES256-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_CAMELLIA_128_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key

Exchange: RSA, Autentication: RSA, Symmetric encryption method: Camellia(128), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: Camellia(128), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_CAMELLIA_256_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: Camellia(256), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: Camellia(256), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength

- Certificate 1:

Issuer:
  Country Name: GB
  State Or Province Name: Greater Manchester
  Locality Name: Salford
  Organization Name: COMODO CA Limited
  Common Name: COMODO RSA Domain Validation Secure Server CA
Recipient:
  Organizational Unit Name: Domain Control Validated
  Organizational Unit Name: PositiveSSL
  Common Name: 18f-ads.noblis.org

Certificate version: 2
Serial number: 00b5c05c3628d624310c5389cb0960a5a2
Finger print: f06aac74d6b0ff72d13ebbb876dc1b36
Algorithm ID: 1.2.840.113549.1.1.11
Valability start: Tue Jun 23 20:00:00 EDT 2015
Valability end: Thu Jun 23 19:59:59 EDT 2016
Expire in: 357 days

- Certificate 2:

Issuer:
  Country Name: GB
  State Or Province Name: Greater Manchester
  Locality Name: Salford
  Organization Name: COMODO CA Limited
  Common Name: COMODO RSA Certification Authority
Recipient:
  Country Name: GB
  State Or Province Name: Greater Manchester
  Locality Name: Salford
  Organization Name: COMODO CA Limited
  Common Name: COMODO RSA Domain Validation Secure Server CA

Certificate version: 2
Serial number: 2b2e6eead975366c148a6edba37c8c07
Finger print: 84fe991e9bd86cb6df95aea01aa479ff
Algorithm ID: 1.2.840.113549.1.1.12
Valability start: Tue Feb 11 19:00:00 EST 2014
Valability end: Sun Feb 11 18:59:59 EST 2029

Expire in: 4973 days

- Certificate 3:

Issuer:
Country Name: SE
Organization Name: AddTrust AB
Organizational Unit Name: AddTrust External TTP Network
Common Name: AddTrust External CA Root
Recipient:
Country Name: GB
State Or Province Name: Greater Manchester
Locality Name: Salford
Organization Name: COMODO CA Limited
Common Name: COMODO RSA Certification Authority

Certificate version: 2
Serial number: 2766ee56eb49f38eabd770a2fc84de22
Finger print: 1e1d2ac882313267c9d93aeeb942c699
Algorithm ID: 1.2.840.113549.1.1.12
Valability start: Tue May 30 06:48:38 EDT 2000
Valability end: Sat May 30 06:48:38 EDT 2020
Expire in: 1793 days

Multiple web servers detected

List of web servers (and corresponding URLs) detected on this website:

- Apache/2.2.15 (CentOS) => /
- Apache-Coyote/1.1 => /myHealthAlerts

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- css => 10 file(s)
- js => 8 file(s)
- otf => 1 file(s)

List of client scripts

These files contain Javascript code referenced from the website.

- /myHealthAlerts/assets/application-53a84ac2c2e94b8b968c583144856503.js
- /myHealthAlerts/assets/registerAjax-7a569a23001c47d9e96b30b53aabb57b.js
- /myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/js/jquery-ui-1.10.4.custom.min.js
- /myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/jquery/jquery.jgrowl.js
- /myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/jquery/jquery.checkbox.js
- /myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/spring-security-ui.js
- /myHealthAlerts/plugins/jquery-1.11.1/js/jquery/jquery-1.11.1.min.js
- /myHealthAlerts/js/select2.js

List of files with inputs

These files have at least one input (GET or POST).

- / - 2 inputs
- /myHealthAlerts/j_spring_security_check - 2 inputs
- /myHealthAlerts/register/register - 2 inputs
- /myHealthAlerts/login/authfail - 1 inputs
- /myHealthAlerts/login/auth - 2 inputs

Alerts summary

XML external entity injection

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-611

Affected items	Variation
/myHealthAlerts/register/register	2

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-352

Affected items	Variation
/myHealthAlerts	2
/myHealthAlerts/login/auth (3a8eca3a176fe87a2f7602251adaed20)	1
/myHealthAlerts/register	1

Login page password-guessing attack

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-307

Affected items	Variation
/myHealthAlerts/j_spring_security_check	2

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/myHealthAlerts	2

Alert details

XML external entity injection

Severity	**High**
Type	Configuration
Reported by module	Scripting (XXE_File.script)

Description

XML supports a facility known as "external entities", which instruct an XML processor to retrieve and perform an inline include of XML located at a particular URI. An external XML entity can be used to append or modify the document type declaration (DTD) associated with an XML document. An external XML entity can also be used to include XML within the content of an XML document.

Now assume that the XML processor parses data originating from a source under attacker control. Most of the time the processor will not be validating, but it MAY include the replacement text thus initiating an unexpected file open operation, or HTTP transfer, or whatever system ids the XML processor knows how to access.

below is a sample XML document that will use this functionality to include the contents of a local file (/etc/passwd)

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE acunetix [
  <!ENTITY acunetixent SYSTEM "file:///etc/passwd">
]>
<xxx>&acunetixent;</xxx>
```

Impact

Attacks can include disclosing local files, which may contain sensitive data such as passwords or private user data, using file: schemes or relative paths in the system identifier. Since the attack occurs relative to the application processing the XML document, an attacker may use this trusted application to pivot to other internal systems, possibly disclosing other internal content via http(s) requests.

Recommendation

If possible it's recommended to disable parsing of XML external entities.

References

XML External Entity (XXE) Processing
XXE (Xml eXternal Entity) attack
CWE-611: Information Exposure Through XML External Entity Reference

Affected items

/myHealthAlerts/register/register

Details

POST data was set to <?xml version="1.0" encoding="utf-8"?> <!DOCTYPE dtdkyct [<!ENTITY dtdkyctent SYSTEM "http://hitWff2Czp33q.bxss.me/">]> <register>&dtdkyctent;</register>

An HTTP request was initiated for the domain hitWff2Czp33q.bxss.me which indicates that this script is vulnerable to XXE injection.

HTTP request details:
IP address: 65.216.138.173
User agent: Java/1.7.0_71

Request headers

```
POST /myHealthAlerts/register/register HTTP/1.1
Content-type: text/xml
Host: 18f-ads.noblis.org
Content-Length: 163
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

```
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE dtdkyct [
  <!ENTITY dtdkyctent SYSTEM "http://hitWff2Czp33q.bxss.me/">
]>
<register>&dtdkyctent;</register>
```

/myHealthAlerts/register/register

Details

POST data was set to <?xml version="1.0" encoding="utf-8"?> <!DOCTYPE dtqbspc [<!ENTITY dtqbspcent SYSTEM "http://hitO5trSCAOnn.bxss.me/">]> <register>&dtqbspcent;</register>

An HTTP request was initiated for the domain hitO5trSCAOnn.bxss.me which indicates that this script is vulnerable to XXE injection.

HTTP request details:
IP address: 65.216.138.173
User agent: Java/1.7.0_71

Request headers

```
POST /myHealthAlerts/register/register HTTP/1.1
Content-type: application/xml
Host: 18f-ads.noblis.org
Content-Length: 163
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE dtqbspc [
  <!ENTITY dtqbspcent SYSTEM "http://hitO5trSCAOnn.bxss.me/">
]>
<register>&dtqbspcent;</register>
```

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/myHealthAlerts

Details

Form name: registerForm
Form action: https://18f-ads.noblis.org/myHealthAlerts/register/register
Form method: POST

Form inputs:

- actionUrl [Hidden]
- username [Text]
- password [Password]
- password2 [Password]

Request headers

```
GET /myHealthAlerts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://18f-ads.noblis.org/myHealthAlerts/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*
```

/myHealthAlerts

Details

Form name: loginForm
Form action: https://18f-ads.noblis.org/myHealthAlerts/j_spring_security_check
Form method: POST

Form inputs:

- j_username [Text]
- j_password [Password]
- login [Submit]

Request headers

```
GET /myHealthAlerts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://18f-ads.noblis.org/myHealthAlerts/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*
```

/myHealthAlerts/login/auth (3a8eca3a176fe87a2f7602251adaed20)

Details

Form name: <empty>
Form action: https://18f-ads.noblis.org/myHealthAlerts/j_spring_security_check
Form method: POST

Form inputs:

- j_username [Text]
- j_password [Password]
- _spring_security_remember_me [Checkbox]

Request headers

```
GET /myHealthAlerts/login/auth?format=&login_error=1 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://18f-ads.noblis.org/myHealthAlerts/login/authfail?login_error=1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: JSESSIONID=8A7AD6E4904A3C3803EDCCA334191915
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*
```

/myHealthAlerts/register

Details

Form name: registerForm
Form action: https://18f-ads.noblis.org/myHealthAlerts/register/register
Form method: POST

Form inputs:

- actionUrl [Hidden]
- username [Text]
- password [Password]
- password2 [Password]

Request headers

```
GET /myHealthAlerts/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*
```

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected items

/myHealthAlerts/j_spring_security_check

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /myHealthAlerts/j_spring_security_check HTTP/1.1
Content-Length: 39
Content-Type: application/x-www-form-urlencoded
Referer: https://18f-ads.noblis.org
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*

j_password=SWtZTtfX&j_username=YBQV2xh2
```

/myHealthAlerts/j_spring_security_check

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /myHealthAlerts/j_spring_security_check HTTP/1.1
Content-Length: 51
Content-Type: application/x-www-form-urlencoded
Referer: https://18f-ads.noblis.org
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

```
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*

login=LOGIN&j_password=6cmgZboH&j_username=fJ1oRqdd
```

Password type input with auto-complete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/myHealthAlerts

Details

Password type input named password from form named registerForm with action /myHealthAlerts/register/register has autocomplete enabled.

Request headers

```
GET /myHealthAlerts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://18f-ads.noblis.org/myHealthAlerts/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*
```

/myHealthAlerts

Details

Password type input named password2 from form named registerForm with action /myHealthAlerts/register/register has autocomplete enabled.

Request headers

```
GET /myHealthAlerts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://18f-ads.noblis.org/myHealthAlerts/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 18f-ads.noblis.org
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

```
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*
```

Scanned items (coverage report)

Scanned 43 URLs. Found 4 vulnerable.

URL: https://18f-ads.noblis.org/

No vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
/	Path Fragment
/myHealthAlerts/	Path Fragment

Input scheme 2	
Input name	Input type
Host	HTTP Header

URL: https://18f-ads.noblis.org/myHealthAlerts/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/j_spring_security_check

Vulnerabilities have been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded POST
j_password	URL encoded POST
j_username	URL encoded POST

Input scheme 2	
Input name	Input type
_spring_security_remember_me	URL encoded POST
j_password	URL encoded POST
j_username	URL encoded POST

URL: https://18f-ads.noblis.org/myHealthAlerts/register

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/register/register

Vulnerabilities have been identified for this URL

7 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
actionUrl	URL encoded POST
password	URL encoded POST
password2	URL encoded POST
username	URL encoded POST

Input scheme 2	
Input name	Input type
password	URL encoded POST
password2	URL encoded POST
username	URL encoded POST

URL: https://18f-ads.noblis.org/myHealthAlerts/css/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/css/select2.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/custom-693484281cf88c532cd0506df2ccfe5a.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/frontPage-2e2df9a9c4df9dd5cfee613bd8926628.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/application-53a84ac2c2e94b8b968c583144856503.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/registerAjax-7a569a23001c47d9e96b30b53aabb57b.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/auth-951773c4b605dc2df6b633eb61ff6a3f.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/reset-23c82d3b1ee97a5efad7afe024648c51.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/spring-security-ui-1e89aeb137e301ea92063996df570da9.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/jquery.jgrowl-38b6cac69c3e0e2c40c23c3802859c49.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/assets/jquery.safari-checkbox-603cb22035fc9e252416fa8bb739cd95.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/themes/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/themes/ui-lightness/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/themes/ui-lightness/jquery-ui-1.10.4.custom.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/themes/ui-lightness/images/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/js/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-ui-1.10.4/jquery-ui/js/jquery-ui-1.10.4.custom.min.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/css/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/css/smoothness/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/css/smoothness/jquery-ui-1.10.3.custom.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/css/smoothness/images/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/jquery/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/jquery/jquery.jgrowl.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/jquery/jquery.checkbox.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/spring-security-ui-1.0-RC2/js/spring-security-ui.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-1.11.1/js/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-1.11.1/js/jquery/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/plugins/jquery-1.11.1/js/jquery/jquery-1.11.1.min.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/js/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/js/select2.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/login

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://18f-ads.noblis.org/myHealthAlerts/login/authfail

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
login_error	URL encoded GET

URL: https://18f-ads.noblis.org/myHealthAlerts/login/auth

No vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
format	URL encoded GET
login_error	URL encoded GET

Input scheme 2	
Input name	Input type
format	URL encoded GET