Mark Wagner
SDEV300-7893 Lab5
Prof. Cooper
4/21/2019

Mr. Supervisor of IT Security,

For this security audit, I disassembled the basic login form and it's subsequent pages that were used in the last week's lab.

One thing I realized had to be done was removal of sessions between tests. I could not modify break- captured get or post requests while sessions kept the variables held. I was able to subvert requests to the page and modify the request, hence modifying the response in turn.

The best way to stop hackers from intercepting packets of responses sent to websites is to use SSL encryption and ensure that every page is an https page.

Alert: Web browser XSS protection not enabled, X Content…
Please note that before the tests there were 5 alerts of low to medium severity. One was a reflected XSS warning which was fixed by altering the response header with this:

```
Header set X-XSS-Protection "1; mode=block"
```

Alert: Incomplete or no-cache control on http header:
The next problem in order of Severity was that content could be sniffed by browsers that enable MIME Sniffing (sniffing packet data to determine content type in-lieu of metadata specifying type (jpg, pdf, etc). That was fixed by adding this to the headers:

```
Header set X-Content-Type-Options nosniff
```

Alert: Cookie no httpOnly header flag
OWASP A3 Threat – Release of sensitive information:
Finally, this was not part of my initial task for our company website but I thought it would help mitigate a low-level, low-priority threat which allowed third party javascript running on browsers to steal cookie information from the http response and potentially transmit it to a session jacker. This only allows the cookie to be given to http requests and not JS. It is mostly important for IE and Chrome users.

```
Header set Set-Cookie HttpOnly;Secure
```

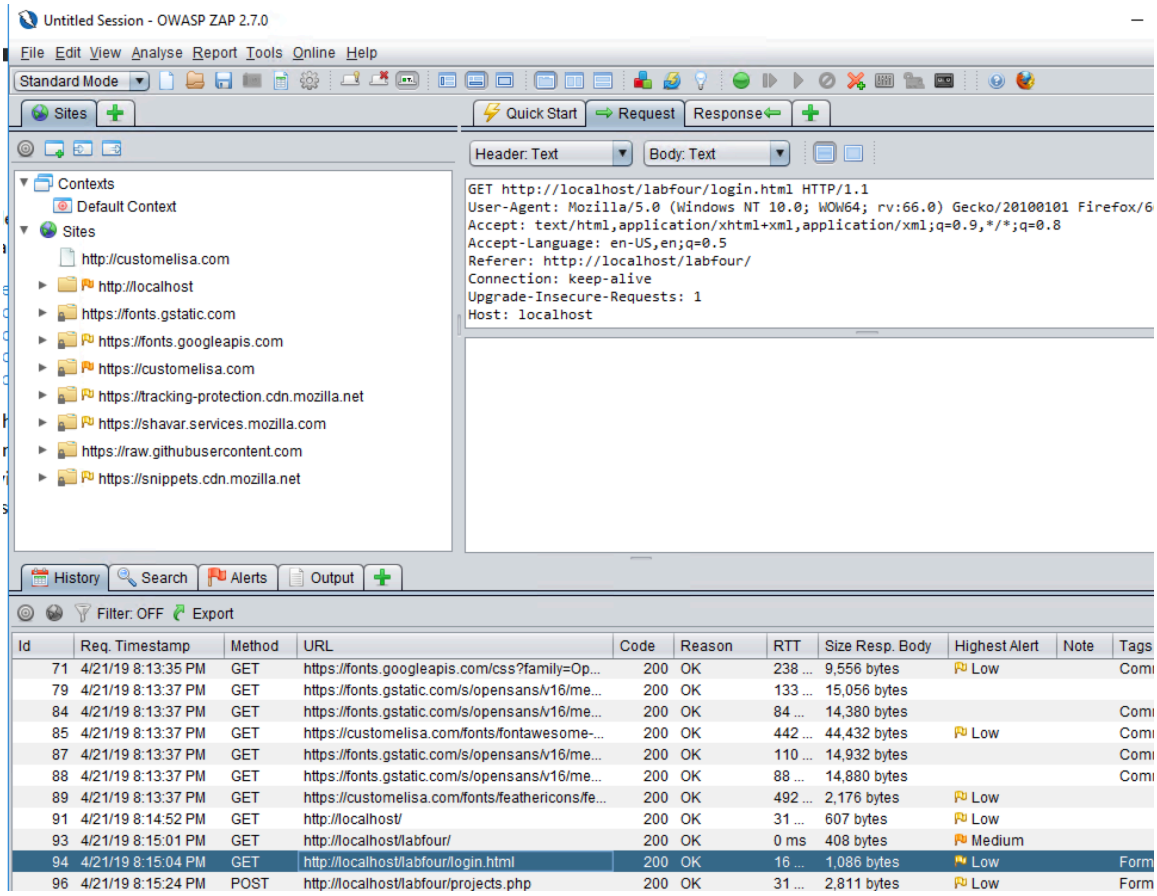
With these vulnerabilities mitigated, all that remains are two false alerts indicating a sitemap present (for seo purposes) and a robot.txt thing that doesn't matter for security purposes.

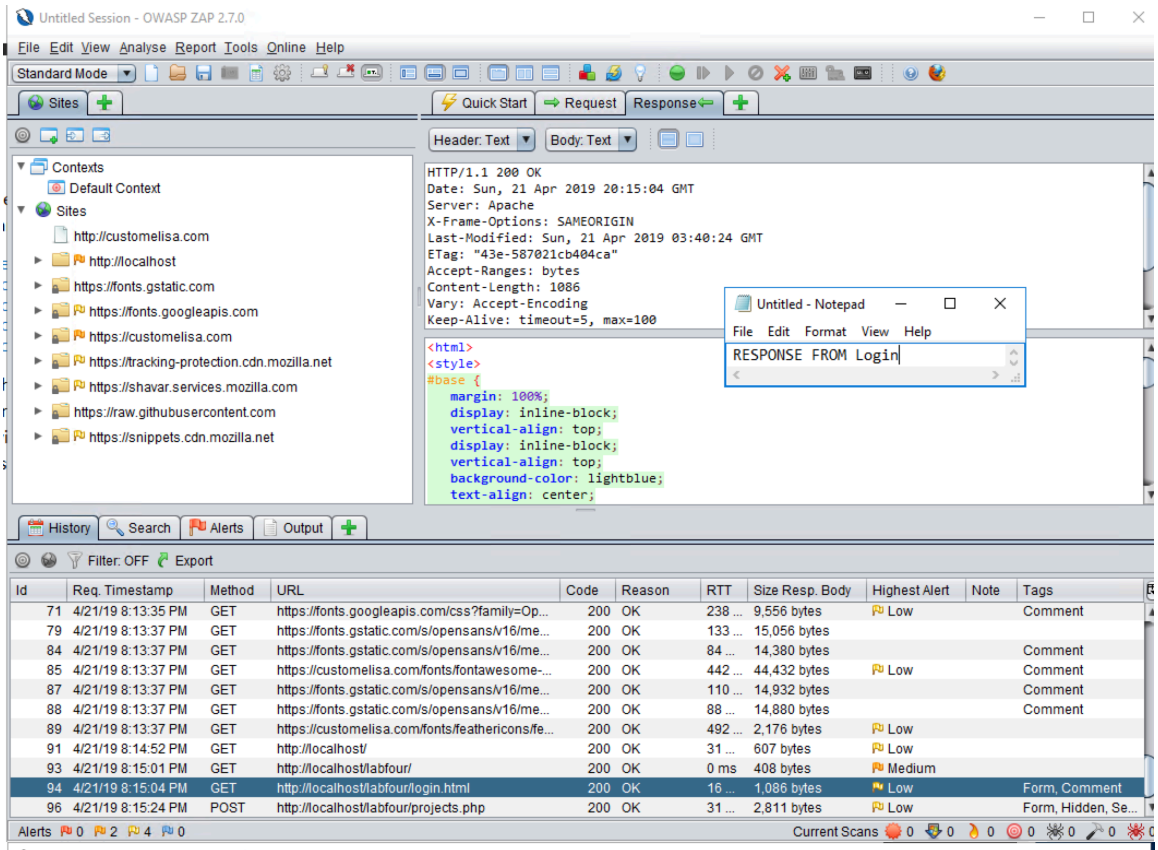
As far as basic scanning and scripting techniques, we are more secure as a result of these changes.

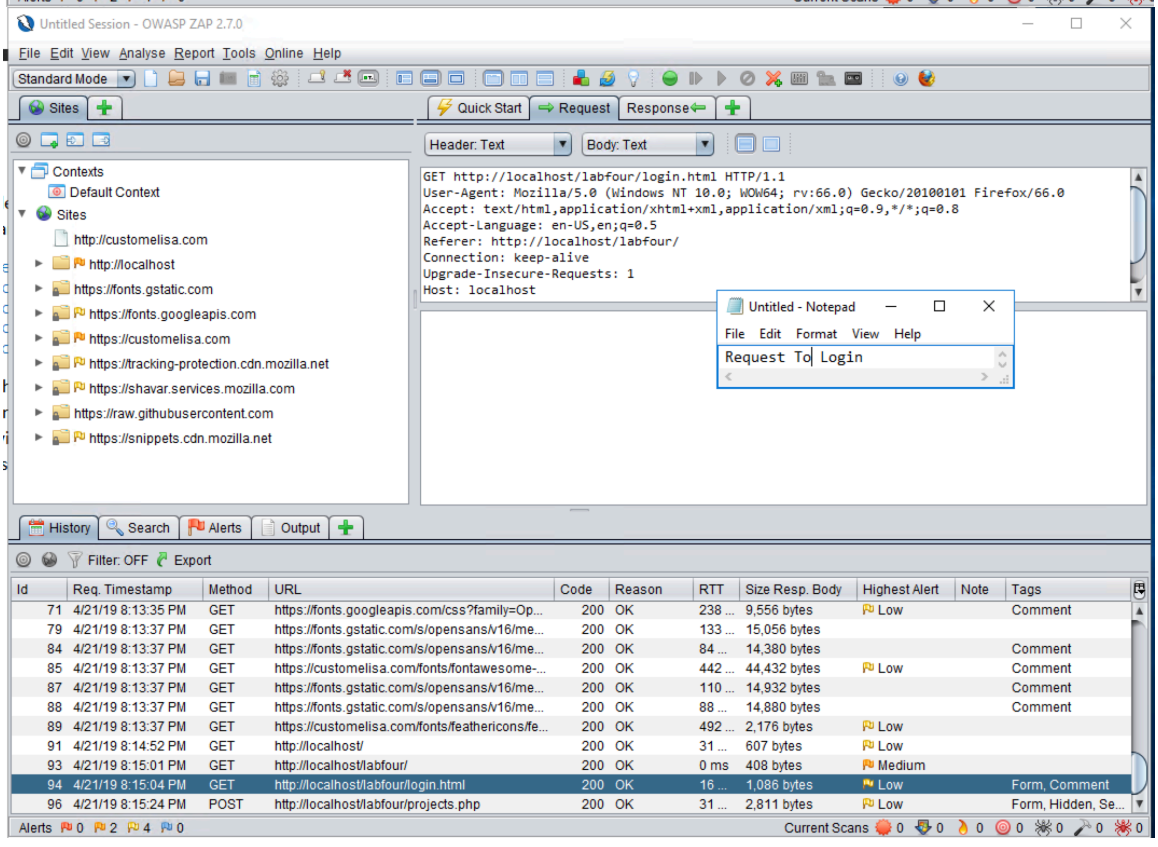
We are safe for now!

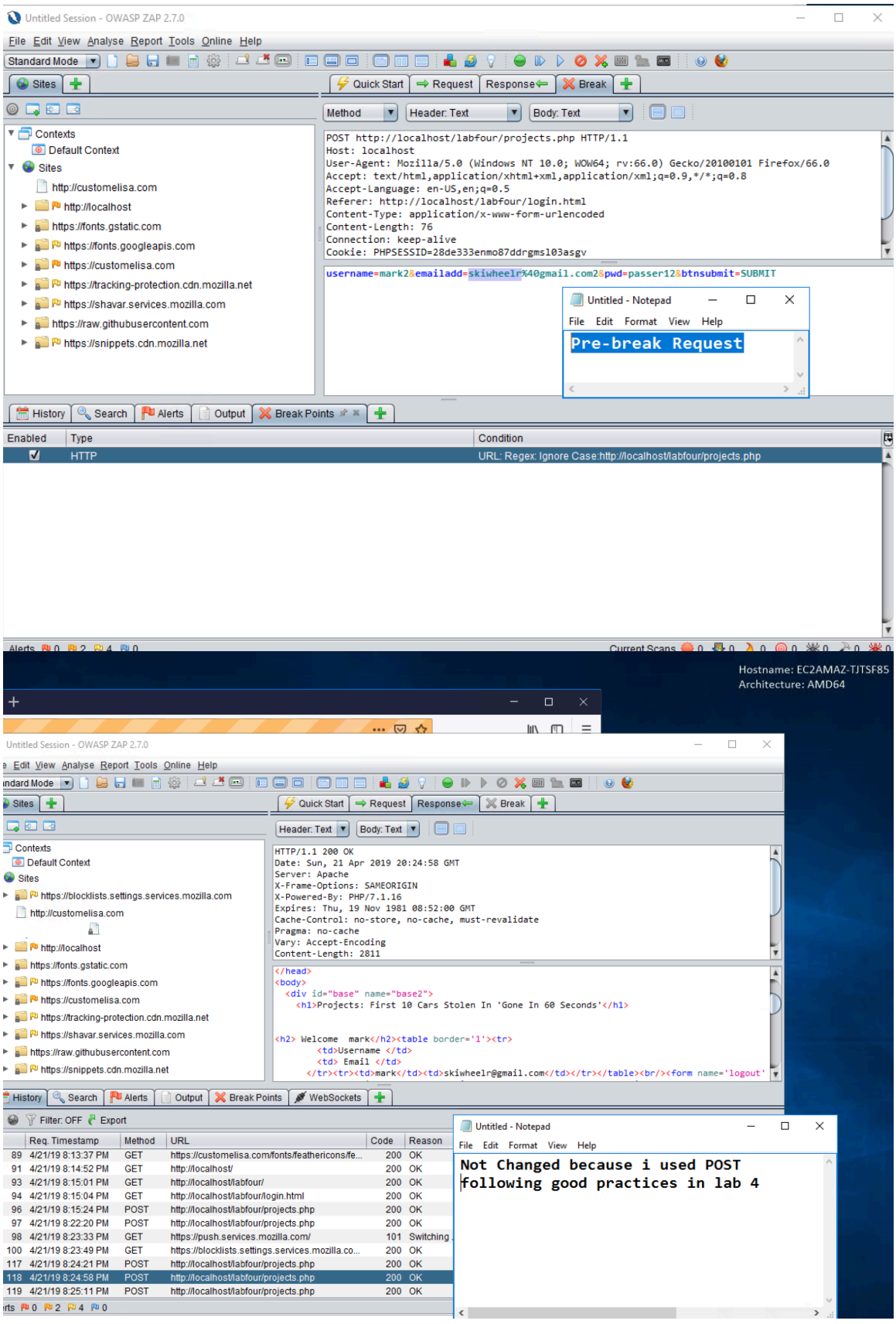
The following are screenshots of what occurred in chronological order with comment boxes detailing them inside.
Attached to this submission are the httpd.conf file, an html error report, and an access.log file.

Citation:
S. O., & Kumar, C. (2018, February 06). Secure cookie with HttpOnly and Secure flag in Apache. Retrieved from https://geekflare.com/httponly-secure-cookie-apache/

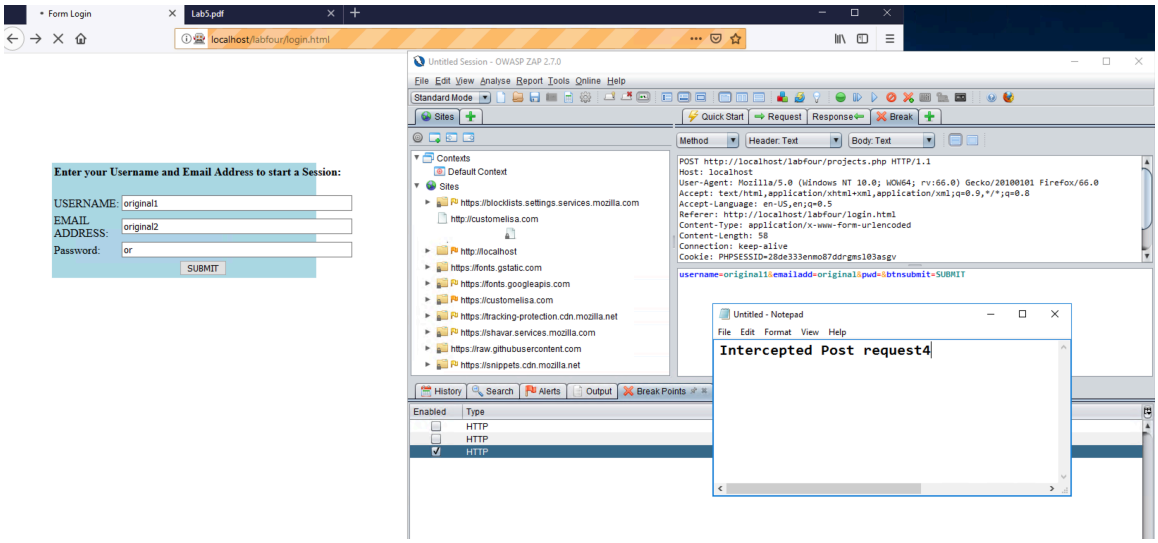



Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
HTTP/1.1 200 OK
Date: Sun, 21 Apr 2019 20:15:04 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Sun, 21 Apr 2019 03:40:24 GMT
ETag: "43e-587021cb404ca"
Accept-Ranges: bytes
Content-Length: 1086
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Untitled - Notepad
File Edit Format View Help
RESPONSE FROM Login
<html>
<style>
#base {
margin: 100%;
display: inline-block;
vertical-align: top;
display: inline-block;
vertical-align: top;
background-color: lightblue;
text-align: center;
History
Search
Alerts
Output
Filter: OFF
Export
Id
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
71 4/21/19 8:13:35 PM GET https://fonts.googleapis.com/css?family=Op... 200 OK 238 ... 9,556 bytes Low Comment
79 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 133 ... 15,056 bytes
84 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 84 ... 14,380 bytes Comment
85 4/21/19 8:13:37 PM GET https://customelisa.com/fonts/fontawesome-... 200 OK 442 ... 44,432 bytes Low Comment
87 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 110 ... 14,932 bytes Comment
88 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 88 ... 14,880 bytes Comment
89 4/21/19 8:13:37 PM GET https://customelisa.com/fonts/feathericons/fe... 200 OK 492 ... 2,176 bytes Low
91 4/21/19 8:14:52 PM GET http://localhost/ 200 OK 31 ... 607 bytes Low
93 4/21/19 8:15:01 PM GET http://localhost/labfour/ 200 OK 0 ms 408 bytes Medium
94 4/21/19 8:15:04 PM GET http://localhost/labfour/login.html 200 OK 16 ... 1,086 bytes Low Form, Comment
96 4/21/19 8:15:24 PM POST http://localhost/labfour/projects.php 200 OK 31 ... 2,811 bytes Low Form, Hidden, Se...
Alerts 0 2 4 0
Current Scans 0 0 0 0 0 0 0

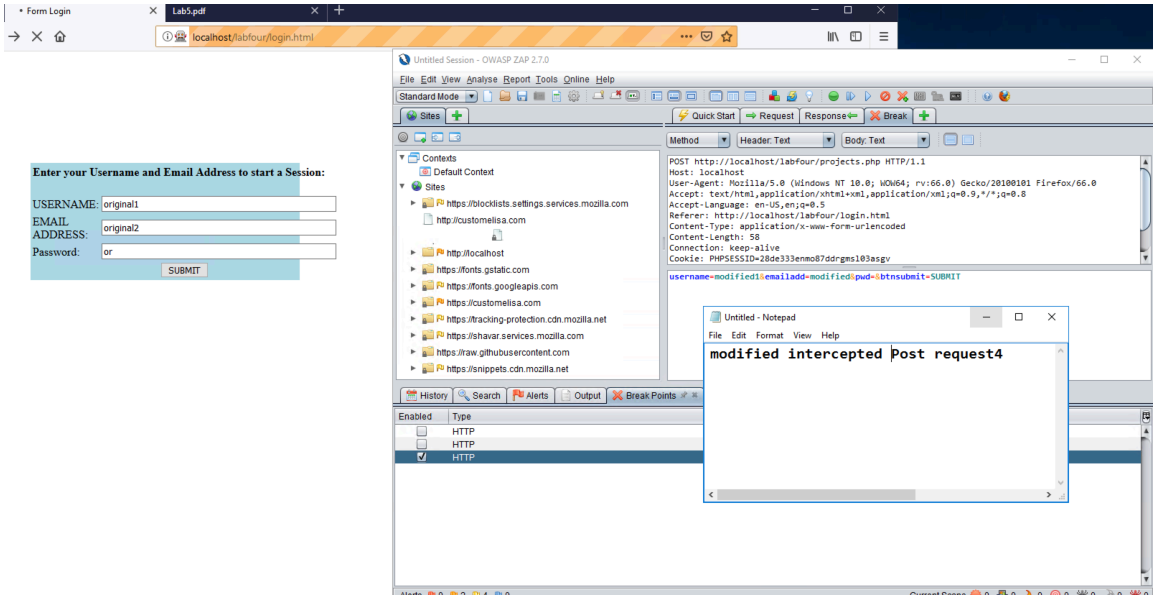

Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
GET http://localhost/labfour/login.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/labfour/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: localhost
Untitled - Notepad
File Edit Format View Help
Request To Login
History
Search
Alerts
Output
Filter: OFF
Export
Id
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
71 4/21/19 8:13:35 PM GET https://fonts.googleapis.com/css?family=Op... 200 OK 238 ... 9,556 bytes Low Comment
79 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 133 ... 15,056 bytes
84 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 84 ... 14,380 bytes Comment
85 4/21/19 8:13:37 PM GET https://customelisa.com/fonts/fontawesome-... 200 OK 442 ... 44,432 bytes Low Comment
87 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 110 ... 14,932 bytes Comment
88 4/21/19 8:13:37 PM GET https://fonts.gstatic.com/s/opensans/v16/me... 200 OK 88 ... 14,880 bytes Comment
89 4/21/19 8:13:37 PM GET https://customelisa.com/fonts/feathericons/fe... 200 OK 492 ... 2,176 bytes Low
91 4/21/19 8:14:52 PM GET http://localhost/ 200 OK 31 ... 607 bytes Low
93 4/21/19 8:15:01 PM GET http://localhost/labfour/ 200 OK 0 ms 408 bytes Medium
94 4/21/19 8:15:04 PM GET http://localhost/labfour/login.html 200 OK 16 ... 1,086 bytes Low Form, Comment
96 4/21/19 8:15:24 PM POST http://localhost/labfour/projects.php 200 OK 31 ... 2,811 bytes Low Form, Hidden, Se...
Alerts 0 2 4 0
Current Scans 0 0 0 0 0 0 0


Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
Contexts
Default Context
Sites
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
POST http://localhost/labfour/projects.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/labfour/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Connection: keep-alive
Cookie: PHPSESSID=28de333enmo87ddrgms103asgv
username=mark2&emailadd=skiwheelr%40gmail.com2&pwd=passer12&btnsubmit=SUBMIT
Untitled - Notepad
File Edit Format View Help
Pre-break Request
History
Search
Alerts
Output
Break Points
Enabled
Type
Condition
HTTP
URL: Regex: Ignore Case:http://localhost/labfour/projects.php
Hostname: EC2AMAZ-TJTSF85
Architecture: AMD64
HTTP/1.1 200 OK
Date: Sun, 21 Apr 2019 20:24:58 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/7.1.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2811
</head>
<body>

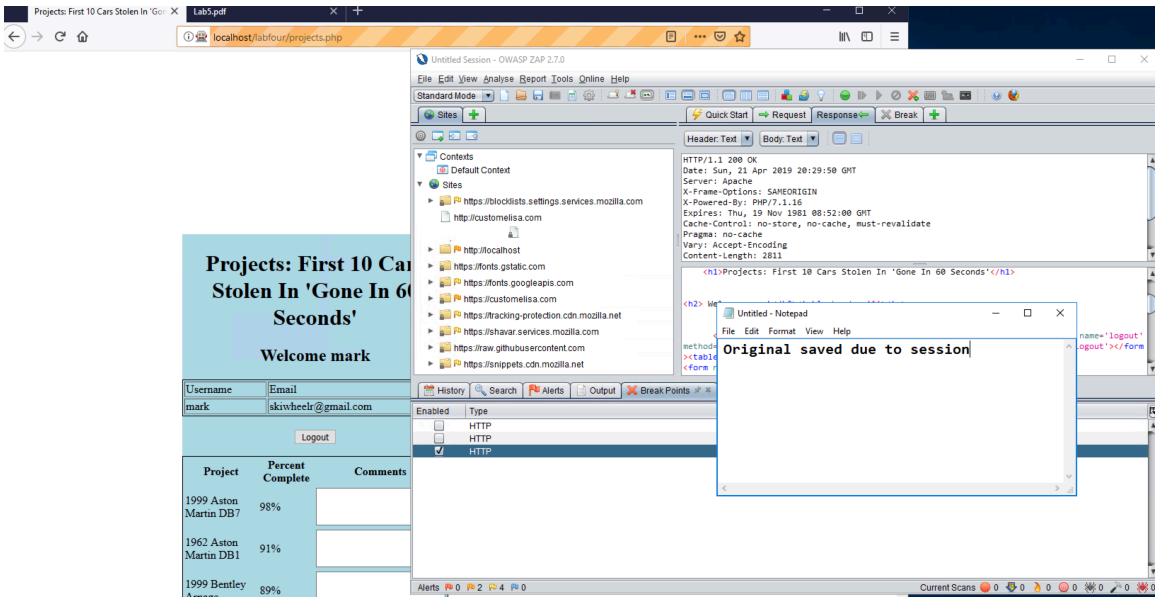
<h1>Projects: First 10 Cars Stolen In 'Gone In 60 Seconds'</h1>
<h2> Welcome mark</h2><table border='1'><tr>
<td>Username </td>
<td> Email </td>
</tr><tr><td>mark</td><td>skiwheelr@gmail.com</td></tr></table>
<form name='logout'
WebSockets
Filter: OFF
Export
Req. Timestamp
Method
URL
Code
Reason
89 4/21/19 8:13:37 PM GET https://customelisa.com/fonts/feathericons/fe... 200 OK
91 4/21/19 8:14:52 PM GET http://localhost/ 200 OK
93 4/21/19 8:15:01 PM GET http://localhost/labfour/ 200 OK
94 4/21/19 8:15:04 PM GET http://localhost/labfour/login.html 200 OK
96 4/21/19 8:15:24 PM POST http://localhost/labfour/projects.php 200 OK
97 4/21/19 8:22:20 PM POST http://localhost/labfour/projects.php 200 OK
98 4/21/19 8:23:33 PM GET https://push.services.mozilla.com/ 101 Switching
100 4/21/19 8:23:49 PM GET https://blocklists.settings.services.mozilla.co... 200 OK
117 4/21/19 8:24:21 PM POST http://localhost/labfour/projects.php 200 OK
118 4/21/19 8:24:58 PM POST http://localhost/labfour/projects.php 200 OK
119 4/21/19 8:25:11 PM POST http://localhost/labfour/projects.php 200 OK
Untitled - Notepad
File Edit Format View Help
Not Changed because i used POST
following good practices in lab 4


Form Login
Lab5.pdf
localhost/labfour/login.html
Enter your Username and Email Address to start a Session:
USERNAME: original1
EMAIL ADDRESS: original2
Password: or
SUBMIT
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
Contexts
Default Context
Sites
https://blocklists.settings.services.mozilla.com
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
POST http://localhost/labfour/projects.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/labfour/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Connection: keep-alive
Cookie: PHPSESSID=28de333enmo87ddrgms103asgv
username=original1&emailadd=original&pwd=&btnsubmit=SUBMIT
Untitled - Notepad
File Edit Format View Help
Intercepted Post request4
History
Search
Alerts
Output
Break Points
Enabled
Type
HTTP
HTTP
HTTP

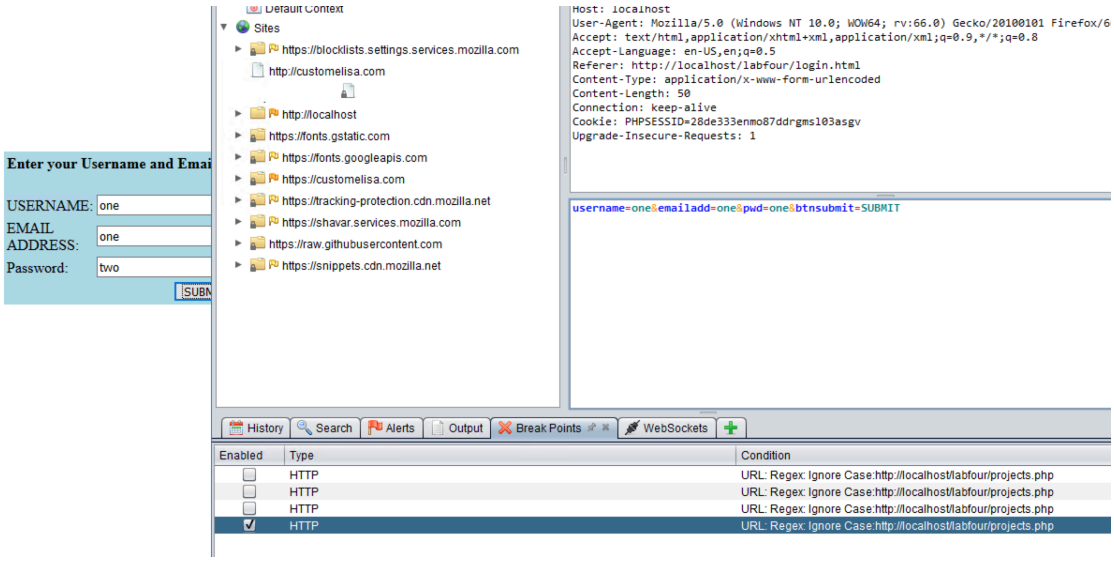
eff

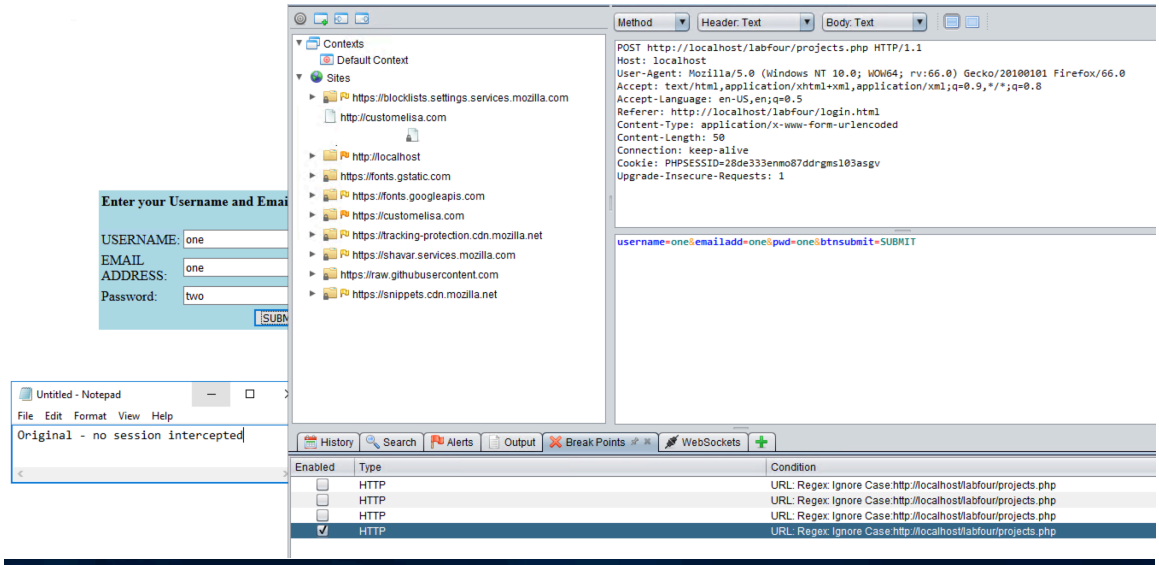

Form Login
Lab5.pdf
localhost/labfour/login.html
Enter your Username and Email Address to start a Session:
USERNAME: original1
EMAIL ADDRESS: original2
Password: or
SUBMIT
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
Contexts
Default Context
Sites
https://blocklists.settings.services.mozilla.com
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
POST http://localhost/labfour/projects.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/labfour/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Connection: keep-alive
Cookie: PHPSESSID=28de333enmo87ddrgms103asgv
username=modified1&emailadd=modified&pwd=&btnsubmit=SUBMIT
Untitled - Notepad
File Edit Format View Help
modified intercepted Post request4
History
Search
Alerts
Output
Break Points
Enabled
Type
HTTP
HTTP
HTTP

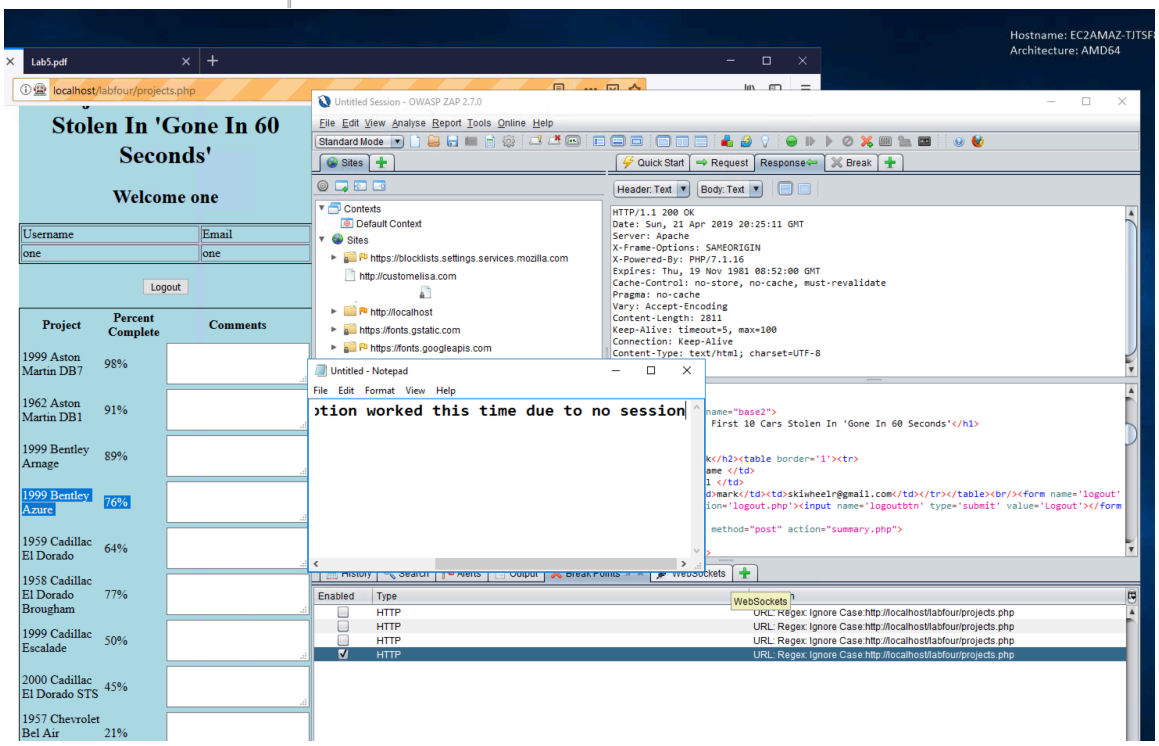
f

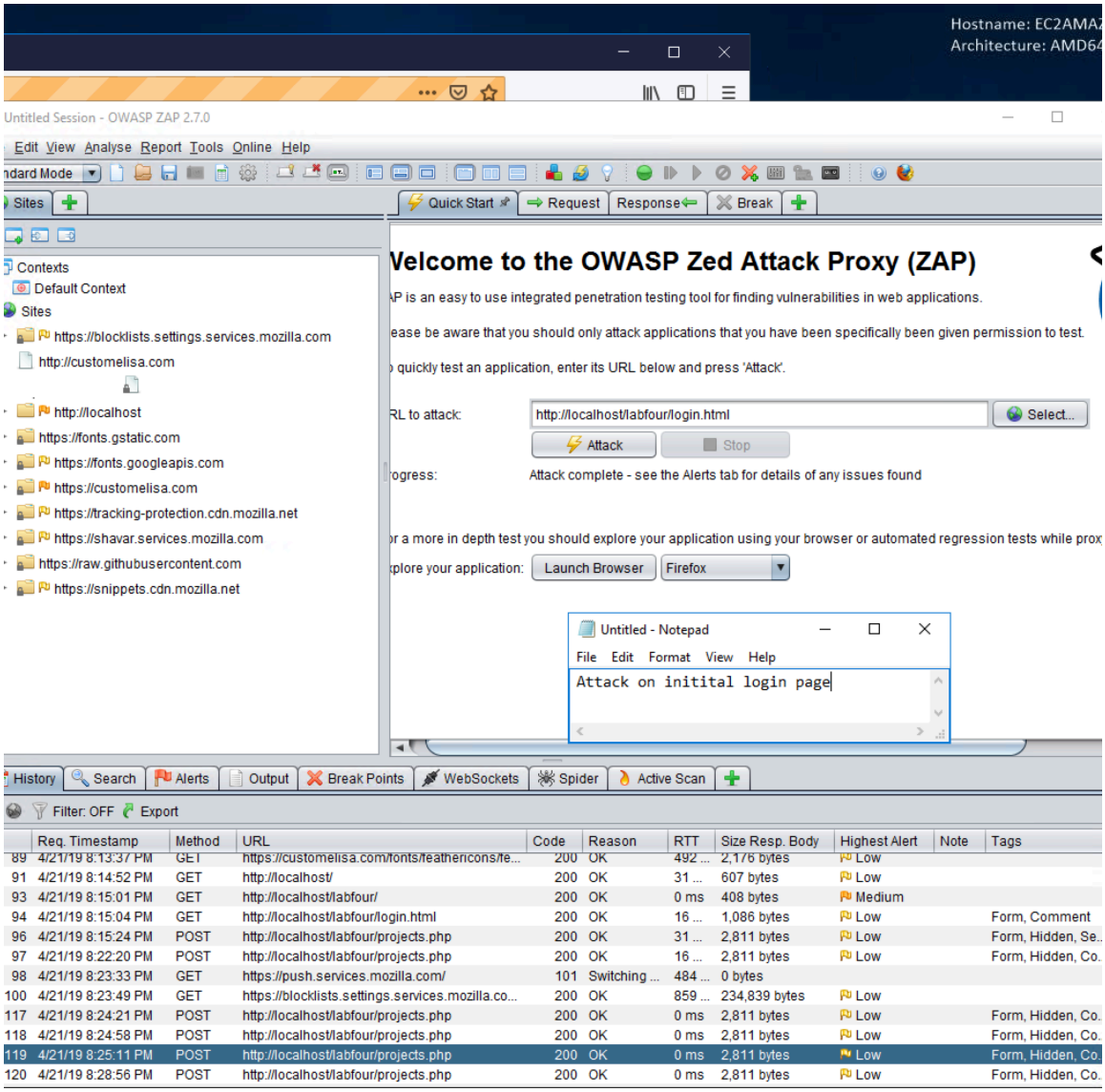

Projects: First 10 Cars Stolen In 'Gone In 60 Seconds'
Welcome mark
Username
Email
mark
skiwheelr@gmail.com
Logout
Project
Percent Complete
Comments
1999 Aston Martin DB7
98%
1962 Aston Martin DB1
91%
1999 Bentley
89%
Original saved due to session
HTTP/1.1 200 OK
Date: Sun, 21 Apr 2019 20:29:50 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/7.1.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2811

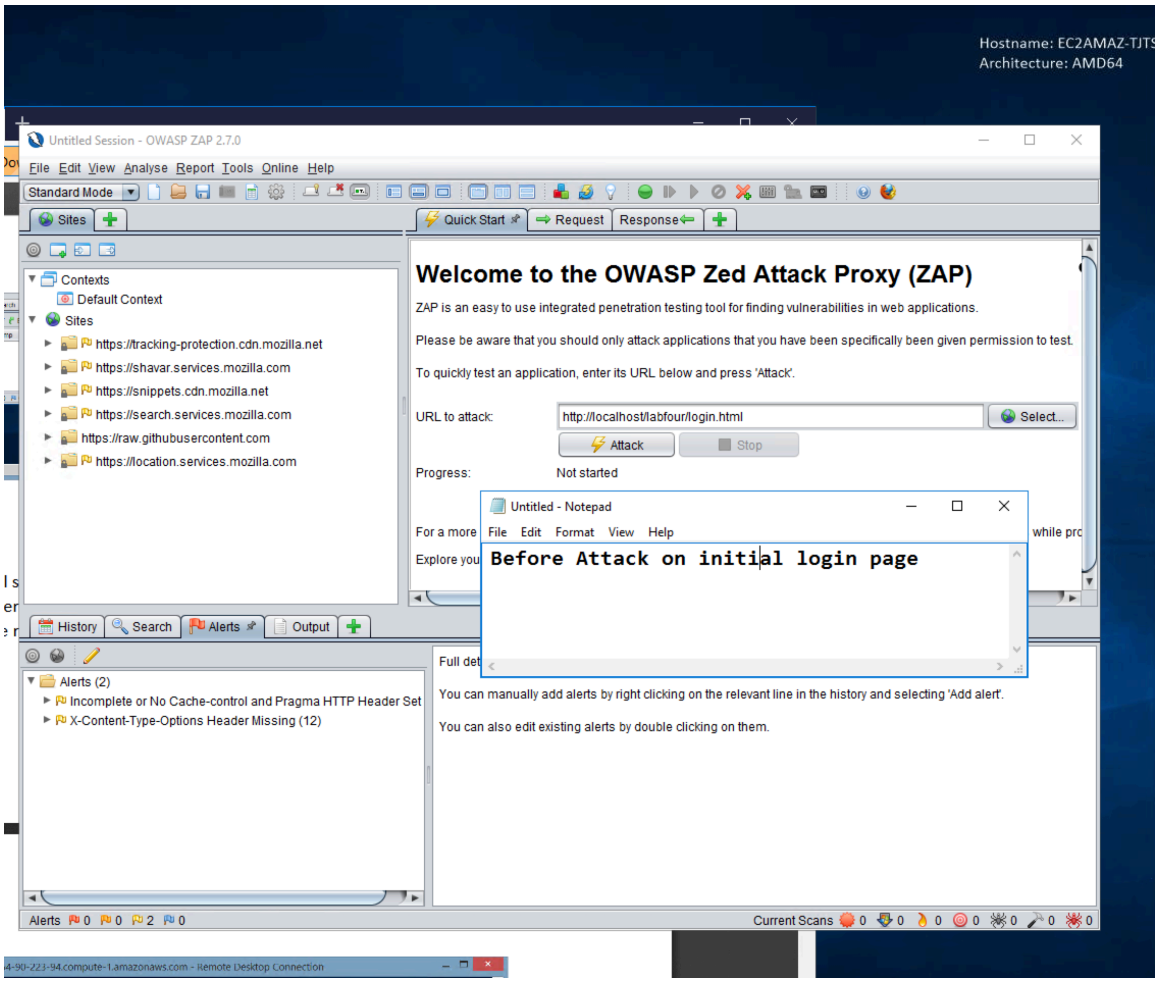
f

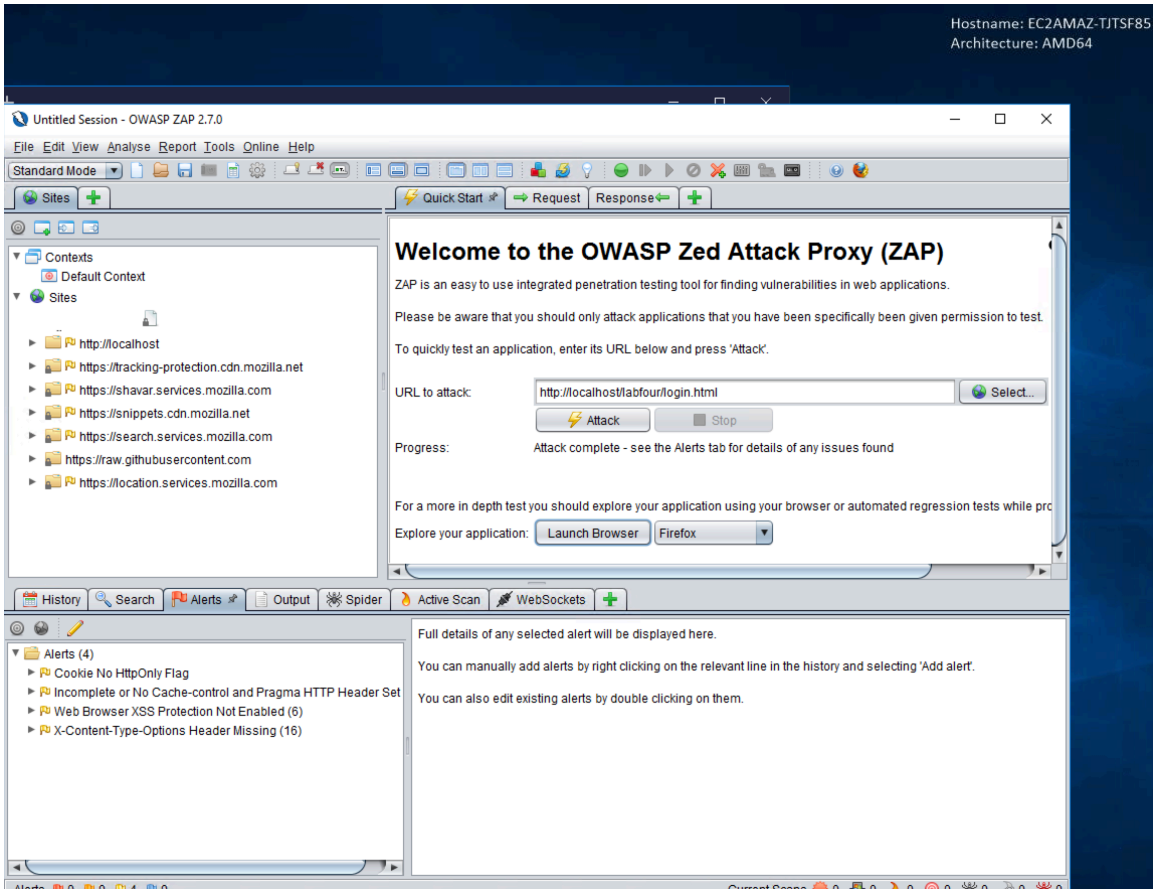

Enter your Username and Emai
USERNAME:
one
EMAIL ADDRESS:
one
Password:
two
Sites
https://blocklists.settings.services.mozilla.com
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/labfour/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Connection: keep-alive
Cookie: PHPSESSID=28de333enmo87ddrgms103asgv
Upgrade-Insecure-Requests: 1
username=one&emailadd=one&pwd=one&btnsubmit=SUBMIT
History
Search
Alerts
Output
Break Points
WebSockets
Enabled
Type
Condition
HTTP
URL: Regex: Ignore Case:http://localhost/labfour/projects.php

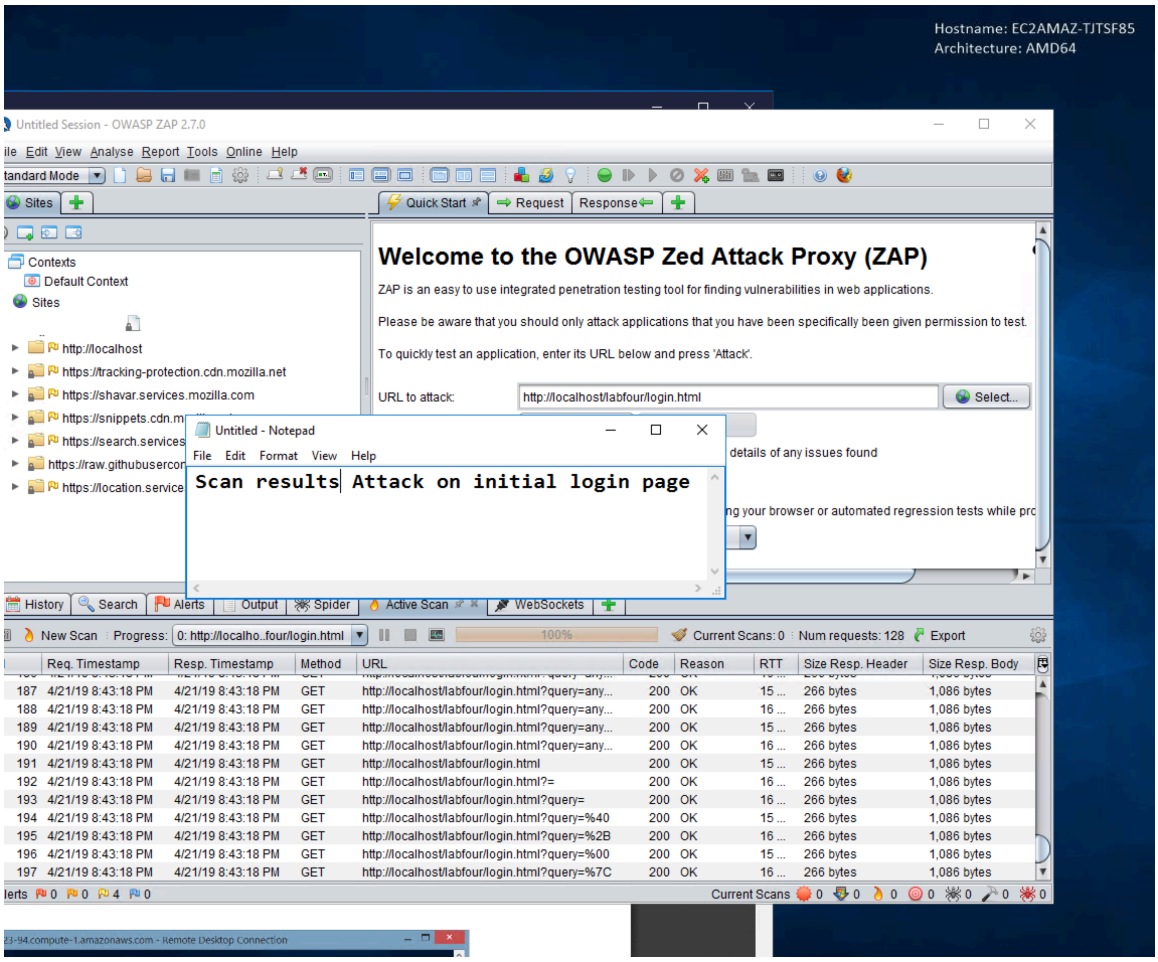

Enter your Username and Emai
USERNAME: one
EMAIL ADDRESS: one
Password: two
SUBN
Untitled - Notepad
File Edit Format View Help
Original - no session intercepted
Contexts
Default Context
Sites
https://blocklists.settings.services.mozilla.com
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
Method
Header: Text
Body: Text
POST http://localhost/labfour/projects.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/labfour/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Connection: keep-alive
Cookie: PHPSESSID=28de333enmo87ddrgms103asgv
Upgrade-Insecure-Requests: 1
username=one&emailadd=one&pwd=one&btnsubmit=SUBMIT
History
Search
Alerts
Output
Break Points
WebSockets
Enabled
Type
Condition
HTTP
URL: Regex: Ignore Case:http://localhost/labfour/projects.php

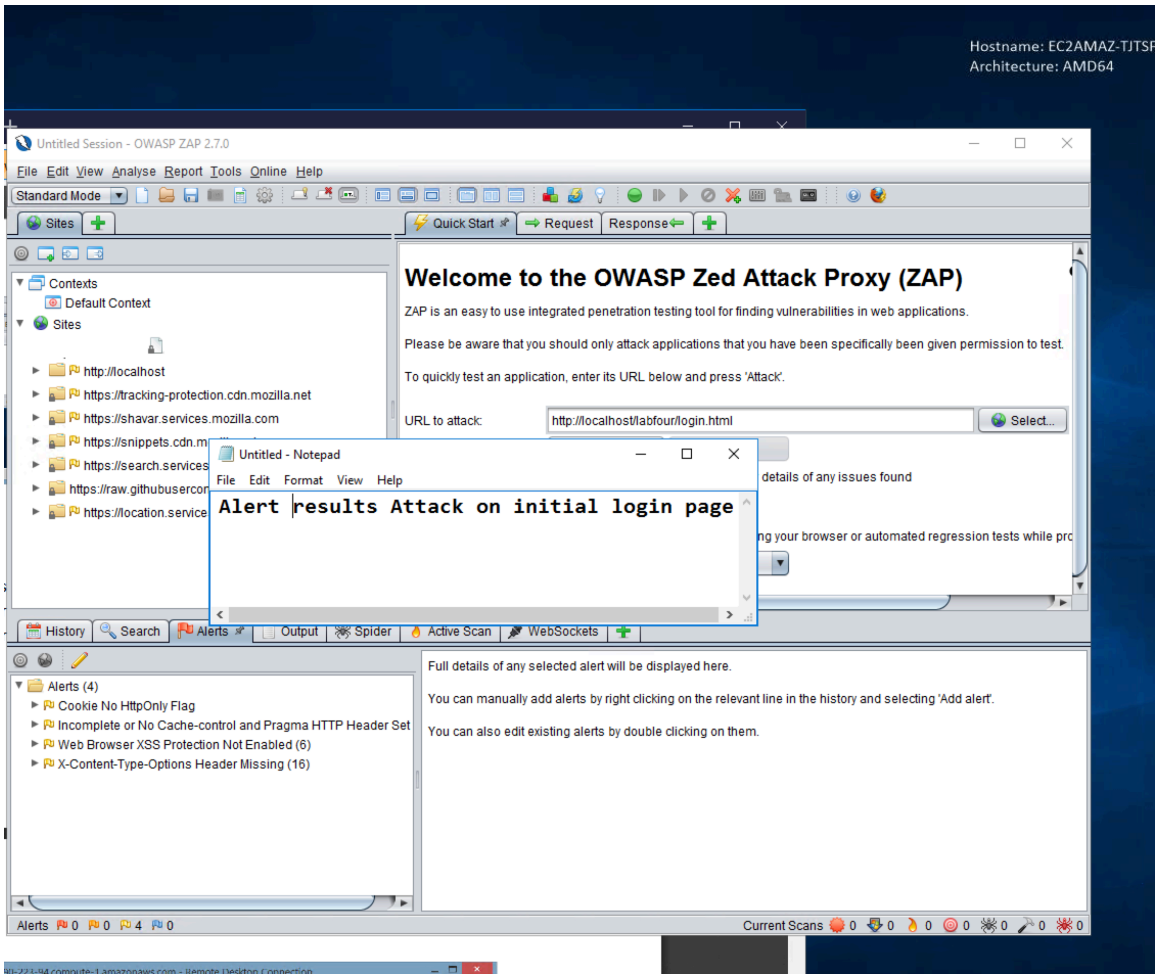

Hostname: EC2AMAZ-TJTSF
Architecture: AMD64
Lab5.pdf
localhost/labfour/projects.php
Stolen In 'Gone In 60 Seconds'
Welcome one
Username
Email
one
one
Logout
Project
Percent Complete
Comments
1999 Aston Martin DB7 98%
1962 Aston Martin DB1 91%
1999 Bentley Arnage 89%
1999 Bentley Azure 76%
1959 Cadillac El Dorado 64%
1958 Cadillac El Dorado Brougham 77%
1999 Cadillac Escalade 50%
2000 Cadillac El Dorado STS 45%
1957 Chevrolet Bel Air 21%
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Contexts
Default Context
Sites
https://blocklists.settings.services.mozilla.com
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
Header: Text
Body: Text
HTTP/1.1 200 OK
Date: Sun, 21 Apr 2019 20:25:11 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/7.1.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2811
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Untitled - Notepad
File Edit Format View Help
tion worked this time due to no session
WebSockets
Enabled
Type
HTTP
URL: Regex: Ignore Case:http://localhost/labfour/projects.php


Hostname: EC2AMAZ
Architecture: AMD64
Untitled Session - OWASP ZAP 2.7.0
Edit View Analyse Report Tools Online Help
Sites
Quick Start
Request
Response
Break
Contexts
Default Context
Sites
https://blocklists.settings.services.mozilla.com
http://customelisa.com
http://localhost
https://fonts.gstatic.com
https://fonts.googleapis.com
https://customelisa.com
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://raw.githubusercontent.com
https://snippets.cdn.mozilla.net
Welcome to the OWASP Zed Attack Proxy (ZAP)
AP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
ease be aware that you should only attack applications that you have been specifically been given permission to test.
quickly test an application, enter its URL below and press 'Attack'.
RL to attack:
http://localhost/labfour/login.html
Select...
Attack
Stop
rogress:
Attack complete - see the Alerts tab for details of any issues found
r a more in depth test you should explore your application using your browser or automated regression tests while prox
xplore your application:
Launch Browser
Firefox
Untitled - Notepad
File Edit Format View Help
Attack on initital login page
History
Search
Alerts
Output
Break Points
WebSockets
Spider
Active Scan
Filter: OFF
Export
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
89 4/21/19 8:13:37 PM GET https://customelisa.com/fonts/feathericons/fe... 200 OK 492 ... 2,176 bytes Low
91 4/21/19 8:14:52 PM GET http://localhost/ 200 OK 31 ... 607 bytes Low
93 4/21/19 8:15:01 PM GET http://localhost/labfour/ 200 OK 0 ms 408 bytes Medium
94 4/21/19 8:15:04 PM GET http://localhost/labfour/login.html 200 OK 16 ... 1,086 bytes Low Form, Comment
96 4/21/19 8:15:24 PM POST http://localhost/labfour/projects.php 200 OK 31 ... 2,811 bytes Low Form, Hidden, Se..
97 4/21/19 8:22:20 PM POST http://localhost/labfour/projects.php 200 OK 16 ... 2,811 bytes Low Form, Hidden, Co..
98 4/21/19 8:23:33 PM GET https://push.services.mozilla.com/ 101 Switching ... 484 ... 0 bytes
100 4/21/19 8:23:49 PM GET https://blocklists.settings.services.mozilla.co... 200 OK 859 ... 234,839 bytes Low
117 4/21/19 8:24:21 PM POST http://localhost/labfour/projects.php 200 OK 0 ms 2,811 bytes Low Form, Hidden, Co..
118 4/21/19 8:24:58 PM POST http://localhost/labfour/projects.php 200 OK 0 ms 2,811 bytes Low Form, Hidden, Co..
119 4/21/19 8:25:11 PM POST http://localhost/labfour/projects.php 200 OK 0 ms 2,811 bytes Low Form, Hidden, Co..
120 4/21/19 8:28:56 PM POST http://localhost/labfour/projects.php 200 OK 0 ms 2,811 bytes Low Form, Hidden, Co..

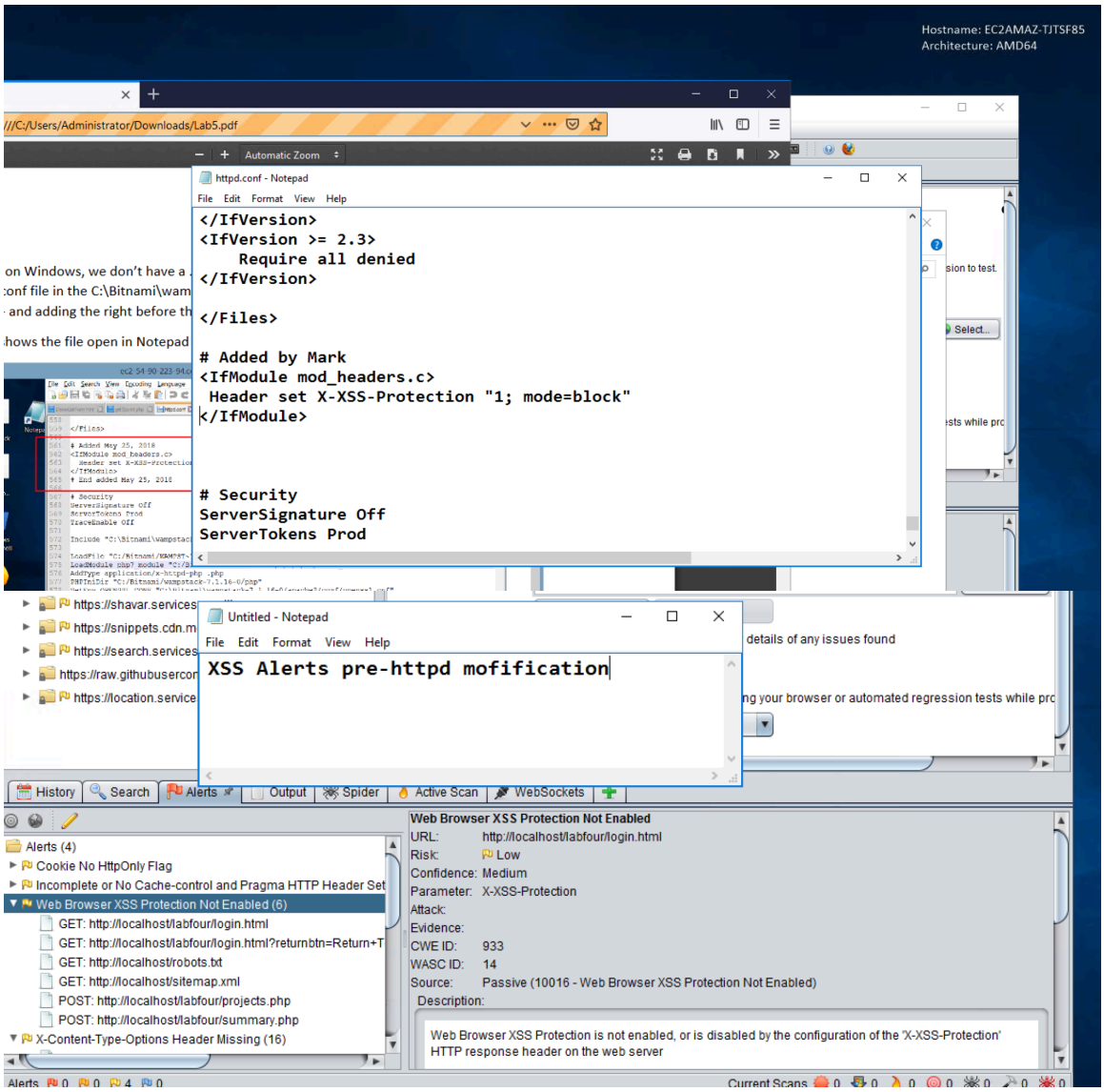

Hostname: EC2AMAZ-TJT
Architecture: AMD64
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://snippets.cdn.mozilla.net
https://search.services.mozilla.com
https://raw.githubusercontent.com
https://location.services.mozilla.com
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://localhost/labfour/login.html
Select...
Attack
Stop
Progress:
Not started
Untitled - Notepad
File Edit Format View Help
Before Attack on initial login page
History
Search
Alerts
Output
Alerts (2)
Incomplete or No Cache-control and Pragma HTTP Header Set
X-Content-Type-Options Header Missing (12)
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts 0 0 2 0
Current Scans 0 0 0 0 0 0 0
4-90-223-94.compute-1.amazonaws.com - Remote Desktop Connection

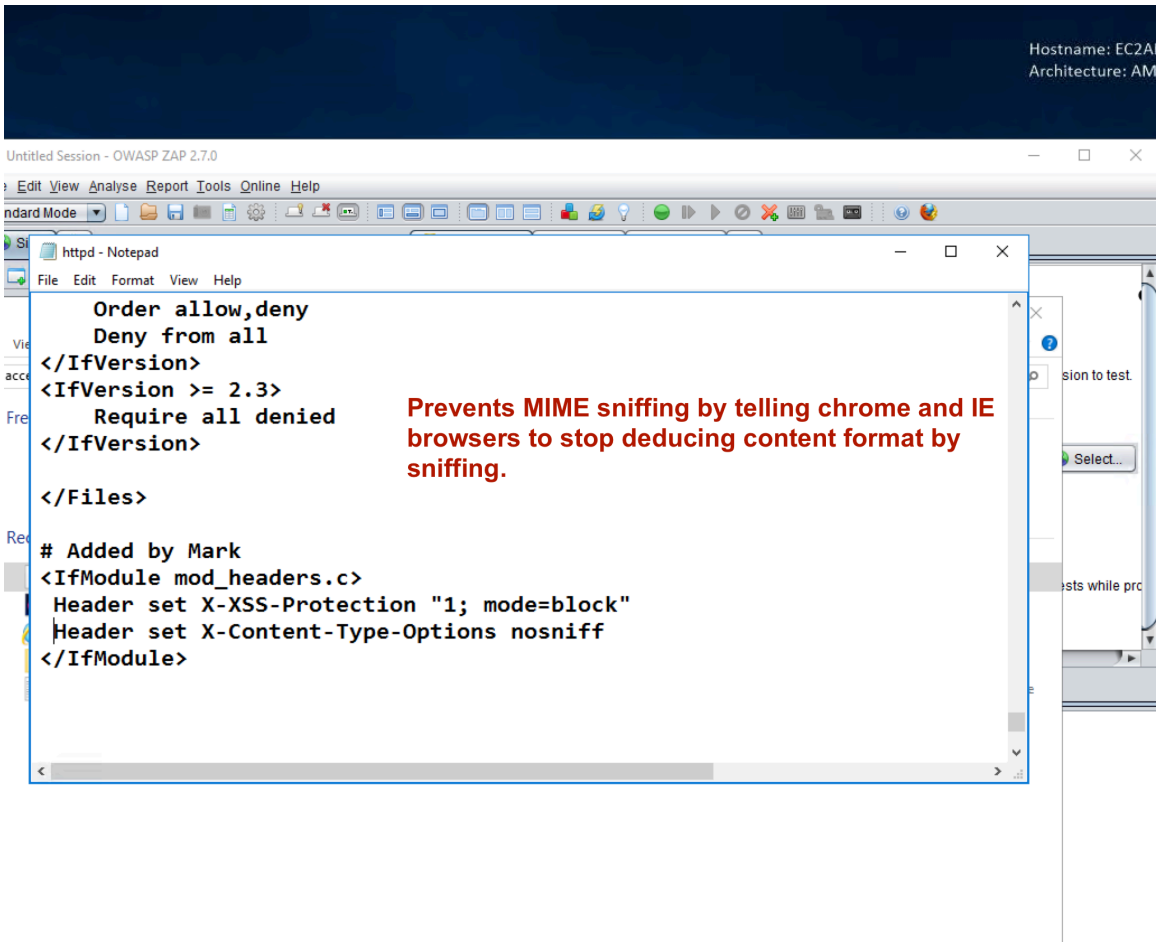

Hostname: EC2AMAZ-TJTSF85
Architecture: AMD64
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
http://localhost
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://snippets.cdn.mozilla.net
https://search.services.mozilla.com
https://raw.githubusercontent.com
https://location.services.mozilla.com
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://localhost/labfour/login.html
Select...
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
For a more in depth test you should explore your application using your browser or automated regression tests while prc
Explore your application:
Launch Browser
Firefox
History
Search
Alerts
Output
Spider
Active Scan
WebSockets
Alerts (4)
Cookie No HttpOnly Flag
Incomplete or No Cache-control and Pragma HTTP Header Set
Web Browser XSS Protection Not Enabled (6)
X-Content-Type-Options Header Missing (16)
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

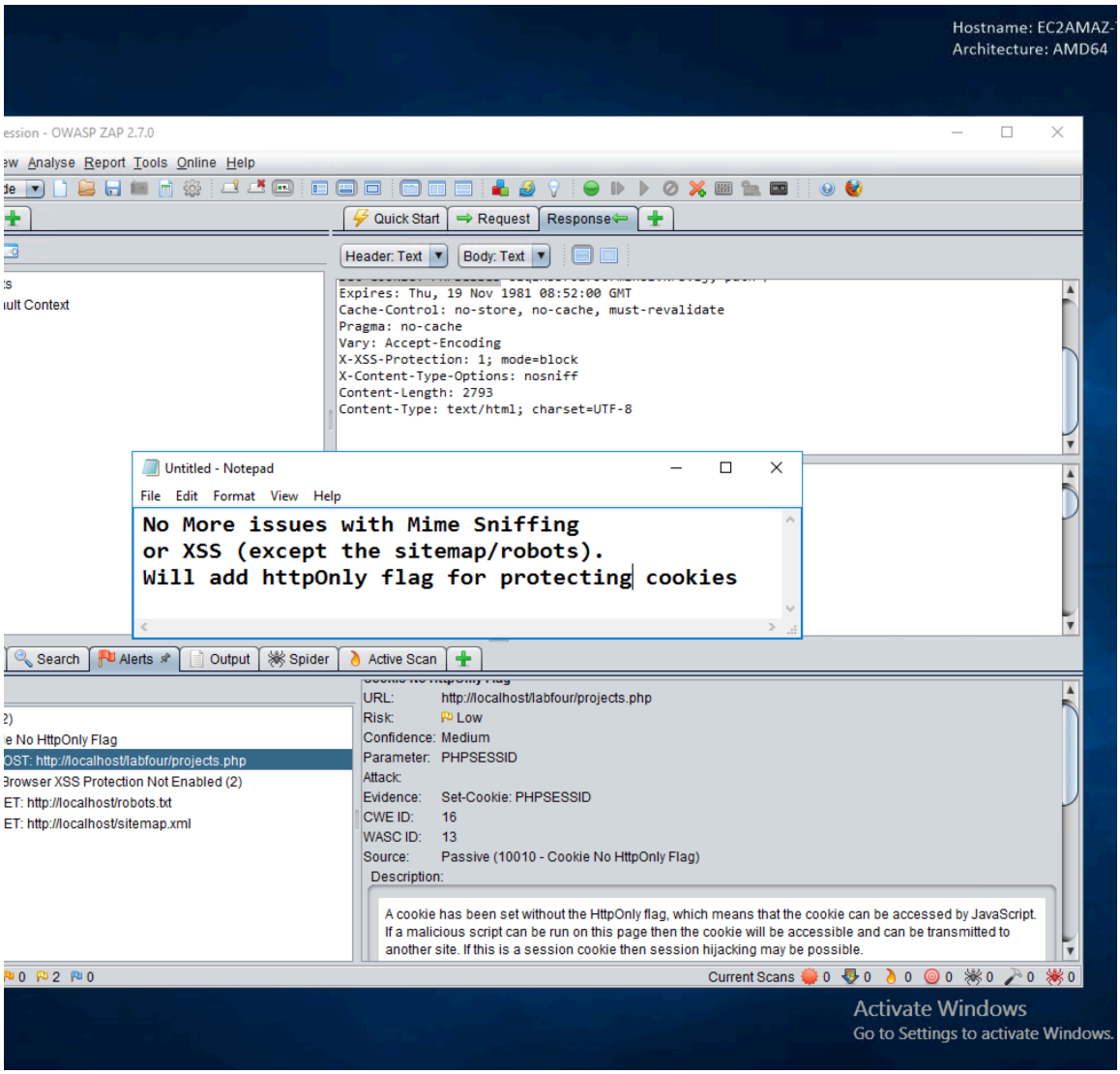

Hostname: EC2AMAZ-TJTSF85
Architecture: AMD64
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
http://localhost
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://search.services
https://location.service
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://localhost/labfour/login.html
Select...
details of any issues found
Untitled - Notepad
File Edit Format View Help
Scan results Attack on initial login page
History
Search
Alerts
Output
Spider
Active Scan
WebSockets
New Scan
Progress:
0: http://localho..four/login.html
100%
Current Scans: 0
Num requests: 128
Export
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
187 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=any... 200 OK 15 ... 266 bytes 1,086 bytes
188 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=any... 200 OK 16 ... 266 bytes 1,086 bytes
189 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=any... 200 OK 15 ... 266 bytes 1,086 bytes
190 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=any... 200 OK 16 ... 266 bytes 1,086 bytes
191 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html 200 OK 15 ... 266 bytes 1,086 bytes
192 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?= 200 OK 16 ... 266 bytes 1,086 bytes
193 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query= 200 OK 16 ... 266 bytes 1,086 bytes
194 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=%40 200 OK 15 ... 266 bytes 1,086 bytes
195 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=%2B 200 OK 16 ... 266 bytes 1,086 bytes
196 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=%00 200 OK 15 ... 266 bytes 1,086 bytes
197 4/21/19 8:43:18 PM 4/21/19 8:43:18 PM GET http://localhost/labfour/login.html?query=%7C 200 OK 16 ... 266 bytes 1,086 bytes
Alerts 0 0 4 0
Current Scans 0 0 0 0 0 0 0
23-94.compute-1.amazonaws.com - Remote Desktop Connection

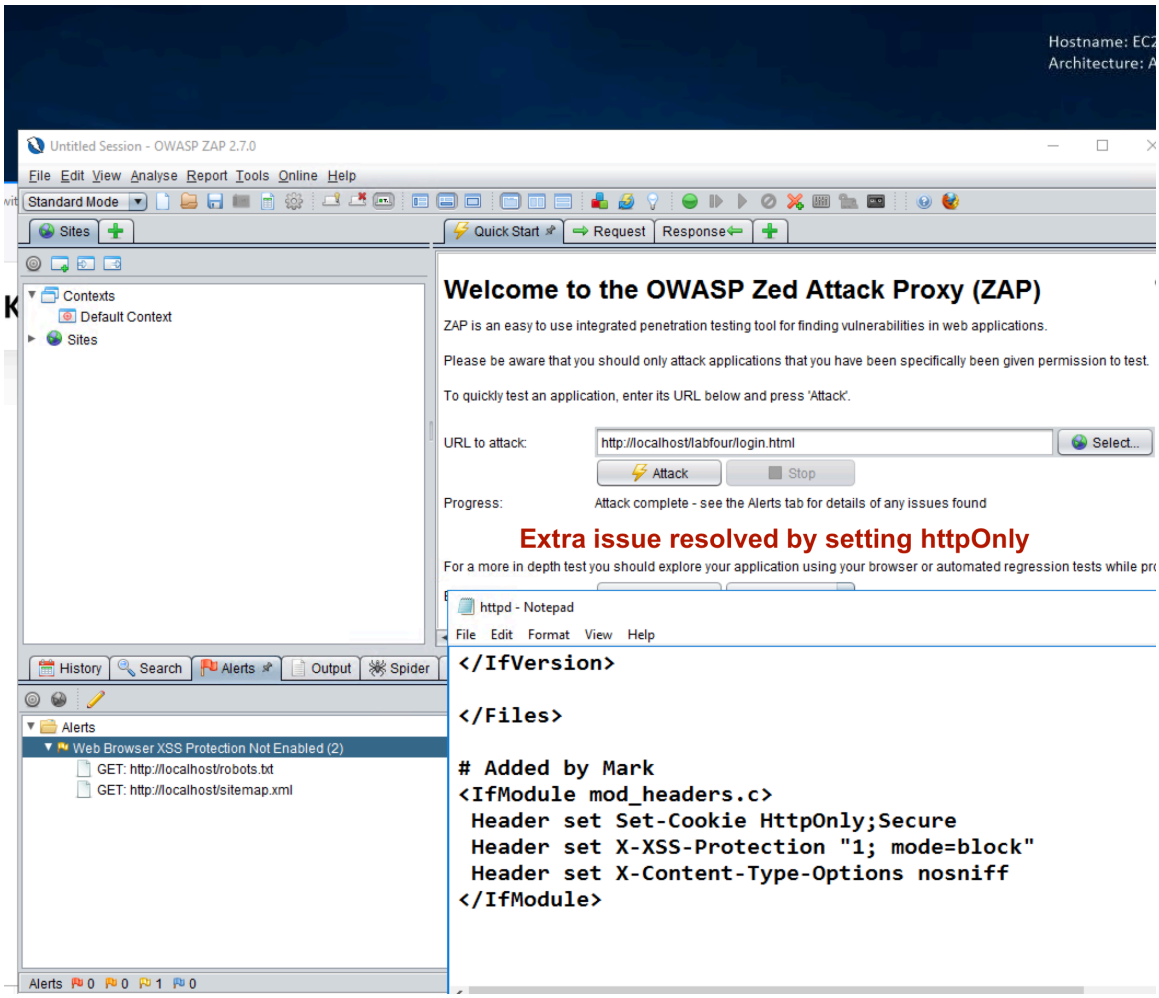

Hostname: EC2AMAZ-TJTSF
Architecture: AMD64
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
http://localhost
https://tracking-protection.cdn.mozilla.net
https://shavar.services.mozilla.com
https://search.services
https://raw.githubusercon
https://location.service
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://localhost/labfour/login.html
Select...
details of any issues found
ng your browser or automated regression tests while pro
Untitled - Notepad
File Edit Format View Help
Alert results Attack on initial login page
History
Search
Alerts
Output
Spider
Active Scan
WebSockets
Alerts (4)
Cookie No HttpOnly Flag
Incomplete or No Cache-control and Pragma HTTP Header Set
Web Browser XSS Protection Not Enabled (6)
X-Content-Type-Options Header Missing (16)
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts 0 0 4 0
Current Scans 0 0 0 0 0 0 0


ZAP Scanning Report
file:///C:/Users/Administrator/Documents/.html
ZAP Scanning Report
Summary of Alerts
Risk Level
Number of Alerts
High
0
Medium
0
Low
11
Informational
0
Alert Detail
Low (Medium)
Web Browser XSS Protection Not Enabled
Description
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL
http://localhost/labfour/projects.php
Method
POST
Parameter
X-XSS-Protection
URL
http://localhost/robots.txt
Method
GET
Parameter
X-XSS-Protection
URL
http://localhost/sitemap.xml
Method
GET
Parameter
X-XSS-Protection
URL
http://localhost/labfour/login.html?returnbtn=Return+To+Login+To+Comment
Method
GET


Hostname: EC2AMAZ-TJTSF85
Architecture: AMD64
///C:/Users/Administrator/Downloads/Lab5.pdf
Automatic Zoom
httpd.conf - Notepad
File Edit Format View Help
</IfVersion>
<IfVersion >= 2.3>
Require all denied
</IfVersion>
</Files>
Added by Mark
<IfModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
</IfModule>
Security
ServerSignature Off
ServerTokens Prod
Untitled - Notepad
File Edit Format View Help
XSS Alerts pre-httpd mofification
History
Search
Alerts
Output
Spider
Active Scan
WebSockets
Alerts (4)
Cookie No HttpOnly Flag
Incomplete or No Cache-control and Pragma HTTP Header Set
Web Browser XSS Protection Not Enabled (6)
GET: http://localhost/labfour/login.html
GET: http://localhost/labfour/login.html?returnbtn=Return+T
GET: http://localhost/robots.txt
GET: http://localhost/sitemap.xml
POST: http://localhost/labfour/projects.php
POST: http://localhost/labfour/summary.php
X-Content-Type-Options Header Missing (16)
Web Browser XSS Protection Not Enabled
URL: http://localhost/labfour/login.html
Risk: Low
Confidence: Medium
Parameter: X-XSS-Protection
Attack:
Evidence:
CWE ID: 933
WASC ID: 14
Source: Passive (10016 - Web Browser XSS Protection Not Enabled)
Description:
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server


Hostname: EC2A
Architecture: AM
Untitled Session - OWASP ZAP 2.7.0
Edit View Analyse Report Tools Online Help
ndard Mode
httpd - Notepad
File Edit Format View Help
Order allow,deny
Deny from all
</IfVersion>
<IfVersion >= 2.3>
Require all denied
</IfVersion>
</Files>
Added by Mark
<IfModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
Header set X-Content-Type-Options nosniff
</IfModule>
Prevents MIME sniffing by telling chrome and IE browsers to stop deducing content format by sniffing.
sion to test.
Select...


Hostname: EC2AMAZ-
Architecture: AMD64
ession - OWASP ZAP 2.7.0
ew Analyse Report Tools Online Help
Quick Start
Request
Response
Header: Text
Body: Text
ult Context
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 2793
Content-Type: text/html; charset=UTF-8
Untitled - Notepad
File Edit Format View Help
No More issues with Mime Sniffing
or XSS (except the sitemap/robots).
Will add httpOnly flag for protecting cookies
Search
Alerts
Output
Spider
Active Scan
e No HttpOnly Flag
OST: http://localhost/labfour/projects.php
Browser XSS Protection Not Enabled (2)
ET: http://localhost/robots.txt
ET: http://localhost/sitemap.xml
URL: http://localhost/labfour/projects.php
Risk: Low
Confidence: Medium
Parameter: PHPSESSID
Attack:
Evidence: Set-Cookie: PHPSESSID
CWE ID: 16
WASC ID: 13
Source: Passive (10010 - Cookie No HttpOnly Flag)
Description:
A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Current Scans
Activate Windows
Go to Settings to activate Windows.


Hostname: EC
Architecture: A
Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://localhost/labfour/login.html
Select...
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
Extra issue resolved by setting httpOnly
For a more in depth test you should explore your application using your browser or automated regression tests while pr
History
Search
Alerts
Output
Spider
Alerts
Web Browser XSS Protection Not Enabled (2)
GET: http://localhost/robots.txt
GET: http://localhost/sitemap.xml
Alerts 0 0 1 0
httpd - Notepad
File Edit Format View Help
</IfVersion>
</Files>
Added by Mark
<IfModule mod_headers.c>
Header set Set-Cookie HttpOnly;Secure
Header set X-XSS-Protection "1; mode=block"
Header set X-Content-Type-Options nosniff
</IfModule>