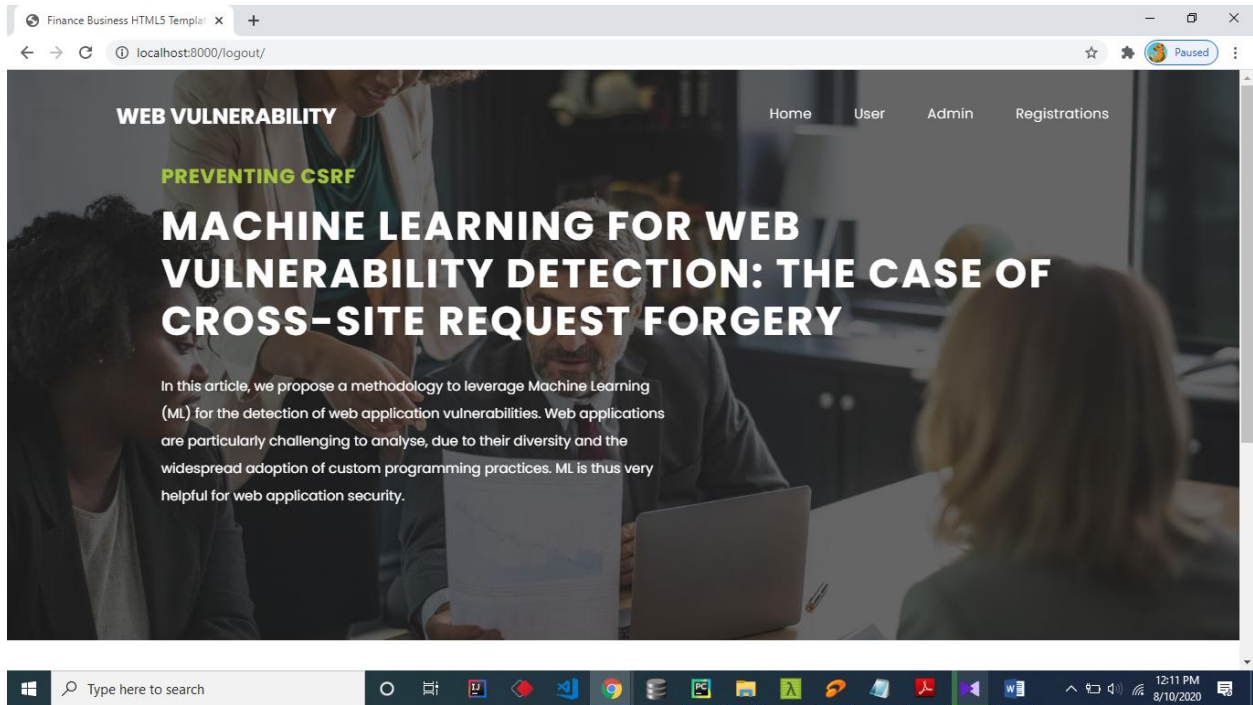
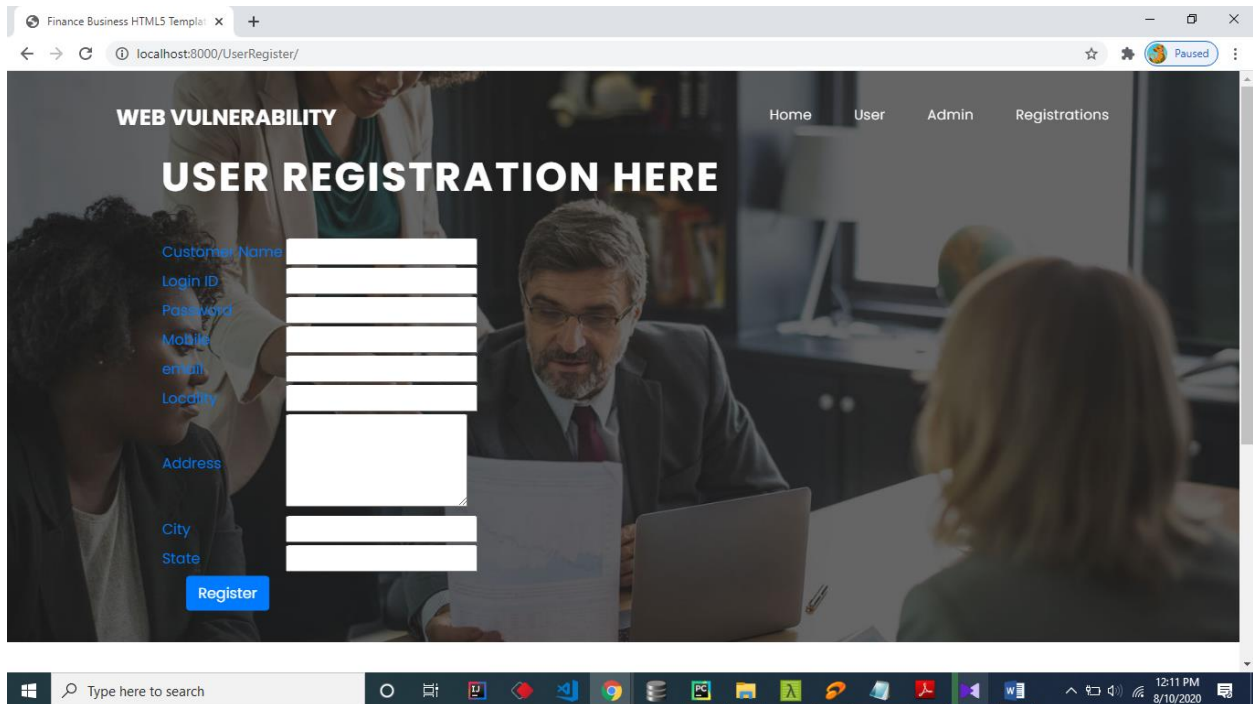


SCREEN SHOTS

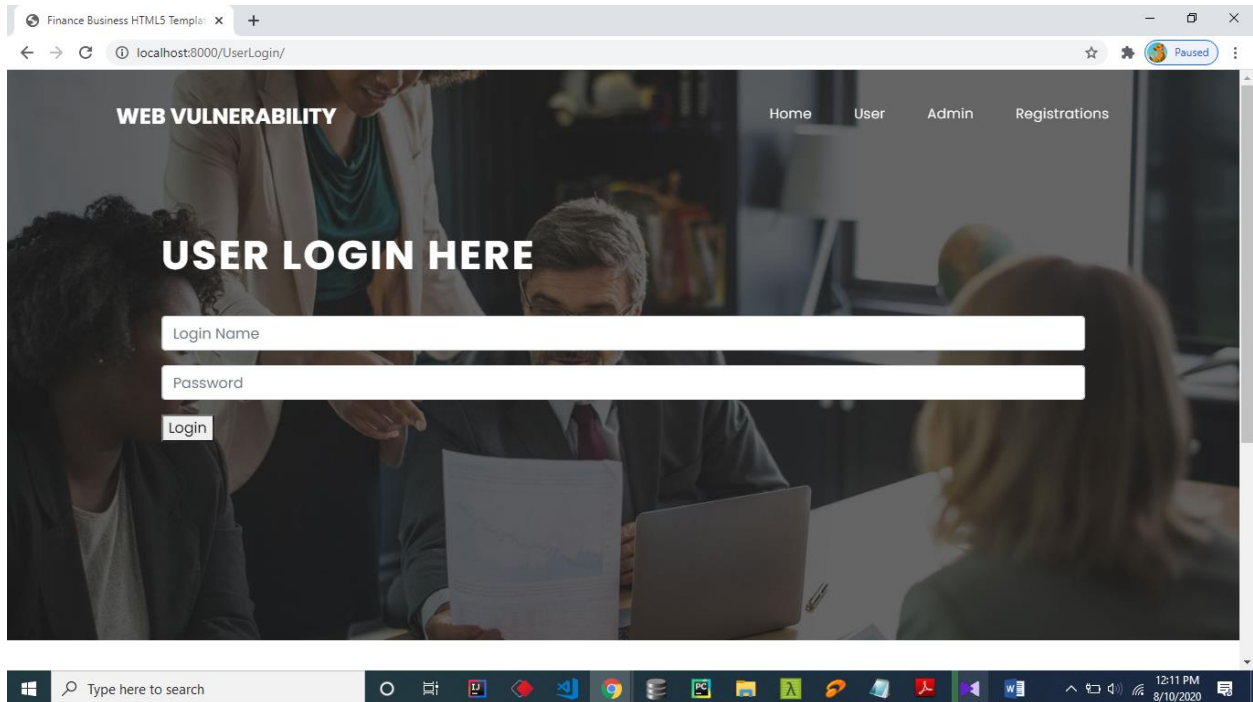
Home page:



User Registration Form

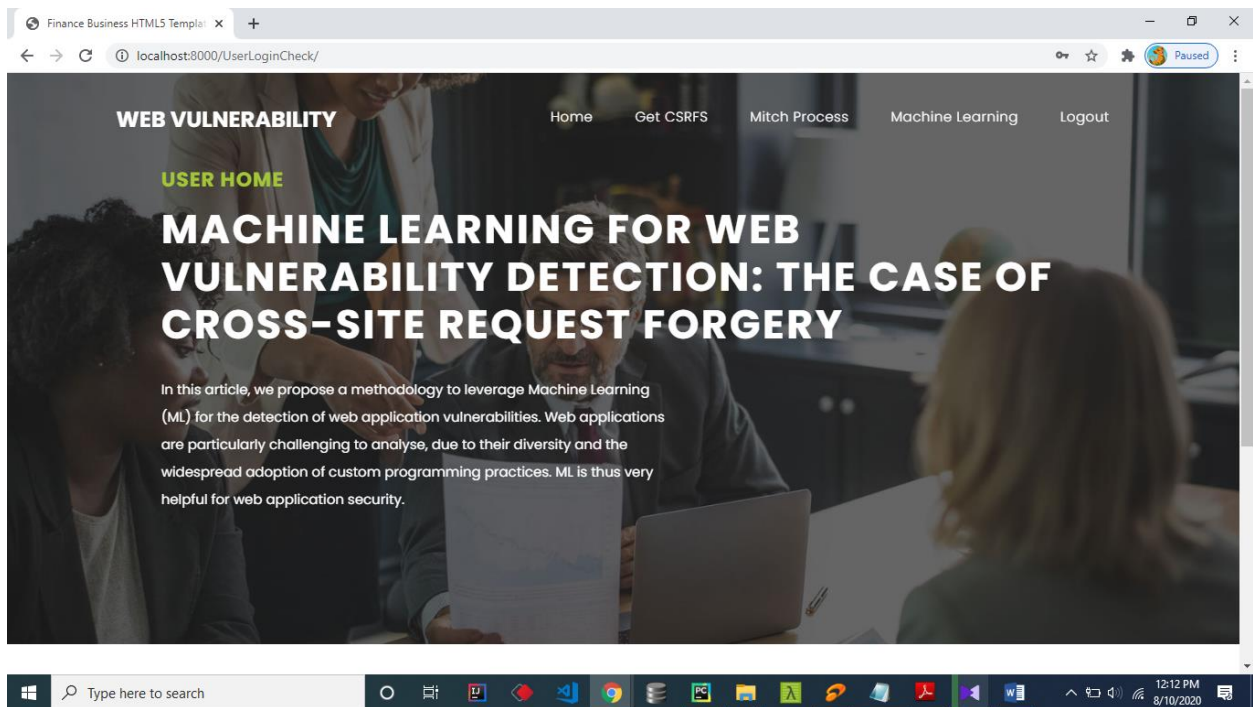


User Login Form:



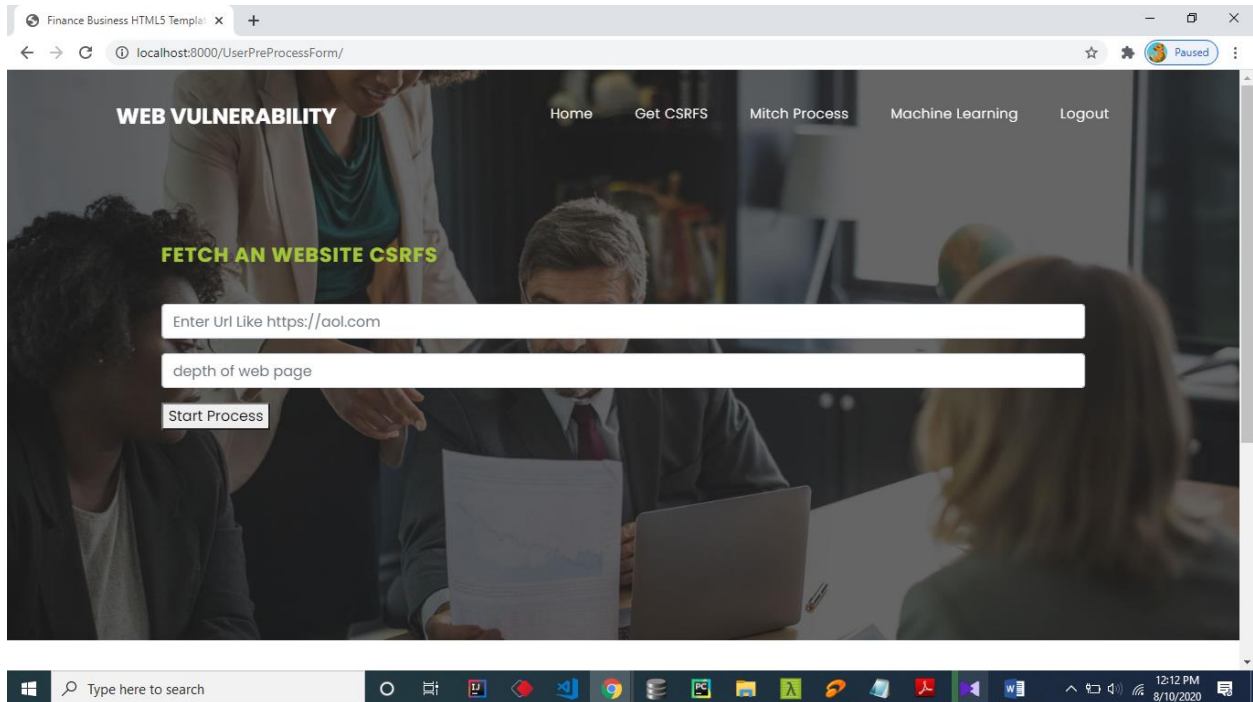
The screenshot shows a web browser window with the address bar displaying "localhost:8000/UserLogin/". The page has a dark background with a group of people working. The header includes the text "WEB VULNERABILITY" and navigation links: "Home", "User", "Admin", and "Registrations". The main content area features the text "USER LOGIN HERE" in large white letters. Below this, there are two input fields: "Login Name" and "Password", followed by a "Login" button. The Windows taskbar at the bottom shows the search bar and various application icons.

User Home:

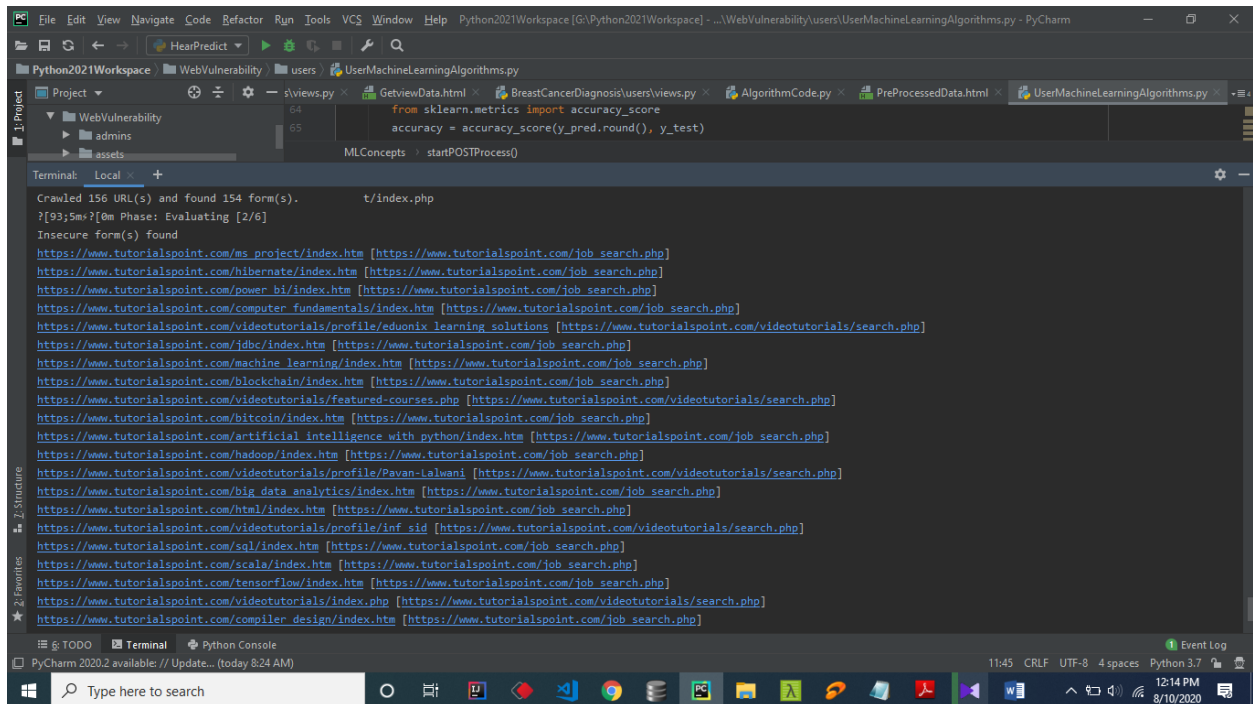


The screenshot shows a web browser window with the address bar displaying "localhost:8000/UserLoginCheck/". The page has a dark background with a group of people working. The header includes the text "WEB VULNERABILITY" and navigation links: "Home", "Get CSRS", "Mitch Process", "Machine Learning", and "Logout". The main content area features the text "USER HOME" in green, followed by the title "MACHINE LEARNING FOR WEB VULNERABILITY DETECTION: THE CASE OF CROSS-SITE REQUEST FORGERY" in large white letters. Below the title, there is a paragraph of text: "In this article, we propose a methodology to leverage Machine Learning (ML) for the detection of web application vulnerabilities. Web applications are particularly challenging to analyse, due to their diversity and the widespread adoption of custom programming practices. ML is thus very helpful for web application security."

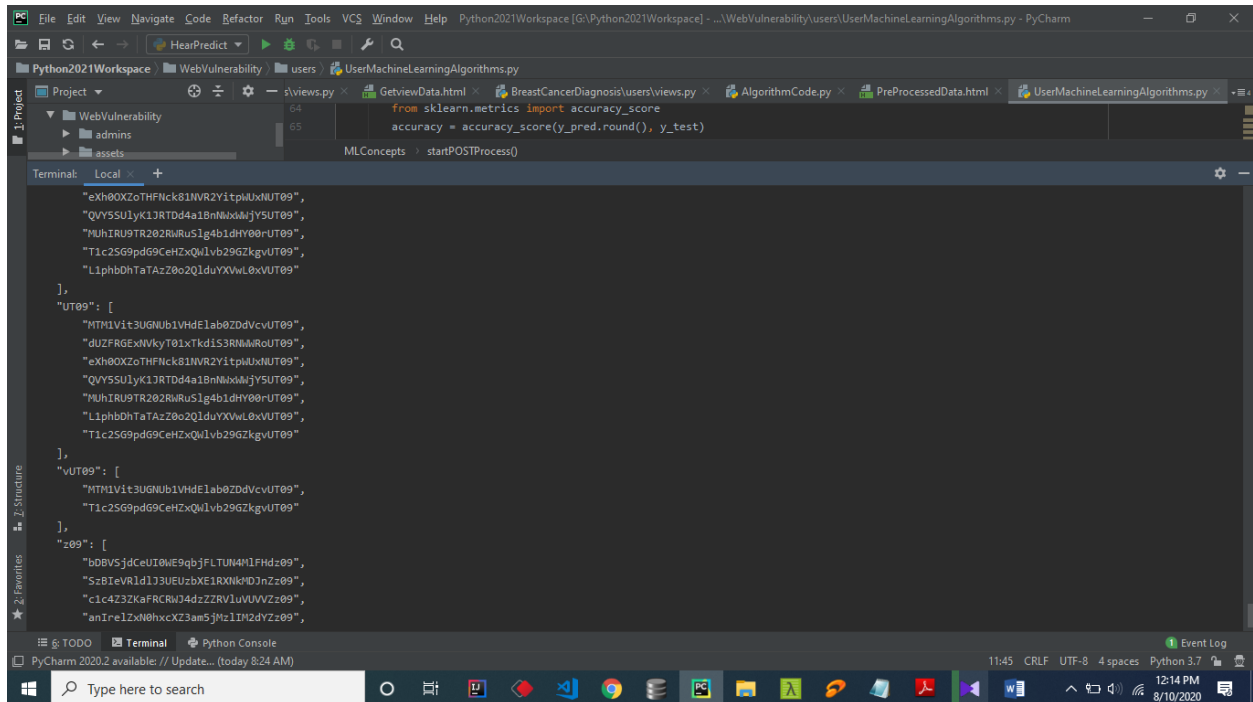
Getting website csrfs:



Scanning urls:



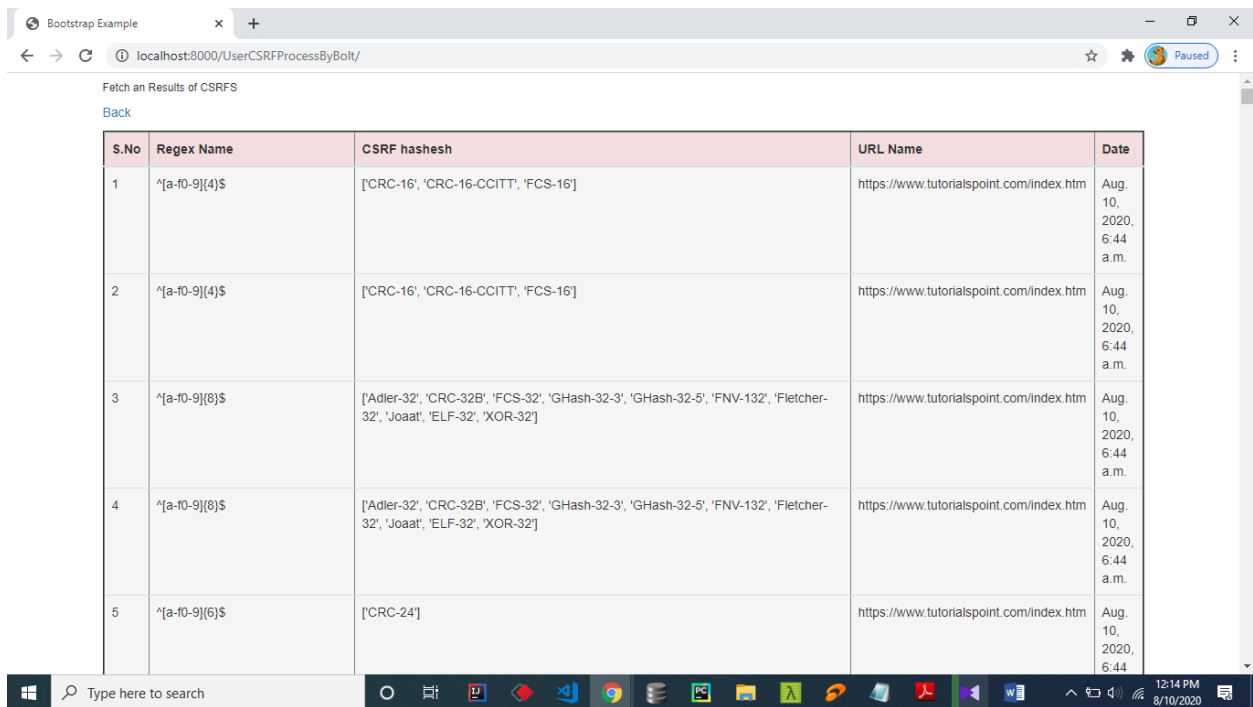
CSRF token:



```
File Edit View Navigate Code Refactor Run Tools VCS Window Help Python2021Workspace [G:\Python2021Workspace] - ...WebVulnerability\Users\UserMachineLearningAlgorithms.py - PyCharm
Python2021Workspace WebVulnerability users UserMachineLearningAlgorithms.py
Project WebVulnerability users UserMachineLearningAlgorithms.py
WebVulnerability
  admins
  assets
  MLConcepts
    startPOSTProcess()
views.py
  64
  65
  from sklearn.metrics import accuracy_score
  accuracy = accuracy_score(y_pred.round(), y_test)
AlgorithmCode.py
PreProcessedData.html
UserMachineLearningAlgorithms.py
Terminal Local
"exh00XZ0tHFncK81NVR2YitpMxNUT09",
"QVY5SUlyK1JRTDd4a18nNmXmJYSUT09",
"MuHlRU9TR202RwRuS1g4b1dHY00rUT09",
"11c2SG9pdG9CeH2xQwLvb29GZkgvUT09",
"11phbDhTaTaZ00zQ1duYXVwL0xvUT09"
],
"UT09": [
"MTM1V1t3UGNub1VHdElab0ZDdVcvUT09",
"dUZFRGEwMkyT01xTkd1S3RNMwRoUT09",
"exh00XZ0tHFncK81NVR2YitpMxNUT09",
"QVY5SUlyK1JRTDd4a18nNmXmJYSUT09",
"MuHlRU9TR202RwRuS1g4b1dHY00rUT09",
"11c2SG9pdG9CeH2xQwLvb29GZkgvUT09",
"11phbDhTaTaZ00zQ1duYXVwL0xvUT09"
],
"vUT09": [
"MTM1V1t3UGNub1VHdElab0ZDdVcvUT09",
"11c2SG9pdG9CeH2xQwLvb29GZkgvUT09"
],
"z09": [
"b0BV5jdCeUI0wE9qbJFLTUN4M1Fhdz09",
"5z8IevR1d1J3UeUzbXE1RXNkMDnZz09",
"1c1c4Z3ZKaFRcRwJ4dzZ2Rv1uVUVVZz09",
"anIre1Zw0hxcXZ3an5Mz1Ih2dYz09",

```

Given website csrf results



S.No	Regex Name	CSRF hashset	URL Name	Date
1	^[a-f0-9]{4}\$	['CRC-16', 'CRC-16-CCITT', 'FCS-16']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.
2	^[a-f0-9]{4}\$	['CRC-16', 'CRC-16-CCITT', 'FCS-16']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.
3	^[a-f0-9]{8}\$	['Adler-32', 'CRC-32B', 'FCS-32', 'GHash-32-3', 'GHash-32-5', 'FNV-132', 'Fletcher-32', 'Joaat', 'ELF-32', 'XOR-32']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.
4	^[a-f0-9]{8}\$	['Adler-32', 'CRC-32B', 'FCS-32', 'GHash-32-3', 'GHash-32-5', 'FNV-132', 'Fletcher-32', 'Joaat', 'ELF-32', 'XOR-32']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.
5	^[a-f0-9]{6}\$	['CRC-24']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.

MD5 Token

Bootstrap Example					
localhost:8000/UserCSRFPProcessByBolt/					
27	^[a-f0-9]{32}(.+)?\$	['MD5', 'MD4', 'Double MD5', 'LM', 'RIPEMD-128', 'Haval-128', 'Tiger-128', 'Skein-256(128)', 'Skein-512(128)', 'Lotus Notes/Domino 5', 'Skype', 'ZipMonster', 'PrestaShop', 'md5(md5(md5(\$pass)))', 'md5(strtoupper(md5(\$pass)))', 'md5(sha1(\$pass))', 'md5(\$pass.\$salt)', 'md5(\$salt.\$pass)', 'md5(unicode(\$pass.\$salt)', 'md5(\$salt.unicode(\$pass))', 'HMAC-MD5 (key = \$pass)', 'HMAC-MD5 (key = \$salt)', 'md5(md5(\$salt.\$pass)', 'md5(\$salt.md5(\$pass))', 'md5(\$pass.md5(\$salt))', 'md5(\$salt.\$pass.\$salt)', 'md5(md5(\$pass).md5(\$salt))', 'md5(\$salt.md5(\$salt.\$pass))', 'md5(\$salt.md5(\$pass.\$salt))', 'md5(\$username.0.\$pass)']	https://www.tutorialspoint.com/index.htm	6:44 a.m.	Aug. 10, 2020, 6:44 a.m.
28	^[a-f0-9]{32}(.+)?\$	['MD5', 'MD4', 'Double MD5', 'LM', 'RIPEMD-128', 'Haval-128', 'Tiger-128', 'Skein-256(128)', 'Skein-512(128)', 'Lotus Notes/Domino 5', 'Skype', 'ZipMonster', 'PrestaShop', 'md5(md5(md5(\$pass)))', 'md5(strtoupper(md5(\$pass)))', 'md5(sha1(\$pass))', 'md5(\$pass.\$salt)', 'md5(\$salt.\$pass)', 'md5(unicode(\$pass.\$salt)', 'md5(\$salt.unicode(\$pass))', 'HMAC-MD5 (key = \$pass)', 'HMAC-MD5 (key = \$salt)', 'md5(md5(\$salt.\$pass)', 'md5(\$salt.md5(\$pass))', 'md5(\$pass.md5(\$salt))', 'md5(\$salt.\$pass.\$salt)', 'md5(md5(\$pass).md5(\$salt))', 'md5(\$salt.md5(\$salt.\$pass))', 'md5(\$salt.md5(\$pass.\$salt))', 'md5(\$username.0.\$pass)']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.	Aug. 10, 2020, 6:44 a.m.
29	^(\\${\$nefru\$})?[a-f0-9]{32}\$	['Snefru-128']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.	Aug. 10, 2020, 6:44 a.m.
30	^(\\${\$nefru\$})?[a-f0-9]{32}\$	['Snefru-128']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.	Aug. 10, 2020, 6:44 a.m.

Mitch Detected sites:

Bootstrap Example					
localhost:8000/UserMitchProcess/					
12	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '2488', url: 'https://it.youporn.com/videoview/360922/'}}				
13	{comment: 'like video', flag: 'y', req: {method: 'POST', params: {rating: [5]}, reqId: '2490', url: 'https://it.youporn.com/change/rate/360922/'}}				
14	{comment: 'add video to favorites', flag: 'y', req: {method: 'POST', params: {video_id: [360922]}, reqId: '2493', url: 'https://it.youporn.com/change/videos/360922/add_favorites/'}}				
15	{comment: '', flag: 'n', req: {method: 'GET', params: {_: [1513352752532]}, reqId: '2496', url: 'https://it.youporn.com/mycollections.json'}}				
16	{comment: 'create collection', flag: 'y', req: {method: 'POST', params: {list[_token]: [2507819173276360704], list[title]: [prova], video_id: [WQIwWy/uM1omR3oS9kE=]}, reqId: '2503', url: 'https://it.youporn.com/collections/create/'}}				
17	{comment: 'add to collection', flag: 'y', req: {method: 'POST', params: {action: [add], item_id: [WQIwWy/uM1omR3oS9kE=], item_type: [video], list_id: [1312281]}, reqId: '2504', url: 'https://it.youporn.com/collections/add/'}}				
18	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '2507', url: 'https://it.youporn.com/favorites/'}}				
19	{comment: 'remove from favorite', flag: 'y', req: {method: 'POST', params: {video_id: [360922]}, reqId: '2639', url: 'https://it.youporn.com/change/videos/360922/remove_favorites/'}}				
20	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '2642', url: 'https://it.youporn.com/myuploads/'}}				
21	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '2699', url: 'https://it.youporn.com/mycollections/'}}				
22	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '2753', url: 'https://it.youporn.com/collections/edit/1312281/'}}				
23	{comment: 'delete collection', flag: 'y', req: {method: 'POST', params: {}, reqId: '2808', url: 'https://it.youporn.com/collections/delete/1312281/'}}				
24	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '2856', url: 'https://it.youporn.com/subscriptions/videos/'}}				
25	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '2929', url: 'https://it.youporn.com/subscriptions/'}}				
26	{comment: '', flag: 'n', req: {method: 'GET', params: {}, reqId: '3029', url: 'https://it.youporn.com/pornstar/21642/keisha-grey/'}}				
27	{comment: 'subscribe to channel', flag: 'y', req: {method: 'POST', params: {_token: [2507819173276360704], key: [pornstar], value: [21642]}, reqId: '3118', url: 'https://it.youporn.com/channel/subscribe/'}}				
28	{comment: 'unsubscribe from channel', flag: 'y', req: {method: 'POST', params: {_token: [2507819173276360704], key: [pornstar], value: [21642]}, reqId: '3119', url: 'https://it.youporn.com/channel/unsubscribe/'}}				

Machine Learning Results:

The screenshot shows a web browser window with the URL `localhost:8000/UserMachineLearning/`. The page has a dark background with a group of people working. At the top, there is a navigation bar with the text "WEB VULNERABILITY" and links for "Home", "Get CSFRS", "Mitich Process", "Machine Learning", and "Logout". The main content area is titled "Machine Learning Results" and contains a table with the following data:

Method	Accuracy	Precesion	Recall
POST	0.8507604562737643	0.7838452787258248	0.8474784747847478
GET	0.8151140684410646	0.8769363166953529	0.8055335968379447

The Windows taskbar at the bottom shows the time as 12:16 PM on 8/10/2020.

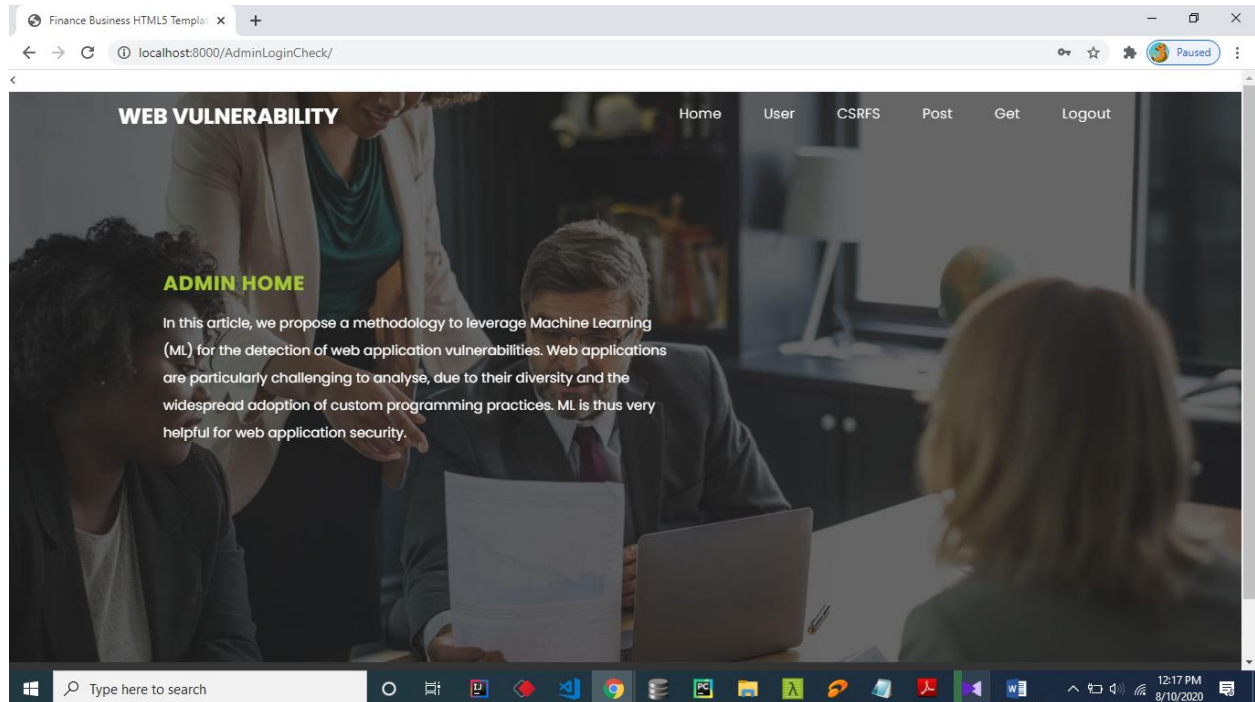
Admin Login:

The screenshot shows a web browser window with the URL `localhost:8000/AdminLogin/`. The page has a dark background with a group of people working. At the top, there is a navigation bar with the text "WEB VULNERABILITY" and links for "Home", "User", "Admin", and "Registrations". The main content area is titled "ADMIN LOGIN HERE" and contains a login form with the following fields:

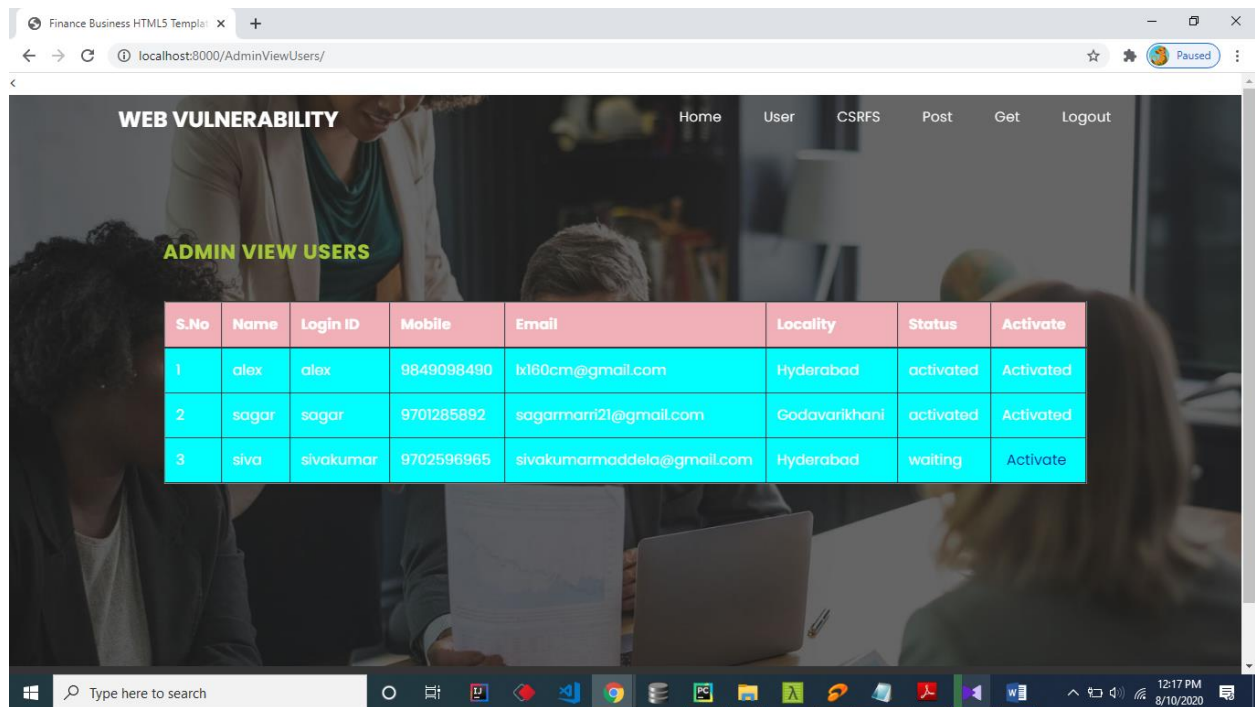
- Login Name
- Password
- Login button

The Windows taskbar at the bottom shows the time as 12:17 PM on 8/10/2020.

Admin Home Page:



View Registered users:



Admin View All CSRFs:

Bootstrap Example

localhost:8000/adminviewallcsrf/

Fetch an Results of CSRFs

[Back](#)

S.No	Regex Name	CSRF hashesh	URL Name	Date
1	^[a-f0-9]{4}\$	['CRC-16', 'CRC-16-CCITT', 'FCS-16']	https://www.geeksforgeeks.org/	Aug. 8, 2020, 6:44 a.m.
2	^[a-f0-9]{4}\$	['CRC-16', 'CRC-16-CCITT', 'FCS-16']	https://www.geeksforgeeks.org/	Aug. 8, 2020, 6:44 a.m.
3	^[a-f0-9]{8}\$	['Adler-32', 'CRC-32B', 'FCS-32', 'GHash-32-3', 'GHash-32-5', 'FNV-132', 'Fletcher-32', 'Joaat', 'ELF-32', 'XOR-32']	https://www.geeksforgeeks.org/	Aug. 8, 2020, 6:44 a.m.
4	^[a-f0-9]{8}\$	['Adler-32', 'CRC-32B', 'FCS-32', 'GHash-32-3', 'GHash-32-5', 'FNV-132', 'Fletcher-32', 'Joaat', 'ELF-32', 'XOR-32']	https://www.geeksforgeeks.org/	Aug. 8, 2020, 6:44 a.m.
5	^[a-f0-9]{6}\$	['CRC-24']	https://www.geeksforgeeks.org/	Aug. 8, 2020, 6:44 a.m.

Type here to search

12:18 PM 8/10/2020

CSRFs:

Bootstrap Example

localhost:8000/adminviewallcsrf/?page=20

17	^[\smyqlna\$[a-f0-9]{40}[-*][a-f0-9]{40}\$	['MySQL Challenge-Response Authentication (SHA1)']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.
18	^[\smyqlna\$[a-f0-9]{40}[-*][a-f0-9]{40}\$	['MySQL Challenge-Response Authentication (SHA1)']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.
19	^[\spdf\$[24]*[34]*128*[0-9-]{1,5}*1*[16]{32}*[a-f0-9]{32,64}*32*[a-f0-9]{64}*[8]{16}{32}*[a-f0-9]{16,64}\$	['PDF 1.4 - 1.6 (Acrobat 5 - 8)']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.
20	^[\spdf\$[24]*[34]*128*[0-9-]{1,5}*1*[16]{32}*[a-f0-9]{32,64}*32*[a-f0-9]{64}*[8]{16}{32}*[a-f0-9]{16,64}\$	['PDF 1.4 - 1.6 (Acrobat 5 - 8)']	https://www.tutorialspoint.com/index.htm	Aug. 10, 2020, 6:44 a.m.

« 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 »

Type here to search

12:18 PM 8/10/2020

Post Data View:

localhost:8000/PostRequestdata/ x +

localhost:8000/PostRequestdata/ ☆ ⚙ Paused

Machine Learning for Web Vulnerability Detection: The Case of Cross-Site Request Forgery

Post Requested Data View

[Back](#)

	numOfParams	numOfBools	numOfIds	numOfBlobs	reqLen	isPOST
0	0	0	0	0	0	0
1	1	0	0	1	1519	1
2	1	0	0	0	629	1
3	1	0	0	0	3365	1
4	1	0	0	0	567	1
5	4	0	0	0	281	1
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	5	2	0	0	64	0
16	5	2	0	0	64	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0

Type here to search

12:19 PM 8/10/2020

Get Data:

localhost:8000/PostRequestdata/ x +

localhost:8000/PostRequestdata/ ☆ ⚙ Paused

Machine Learning for Web Vulnerability Detection: The Case of Cross-Site Request Forgery

Post Requested Data View

[Back](#)

	numOfParams	numOfBools	numOfIds	numOfBlobs	reqLen	isPOST
0	0	0	0	0	0	0
1	1	0	0	1	1519	1
2	1	0	0	0	629	1
3	1	0	0	0	3365	1
4	1	0	0	0	567	1
5	4	0	0	0	281	1
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	5	2	0	0	64	0
16	5	2	0	0	64	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0

Type here to search

12:19 PM 8/10/2020

Attribute Descriptions:

6290	6	2	0	0	63	1
6291	5	1	0	0	48	1
6292	2	1	0	0	20	1
6293	4	1	0	2	196	1
6294	2	1	0	0	20	1
6295	4	1	0	2	196	1
6296	2	1	0	0	20	1
6297	4	1	0	2	196	1
6298	2	1	0	0	20	1
6299	4	1	0	2	196	1
6300	2	1	0	0	20	1
6301	4	1	0	2	196	1
6302	6	3	0	0	53	1
6303	2	1	0	0	20	1
6304	4	1	0	2	196	1
6305	4	1	0	2	196	1
6306	4	1	0	2	196	1
6307	2	1	0	0	20	1
6308	2	1	0	0	20	1
6309	4	0	0	1	130	0
6310	0	0	0	0	0	1
6311	4	1	0	1	3102	0

1. **numOfParams**: the total number of parameters
2. **numOfBools**: the number of request parameters bound to a boolean value
3. **numOfIds**: the number of request parameters bound to an identifier, i.e., a hexadecimal string, whose usage was empirically observed to be common in our dataset
4. **numOfBlobs**: the number of request parameters bound to a blob, i.e., any string which is not an identifier
5. **reqLen**: the total number of characters in the request, including parameter names and values.